MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BULUT BİLİŞİMDE VERİ GÜVENLİĞİ VE KRİPTOGRAFİ

HÜSEYİN ÖCAL

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği

Anabilim Dalı

Bilgisayar Mühendisliği Yüksek Lisans Programı

DANIŞMAN

Doç. Dr. Bahattin YALÇINKAYA

İSTANBUL, 2022

MARMARA UNIVERSITY

INSTITUTE FOR GRADUATE STUDIES

IN PURE AND APPLIED SCIENCES

DATA SECURITY AND CRYPTOGRAPY IN CLOUD COMPUTING

HÜSEYİN ÖCAL

MASTER THESIS

Department of Computer Engineering

Computer Engineering Master Program

Thesis Supervisor

Doç. Dr. Bahattin YALÇINKAYA

ISTANBUL, 2022

ÖNSÖZ/ TEŞEKKÜR

Bu tez çalışmasının yapılmasına imkân sağlayan, tecrübeleriyle bana yol gösteren, desteğini hiç esirgemeyen çok değerli danışman hocam Doç Dr. Bahattin Yalçınkaya'ya, Doç. Dr. Buket Doğan ve Dr. Banu Fulya Yıldırım'a sonsuz teşşekürlerimi sunarım.

İÇİNDEKİLER

ÖZET

BULUT BİLİŞİMDE GÜVENLİK VE KRİPTOGRAFİ

Bulut Bilişim, günümüzde BT altyapılarında sıkça kullanılan ve gelişimini sürdüren önemli bir teknolojidir. Birçok kurum, bulut bilişim sistemleri geliştirme ve hizmetlerini daha fazla kullanıcıya sunmak için geliştirme yapmaya devam etmektedir. Bu çalışmalar yapılsa da kullanıcıların bulut sistemlerini kullanmalarının önünde güvenlik, gizlilik ve mahremiyet sorunları ile ilgili engeller bulunmaktadır. Bu tez çalışmasında, bulut bilişim sistemlerinin yapısı, mimarisi, altyapısı, servis ve dağıtım modelleri, bulut bilişimin sunduğu avantaj ve dezavantajlardan ayrıntılı olarak bahsedilecektir. Sistemde yer alan güvenlik, gizlilik ve mahremiyet ile ilgili saldırı, zafiyet ve tehditlerden, bunlara ne gibi çözümler bulunduğundan ve bulut sistemlerinde yer alan kriptografik türlerinin neler olduğu anlatılmaya çalışılacaktır. Ayrıca tez kapsamında bulut bilişim sistemlerinde kullanıcıların anahtarlarının her platforma özel yazılımsal ve donanımsal olarak nasıl saklanması gerektiği anlatılacaktır. Bu tez kullanıcıların, bulut bilişim hizmetlerini olumlu ve olumsuz yönleri; güvenlik, gizlilik ve mahremiyet konularıyla ilgili anlatılan detaylı bilgiler ile birlikte daha iyi bir değerlendirme yapılmasına yardımcı olmak, bulut hizmeti sağlayıcılarının ise, daha iyi bulut çözümleri geliştirmesi noktasında farkındalık oluşturması beklenmektedir.

ABSTRACT

SECURITY AND CRYPTOGRAPHY IN CLOUD COMPUTING

Cloud Computing is an important technology that is frequently used in IT infrastructures and continues to develop. Many institutions continue to develop cloud computing systems to offer their services and services to more users. Although these studies are carried out, there are obstacles related to security, privacy and privacy issues in front of users from using cloud systems. In this thesis, the structure, architecture, infrastructure, service and distribution models of cloud computing systems, the advantages and disadvantages of cloud computing will be discussed in detail. It will be tried to explain the attacks, vulnerabilities and threats related to security, privacy and privacy in the system, what solutions are available for them, and what cryptographic types are in cloud systems. In addition, within the scope of the thesis, it will be explained how the keys of the users in cloud computing systems should be stored in software and hardware specific to each platform. In this thesis, the positive and negative aspects of cloud computing services; It is expected to help make a better assessment together with detailed information on security, privacy and privacy issues, and to raise awareness for cloud service providers to develop better cloud solutions.

SEMBOLLER/SYMBOLS

$\in$: Elemanıdır

mod : Kalan hesaplama

* : Çarpma işlemi

KISALTMALAR/ABBREVIATIONS

ABD : Amerika Birleşik Devletleri

AES : Advanced Encryption Standart

API : Application Programming Interface

ASCII : American Standard Code For Information Interchange

ASLR : Address Space Layout Randomization

AWS : Amazon Web Services

BT : Bilişim Teknolojileri

CAAS : Communication As A Service

CASB : Cloud Access Security Broker

CP-ABE : Şifreli Metin-Politika Nitelik Tabanlı Şifreleme

CPU : Central Processing Unit

CRHF : Collision-Resistant Hash Function

CRM : Customer Relationship Management

CSP : Content Security Principle

DAAS : Desktop As A Service

DBAAS : Database As A Service

DDOS : Dağıtılmış Hizmet Reddi

DDR : Double Data Rate

DES : Data Encryption Standart

DLP : Data Loss Prevention

DOM : Document Object Model

DRAAS : Hizmet Olarak Felaket Kurtarma

DRAM : Dynamic Random Access Memory

DSS : Data Security Standart

FTP : File Transfer Protocol

GDPR : General Data Protection Regulation

GUI : Graphical User Interface

HAAS : Hardware As A Service

HDD : Hard Disk Drive

HIDS : Host-based Intrusion Detection System

HIPAA : Health Insurance Portability and Accountability Act of 1996

HSM : Hardware Secure Module

HTML : HyperText Markup Language

HTTPS : Hypertext Transfer Protocol

HTTPS : Hypertext Transfer Protocol Secure

IAAS : Infrastructure As A Service

IAM : Identity and Access Management

IBM : International Business Machines Corporation

ICMP : Internet Control Message Protocol

IDPS : Intrusion Detection and Prevention System

IDS : Intrusion Detection System

IP : Internet Protocol

IPS : Intrusion Prevention System

ISO / IEC : International Organization for Standardization/International Electrotechnical Commission

IT : Information Technology

KOBİ : Küçük ve Orta Bütçeli İşletmeler

KP-ABE : Key-Policy Attribute Based Encryption

LAN : Local Area Network

MAAS : Monitoring As A Service

MID : Mobile Internet Devices

NAAS : Network As A Service

NERC : The North American Electric Reliability Corporation

NIDS : Network Based Intrusion Detection System

NIST : Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standarts and Technology)

OWHF : Tek Yönlü Hash Fonksiyonları

OWASP : Open Web Application Security Project

ÖAÜ : Özel Anahtar Üreticisi

PAAS **:** Platform As A Service

PCI **:** Payment Card Industry

PIN **:** Personal Identification Number

PKG **:** Private Key Generator

PKI **:** Public Key İnfrastructure

PLC **:** Partion Locked Cache

RSA **:** Rivest, Shamir, & Adleman

SAAS **:** Software As A Service

SAML **:** Security Assertion Markup Language

SAP **:** System Application and Product in Processing

SECAAS **:** Security As A Service

SLA **:** Hizmet Seviyesi Anlaşması (Service Level Aggrement)

SM **:** Sanal Makine

SOAP **:** Simple Object Authentication Protocol

SOX **:** Sarbanes Oxley

SSD **:** Solid-State Drive

SSH **:** Secure Shell

SSL **:** Secure Socket Layer

SSO **:** Single Sign-On

STAAS **:** Storage As A Service

SQL **:** Structured Query Language

TCP **:** Transmission Control Protocol

TEE **:** Trusted Execution Environment

TPM **:** Trusted Platform Module

TTP **:** Trusted Third Party

UOWFH **:** Evrensel Tek yönlü Hash Fonksiyonları

UPS **:** Uninterruptible Power Supply

URL **:** Uniform Resource Locator

VM **:** Virtual Machine

VMHIDS **:** Virtual Machine Hypervisor Based Intrusion Detection System

VMM : Virtual Machine Monitor

VPN **:** Virtual Private Network

WAF **:** Web Application Firewall

WPA/WPA2: Wi-Fi Protected Access

XAAS **:** Anything As A Service

XSS **:** Siteler arası komut dosyası çalıştırma

ŞEKİL

TABLO LİSTESİ/LIST OF TABLES

1 GİRİŞ

Bulut bilişim en basit tabiriyle sunucu, depolama, veritabanı, ağ, yazılım, analiz gibi bilgi işlem diye adlandırdığımız sektörün başlıca hizmetlerinin internet üzerinden sağlanarak daha hızlı geliştirme yapılması, esnek ve kolay kullanımlı kaynaklar ve bazı ekonomik ücretlendirmelerle sunulması anlamına gelmektedir. Bulut bilişimin esnek ve kullanımı kolay altyapısı, ağ tabanlı mimari yaklaşımı ve kolay erişilebilir olması sebebiyle her ölçekteki firma ve kurum gibi birçok organizasyon tarafından kullanımı giderek artmaktadır. Ayrıca bulut bilişim sistemleri kişisel bilgiler gibi hassas verilerin saklanması için gelecek adına en önemli depolama birimleri olarak görülmektedir. Bulut bilişim teknolojisi, içinde bulunan tüm katmanlar için farklı farklı servisler sunduğundan dolayı her katmanda kullanılmakta olan teknolojiler de farklılık göstermektedir. Bulut bilişimin temelini aslında sanallaştırma teknolojisinden almaktadır. Bu sayede her türlü veri kullanıcılara ulaştırılabilmektedir. Bu avantajların doğurabileceği güvenlik sıkıntıları bulut bilişim hizmetlerinin yanında gelmektedir. Genel olarak kurumların üçüncü taraf yazılım kullanmaları ve bu hizmetlerin ağ trafiği sayesinde gelmesinden kaynaklı güvenlik zafiyetleri gibi bunlara bağlı birçok riskler oluşturabilmektedir. Bu tip dezavantajlar için bulut bilişim sistemlerinin kullandığı güvenlik yöntemleri de bulunmaktadır.

Diğer yandan bulut bilişim sistemlerinde en önemli endişeler arasında bu sistemleri kullanan kişi veya kurumların verilerinin sağlam bir şekilde korunmasıdır. Tam bu noktada bulut bilişim teknolojileri için verinin gizliliği ve güvenilirliği konusu daha önemli bir hale gelmektedir. Bu konular için bulut bilişimde çok fazla atak, tehdit ve zafiyet bulunmaktadır. Ancak bulut bilişim bizlere bunlara yönelik bazı çözümler sunmaktadır. Kullanıcılar ve kurumların giderek yaygınlaşan ve büyüyen bulut bilişim sistemleri kullanımı için bu çözümler çok önem arz etmektedir.

1.1 Amaç, Hedef ve Hipotez

Bu tez çalışmasının amacı, bulut bilişim, güvenlik gizlilik ve mahremiyet ve kriptografinin bulut bilişimdeki rolleri hakkında detaylı bir inceleme sunmaktır. Bu

amaçla bulut bilişim kullanım ve hizmet çeşitleri, mimarisi, çalışma prensibi, bulut bilişimin avantajları ve dezavantajları detaylıca anlatılmıştır. Bulut bilişimde güvenlikle alakalı ağ, altyapı, yazılım ve bilgi güvenliği konularının yanında yasal uyumluluk ve standartlar ile kimlik erişim yönetimi konularının ne kadar önemli olduğunun anlaşılması hedeflenmiştir. Ayrıca güvenlik, gizlilik ve mahremiyet konularıyla alakalı tehdit, zafiyet ve ataklardan örnekler verilip bunlara karşı nasıl önlemler alınması gerektiği anlatılarak bilgilendirme yapmak diğer amaçlar arasındadır. Dahası bulut bilişimde kullanılan kriptografik çözümlerden ve yöntemlerden bahsedilerek kriptografinin her güvenlik alanında olduğu gibi bulut bilişim güvenliği için de ne kadar önemli olduğu vurgulanmaya çalışılmıştır.

Bulut bilişim sistemini kullanmak ve değerlendirmek isteyen kişilere ve kurumlara yol göstermek, araştırmacılara temel bir kaynak oluşturmak ve mevcut sorulara cevap aramak açısından geleceğe ilişkin bir yön çizmek hedeflenmiştir. Bu tez çalışması ile birlikte konuyla ilgilenen kişiler ve kurumlar için önemli bir kaynak olması ve yapılacak uygulamalarda kullanılabilecek değerli bilgiler bütünü olması hedeflenmektedir.

Bulut bilişim teknolojisi kullanım itibariyle sağladığı esneklik sayesinde gelecekte kullanımını daha da artması beklenmektedir. Kullanımının yaygın olacağı alanların da genişleyeceği aşikârdır. Belki de ileride her türlü sistem ile entegre bir şekilde bulunacak bulut bilişim sistemleri ve uygulamaları kullanıcılar ve kurumlar için vazgeçilmez bir teknoloji olacaktır. Diğer yandan bilgi teknolojisi alanında Türkçe kaynak sıkıntısı giderek azalmasına rağmen devam etmektedir. Bu sebeplerden ötürü gelecekte yapılacak milli veya özel uygulamalar ve çalışmalar için yerli kaynak olması da ayrıca hedefler arasında yer almaktadır. Ayrıca bu tez çalışmasının bu konuda araştırma yapacak öğrenci veya öğretmenlerin de bulut bilişimde kriptografi ve güvenlik konuları için temel bir kaynak olması amaçlanmıştır.

1.2 Konu ve Kapsam

Bu tezin konusu, bulut bilişimde güvenlik ve kriptografinin bulut bilişimdeki yerini ortaya koymaktır. Ülkemizde ve dünyada yeni cihazların üretilmesi, insanların bu cihazlara bağımlılığının ciddi miktarda artması ve sosyal medya başta olmak üzere her mecrada kullanımın giderek artmasından dolayı veriler hızla büyümektedir. Olaya kullanıcı merkezli bakıldığında çoğu insanın artık verilerini kendi cihazlarında taşıması

maddi bir yüke sebep olmaktadır. Bu yüzden bulut bilişim depolama ürünleri başta olmak üzere verilerin bu tür internet üzerinden ve her platformdan kolayca ulaşılabilecek tarzdaki yerlere depolamayı ve saklamayı daha uygun, kullanışlı bulmaktadır. Bu istekler ve arzular da yanında da şöyle bir gerçek vardır ki kurumlarda ve kullanıcılarda kişisel verilerin gizliliğiyle ilgili artan bir endişe vardır. Hem kamu hem de özel kurumlar ve kuruluşlar, büyük miktarlarda kişisel ve hassas bilgi biriktirip bunları depolamaktadır. Ülkemizde bu çok büyük verilerin saklanması olarak algılanmayabilmektedir. Bunun nedeni de ülkemizde altyapısı çok iyi olarak hazırlanmış olan veri merkezlerinin azlığından kaynaklanmaktadır. Kişiler kendileri hakkında depolanan veriler ve bunların nasıl kullanıldığı üzerindeki herhangi bir kontrol hakkına ya sahip değillerdir ya da bu kontrol mekanizması büyük derecede sınırlandırılmıştır. Kullanıcılar verilerini bulut bilişim uygulamalarında depoladıklarında bu kullanıcıların mahremiyetini tehlikeye atan gözetim ve güvenlik ihlalleri vakalarında meydana gelen artışlar, üçüncü tarafların hizmet sağlayıcılarının büyük miktarda kişisel veri topladığı ve kontrol ettiği gerçeğini meydana getirmiştir. Bu tez çalışması bu konuyu kapsamına almıştır ve bununla ilgili konuları detaylıca incelemiştir.

Bu tezin kapsamı genel olarak, bulut bilişimde güvenlik başlıklarının ve kriptografinin detaylıca yer alacağı, veri mahremiyeti ve gizliliği açısından belirtilecek çözümler, bulut bilişimin genel yapısı, yapı çeşitlerine göre halihazırda bulunan çeşitler, bulut bilişimin kullanıcı ve kuruluşlar açısından avantaj ve dezavantajlarının da ince ayrıntılarına girilerek anlatılacağı bir tez çıktısı olacaktır. Bulut bilişimde depolama alanındaki kriptografik algoritmaların kullanımı sırasında gerçeklenebilecek yazılım ve donanım araçlarının her istemci platformu için de ayrı ayrı anlatılarak geniş çapta bilgi vermek kapsam içindedir.

2 BULUT BİLİŞİM

2.1 Bulut Bilişim Tanımı

Bulut bilişimin gerçekte ne anlama geldiği ile alakalı olarak sektörde çok fazla tartışma konusu olmuştur. IBM, Sun Microsystems, Gartner ve Forrester Research, Microsoft gibi büyük BT şirketlerinin ve pazar araştırması şirketlerinin çoğu, bu terimin anlamını tanımlamaya çalışan teknik incelemeler üretti[1] .Tüm bu tanımlara rağmen NIST tarafından yapılan çalışmada bulut bilişim ne olduğu detaylı bir şekilde anlatılarak aslında bu tartışmalara bir nebze sonlandırılmıştır. Bu bilgiler ışığında tanımlamalar aşağıdaki gibidir.

Bulut bilişimde en fazla bilinen ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yapılan tanıma göre, bulut bilişimin an az yönetim çabası ve hizmet sağlayıcı etkileşimi ile hızla tedarik edilebilen ve piyasaya sürülebilen yapılandırılabilir bilişim kaynaklarına paylaştırılan havuzuna isteğe bağlı ağ erişimi sağlayan, kullanışlı ve heryerden erişilebilir bir model olduğu belirtilmiştir[2].

Microsoft tarafından yapılan tanıma göre ise bulut bilişim, daha hızlı yenilik, esnek kaynaklar ve ölçek ekonomileri sunmak için sunucular, depolama, veritabanları, ağ iletişimi, yazılım, analitik ve zeka dahil olmak üzere bilgi işlem hizmetlerinin internet üzerinden sunulmasıdır. Ayrıca bu tanıma ek olarak yalnızca kullanılan bulut hizmeti için ödeme yapıldığı bunun da işletme maliyetlerini azalttığı, altyapıların daha verimli çalıştığına ve iş ihtiyaçlarının değişmesine rağmen kolaylıkla ölçeklendirme yapılabildiğini de sağladığı vurgulanmıştır.[3]

IBM tarafından yapılan tanıma göre, bulut bilişim, BT hizmetlerinin edinilmesi ve sunulması için son derece otomatik, dinamik bir alternatif sağlayan bu tür esneklik ihtiyacına olası bir cevap olduğu belirtilmiştir[4]. Buna ek olarak şirketlerin, sorunları daha önce mümkün olmayan şekillerde çözmek için bulut bilişimin ölçeklenebilirlik özelliliğinden yararlandığını ve bulutun sanallaştırma, standardizasyon ve diğer temel özellikleri BT maliyetini düşürdüğünü, BT hizmet yönetimini basitleştirdiğini de belirtiyor.

451 Group'un tanımı ise, bulut bilişim BT sunumu, altyapı bileşenleri, mimari bir yaklaşım ve ekonomik bir model için genel bir düzenleme ilkesini birleştiren ve temelde,

grid hesaplama, sanallaştırma, yardımcı bilgi işlem, barındırma ve hizmet olarak yazılım içeren bir model olduğu söylenmiştir[5]. Ya da daha basit bir ifadeyle, bulutun BT'nin kendisi olduğu, kullanıcıya bir hizmet olarak sunulup konumdan bağımsız sanallaştırılmış kaynaklar tarafından sağlandığı da açıklanmıştır.

Gartner'ın yaptığı tanımlamada ise bulut bilişimde var olan ölçeklenebilir ve esnek BT özellikli yeteneklerin internetin kullanılarak yapılan bir servis nitelendirilmesi yapılmıştır[6].

Rayport ve Heyward'ın tanımında ise, bulut bilişim, kullanıcılara internet teknolojisi arayıcılığıyla bilgilere erişim, bunlar üzerinde çalışma, paylaşma ve depolama gibi özellikleri tedarik etmek için bilgi işlem teknolojisini dâhil etmenin yeni bir yöntemi olarak değerlendirilmiştir. Bulutun kendisinin kullanıcıların internet üzerinden sağlanan güçlü uygulamalara, platformlara ve hizmetlere erişimini sağlayarak kişisel veya iş bilgisayarındaki yazılım işlevlerini gerçekleştirebilen, her biri birlikte çalışan binlerce bilgisayardan oluşan bir veri merkezleri ağı olduğu belirtilmiştir[7].

Buyya ve Venugopal'a göre, bulut bilişim, hizmet sağlayıcısı ile tüketiciler arasındaki görüşmeler yoluyla oluşturulan hizmet düzeyi sözleşmelerine dayalı olarak dinamik olarak sağlanan ve bir veya daha fazla birleşik bilgi işlem kaynağı olarak sunulan birbirine bağlı ve sanallaştırılmış bilgisayarlar koleksiyonundan oluşan paralel ve dağıtılmış bir sistemdir[8].

McFedries'e göre, bulut bilişimin kişisel bilgisayarların bir uzantısı olduğunu belirterek sadece verilerimizin değil, yazılımımızın bile bulut içinde yer alır ve her şeye sadece bilgisayarlarımızla değil, aynı zamanda akıllı telefonlar, bilgi işlem cihazları, oyun konsolları ve hatta arabalar gibi bulut dostu cihazlarımızla da erişileceğinden bahsetmektedir[9].

Öte yandan, Borenstein ve Blake, bulut bilişimi, genellikle üçüncü taraflarca merkezi olarak sağlanan hizmetleri dağıtmak için hızlı, yüksek bant genişliğine sahip İnternet bağlantılarının kullanımı olarak görmektedir. Böylece BT yönetiminin maliyetini ve zorluğunu en aza indirilmiş ve bu kuruluşlara destek sağlanmaktadır[10].

Michael Armbrust'a göre bulut bilişim, hem internet üzerinden hizmet olarak sunulan uygulamaları hem de bu hizmetleri sağlayan veri merkezlerinin içerisindeki donanım ve sistem yazılımlarını ifade eder[11]. Hizmetlerin kendileri hizmet olarak

yazılım diye adlandırılan (SaaS)'dır. Veri merkezlerindeki donanım ve yazılımları da bulut olarak tanımlamaktadır.

Eric Griffith'e göre, en basit tabirle, bulut bilişim, verilerin ve programların bilgisayarınızın sabit diski yerine internet üzerinden depolanması ve bunlara erişilmesi anlamına gelir[12].

Wikipedi tarafından yapılan tanım ise, bulut bilişim bilgisayarlar ve diğer cihazlar için, istendiği zaman kullanılabilen ve kullanıcılar arasında paylaşılan bilgisayar kaynakları sağlayan, internet tabanlı bilişim hizmetlerinin genel adıdır. Bulut bilişim bu yönü itibariyle bir ürün değil, hizmet olduğu vurgulanmıştır. Ayrıca bulut bilişimin temel kaynaktaki yazılım ve bilgilerin paylaşımı sağlanarak, mevcut bilişim hizmetinin, bilgisayarlar ve diğer aygıtlardan elektrik dağıtıcılarına benzer bir biçimde bilişim ağı üzerinden kullanılması olarak da tanımlaması yapılmıştır[13].

2.2 Bulut Bilişim Tarihçesi ve Gelişimi

Bulut tipindeki bir sistemde işlemler yapma ve etkileşim oluşturma olarak nitelendireceğimiz bir terim için geriye dönüp bakıldığında 1961 yılında John McCharthy'nin yaptığı şu açıklama göze çarpmaktadır. Bu açıklamada 'Savunduğum türde bilgisayarlar, geleceğin bilgisayarı olacak ve belki de bir gün günümüzün telefon sistemi gibi ortak bir ağda birleşip veri değişimi yapabilecekler. Bilgisayar yeni ve önemli bir sektör olabilir." şeklindedir.

1960 ve 1970 yıllarında bilişim sadece ana bilgisayar denilen oda büyüklüğündeki cihazlar tarafından geliştirilmekteydi. Bu tip cihazların en önemli dezavantajları maliyetlerinin çok yüksek olmasıydı. Bu sebepten ötürü sadece çok büyük firmalar tarafından alınabilmekteydi. Ayrıca herhangi bir arayüz sunamadığından dolayı da sadece terminaller arayıcılığıyla kullanılabilmekteydi. Bu model de merkezi bir yapıda sunulmak zorunda kalınmıştı.

1980'lere gelindiğinde işlevsiz olan terminallerin bellek ve işlemci kapasitelerinin ve performanslarının artması ve fiyatlarındaki düşüşlerle beraber kişisel bilgisayarların kullanımına başlandı ve yaygınlaştı. Böylelikle kontrol artık merkezi bir yerde olan ana bilgisayarlarda değil kullanıcıların eline geçmiş oldu[14]. Sonuç olarak dağıtık modele geçiş de başlamış oldu.

1990'lı yıllarda ise, Escalante ve Furth yerel alan ağları olarak adlandırılan LAN üzerinden bilgisayarlar arası haberleşme sistemini başarıyla uygulayıp aralarında veri alışverişi yapmaya başladılar. Yerel alan ağlarının artmasıyla birlikte büyük firmaların çoğu kendilerine ait olan sunucu bilgisayarlardan oluşan sistem odalarını kurdular[15].

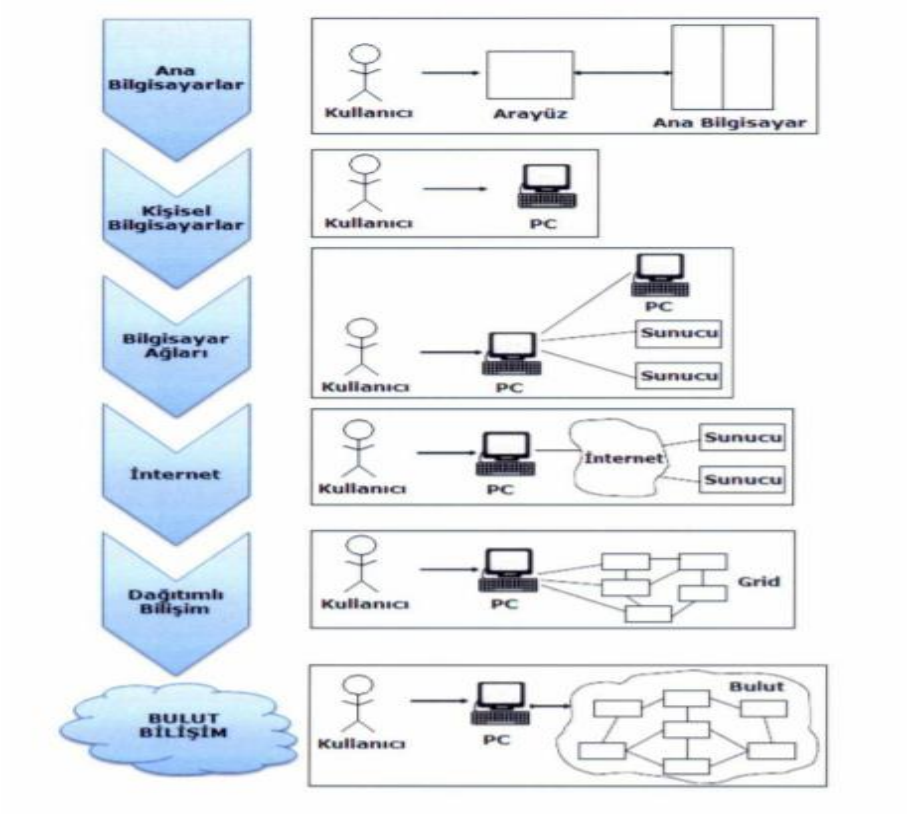
1990'ların sonuna doğru yukarıdaki son gelişmeler sayesinde Edwards ve Waelde tarafından yerel alan ağları birleşerek interneti oluşturdular. Aslında ilk zamanlarında sadece haberleşme maksadıyla oluşturulmuş olsa da zaman içerisinde bant genişliğindeki ve bağlantı hızındaki artış ile bu bağlantıların maliyetlerindeki düşüş sayesinde internet olan ilgi iyice artmaya başladı. Şirketler bazı reklam, pazarlama ihtiyaçlarını internete ortamında sunmaya başladılar. Kullanıcıların ve şirketlerin internete daha fazla dâhil olması da beraberinde güvenlik sorunlarını da getirmiş oldu[14].

2000 yıllarına gelindiğinde, firmalar bilişim hizmetlerinde satın alma, bakım, işletim, iklimlendirme, enerji, güvenlik açığından dolayı masrafların azalması amacıyla arayışlara koyuldular[16]. Bu sebeple bilişim dünyasında dağıtımlı bilişim(grid computing) adı verilen hizmet iyice kendisini geliştirmiş oldu. Dağıtımlı bilişim sunucu, donanım ve ağ cihaz ve birimlerinin ortak bir yerde toplanarak oluşan sanal sistemin adına denmektedir. Böylelikle tüm bu sistem tek bilgisayar gibi gözükmektedir. Ayrıca dağıtımlı bilişimde de bulut bilişimdeki gibi kullandığın kadar öde mantığı esas alınmıştır.

Fakat dağıtımlı bilişimin bu gelişimi zamanla ölçeklenebilirlik, güvenlik, barındırma hizmetleri ve kapasite gibi temel sorunlara karşılık veremeyince bulut bilişimin meydana gelmesini sağlamıştır. BT'de meydana gelen gelişmelerle birlikte işlemcilerde ve bilgisayar ağlarına erişimdeki hız artışı, maliyetlerin azalması ve veri merkezlerinin endüstriyel ölçekli bilişim hizmeti fabrikalarına dönüşmesi bulut bilişim modelinin doğmasına yol açmıştır.

Son olarak da bulut bilişimin sektöre gelmesiyle dağıtımlı bilişimdeki yer alan soyutlama sorunu da kaldırılarak son halini almış oldu.

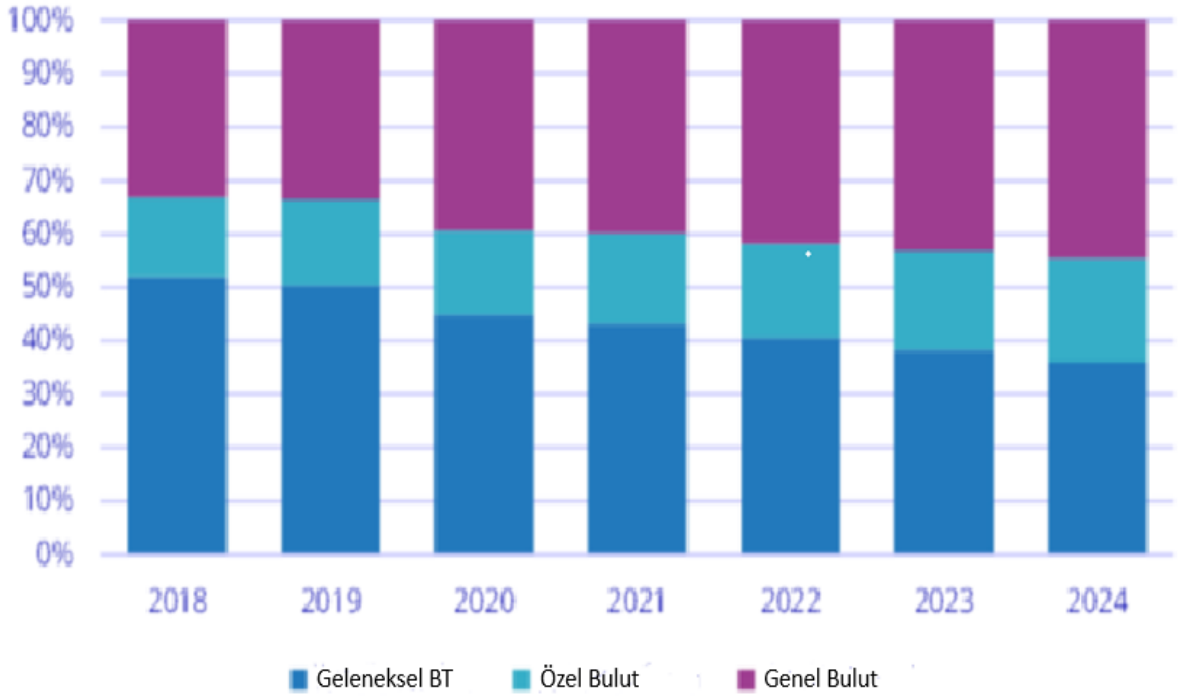
Aşağıdaki görsel bulut bilişimin ana bilgisayarlardan günümüze kadar gelmiş yapılarını göstermekte ve yukarıda anlatılan gelişmeleri özetler niteliktedir.



Şekil 2.1. Bulut bilişim gelişim grafiği[16].

2.3 Geleneksel BT Altyapısı & Bulut Bilişim Altyapısı

BT altyapısı ticari faaliyetlerin yüksek performans ve düşük maliyetlerle güvenli bir şekilde yürütülmesi konusunda önemli bir yer tutmaktadır. Sürekli gelişim içerisinde olan teknolojiye de ayak uydurması gerekmektedir. Bu gelişim olaylarının günümüzde çok hızlı olması ve diğer başlıca sebeplerden ötürü şirketler artık geleneksel BT altyapısı yerine bulut bilişim altyapısına geçmektedirler. Bu yönelimin başlıca sebepleri olarak maliyet, güvenlik ve kolay yönetim olarak sıralanabilir. Ayrıca IDC tarafından yapılan tahmin ve araştırmaya göre bulut bilişim altyapısının harcamaları ve pazarı geleneksel BT altyapısının harcamaları ve pazarının üzerinde olacak. Aşağıdaki görselde yapılan araştırmanın grafik halinde gösterimi yapılmıştır.



Şekil 2.2. Bulut BT altyapısı pazar tahmini[21].

2.3.1 Geleneksel BT altyapısı

Geleneksel bir BT altyapısı veri merkezleri, her sistem için barındırılması gereken sunucular, bilgisayarlar, ağ anahtarları, yönlendiriciler, güvenlik duvarları, yazıcılar, yedekleme sistemleri, çeşitli yazlımlar ve uygulamalar ile bu birimlerde yer alan çalışanlardan oluşmaktadır. Tüm bu cihaz ve yazılımlar için ayrıca sistem odalarına, jeneratörlere, UPS cihazlarına, iklimlendirme, yangın söndürme, güvenlik adına yer alacak kameralara ve erişim cihazlarına ihtiyaç duyulmaktadır.

Genel manada bakılınca tüm bu unsurları bir araya getirilmesi ciddi maliyet, fiziksel alan ve bunların uygulanmasındaki istihdam ve güç gerektirmektedir. Tüm bu altyapı için ayrıca bazı oluşabilecek sorunlar mevcuttur. Bunlar;

- Sistem Güvenliği
- Süreklilik
- Uyarı sistem ve cihazları
- Güncelleme
- Yedekleme

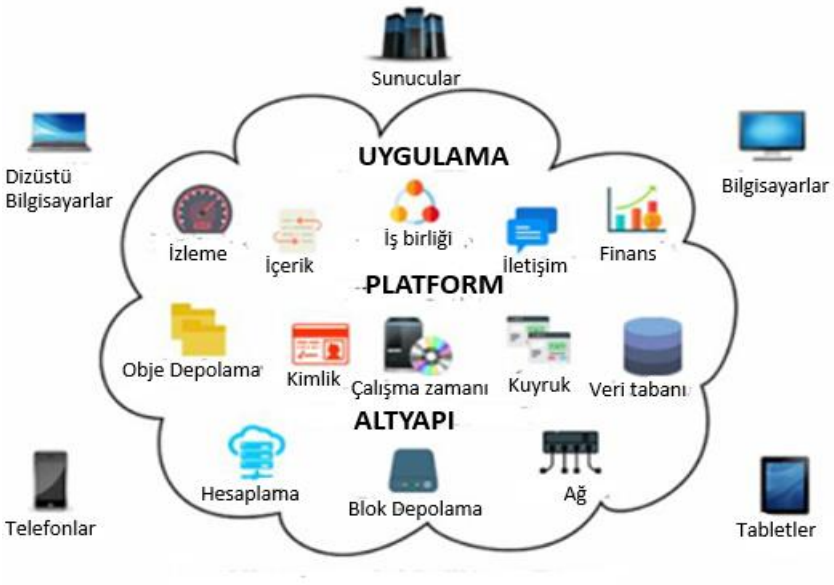
- ❖ Fiziksel alanın güvenliği
- ❖ Yüksek maliyet

2.3.2 Bulut bilişim altyapısı

Bulut bilişim altyapısında ise klasik BT altyapısından farklı olarak sanal bir barındırma söz konusudur. Bulut bilişim, Klasik BT yapısındaki sunucu veri merkezi yazılım, ağ, depolama gibi bileşenlerin kurumlara sanallaştırma yoluyla erişilebilir hale getirilmekle birlikte tüm bilgi işlem kaynaklarının da bu yolla kullanılması olanak sağlar.

Bu yapı ile birlikte artık kurum ve kuruluşlar bazı avantajlara sahip olmaktadır. Bunlar;

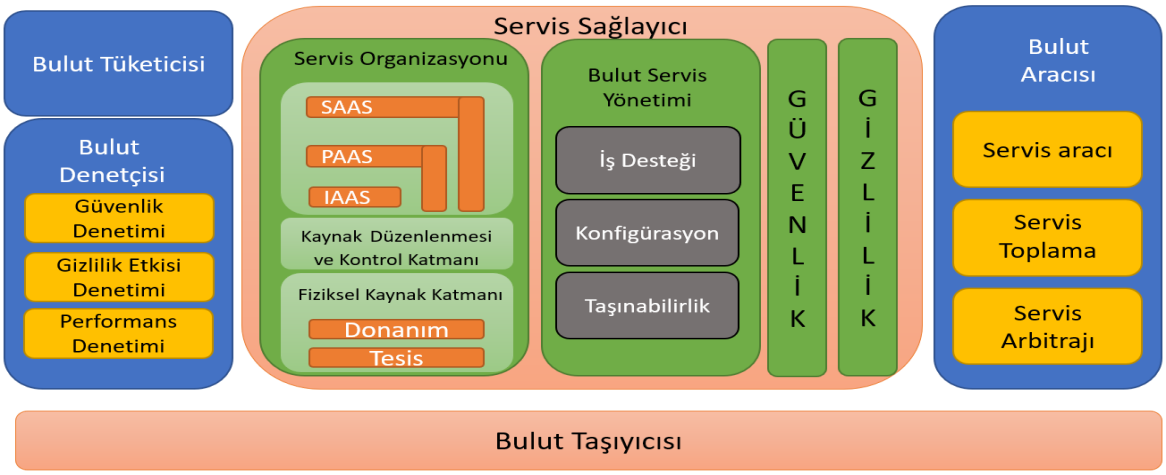
- ❖ Esneklik
- ❖ Ölçeklenebilirlik
- ❖ Otomasyon
- ❖ Düşük maliyet
- ❖ Yüksek güvenlik
- ❖ Verimlilik



Şekil 2.3. Bulut bilişimin konuları[21].

2.4 Bulut Bilişimin Mimarisi

NIST tarafından oluşturulan referans mimariye göre, bulut bilişim mimarisi bulut tüketicisi, servis sağlayıcısı, bulut denetçisi, bulut aracısı ve bulut taşıyıcısı olmak üzere 5 adet aktör veya paydaştan oluşmaktadır. Aşağıdaki şekilde NIST tarafından hazırlanan bulut bilişim referans mimarisi yer almaktadır.



Şekil 2.4. Bulut bilişim referans mimarisi için yığın diyagramı [17].

2.4.1 Bulut tüketicisi

Bulut tüketicisi, bulut bilişim hizmetlerinde ana paydaş rolünü üstlenmektedir. Bulut tüketicisi, bir bulut sağlayıcısıyla iş ilişkisi sürdüren ve hizmeti bir bulut sağlayıcısından kullanan bir kişi veya kuruluşu temsil etmektedir. Bir bulut tüketicisi, bir bulut sağlayıcısından hizmet kataloğundan uygun hizmeti isteyip bulut sağlayıcısı ile hizmet sözleşmeleri yapan ve hizmeti kullanan aktördür[17].

Tablo 2.1. Bulut hizmet modellerine göre tüketici faaliyetleri tablosu.

Hizmet Modeli	**Bulut Tüketicisi Faaliyetleri**
Hizmet Olarak Yazılım	İş süreci operasyonları için uygulama veya hizmet kullanır.
Hizmet Olarak Platform	Bir bulut bilişim yapısındaki yer alan uygulamaların geliştirlmesi, test edilmesi, dağıtımı ve yönetiminin yapıldığı hizmettir.

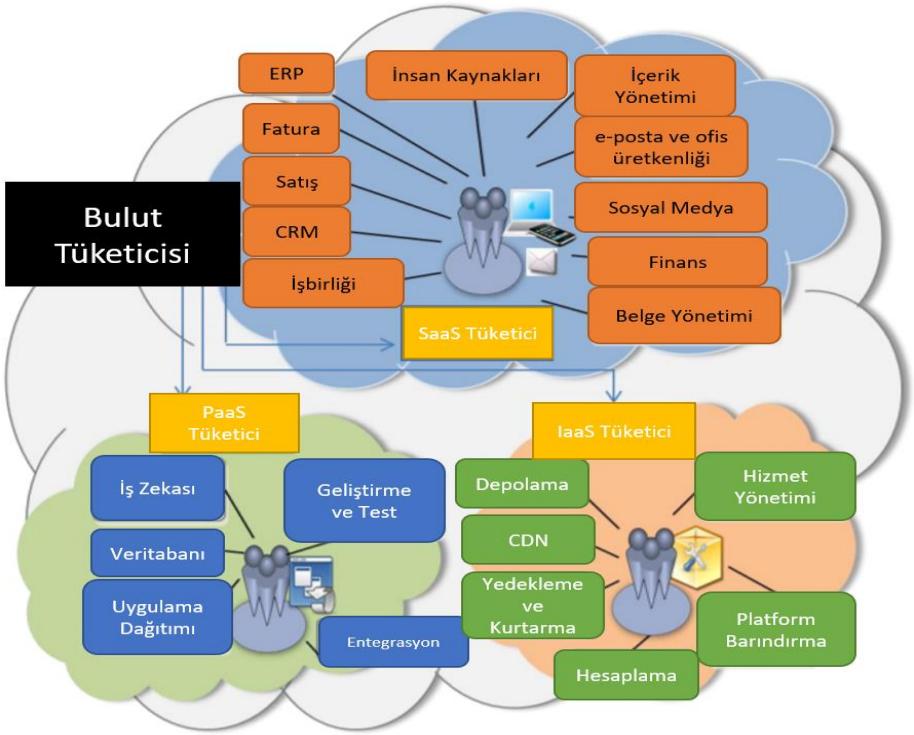
Hizmet Olarak Altyapı	BT altyapısı işlemleri için servislerin oluşturulduğu, yönetilip izlendiği servistir.

Bulut tüketicilerinin sağlanan hizmetler için ödeme yapması ve ödemeyi buna göre ayarlaması gerekebilir. Bulut tüketicilerinin, bulut sağlayıcılarının karşıladığı teknik performans gereksinimlerini belirtmek için SLA'lara ihtiyacı vardır. SLA, hizmet kalitesi, güvenlik ve performans hatası düzeltme önlemleriyle ilgili şartları kapsayabilir.

Hizmet Seviyesi Anlaşması (SLA): Hizmetin arızaya uğraması sebebiyle teknik onarma esnasında bilgilere ulaşmasını sağlayacak hizmet seviyesine ilişkin anlaşmaya denir[20].

Bir bulut sağlayıcısı, SLA'larda, tüketicilere açıkça verilmeyen bir dizi vaat, yani bulut tüketicilerinin kabul etmesi gereken sınırlamalar ve yükümlülükler de listeleyebilir. Bir bulut tüketicisinin, iyi fiyatlandırma ve uygun şartlara sahip olan bir bulut sağlayıcısı seçme hakkı bulunmaktadır ve bunu istediği gibi uygulayabilir.

Aşağıdaki şekil, bir bulut tüketicisinin kullanabileceği bazı örnek bulut hizmetlerini göstermektedir.



Şekil 2.5. Bulut tüketicilerinin kullanabileceği hizmet türleri[17].

2.4.2 Bulut denetçisi

Bulut denetçisi, görüşlerini ifade etmek için bulut hizmeti denetimine ilişkin bağımsız incelemeler yürütebilen bir taraftır. Denetimin amacı, objektif kanıtları gözden geçirerek standartlara uygunluğu doğrulamaktır. Bulut denetçileri, bulut sağlayıcısı tarafından sağlanan hizmetlerin güvenlik kontrolünü, gizlilik etkisini, performansını ve hizmet düzeyindeki sözleşme parametreleriyle uyumluluğunu değerlendirebilir. Ayrıca güvenlik denetimi için, bir bulut denetçisi, denetimlerin ne ölçüde doğru uygulandığını, amaçlandığı şekilde çalıştığını ve sistem için güvenlik gereksinimlerini karşılamaya yönelik olarak istenen sonucu üretebildiğini belirlemek için bilgi sistemindeki güvenlik kontrollerinin bir değerlendirmesini yapabilir[17].

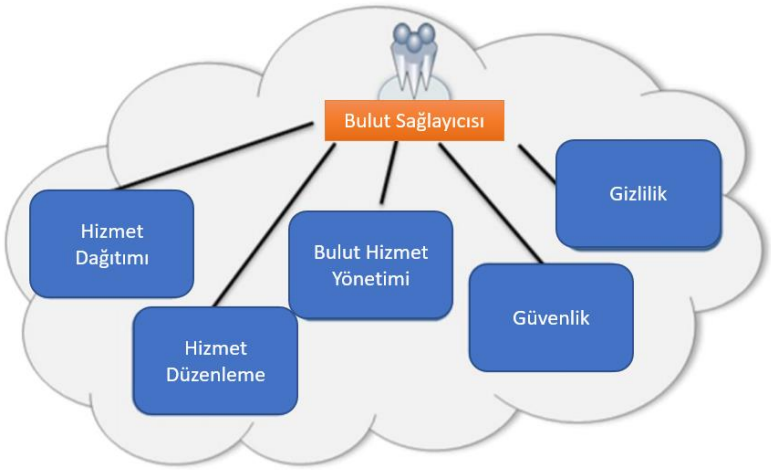
2.4.3 Bulut sağlayıcı

Bulut sağlayıcı, bulut hizmetlerinin gerekli merciilere sunmakla sorumlu olan kişi veya bir kuruluş olarak tanımlanmaktadır. Bir bulut sağlayıcısının sorumlulukları arasında hizmetleri sağlamak için gerekli bilgi işlem altyapısının tedarik edilmesi ve bunların yönetimi, hizmetleri sağlayan yazılımının çalıştırılması ve sağladığı tüm hizmetleri internet kullanarak tüketicilerine sunmak amacıyla düzenlemeler yapması bulunmaktadır. Ayrıca güvenlik ve gizlilikten de sorumlu aktör bulut sağlayıcısıdır[17].

Tablo 2.2. Bulut hizmet modellerine göre sağlayıcı faaliyetleri tablosu.

Hizmet Modeli	**Bulut Sağlayıcı Sorumlulukları**
Hizmet Olarak Yazılım	Sağlanan yazılım uygulamalarının bulut altyapsında yüklenir, doğru zaman aralıklarında bakımları yapılır ve bunlara destek sağlanır.
Hizmet Olarak Platform	Bulut kullanıcılarına bulut altyapısını ve ara yazılımları sağlar ve yönetir. Bunun yanı sıra kullanıcıları için geliştirme, dağıtım ve

	yönetim gibi konularda ek araçlar sağlar.
Hizmet Olarak Altyapı	Hizmet olarak yazılım kullanıcılarına bilgilerini depolayacağı, ağ oluşturup bunların barındırma ortamı ve bulut altyapısını sağlar ve yönetir.



Şekil 2.6. Bulut sağlayıcıların üstlendiği hizmetler[17].

2.4.4 Bulut aracısı

Bulut bilişimin gelişmesiyle birlikte, bulut hizmetlerinin entegrasyonu, bulut tüketicilerinin yönetmesi için çok karmaşık hale gelebilir. Bulut tüketicileri, doğrudan bulut sağlayıcılarıyla iletişim kurmak yerine bulut aracılarından bulut hizmetleri talep edebilir. Bu nedenle, bulut bilişim, bulut aracıları gerektirir.

Bulut aracısı, bulut hizmetlerinin kullanımını, performansını ve dağıtımını yöneten ve bulut sağlayıcıları ile bulut tüketicileri arasındaki ilişkiyi müzakere eden bir katılımcı veya varlık olarak tanımlanır.

Genel anlamda bakıldığında, bulut aracısının sağladığı hizmetler 3 ana başlık etrafında toplanmıştır. Bunlar[17];

- Hizmet Aracılığı: Bulut aracısı, belirli yetenekleri geliştirerek ve bulut tüketicilerine katma değerli hizmetler sağlayarak belirli hizmetleri geliştirir.

İyileştirme, bulut hizmetlerine erişimi yönetme, kimlik yönetimi, performans raporlama, gelişmiş güvenlik gibi hizmetler olmaktadır.

- Hizmet Toplama: Bir bulut aracısı, birden çok hizmeti bir veya daha fazla yeni hizmette birleştirir ve bütünleştirir. Aracı, veri entegrasyonu sağlar ve bulut tüketicisi ile çoklu bulut sağlayıcıları arasında güvenli veri hareketini sağlar.
- Hizmet Arbitrajı: Hizmet arbitrajı, bir araya getirilen hizmetlerin sabit olmaması dışında hizmet kümelemesine benzer. Hizmet arbitrajı, komisyoncuların birden fazla kurum veya kuruluştan hizmetleri esnek bir şekilde seçebileceği anlamına gelir. Örneğin, bulut komisyoncuları, en yüksek puan alan kurumları ölçmek ve seçmek için kredi puanlama hizmetlerini kullanabilir.

2.4.5 Bulut taşıyıcısı

Bir bulut taşıyıcısı, bulut tüketicileri ve bulut sağlayıcıları arasında bulut hizmetlerinin bağlantısını ve taşınmasını sağlayan bir aracı görevi görür[17]. Bulut taşıyıcıları, tüketicilere ağlar, telekomünikasyon ve diğer erişim ekipmanları aracılığıyla erişim sağlamaktadır. Örneğin, bulut tüketicileri bilgisayarlar, dizüstü bilgisayarlar, cep telefonları ve mobil İnternet cihazları (MID) gibi ağ erişim cihazları sayesinde bulut hizmetleri elde edebilmektedir.

Bulut hizmetlerinin dağıtımı genellikle ağ ve telekomünikasyon operatörleri veya ulaşım aracıları tarafından sağlanır; burada, ticari kuruluşlarda fiziksel mobil depolama ortamının (büyük kapasiteli sabit diskler gibi) yerini almak için geçiş aracıları kullanılır.

Bir bulut sağlayıcısının, bulut tüketicilerine sunulan SLA düzeyiyle tutarlı hizmetler sağlamak için bir bulut taşıyıcısıyla SLA'lar ayarlayacağını ve bulut operatörünün, bulut tüketicileri ile bulut sağlayıcıları arasında özel ve güvenli bağlantılar sağlamasını gerekmektedir.

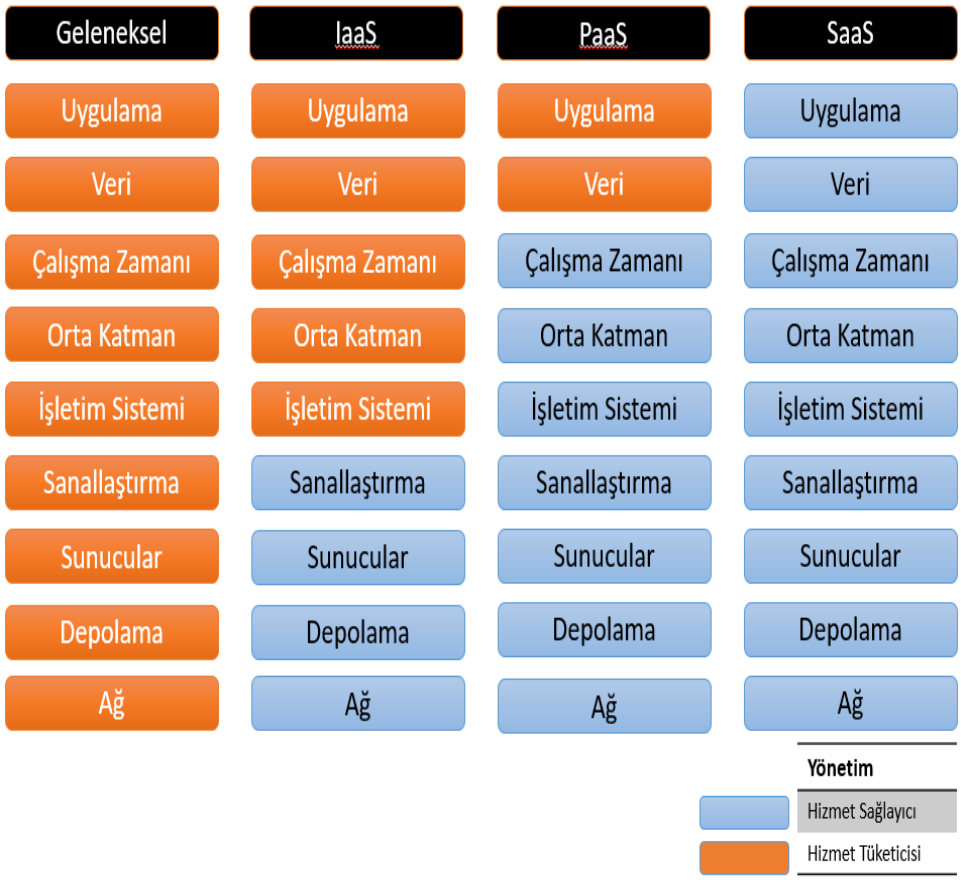
2.5 Bulut Bilişim Servis Modelleri

Hızlı, güvenilir ve güvenli hizmetler için artan müşteri beklentilerini karşılama mücadelesi veren şirketler, BT altyapıları üzerinde önemli bir yük taşımaktadır. Bu şirketler, BT sistemlerinin işlem gücünü ve depolama kapasitesini iyileştirmeye çalıştıklarında, genellikle güçlü, ölçeklenebilir ve güvenli bir BT altyapısı geliştirmenin ve sürdürmenin maliyetinin çok yüksek olduğunun farkına varırlar.. Bu sebeplerden

dolayı günümüzde çoğu şirket artık BT altyapısını bulut bilişim altyapısı olarak kullanmaya başladı.

Bulut bilişim günümüzde iyice artan hizmet modelleriyle birlikte temel olarak 3 tane hizmet vermektedir. Bunlar;

- Servis Olarak Yazılım (SaaS)
- Hizmet Olarak Platform(PaaS)
- Hizmet Olarak Altyapı(IaaS) 'dır.



Şekil 2.7. Bulut hizmetlerinin sağladığı yetenekler [33].

2.5.1 Hizmet olarak yazılım (SaaS)

Hizmet Olarak Yazılım, bulut bilişim sistemlerini kullananlar arasında en sık ve yaygın olarak bilinen ve kullanılan bulut hizmeti modelidir. SaaS, bulut sağlayıcılarının yazılım uygulamalarını barındırdığı ve yönettiği, aynı uygulamaya bulutta erişerek aynı uygulamaya aynı anda bulut tüketicilerine internet üzerinden yazılım uygulamaları sunma yöntemidir. Verilen SAAS hizmeti ücretsiz veya kullandıkça öde modeline dayanmaktadır ve genel olarak son kullanıcıya hitap etmektedir.

Hali hazırda birçok kullanıcının belki de Hizmet Olarak Yazılım olarak bilmeden kullandığı uygulamalarda ayırt edici özelliklerden biri kontrol düzeyindedir[22]. Hizmet Olarak Yazılım, bulut tüketicisine hizmet sağlayıcı tarafından çalıştırılan ve yönetilen tamamlanmış bir ürün sağlar. Bulut tüketicilerinin uygulama tarafından kendilerine has yapılandırılabilir ayarlar dışında hiçbir kontrol yetkisi bulunmamaktadır.

Hizmet Olarak Yazılım bulut tüketicisi hizmetin nasıl sürdürüldüğünü veya temel altyapının nasıl yönetildiği ile ilgilenmez sadece kendisine sunulan belirli parça yazılımı nasıl kullanacağı ile ilgilenir. Verilen hizmet internet üzerinden sağlandığı için indirme, kurulum vb gibi ihtiyaçlara gerek kalmadan kullanılabilmektedir.

Hizmet Olarak Yazılım uygulamalarının esnekliği aşağıda gösterilmektedir.

Şekil 2.8. Hizmet olarak yazılım esneklik şekli [139].

2.5.1.1 Hizmet olarak yazılımın avantajları

- Hızlı ve kolay erişim.
- Daha az donanım gerekliliği
- Kullandığın kadar öde mantığı
- Düşük bakım gerekliliği
- Güncelleme
- Birden çok cihaz ile erişim desteği
- Standart API'ler sayesinde kolay entegrasyon
- Bedava uygulama kullanımı
- Kurulum ihtiyacının olmaması
- Herzaman kullanıma hazır olması

2.5.1.2 Hizmet olarak yazılımın dezavantajları

- İnternet ağı bağımlılığı
- Hizmet Olarak Yazılım veren bulut sağlayıcıları arasında geçiş
- Tamamen bulut sağlayıcısının kontrolündeki uygulamalar
- Kişiselleştirme seçeneklerinin az olması
- Sınırlı özellik(feature)
- Hizmet kullanımının iptalinin zor olması: Bazı bulut sağlayıcıları ürünleri bulut tüketicilerine kullandırtmaya mahkum edebilmektedir.
- Veri sızıntısı riski
- Güvenlik ihlalleri riski
- Uygulamada yer alabilecek hataların çözümünün zamanının uzayabilmesi: Her türlü çözüm, geliştirme sağlayıcıya bağlı olmaktadır.

2.5.1.3 Hizmet olarak yazılım örnekleri

- **Salesforce**

Bulut bilişim alanında en popüler yazılımlardan biri ve seçkin bir hizmet sağlayıcıdır. Tam bir kurumsal müşteri ilişkileri yönetimi paketidir. Salesforce, işletmeler için bu işletmelerin müşteriverilerini tek bir yerden toplanıp, depolaması, erişimi, izlenmesi ve analizi için altyapı sağlar. Bir BT uzmanına sahip olmayan herhangi bir işletmenin çalıştırıp yönetimini yapacağı kusursuz bir bulut tabanlı CRM aracıdır. Salesforce, pazarlama, satış, analiz, etkileşim gibi özellikleri sağlayan birçok aracı da tedarik eder[23].

- **Dropbox**

Dropbox, şirketlerin dosyaları ve verileri her zaman, her yerde kolayca depolamasına, paylaşmasına ve üzerinde işbirliği yapmasına olanak tanıyan popüler bir bulut depolama uygulamasıdır. Çalışanların her yerde çalışabilmeleri için akıllı bir iş yeri sağlar. Dropbox, büyük ölçüde serbest çalışanlara ve uzaktan iş gücüne dayanan işletmeler için mükemmel bir uygulamadır. Ayrıca popüler olmasının en önemli sebebi hem bireysel kullanıcılara hem de kuruluşlara hitap etmesidir. Uygulamayı ücretsiz kullanmak isteyenler için 2 gb depolama alanı sunmaktadır[18].

- **G Suite**

G-Suite, iş hayatını kolaylaştıran çeşitli uygulamalar ve yardımcı programlar içerir. Gmail, Takvim, Hangouts, Google Drive, E-Tablolar, Dokümanlar, Formlar, Slaytlar, Siteler, Uygulama Kasası ve diğer birçok uygulamayı içerir. İş sürümünün, çoğumuzun aşina olduğu uygulamaların ücretsiz sürümünün aksine birkaç avantajı bulunmaktadır. Tüm uygulamalar tamamen bulut tabanlıdır ve internet bağlantısı olan bir tarayıcıdan kolaylıkla erişilebilmektedir[24].

- **Slack**

Yazılımda Agile olarak çalışan küçük ekipler için mükemmel ve uzaktan çalışmayı veya evden çalışmayı teşvik eden modern ofis için gerekli tüm bileşenleri içerisinde barındırmaktadır. Sesli ve görüntülü konferans görüşmeleri, Jira, Confluence gibi takımlar için ideal tüm uygulamaların kurulmasına fırsat vererek hizmet olarak yazılım uygulamalarında önemli bir yer tutmaktadır.

- **Microsoft Office 365**

Ofis dosyalarının herhangi bir cihazdan oluşturulmasına, düzenlenmesine, paylaşılmasına, yönetilmesine ve bunlara erişilmesine olanak sağlar. Kişisel bilgisayarınıza Microsoft Office 365 kurulabilmesi ve kullanılabilmesine rağmen bu platform ile birlikte, dosyalara herhangi bir Microsoft veri merkezinden erişilebildiği için her zaman ve internetin olduğu her yerden erişilebilmektedir.

- **Squibler**

Yazarların çalışmalarını taslak haline getirebildiği, düzenleyip güzelleştirebileceği çevrimiçi yazma aracı olarak bilinmektedir. Squibler, ilk kez kitap yazanların yaratıcı süreçlerini kolaylaştırmasını sağlar. İhtiyaç duyulan tüm araçlarla taslaktan daha hızlı yayın yapılabilen bir hizmet olarak yazılım uygulamasıdır.

2.5.2 Hizmet olarak Platform(PaaS)

Hizmet Olarak Platform (PaaS) olarak da bilinen bulut platformu hizmetleri, esas olarak uygulamalar için kullanılırken belirli yazılımlara bulut bileşenleri sağlar. Hizmet olarak platform, geliştiricilere özelleştirilmiş uygulamalar oluşturmak ve kullanmak için bir ortam sağlar. Tıpkı hizmet olarak altyapı(IaaS) gibi hizmet olarak platform da altyapının sunucu, depolama ve ağ bileşenlerinin yanı sıra ara yazılım, geliştirme araçları, iş zekâsı hizmetleri, veritabanı yönetim sistemleri ve farklı birçok bileşeni de içermektedir. Hizmet olarak platform, oluşturma, test, dağıtım, yönetim ve güncelleme gibi web uygulaması yaşam döngüsünde yer alan her şeyi desteklemek üzere tasarlanmıştır[25].

Hizmet olarak platformun yazılım dünyasını nasıl kolaylaştırdığıyla alakalı daha

derin bilgi verilerek konu detaylıca şöyle açıklanabilmektedir. Bir program geliştirici planladığı bir projeyi hayata geçirip geliştirmek için önce bir işletim sistemine ya da cross-platform bir proje olacaksa Windows, Linux, MacOS gibi birden çok işletim sistemine ihtiyaç duymaktadır. Ayrıca geliştirme yapılacak bilgisayar veya dizüstü bilgisayar araçları bu işletim sistemine uygun yapılandırmalarla donatılması gerekmektedir. Daha sonra işletim sistemi üzerinde çalışacak Visual Studio, Intellij IDEA, Eclipse, Java gibi geliştirme araçlarına ve ortamlarına ve verileri kaydedip kullanabileceği MySQL, PostgreSQL, MongoDB gibi veritabanı teknolojilerine de gerek duyulmaktadır. Sadece bu sayılanların bile kişiler tarafından tedarik edilmesi maliyet, zaman ve yönetim farkındalığı gerektirmektedir[26].

Hizmet olarak platformun teslim yöntemi de yazılımı internet üzerinden sunmak yerine bu geliştirilecek yazılım için uygun platform sağlamaktır. Bu platform web üzerinden geliştiricilere işletim sistemleri, yazılım güncellemeleri, depolama veya altyapı hakkında endişelenmelerine gerek kalmadan sadece yazılımı oluşturmaya veya geliştirmeye konsantre olma olanağı sağlar. Ayrıca bulut tüketicileri hizmet olarak platformu kullandıkça öde esasına dayalı olarak satın alabilmektedir.

Hizmet olarak platform, herhangi bir seviyede yazılım için, altyapı gerektirmeyen belirli bir iş parçası bulunduğunda, akıllarda yer alan proje fikirlerini test etmek istendiğinde ve yazılım için çevik metodolojiyi kullanan kuruluşlar için en ideal çözüm olarak karşımıza çıkmaktadır.

2.5.2.1 Hizmet olarak platformun karakteristik özellikleri

- Sanallaştırma teknolojisine dayalı bir hizmet olduğundan dolayı kurumun boyutuna göre kaynakların azaltılıp arttırılmasına olanak sağlar. Bu aslında hizmet olarak platformun ölçeklenebilir özellikte olduğunun kanıtıdır.
- Uygulamaların geliştirilmesi, test aşamalarının yapılması, dağıtımı için çeşitli hizmetler sunmaktadır.
- Birden fazla kullanıcı tarafından erişilerek hızlı geliştirmeye olanak sağlamaktadır.
- Web hizmetleri veritabanı alanındaki teknolojilerle entegre bir şekilde çalışabilmektedir.
- Kapsamlı sistem yönetimi bilgisi olmadan çalıştırılabilmektedir.

2.5.2.2 Hizmet olarak platformun avantajları

- Uygun maliyetle uygulama geliştirme
- Kodlama süresi ve miktarında gözle görülür azalma
- İş otomasyonu
- Ölçeklenebilir yapı
- Birden fazla platformda ekstra efor kaydetmeden yazılım geliştirme
- Farklı lokasyonlardaki geliştiricilerle beraber çalışma olanağı
- Tek ortamda test, geliştirme ve dağıtım hizmeti
- Lisanslama kolaylığı
- Son teknoloji veri merkezi ve donanımlara erişim
- Esneklik

2.5.2.3 Hizmet olarak platformun dezavantajları

- Bulut sağlayıcıya bağımlılık
- Veri güvenliği
- Uyumluluk
- Eski sistemlerin kişiselleştirilmesi
- Çalışma zamanı (Runtime) sıkıntıları
- Operasyonel sınırlama

2.5.2.4 Hizmet olarak platformun örnekleri

- **AWS Elastic Beanstalk**

AWS Elastic Beanstalk, Apache, Nginxgibi sunucular üzerinde Java, .NET, Node.js, Python, Ruby, Go ve Docker gibi yazılım teknolojileriyle geliştirilmiş web uygulamalarını dağıtımı ve ölçeklendirilmesinde kullanılan Amazonun hizmet olarak platform hizmetlerinden biridir. Elastic Beanstalk dağıtım için sadece uygulama kodlarını sistemine yüklenmesine ihtiyaç duyar ve kalan tüm aşamalarda otomatik olarak yönetimi

sağlamaktadır. Hizmet kaynaklarına erişim ve denetim hakkını da bulut tüketicilerine bırakmaktadır.

- **Windows Azure**

Microsoft Azure sektördeki en popüler hizmet olarak platform örneklerinden biridir. Popülerliği, dünya çapında çok yaygın olarak kullanılmasından kaynaklanmaktadır. Microsoft Azure aslında üç temel bulut modelini de kapsayan geniş içerikli bulut sağlayıcılarından biridir. İlk kod parçasından kodun son dağıtımına kadar uygulama geliştirme sürecindeki her adımı desteklemesi onu öne çıkaran özelliğidir. Bulut tüketicilerinin tüm uygulamalarını ve altyapılarını kolayca taşımaları için en basit yeteneği bile geliştirmelerine yardımcı olur. İş analizinde gelişmiş uygulamaları ve mobil servisleri içerir. Düşük maliyetiyle kullandıkça öde mantığına dayanan bir temele de sahiptir[27].

- **Heroku**

Heroku, kurumsal bir platform olarak adlandırılmamaktadır. Veri entegrasyonu için de alanı olmasına rağmen çoğunlukla tamamen platform içinden erişilebilen ekosistemlerden oluşmaktadır. Kullanıcı dostu arayüzüyle kullanımda sağladığı hizmetler onu prodüksiyon geliştiriciler ve sadece eğlence için uygulama geliştirenler arasında favori haline getirmiştir. Ancak, hizmet olarak platform örnekleri arasında ölçeklenebilirlik sorunu bulunmaktadır. Heroku'da bulunan geliştirici deneyimi modülü, doğrudan GitHub ve Git gibi popüler depolardan dağıtım yapılmasına olanak tanımaktadır. Düzenli olarak güncelleme yapılan Heroku birçok dilde hizmet vermektedir.

- **Google App Engine**

Google App Engine, Google Cloud'un bir parçasıdır ve yüksek düzeyde ölçeklenebilir uygulamalar ve araçlar sunmaktadır. Birden çok dil desteği de mevcuttur. Ölçeklenebilirliği ile bulut tüketicilerinin uygulamalarını pazara sunma süresini azaltmaktadır. Uygulama içindeki trafiğin arttığı durumlarda ölçeklenebilirliği otomatik hale getirerek kolay bir yönetim sunmaktadır. Ayrıca, kolay kullanımı ve çeşitli API'ler ile uyumlu olması diğer artı özelliklerindendir. Google App Engine, sunucusuz bir

tasarıma sahiptir ve herhangi bir kesinti olmaksızın sürekli olarak kullanılabilmektedir.

- **OpenShift**

OpenShift, kullanıcılara uygulamaları oluşturmak ve dağıtımını yapmak için kolay bir yol sunmaktadır. Aynı zamanda kapsamlı API desteğine ile bulut tüketicisinin sadece platformun kendisine sunduğu imkânlarla yetinmemesini sağlamaktadır. Bulut tüketicilerine sunduğu çeşitli özellikler vardır. Kubernetes'e dayanır ve tüm bileşenleri bulutta kullanıma sunmaktadır. Basit bir kullanıcı arayüzü içerir ve belki de en önemli özelliği, izinsiz girişleri engellemek ve yetkisiz erişimi dahili olarak önlemek için sunduğu güvenlik seçenekleridir.

- **SAP Cloud**

SAP Cloud, çok çeşitli farklı alanlarda uygulama oluşturmaya olanak tanıyan geniş bir uygulama koleksiyonu olduğundan, kendisi sadece bir hizmet olarak platform değildir. SAP Cloud, tümüne bulut üzerinden erişilebilen yerleşik 1.300'den fazla uygulamaya sahiptir. SAP ayrıca bazı çok kullanışlı analiz araçları sağlar ve IoT ve güvenlik uygulamaları için bir uygulamaya sahiptir. SAP bulutunda sağlanan veri depolama ve geliştirme ve operasyon hizmetleri dünya çapında yaygın olarak kullanılmaktadır. SAP Cloud ayrıca bulut ve yerel uygulamaları entegre etme fırsatları da sağlar [28].

2.5.3 Hizmet olarak Altyapı (IaaS)

Bulut bilişimdeki en önemli üç servis modelinin en çok ölçeklenebilirlik sağlayan servisi olan hizmet olarak altyapı, en önemli BT altyapıları olan sunucular, sanal makineler, depolama, ağ ve işletim sistemi gibi hizmetleri içerisinde barındıran, kullandıkça öde prensibi ile hizmet veren modeldir.

Kurumlar uygulama geliştirirken veya ürün ortaya koyacakları vakit donanım, ağ bileşenleri ve depolama alanlarına ihtiyaç duymaktadır. Günümüzde veri merkezlerini yapılandırmak ve yönetmek bazı bağımlılıklardan ötürü epeyce maliyetli görülmektedir. Örneğin bir veri merkezi inşa edileceği zaman, en önemli konu yer seçimi olmaktadır. Veri merkezinin kurulacağı yerin fiziksel ve stratejik konumu doğal afetlere karşı korunabilir bir bölgede olması gerekmektedir. Daha sonra veri merkezi içerisindeki

yönetim ve donanımların sağlanması diğer bir husus olarak önümüze konmaktadır. Ayrıca veri merkezlerinde sunucular, ağ ekipmanları da ek olarak maliyeti arttıran diğer unsurlardır. Bunlara ilaveten veri merkezinin sürekli olarak ayakta olmasını sağlayacak fiziksel ve yazılımsal gereklilikler de bulunmaktadır. Günümüzde kurumlar ve bulut sağlayıcıları da veri merkezlerini birden farklı yerde de kurarak yedekleme sistemini kullanmaktadırl[29].

Yukarıda anlatılan örnekle aslında hizmet olarak altyapının kurumlara ne kadar önemli bir maliyet açığını kapattığını ve ürün geliştirme hızını da ne kadar arttırdığı anlaşılmaktadır. Sağladığı tüm altyapı hizmetleriyle kurumlara gereken ağ, sunucu, veri merkezi gibi bileşenleri sağlayarak ve bu kaynakların kullanımına göre ölçeklenebilir bir ödeme seçeneği sunarak bulut tüketicilerine büyük katkı sağlamaktadır.

Hizmet olarak altyapı, web siteleri ve uygulama barındırma, depolama, yedekleme ve kurtarma gibi veri yönetimi hizmetlerini sağlama, yüksek performanslı bilişim işlemleri için ve büyük veri analizi gibi önemli ihtiyaçlar için kullanılabilen bulut bilişim hizmet modellerindendir. Ayrıca hizmet olarak altyapı kurumlarda BT yönetimi için sıklıkla kullanılmaktadır.

Hizmet olarak altyapı, temelini sanallaştırma teknolojisinden alarak bulut tüketicilerinde sunucular, ağ, işletim sistemleri ve depolama dâhil olmak üzere bulut bilişim altyapısı sunmaktadır. Bu bulut sunucuları genellikle tüketiciye API aracılığıyla sağlayarak dağıtımı sağlanmış olur ve böylelikle tüketicilerin tüm altyapı üzerinde tam kontrol sahibi olmasını sağlamış olur. Bulut tüketicileri sunucularına ve depolama alanlarına doğrudan erişmeye devam etmesine rağmen bunların tümü bulut sağlayıcılarının fiziksel veri merkezleri üzerinden sağladığı bir sanal veri merkezi aracılığıyla dış kaynak olarak gelmektedir[25].

Hizmet olarak yazılım ve platformun aksinde, hizmet olarak altyapı tüketicilerin uygulama, çalışma zamanı, işletim sistemleri, veri gibi hususları yönetmekten sorumludur. Ancak, hizmet olarak altyapı sağlayıcıları, sunucuları, sabit sürücüleri, ağı, sanallaştırmayı ve depolamayı yönetmektedir.

2.5.3.1 Hizmet olarak altyapının karakteristik özellikleri

- Birden fazla yerde verinin kopyasını barındırma
- İhtiyaca yönelik kaynak sağlama
- Ölçeklenebilirlik
- Platform sanallaştırma teknolojisi
- GUI veya API tabanlı erişim
- Yüksek güvenilirlik ve esneklik

2.5.3.2 Hizmet olarak altyapının avantajları

- Kullandığın kadar ödeme imkânı
- Çok sayıda donanım ve yazılım hizmeti
- Bir sunucunun durması tehlikesine karşı farklı konumlara yerleştirilmiş birden çok sunucu ile kullanılabilirliği garanti altına alması
- Her konumdan kaynaklara erişim hizmeti
- Bulut tüketicilerinin isteklerine göre ölçeklendirilebilir yapısı
- Cihazların kolaylıkla entegre edilmesi
- Bulut tüketicilerin BT altyapısında kontrol hakkı
- Düşük maliyetle donanım kiralama sağlaması

2.5.3.3 Hizmet olarak altyapının dezavantajları

- Bulut tüketicisi uygulamaları, verileri, ve işletim sistemi platformunu kontrol ederken, güvenlik tehditleri sanal makinelerden (VM) kaynaklanabilir. İçeriden gelen tehdit veya sistem güvenlik açıkları, ana makine altyapısı ile sanal makineler arasındaki veri iletişimini yetkisiz varlıkların erişmesine yol açabilir.
- Bulut tüketicisi olan kurumların altyapıyı etkin bir şekilde kullanıp yönetebilmesi için ek kaynaklara ve eğitime ihtiyaç duyulabilmektedir. Kontrol hakkını tam olarak verilmemesi gibi sorunlardan dolayı kaynakların izlenmesi ve yönetimi zor olabilmektedir.
- Bulut sağlayıcıları hizmet olarak altyapıda donanım kaynaklarını kullanıma sunulduğu şekilde kullanıcılar arasında dinamik olarak tahsis etmektedir. Bu

yüzden bulut sağlayıcısının, diğer tüketicilere önceki tüketiciler tarafından depolama varlıklarında depolanan verilere erişmemesini sağlaması gerekmektedir. Buna ek olarak bulut tüketicilerinin, sanal makinelerin çok kiracılı bulut mimarisi içinde yeterince izole edildiğinden emin olması konusunda bulut sağlayıcıya güvenmek dışında bir seçeneği bulunmamaktadır.

2.5.3.4 Hizmet olarak altyapının örnekleri

- **AWS EC2**

Hizmet olarak altyapının en önemli örneklerinden biri olan EC2, bulut tabanlı uygulamaları barındırmak isteyen şirketler için ölçeklenebilir bir altyapı sağlamaktadır. EC2 kullanan bulut tüketicileri fiziksel sunuculara sahip değildir. AWS, çoğu hizmet olarak altyapı gibi sanal sunucular arayıcılığıyla hizmetini sunmaktadır. Bu nedenle, tüketiciler yalnızca sunucuların kullanımı için ödeme yaparak, fiziksel donanıma yatırım yapma maliyetlerinden tasarruf sağlamış olurlar[30].

- **Google cloud compute engine**

Google, dünyadaki en büyük veri merkezlerini sorunsuz bir şekilde birbirine bağlayan en büyük ağ sistemlerinden birine sahip nadir şirketlerden biridir. Google Cloud'un sunduğu Compute Engine, sanal makineleri, yeniden başlatmaya gerek kalmadan ana sistemler arasında canlı geçiş yapılmasına, sanal makine üzerindeki işletim sistemlerinin yönetilmesine, sanal makine örnekleri için HDD ve SSD formatlarında diskler oluşturulmasına, gelecek isteklere bağlı yük dengelemesi (load balancing) yapılmasına ve kullanılan işlem süresine göre ücretlendirme gibi önemli hizmetleri barındırmaktadır.

- **Rackspace openstack**

OpenStack, özel ve genel bulutlar için açık kaynaklı bir yazılımdır. Hizmet Olarak Altyapı (IaaS) hizmeti olarak kullanılan OpenStack, şirketlerin bulutlarına sunucu, depolama ve ağ bileşenlerini kolay ve verimli bir şekilde eklemesine olanak tanımaktadır. Bulut tüketicilerine sanal makineleri, uygulamaları ve diğer kaynakları kolay ve hızlı bir şekilde dağıtımını yapmasını sağlamaktadır. Ayrıca ücretsiz ve açık kaynak olan

Openstack, genel, özel veya hibrit olarak dağıtım modeli çeşitlerine de sahiptir. Buna ek olarak Openstack açık kaynaklı bir proje olduğundan, koduna ihtiyaçlara göre erişilebilir ve değiştirilebilir durumdadır.

- **Microsoft azure**

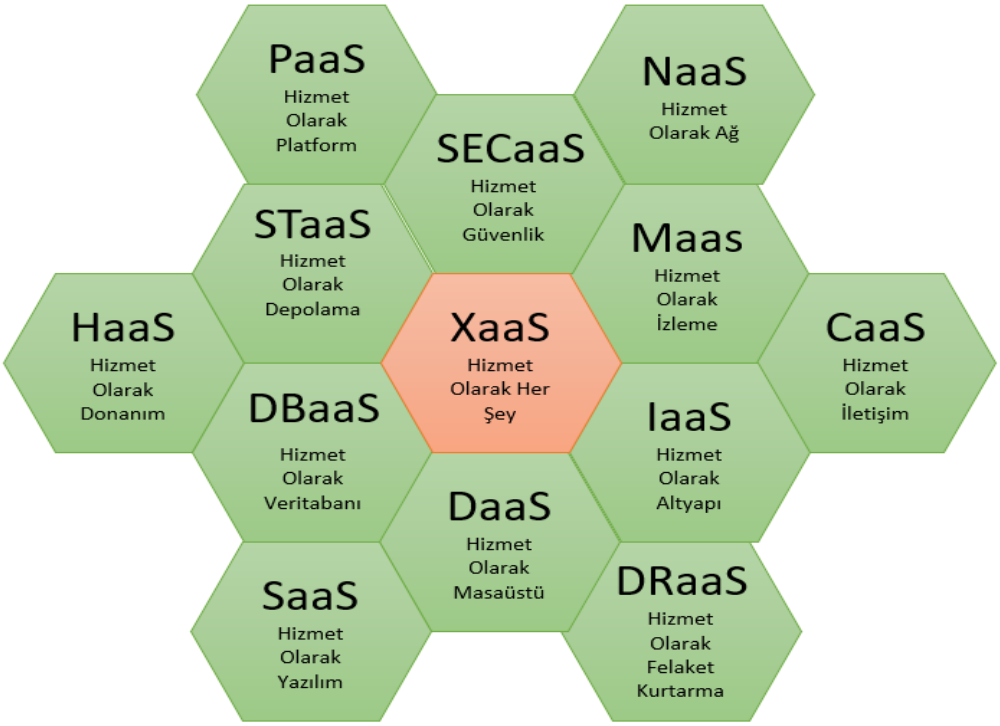
Hizmet olarak yazılım ve platform olarak da hizmet veren Microsoft Azure hizmet olarak altyapı hizmetleri de sağlamaktadır. Depolama, ağ, BT altyapısı güvenliği, bulut kaynakları yönetimi, Windows sanal masaüstü, yüksek performanslı bilgi işlem (computing) gibi birçok hizmet vermektedir.

- **Oracle bulut altyapısı**

Oracle Bulut Altyapısı, hizmet olarak altyapı modelidir. Bu sayede, güçlü bilgi işlem ve ağ, sanallaştırma, depolama gibi diğer altyapı bileşenleri ile ilgili hizmetler sağlar. Oracle bulut altyapsı ölçeklenebilirlik özelliğiyle büyük ölçekli kuruluşların taleplerini kolaylıkla karşılamasını sağlamaktadır.

2.5.4 Diğer Bulut Bilişim Hizmet Modelleri

Bulut bilişim teknoloji geliştikçe hizmet modellerinin arttığı bir platformdur. Son zamanlarda hizmet olarak her şey(XaaS) olarak adlandırılan hizmet çeşidi aslında yukarıda anlatılan üç önemli hizmet modellerinin kombinasyonu olarak düşünülebilmektedir. Bulut sağlayıcıları kurumların istekleri üzerine sadece küçük bir servis hizmeti verebilmektedirler. Bunun sayesinde tüketiciler gereksiz olan veya kurumların BT yapısında bulunan donanım ve yazılımları alma zorunluluğunu ortadan kaldırmış olur ve kendilerini ekstra maliyetlerden kurtarmış olmaktadırlar. Ayrıca bu tür küçük servisleri kuruma sağladıktan sonra tüketiciler, yeni uygulamalar ve çözümlerle değişen pazar koşullarına hızla uyum sağlayabilmektedirler.



Şekil 2.9. Bulut bilişim hizmet türleri.

2.5.4.1 Hizmet olarak her şey örnekleri

Hizmet olarak her şey modelinde bulut tüketicileri kurumlarının ihtiyaçlarına göre depolama, donanım, iletişim, ağ, izleme, felaket kurtarma, veritabanı, güvenlik, masaüstü gibi bir çok hizmeti kullandıkça ödeme temeliyle kiralayabilir.

- **Hizmet olarak donanım (HaaS)**

Özellikle küçük ve orta ölçekli kurumlar için daha uygun olan hizmet olarak donanım, lisanslama veya kiralama iş modelleri mantığıyla yürütülmektedir. Burada bulut tüketicisi, temel donanımın kendisine sahip olmak yerine hizmet tarafından sağlanan değeri öder. Hizmet olarak donanım, kurumların teknoloji varlıklarını satın almak yerine bir hizmet sağlayıcıdan kiralayabilmesini sağlar. Örneğin, kurumun yeni ekipman satın alma konusunda bütçeyle ilgili endişeleri varsa, maliyetleri düşürmek ve en son teknolojiden yararlanmak için bir hizmet sağlayıcıdan donanım kiralamak daha mantıklıdır[31]. Bu sayede bulut tüketicileri her geçen gün daha hızlı gelişen BT altyapısına en güncel donanımları ekleyerek pazarda etkin rol alabilmektedir.

- **Hizmet olarak iletişim (CaaS)**

Hizmet olarak iletişim, bulut sağlayıcısının bulutunda barındırılan VoIP (IP üzerinden ses veya internet telefonu), IM (anlık mesajlaşma), video konferans uygulamaları gibi farklı iletişim çözümlerini sunmaktadır. Bir kurum, belirli bir süre için mevcut ihtiyaçlarına en uygun iletişim uygulamalarını seçerek dağıtımını yapabilmekte ve yalnızca bu kullanım süresi için ödeme yapabilmektedir. Böyle bir yaklaşım sayesinde kurumlar kısa süreli iletişim ihtiyaçları için maliyetleri azaltmış olmaktadırlar.

- **Hizmet olarak masaüstü (DaaS)**

Hizmet olarak masaüstünde, masaüstü bilgisayarlar, kullanım için gerekli uygulamalarla birlikte bulut sağlayıcıları tarafından sanal hizmetler olarak sunulmaktadır. Böylelikle bir bulut tüketicisi, üçüncü taraf bir bilgisayardan çok daha güçlü olabilecek sunucuların bilgi işlem kapasitelerini kullanarak kişisel bir bilgisayarda çalışabilir. Bir hizmet olarak masaüstü sağlayıcısı, genellikle kullanıcı verilerinin depolanmasından, güvenliğinin sağlanmasından ve yedeklenmesinden ve desteklenen tüm masaüstü uygulamaları için yükseltmelerin sağlanmasından sorumlu olmaktadır. Bu bir nevi tüketicinin sanal masaüstü bilgisayarı kullanırken depolama ve güvenlik ihtiyaçlarını da sağlamaktadır.

- **Hizmet olarak güvenlik (SecaaS)**

Hizmet Olarak Güvenlik, kurumlardaki güvenlik hizmetlerinin dış kaynaktan sağlandığı bir bulut hizmeti modeli olarak tanımlanmaktadır. Hizmet olarak güvenlikte bulut sağlayıcıları tarafından bulundurulan güvenlik hizmetlerine erişim abonelik sistemiyle gerçekleştirilmektedir. Hizmet olarak güvenlik, güvenlik ekibinin sorumluluğunu azaltmak, iş büyüdükçe güvenlik gereksinimlerini genişletmek ve kurum içinde tutulabilecek alternatiflerin ve bunların bakımının maliyetini önlemek için kullanılır. Buna en basit örnek olarak internet üzerinden kullanılan antivirüs yazılımları söylenebilir. Hizmet olarak güvenlik ayrıca veri kaçağı önleme sistemi(DLP), e-posta, ağ ve web güvenliği, antivirüs, kimlik ve erişim yönetimi(IAM) gibi çözümler sunmaktadır.

- **Hizmet olarak veritabanı (DbaaS)**

Hizmet olarak veritabanı, fiziksel donanımı korumaya ve her türlü yapılandırmayı işlemeye gerek kalmadan çeşitli veritabanlarını depolamak ve yönetmek için bulut tabanlı bir hizmettir. Hizmet olarak veritabanında veritabanındaki verileri işleyen ve bu işlemleri izleyen veritabanı yöneticisi bulunmaktadır. Yönetici veritabanına bir API arayıcılığıyla erişir ve kontrol sağlamaktadır. Kullanıcı web üzerinden sağlanan API'ler arayıcılığıyla erişim sağlayabilmektedir. Kullanıcının veritabanı üzerinde yapılandırma, yönetim gibi her türlü işlemi yapmaya yetkisi bulunmaktadır. Ancak yönetim, yapılandırma bulut sağlayıcısı tarafından gerçekleştirilebileceğinden kullanıcı sadece hizmeti kullanamaya odaklanabilmektedir. Hizmet olarak yazılıma çok benzer olmasının yanı sıra sadece verilere odaklı bir hizmet anlayışı bulunmaktadır. Microsoft Azure SQL, MongoDB Atlası ve Amazon İlişkisel Veritabanı Hizmeti en önemli örneklerindendir.

- **Hizmet olarak depolama (STaas)**

Hizmet olarak depolama, bir kurumun veri depolamak için depolama altyapısını başka bir kuruma veya kişilere kiraladığı bir bulut hizmet modelidir. Küçük ölçekli kurumlar ve bireyler bunu genellikle yedeklemeleri yönetmek ve personel, donanım ve fiziksel alanda maliyet tasarrufu sağlamak için tercih etmektedirler. Hizmet olarak depolamada tüketici, depolamaya yönelik verileri hizmet sağlayıcıya depolama sağlayıcısının geniş alan ağı veya internet üzerinden belirli bir programa göre aktarır. Depolama sağlayıcısı, tüketiciye depolanan verilerine erişmesi için gereken yazılımı sağlar. Tüketiciler, veri aktarımları ve veri yedeklemeleri dahil olmak üzere depolamayla ilgili tüm görevleri gerçekleştirmek için sağlayıcı tarafından sağlanan bu yazılımı kullanır. Ayrıca hizmet olarak depolama yazılımları, bozuk veya kaybolan tim kurum verilerini kolayca geri yükleme becerisine sahiptir.

- **Hizmet olarak ağ (NaaS)**

Hizmet olarak ağ, tüketicilerin bulut sağlayıcılarından ağ hizmetleri kiraladıkları bir bulut hizmeti modelidir. Hizmet olarak ağ, bulut tüketicilerinin kendi ağ altyapılarını kurup yönetmeden, kendi ağlarını çalıştırmalarına olanak tanımaktadır. Diğer bulut hizmetleri gibi, hizmet olarak ağ sağlayıcıları da yazılım kullanarak ağ oluşturma

işlemlerini halleder ve temelde kurumların kendi ağlarını tamamen donanım olmadan kurmalarına izin verir. Hizmet olarak ağda bulut tüketicisi için gerekli tek şey internettir. Hizmet olarak ağ yapısında isteğe bağlı olarak özel ağ(VPN), bant genişliği, özel yönlendirme, çok noktaya yayın protokolleri, güvenlik duvarı, izinsiz giriş algılama(IDS) ve önleme(IPS) sistemleri, geniş alan ağı (WAN), içerik izleme ve filtreleme ve antivirüs gibi birçok elementi de beraberinde getirebilmektedir.

- **Hizmet olarak felaket kurtarma (DRaaS)**

Hizmet olarak felaket kurtarma (DRaaS), bulut sağlayıcılarının veri korumasını sağlamak, kesinti süresini sınırlandırmak ve bir felaket meydana geldiğinde kurtarma noktası hedeflerini (RPO-Recovery Point Objective) kısaltmak için küçük ve büyük işletmelere sunduğu bulut tabanlı bir çözümdür. Hizmet olarak felaket kurtarma, felaket kurtarma çözümü sağlayıcısına bağlı olarak yedekleme yazılımı için herhangi bir depolama, bant genişliği, RAM, işlem maliyeti ve lisans ücreti kombinasyonuna dayalı ödeme ile bir sözleşmeyle veya kullandıkça öde modeli olarak sunulmaktadır. Hizmet Seviyesi Anlaşmaları (SLA) maliyetleri etkileyebilmektedir.

- **Hizmet olarak izleme (MaaS)**

Hizmet olarak izleme, buluttaki diğer çeşitli hizmetler ve uygulamalar için izleme fonksiyonlarının dağıtılmasına yardımcı olan bir hizmet modelidir. En yaygın hizmet olarak izleme uygulaması, belirli uygulamaların, ağların, sistemlerin veya bulutta dağıtılabilen herhangi bir şeyin belirli durumunu durmaksızın izleyen çevrimiçi durum izleme olarak adlandırılmaktadır. Günümüzde modern BT altyapı boyutları gitgide artmaktadır. Bu da altyapıda büyük karmaşıklara neden olmaktadır. Hizmet olarak izleme bu karmaşıklaşmış yapıların izlenmesi, verilerin toplanması, analiz edilmesi ve görselleştirilmesi ihtiyacına çok uygun bir çözüm olarak sunulmaktadır.

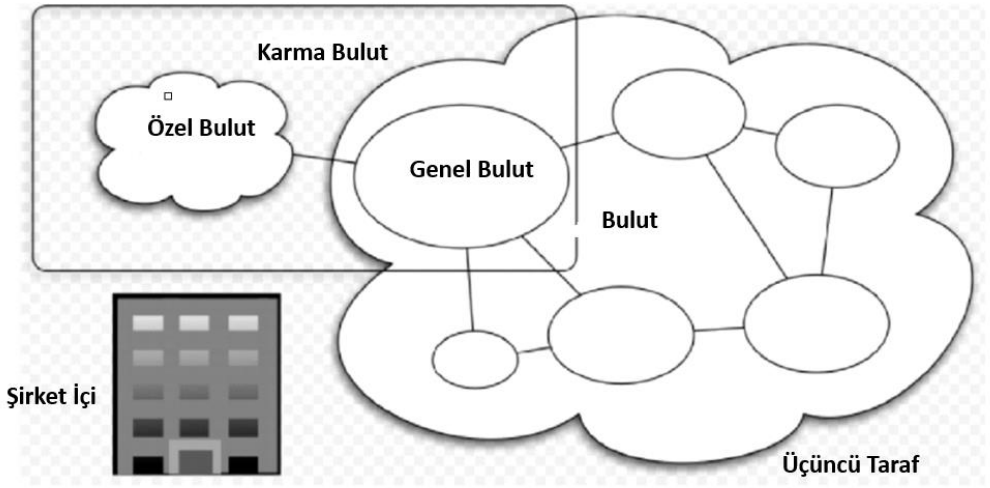
2.6 Bulut Bilişim Dağıtım Modelleri

Bulut bilişimde çalışma mekanizmasının daha iyi anlaşılır olması için bulut bilişimdeki dağıtım modellerinin hepsinin bilinmesi gerekmektedir. Bulut bilişimde dağıtım modelleri, bulut kaynaklarına kimlerin erişebileceğini ve kaynaklara nasıl erişilebileceğini belirlemektedir[32]. Dağıtım modeli, sunucuların fiziksel konumunu ve onlardan sorumlu tüm varlıkları tanımlar.

Bulut dağıtım modelinin seçimi, kuruluşun hedeflerine ve iş gereksinimlerine bağlıdır. Bir kuruluşun, hangi dağıtım modelini seçeceğine karar vermeden önce dağıtım modellerinin güvenlik, güvenilirlik ve performans sorunlarını incelemesi gerekmektedir. Böylece kendilerine daha uygun olan dağıtım modeliyle rahat çalışma ortamı oluşturulabilir[33].

Bulut bilişimde dağıtım modelleri birbirleriyle bazı benzerlik ve farklılıklar bulundurmaktadır[34]. Bulut bilişim teknolojilerinde yer alan dağıtım modelleri aşağıdaki modellerden oluşmaktadır. Bunlar

- Genel Bulut
- Özel Bulut
- Karma Bulut
- Topluluk Bulutu



Şekil 2.10. Bulut bilişim dağıtım modelleri[140].

2.6.1 Genel Bulut

Genel olarak bulut bilişim temel yapısını oluşturan genel bulut, bulut sağlayıcılar tarafından sunulan tüm hizmetlerin internet üzerinden birden çok kurum, kuruluş ve bireylere paylaştırmaktadır[29].

Bazı genel bulut sağlayıcıları kaynakları ücretsiz sunarken, müşteriler diğer kaynaklar için abonelik veya kullandıkça öde mantalitesiyle çalışmaktadır. Bulut hizmetleri bireysel kullanıcılar tarafından da kullanılabilmektedir ve fiyatları kullanıcının belirleyeceği kaynaklara göre ölçeklendirilmektedir[35].

2.6.1.1 Genel bulut avantajları

Düşük Maliyet: Genel bulutların en önemli özelliği kullandıkça öde matığıyla ilerlemeleridir. Bir kurum büyüdüğünde veya küçüldüğünde, maliyetler de bunlara paralel olarak artar veya azalır. Özel bir bulut ile genel bir bulut arasındaki fark, özel bir bulutun büyümenin üstesinden gelebilmesi için altyapının tasarlanmasının gerekli olabilmesi ve bu da onu daha maliyetli hale getirmesidir. Ancak bir kuruluşun ihtiyaçları azaldığında maliyetler aynı kalır. Böylece genel bulutlar ölçeklenebilirliğiyle ön plana çıkmaktadır[33].

Sorunsuz Altyapı Yönetimi: Bulut bilişim altyapısını çalıştıran üçüncü bir taraf servis sağlayıcısı olması yönetim açısından ihtiyaç olabilmektedir. Yazılımı geliştirmeye ve bakımının yapılmasına gerek olmaz, çünkü servis sağlayıcı bu işlemlerin hepsini kendi yönetmektedir. Ayrıca altyapı kurulumu ve kullanımı karmaşık değildir[36].

Çalışma Süresi: Bulut sağlayıcısı sunucularının kapsamlı ağı, altyapının sürekli kullanılabilir olmasını ve çalışma süresinin iyileştirilmesini sağlar. Böylelikle 7/24 çalışır bir sistem ortaya çıkmaktadır.

2.6.1.2 Genel bulut dezavantajları

Yanlış Bulut Sağlayıcısı: Yanlış bir genel bulut sağlayıcısı seçildiğinde bazı tehlikeler mevcut hale gelmektedir. Bir bulut sağlayıcısı kendisinde yer alan donanım cihazlarını güncel tutmazsa, kullanıcılar uyumluluk ve yürütme hızı ile alakalı bazı sorunları yaşayabilmektedir[37].

Azaltılmış Kontrol: Yönetimsel argümanlar genel bulut sağlayıcısı tarafından kontrol edildiğinden, kullanıcılar özel bir bulutta olduğu kadar fazla kontrole sahip değildir. Bu altyapıda rahatlık getirebildiği gibi kontrol yetkilerinin azalması birçok sorunu beraberinde getirmektedir.

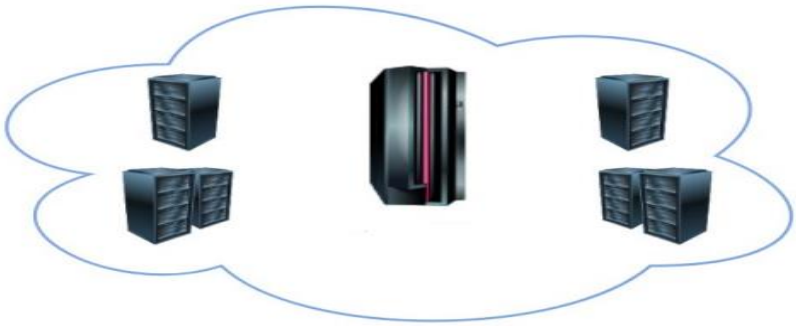
Güvenlik: Veri güvenliği ve mahremiyet ile ilgili konular bulut tüketicileri için bazı durumlarda endişe verici olmaktadır. Verilere erişim kolay olsa da, halka açık bir dağıtım modeli, kullanıcıları bilgilerinin nerede tutulduğunu ve bunlara kimin erişimi olduğunu bilinmesini gizli tuttuğundan dolayı güvenlik açısından riskli bir yapıdadır[36].

Hizmet Kısıtları: Hizmet sağlayıcıların yalnızca standartlaştırılmış hizmet seçenekleri bulunduğundan dolayı, genellikle daha karmaşık gereksinimleri karşılayamamaktadır[36].

2.6.2 Özel Bulut

Özel bulut konumlandırma modeli sadece bir kurumun veya işletmenin sahibi olduğu veya kiraladığı bulut modeline denmektedir. Buradaki bulut altyapısı tamamen sahibi olduğu kurum için çalıştırılır. Yönetimi ise bu kurum tarafından veya 3.taraf tarafından sağlanabilmekte ve kurumun tesislerinin içinde veya dışında konumlandırılabilmektedir[38].

Özel bulutun yönetimi kurum içinde yapıldığından dolayı en güvenilir bulut modeli olarak karşımıza çıkmaktadır. Ayrıca özel bulut modelinde depolanan tüm verileri yalnızca sahibi olduğu kurumun kullanıcıları arasında paylaşılmaktadır. Bunun yanı sıra kurumun belirleyeceği yöntemlere göre üçüncü taraf ile paylaşım mümkündür. Amazon Virtual Private Cloud (Amazon VPC), IBM SmartCloud Foundation ve Microsoft Private Cloud özel bulutlar için en bilinen ve yaygın olarak kullanılanlardandır[39].



Şekil 2.12. Özel bulut modeli yapısı[141].

Bir kurum veya kuruluş aşağıdaki dört sebepten ötürü özel buluta geçmek durumundadır[40].

- Kurum içindeki tüm kaynakların kullanımını en üst düzeye çıkarmak ve optimize etmek.
- Veri gizliliği ve mahremiyeti açısından güvenlik endişeleri bulunması.

- Yerel BT altyapısından genel buluta veri aktarımı maliyetinin hala oldukça fazla olması.
- Veriler üzerinde tamamen kontrol hakkına sahip olunmak istenmesi.

Özel bulutlar ikiye ayrılmaktadır;

Şirket İçi Özel Bulut: Bu özel bulut modeline "dahili bulut" da denmekte ve kuruluşun kendi veri merkezinde barındırılır. Daha standart bir süreç ve koruma sağlar, ancak genellikle ölçek ve ölçeklenebilirlik açısından kısıtlamalar bulunmaktadır. Ayrıca bu özel bulut çeşidinde, kurumun BT departmanı, fiziksel kaynaklar için sermaye ve operasyonel maliyetlerin tamamını kendi tedarik etmek durumundadır. Şirket içi özel bulutlar, altyapının ve güvenliğin tam kontrolünü ve yapılandırılmasını gerektiren uygulamalar için en ideal seçim olarak gözükmektedir[39].

Dış Kaynaklı Özel Bulut: Bu özel bulut modeli, şirket içi özel bulutun aksine üçüncü taraf bir bulut bilişim sağlayıcısı tarafından barındırılmaktadır. Hizmet sağlayıcı, tam gizlilik garantisiyle özel bir bulut ortamını kolaylaştırmaktadır. Bu model, fiziksel kaynakların paylaşımıyla ilgili riskler nedeniyle genel bir bulut altyapısını kullanmamayı tercih eden kuruluşlar için önerilir[39].

2.6.2.1 Özel bulut avantajları

Gelişmiş güvenlik: Bir kurumda güvenlik özellikle bankacılık sektöründeki kurumlar için aranan en önemli özelliklerden biridir. Özel bulut modelinde özelleştirilebilir ve kapsamlı bir güvenlik duvarı bulunmaktadır ve bilgisayar korsanlığı gibi birçok yasa dışı kullanımlara karşı güvenliği garanti eden çok sayıda güvenlik ve gizlilik yöntemleri ile kurumlara güvenlik konusunda rahatlatıcı seçenekler sunmaktadır[41].

Esneklik: Özel bulut modeli, bir kurumun tüm isteklerinde cevap verebilecek ve bu istekleri tedarik edebileceğinden dolayı özelleştirilebilir bir yapıdadır. Bu yapı sayesinde

kurumlar kendi verileri üzerinde ek kontrol sahibi olmasından dolayı güvenliğini sağlamak daha kolay hale gelmektedir. Kurumlar kendi verileri üzerinde kontrolleri sayesinde her türlü tedbir alabilmekte ve güvenlik gereksinimlerini sağlayabilmektedir[41].

Performans: Sadece kurum içinde veri paylaşıldığından dolayı her zaman önemli bir transfer oranı vardır. Bu nedenle, Özel bulut daha yüksek düzeyde performans sağlar[42].

Kullanılabilirlik: Tüm bulut bilişim modelleri, hizmetlerine her zaman, her yerden erişmelerini sağlar. Özel bulut modelinde ise erişim olanağı daha kolaydır. Özel bulut, kullanıcıların teslimatı kontrol etmesine ve en yüksek düzeyde kullanılabilirlik sağlamasına yardım eden altyapısıyla gayet kullanışlıdır[42].

2.6.2.2 Özel bulut dezavantajları

Maliyet: Şirket içi özel bulut modelinde maliyetler bir hayli önem arz etmektedir. Maliyetler personel, donanım ve operasyonel süreçleri içerisinde barındırmaktadır. Bu da maliyeti arttıran önemli nedenlerden biridir. Dış kaynaklı özel bulut modelinde ise maliyet, kaynak başına kullanımı içereceğinden hizmet sağlayıcının takdirine bağlı olarak değişiklik gösterecektir[43].

Yetersiz Kullanım: Bazı durumlarda tedarik edilen kaynaklar yetersiz kullanılabilmektedir. Bu nedenle, tüm kaynakların kullanımını optimize etmek bir bir zorluk oluşturabilmektedir[43].

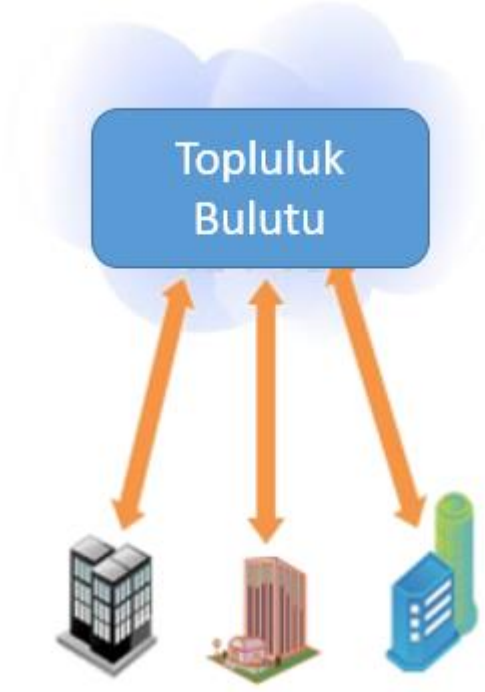
Kapasite: Bazen hizmet sağlayıcısı fiziksel donanım sınırlamalarına sahip olabilmektedir. Bu nedenle yalnızca belirli miktarda sunucuyu veya depolamayı işlemek için kapasitede yetersizlik belirebilmektedir[43].

Satıcı Bağımlılığı: Bu, özellikle donanım ve altyapı dış kaynaklı olduğunda özel bulutun benimsenmesinde büyük bir engel olabilir. Bu, müşteri şirketin aynı hizmet sağlayıcıyla devam etmeye zorlandığı ve böylece müşterinin başka bir satıcıya geçmesini engellediği bir hizmet sağlama tekniğidir. Bu teknikten ötürü bulut tüketicileri bulut sağlayıcıya bağlı kalmak zorunda olabilmektedir[43].

2.6.3 Topluluk Bulutu

Birkaç kuruluşun benzer gereksinimlere sahip olduğu ve bulut bilişimin bazı

avantajlarını kullanmak için altyapının paylaşıldığı bulut modeline denmektedir[44]. Topluluk bulutunda farklı kurumların bir araya gelebilmesinin yanı sıra birden fazla şirketi olan ve projelerini ve sistemlerini aynı bulut altyapısında yönetmek ve geliştirmek isteyenler için en ideal bulut dağıtım modelidir.



Şekil 2.13. Topluluk bulut modeli yapısı[142].

Topluluk bulutunun yapısı yukarıdaki şekilde gösterilmiştir. Şekilde iki farklı kurum kullanıcıların aynı bulut altyapısına erişebildiği gözlemlenebilmekte böylelikle birden fazla farklı kuruluşun aynı ortamdan kaynak tedarik elde edebilmesi ve erişebilmesine olanak sağlanmış olur.

2.6.3.1 Topluluk bulutu avantajları

- Açık sistemlerdir ve kuruluşların bulut hizmeti sağlayıcılarına olan bağımlılığını ortadan kaldırırlar. Kuruluşlar hem genel hem de özel bulutların dezavantajlarından kaçınırken birçok fayda elde edebilir[45].
- Her kullanıcı için uyumluluk sağlanır ve özellikleri kendi kullanım durumlarına

göre değiştirmelerine olanak tanır. Böylelikle donanım kaynakları, hizmetler için ayrı ayrı ölçeklenebilirlik sunar ve esnekliği arttırır. Ayrıca, şirketlerin uzaktaki çalışanlarıyla etkileşime girmesine ve akıllı telefon veya tablet gibi farklı cihazların kullanımını desteklemesine olanak tanır[45].

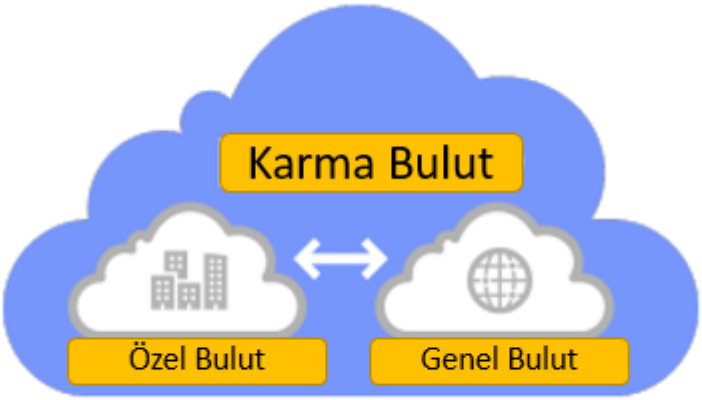
- Verileri ve uygulamaları doğal afet benzeri öngörülemeyen koşullardan korumak için farklı yerlerde yedekleyerek, diğer bulut hizmetlerinde olduğu gibi verilerinizi de korur. Yedekli yapı sayesinde her an ve her yerden erişilebilirlik sağlar[45].
- Topluluk bulutu güvenlik açısından genel buluta nazaran daha fazla güvenliklidir.
- Bu model ile birlikte birden çok veri merkezi, bu saklanan verilerin yönetimi ve gerekli kaynaklar merkezi bir yapı olduğundan azaltılmış olur.
- Tüm ihtiyaçlar tek bir platform üzerinden sağlandığından kurum ve kuruluşlar arasında tüm kaynaklar ve altyapı paylaşılmış olur.

2.6.3.2 Topluluk bulutu dezavantajları

- Her kullanıcının verilere erişim yetkisine sahip olmasından dolayı kuruluşlar, kısıtlanmış verileri paylaşmadıklarından emin olmalıdır.
- Topluluk bulutu modelinde uyumlulukla ilgili kurallar ve düzenlemeler örtüşmeyebilir. Bu modeli kullanacak kuruluşlar, diğer kuruluşların sistem, kural ve düzenlemelerine uyum sağlamak zorunluluğu bulunabilmektedir.

2.6.4 Karma Bulut

Karma bulut modeli özel bulut tabanlı sistemlerle genel bulut tabanlı sistemlerin bir araya gelmesiyle oluşan ve bu sistemlerin bir arada çalışmasını sağlayan model olarak tanımlanmaktadır. Karma bulut modelinde iş yükünün belirlenen bir kısmı genel bulutta çalışırken, diğer kalan kısımlar ise özel bulutta çalışmaktadır. Bu sayede hem özel hem de genel bulut modellerinden daha fazla esneklik sunabilmektedir. Birkaç farklı stratejiden dolayı karma bulut kullanılabilmektedir.



Şekil 2.14. Karma bulut modeli yapısı[143].

2.6.4.1 Özel bulut kullanım senaryoları

- Bir kurumun tüm hassas verilerini kurum içinde saklamak ve kurumca belirlenen hassas olmayan verilerin bulut sunucularında depolanmasını istediğinde[46]
- Bir kurumun tüm verilerinin şirket içinde saklamak ve yalnızca harici bir bulutun bilgi işlem gücünden faydalanmak istediğinde[46]
- İkinci seçeneğin tam aksine, bir kurumun bilgi işlem gücü kurum içinde sağlarken, tüm verilerini bulutta depolamak istediğinde[46]
- Doğal afetler sonrasında verilerin yedeklenerek korunması istendiğinde[47]
- Kurum içindeki uygulamaları geliştirmek ve test etmek açık bulutta fiziksel donanım satın almaya ve kurmaya gerek olmadığından, daha uygun maliyetli hızlı geliştirme ve test yapılmak istendiğinde[[47]]
- Ölçeklenebilir iş yükü sağlanmak istendiğinde[47] karma bulut modeline ihtiyaç duyulmaktadır.

2.6.4.2 Özel bulut avantajları

- Hem özel hem de genel bulutu içerisinde bulundurduğundan bu modellerin düşük maliyetinden ve esnekliğinden yararlanır[48].
- Ölçeklenebilirliği diğer bulut dağıtımın modellerinde göre az bir maliyetler ölçeklenebilirliği arttırarak, bulut kaynaklarının daha düşük maliyetle küçük ölçekli geliştirme projeleri için tedarik edilmesine yardımcı olur ve bu genellikle

kurumların altyapısındaki yapılacak değişiklikleri önler[48].

- Bulut sistemlerine geçmekte isteksiz olan kurumlar için bulutu daha düşük bir maliyetle ve çok daha düşük riskle sistematik olarak deneme fırsatı sunar[48].
- Kurum verilerini kurum içinde özel bulutlar yardımıyla saklayarak daha güvenli bir sistem elde edinilmesini sağlar[49].
- Periyodik zaman aralıklarıyla kurum verilerinin, kullanıcı bilgilerinin ve sistemlerin yedeklerini alır ve aynı zamanda olası bir doğal afet sonrasında tüm bu verilerin kaybolmasını önleyerek, iş sürekliliği sağlar[49].

2.7 Bulut Bilişimin Avantajları

Bulut bilişim kullanan veya kullanmaya başlayan ker kurum ve kuruluş bulut bilişimin ne kadar güçlü bir yapısı olduğunu ve bunun kendilerine ne kadar yarar sağladığını görebilmektedirler. Her geçen gün artışını sürdüren yüksek veriler, bu verilerin bakımı, yönetimi ve bunlar için gerekli personeller ve geleneksel BT altyapısının sunamadığı diğer önemli özellikler kurumları bulut bilişim altyapısına doğru yönlendirmektedir.

Bulut bilişimi düşük maliyet, esneklik, erişilebilirlik, yönetim, raporlama, yedekleme, depolama, bakım, performans ve ölçeklenebilirlik gibi birçok avantaj sağlamaktadır. Bulut bilişimin sağladığı tüm bu avantajları her kurumun kendi yapısı ve ihtiyaçları doğrultusunda kendilerine önemli yararlar sağlamaktadır.

Bulut bilişimin en önemli avantajları aşağıdaki gibi sıralanmaktadır.

- Maliyet[50-51]:

Bulut bilişimin getirdiği en önemli avantajlardan biri maliyettir. Bulut bilişim sayesinde kaynakları yeterli seviyede bulunmayan KOBİ'ler, yeni kurulan start-up şirketler, kendilerine nazaran büyük şirketlerin sahip olduğu çoğu bulut bilişim hizmetlerini bünyelerine uygun maliyetlerle tedarik edebilmektedirler. Böylece küçük buyottaki firmaların piyasaya düşük maliyetlerle daha hızlı bir giriş yapmaları kolaylaşmaktadır.

Bunun yanı sıra bulut bilişim sistemi kullanan kurum ve kuruluşlar sunucu tarafında bilgisayarlar, ağ cihazları, sistem odaları gibi tüm donanımların çalışmaları ve

bunların soğutulması gibi yapılması gereken işlemlerin doğuracağı tüm enerji maliyetlerinden de tasarruf edilmiş olunacaktır.

Ayrıca bulut bilişim sayesinde kurumlar BT işlemlerinin işletimi, bakımı ve onarımı için ekstra personel, bakım ve işletim maliyetlerinden de kurtulmuş olmaktadır. Böylece kurumların bu maliyetlerden yapacağı yüksek tasarrufla gerekli diğer donanımsal veya yazılımsal ihtiyaçlarını giderebilmektedir.

Bulut bilişim maliyetle ilgili sunduğu önemli özelliklerden biri de ödeme imkânlarında kullanılan kullandıkça öde mantalitesidir. Böylece kurum ve kuruluşlar ihtiyacı olmayan veya tüketmediği kaynaklar için ekstradan harcama yapmak zorunda kalmadan tasarruf etmiş olmaktadır.

Maliyetle ilgili son olarak işletmelerin kendi BT altyapılarını kurmak bunların bakımını ve her türlü ihtiyacını tedarik etmek önemli bir zaman kaybına yol açmaktadır. Bulut bilişim işletmelerin bu tür ihtiyaçlarını fazla finans gücü ayırmadan sağlayabilmektedir. Böylece işletmeler yaptığı yatırımların hızlıca piyasaya sunulması sağlanmakta ve önemli bir sermaye yatırımına ihtiyaç ortadan kalkmaktadır.

- Erişilebilirlik[52-53]:

Günümüzde teknolojinin çok hızlı derecede ilerlemesi yeni cihazların ortaya çıkmasını sağlamıştır ve bu cihazların da internet erişimi olması ve her yerde kullanılabilmesi artık bulut bilişim altyapısı kullanan kurum ve işletmeler için verilerin her yerden ve her an erişilmesi ihtiyacını doğurmuştur. Bulut bilişim sayesinde bulut tüketicileri verilerini geniş bant erişimi olan her yerden depolama, erişim ve güncelleme gibi tüm işlemleri kolaylıkla yapabilmektedir.

Ayrıca bulut bilişim, tüketicilerin elinde var olan ve internet bağlantısı yapabildikleri çoğu cihazdan da bu işlemleri yapabilme yeteneğini sağlamaktadır.

- Yönetim ve Raporlama[54]:

İşletmeler için uygulamaların izlenmesi, yönetimi ve raporlanması normal şartlarda karmaşık bir durumdur ve bazen bununla başa çıkılması gerçekten zor olabilmektedir. Fakat bulut bilişim ile birlikte bu işlemler bulut sağlayıcı tarafında yapılabildiği ve sağlayıcının raporlama ve analiz etmek için sunduğu arayüzler sayesinde

karmaşıklığını yitirmektedir. Bunun yanı sıra doğru şekilde raporlanan verilerle işletmelerin ihtiyaç duyduğu tüm bilişim kaynakları belirlenip ihtiyaca göre arttırılıp azaltılabilir ve maliyetten tasarruf edilebilir. İşin yönetme kısmı ise analizlerin doğru ve karmaşık olmamasından dolayı daha kolay bir hal almaktadır.

- Yedekleme, Onarım ve Depolama[50,53]:

Bulut bilişim verilerin yedeklenmesi ve kurtarılması işlemlerini de tedarik etmektedir. Çünkü bunlar artık fiziksel bir cihazda değil bulutta bulunmaktadır ve daha güvenli bir seçenek olarak öne çıkmaktadır. Birçok bulut sağlayıcısı, güvenilir ve esnek yedekleme kurtarma çözümleri sağlamaktadır.

Bazı durumlarda, bulutun kendisi de yalnızca yerel bilgisayarda bulunan veriler için bir yedekleme havuzu olarak kullanılır. Bunun yanı sıra altyapıdaki yedekli çalışan sistemlerin sayesinde oluşabilecek tüm veri kaybı sorunları da en aza indirilmektedir.

- Bakım[29,55]:

Geleneksek BT yapılarında bulunan her bilgisayar ve sunucu için ayrı bakım yapılmaktadır ve bu sistemin daha çok maliyetli çalışmasına, güncelleme sıkıntılarına ve zaman kaybına yol açmaktadır. Fakat bulut bilişimle beraber tedarik edilen her donanım çalışır durumdayken bulut sağlayıcı tarafından güncellemeleri ve bakımı yapılarak yukarıda belirtilen maliyet ve zaman sorunları giderilmiş olur. Ayrıca bu bakım işlemlerinin periyodik bir zaman aralıklarında yapılması sistemin sürekli olarak çalışmasını da sağlayarak hizmet kesintisi olmasını engellemektedir. Kısacası tüm oluşabilecek riskler en aza indirgenmiş olmaktadır.

- Performans[56-57]:

Bulut bilişimin sağladığı en önemli artılardan biri de hizmetteki performans veya hizmet kalitesidir. Bulut sağlayıcıları tüketiciler için gerekli olan en güncel sistem, ağ ve donanımları sağlamakla kalmaz bunun yanında bunlarla ilgili her türlü bakım, onarım ve yönetim için çalıştırdıkları uzmanlar ile yüksek dereceli performans sağlarlar. Ayrıca bulut servis sağlayıcıları yedekleme, güvenlik ve sürdürülebilir bir hizmet sağlayarak verilerin olağanüstü durumlarda kaybolmasına, herhangi bir zafiyetten ötürü çalınmasına ve hizmette oluşabilecek her türlü kesintiyi de engellemiş olmaktadır.

- Ölçeklenebilirlik[58-59]:

Bulut tüketicileri ihtiyaçları ve istekleri doğrultusunda bazı donanımları veya servisleri az veya daha fazla kullanmaktadırlar. Bulut bilişim sayesinde tüketiciler ihtiyaçlarına göre ayarlama yaparak ölçeklenebilirlik sağlanabilmektedirler. Bu sağlanan hizmet sürekli ve aktiftir. Böylece tüketicinin kullanımına göre bir hesaplama yapılarak maliyetlerin de azaltılmış olması sağlanmaktadır. Bulut tüketicileri kullandıkları kaynakların artması durumunda otomatik olarak kaynaklar genişletilerek oluşabilecek kaynak kısıtlaması sıkıntıları da giderilmiş olmaktadır. Bu yöntem, yalnızca yoğun dönemlerde kullanılan ve genellikle bir miktar kapasiteyi koruyan yerel sistemlere bir alternatif sağlar.

- Esneklik[60]:

Bulut bilişimin en önemli avantajlarında biri de sunduğu esnek yapısıdır. Bu yapıyla birlikte servis sağlayıcıları servis tüketicileri için donanımdan bağımsız kaynaklara erişilmesine, her yerden ve her zaman kaynaklara erişilmesine, tüm yazılım ve donanım güncellemelerinin kolaylıkla kesinti olamadan yapılmasına, sunduğu ölçeklenebilir yapıyla ihtiyaca göre kaynakların arttırılıp azaltılmasına, yedekli yapılarla veri kaybının engellenmesine kadar birçok hizmeti sağlamaktadır.

- Süreklilik[29]:

Bulut bilişimle birlikte doğal afet veya olağanüstü durumlarda yapılan yedekleme sistemleri sayesinde herhangi bir veri kaybına yol açılmasının önüne geçilerek kaynaklara kesintisiz olarak erişilmesi sağlanmaktadır. Ayrıca servis sağlayıcılarla yapılan SLA'larla birlikte işletmeler aldığı hizmetlerin kesintisiz olarak çalışacaklarına dair anlaşma imzalamış olmaktadır. Böylece oluşabilecek kesinti sorunları en aza indirgenmiş olmaktadır.

- Çevre Dostu[57]:

Servis sağlayıcının sunduğu altyapı ve platformlar ile birlikte ekstra altyapı harcamaları yapılması engellenir. Ayrıca kullanılan altyapı şirketler tarafından ortak kullanıldığı için geleneksel BT altyapılarına göre daha fazla elektrik tasarrufuna ve daha düşük karbon salınımına yol açar. Bunun yanı sıra bulut bilişimde yer alan veri

merkezlerinin elektrik kullanımının artmasıyla birlikte elektrik harcamalarının da yüksek oranlar da azalacağı öngörülmektedir. Böylece bulut bilişimle birlikte çevre dostu sistemler inşa edilebilir duruma gelmektedir.

- Bağımsızlık:

Bulut bilişimde bulut tüketicilerinin kaynaklara erişmesi için herhangi bir cihaz bağımlılığı bulunmamaktadır. İnternet erişimi olan tüm cihazlardan kaynaklara erişim sağlanabilmektedir.

2.8 Bulut Bilişimin Dezavantajları

Her teknoloji beraberinde birçok avantajla geldiği gibi kendisinde dezavantajları, riskleri ve endişeleri beraberinde getirmektedir. Bulut bilişimin de üzerinde önemle durulup düşünülmesi gereken birçok dezavantajları bulunmaktadır. Bunları aşağıdaki gibi sıralayabiliriz.

- Hizmet sağlayıcıya bağımlılık:

Bulut bilişimin önemli dezavantajlarından biri hizmet sağlayıcıya olan bağımlılıktır. İşletmelerin kendi BT altyapısını kurmadığı için bulut bilişim hizmetleri almasıyla bu hizmetlerin veren üçüncü tarafa bağımlılık oluşmaktadır. Bu bağımlılık dolayısıyla hizmet sağlayıcının sunduğu altyapıdaki herhangi bir zayıflık beraberinde saldırıları ve tehditleri de beraberinde getirmektedir.

Bunun yanı sıra bulut tüketicisinin hizmet sağlayıcıda yapacağı herhangi bir değişiklik de beraberinde birçok zorluğu getirmektedir. Bu zorluklardan bazıları altyapıdaki sunucu, ağ vb. herhangi bir donanım değişikliğinden dolayı oluşacak donanım maliyetleri ve bu donanımların test edilmesindeki oluşacak personel maliyetidir.

Bu yüzden hizmet alınacak bulut sağlayıcıya karar verirken güvenlik, gizlilik, mahremiyet, süreklilik, hizmet sağlayıcının sektördeki tecrübe ve konumu gibi önemli faktörler göz önünde bulundurulmalıdır.

- Bant Genişliği:

Günümüzde ortaya çıkan birçok cihazın internet erişiminin olmasıyla beraber, kişiler ve kurumlar da yüksek bant genişliği ihtiyacı doğurmaktadır. Bulut bilişim hizmetlerinin

de kesintisiz ve hızlı bir şekilde gerçekleşmesinin ana faktörü bant genişliğidir. İnternet ağında oluşabilecek kopmalar veya sorunlar hizmetlere erişimde yaşanılacak birçok sıkıntıyı beraberinde getirmektedir.

Bulut bilişim hizmetlerinin etkili bir şekilde kullanılması için tedarik edilecek yüksek bant genişliği işletmelere ekstra maliyet getirmektedir. Ayrıca bant internet bağlantısındaki yükleme hızlarının da yüksek olması gerekmektedir. Yedekleme ve depolama için yükleme hızları bulut hizmetinin kalitesi için önemli bir etkendir.

- Sabit İnternet Gereksinimi:

Bulut bilişim getirdiği diğer dezavantaj da hizmetin kesinlikle internet bağımlılığı bulunmasıdır. Bu yüzden tüketicinin sahip olduğu internet ağındaki herhangi bir kopma verilere erişimi engellemektedir. Böylelikle bulut üzerinde çalışmak da internet bağlantısı sağlanana kadar mümkün olmayacaktır.

- Kontrol:

Hizmet sağlayıcı bulut altyapısının sahibi olduğundan dolayı bulutun yönetimi ve izlenmesi gibi durumları kendileri gerçekleştirmektedir. Bu yüzden bulut bilişim hizmetlerinin bazılarında kontrol bazen tamamen sağlayıcıya ait olabilmekte bazen de bulut tüketicilerinin kısmi bir kontrol hakkına sahip olduğu durumlar oluşmaktadır. Bu kontrollerin tüketicilerin elinde olmaması beraberinde verilerin güvenliğinde bazı endişeleri beraberinde getirmektedir. Bu endişeleri en aza indirgemek adına risk değerlendirmesi yapılarak bulut hizmetleri ve sağlayıcı ile ilgili karar alınmalıdır.

- Verilerin konumu:

Verilerin kontrolünde bulunan endişeleri verilerin nerede olduğu konusunda da tekrarlamak mümkündür. Bulut bilişimde verilerin nerde ve nasıl depolandığı, verilerin yönetimindeki kullanılan yönetim, erişimin kimler tarafından yapıldığı, verilerin depolanan yerde ne gibi tedbirlerle korunduğu, olası felaket senaryolarında bulut sağlayıcıların yedekleme gibi tedbirler alıp almadığı önemli endişeler arasında sayılmaktadır[51].

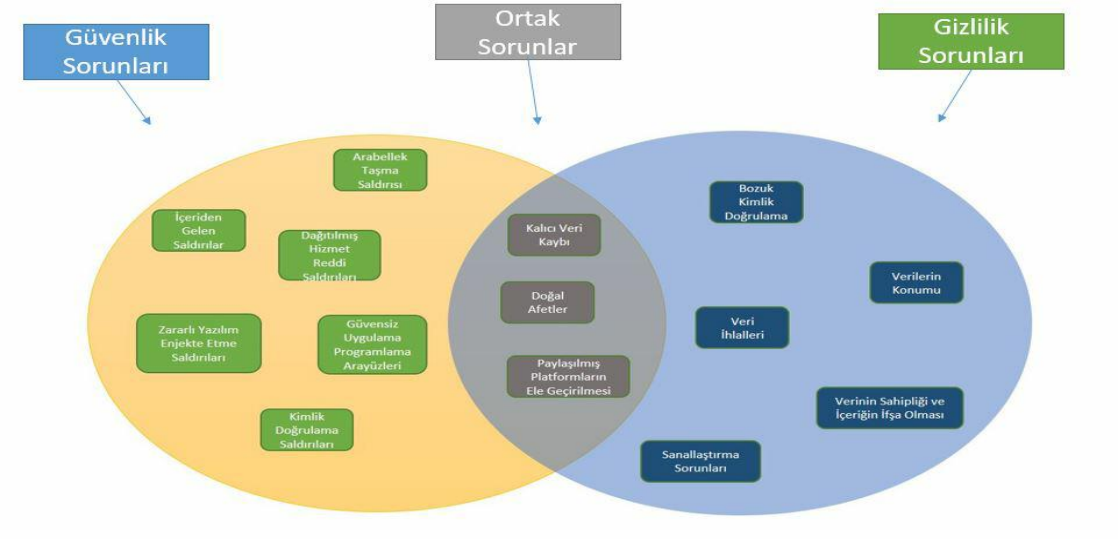
- Güvenlik ve Gizlilik

Bulut hizmeti sağlayıcıları en iyi güvenlik standartlarını ve endüstri sertifikalarını barındırmasına ve bunları uygulamasına rağmen, verileri ve önemli dosyaları üçüncü taraf hizmet sağlayıcılarda depolamak her zaman riskleri meydana getirmektedir.

Yukarıda bahsedilen çoğu dezavantajın asıl konusu güvenlik ve gizlilik hakkındaki endişelerdir. Verilerin depolanması, bu verilerin konumu, kontrolü elinde bulunduran bulut sağlayıcının ne kadar güvenilir olduğu, verilerin depolanması, yönetilmesi ve sağlayıcı tarafından erişimi sırasında alınacak tedbirlerin var olup olmaması veya zayıf tedbirler alınması gibi birçok güvenlik endişeleri bulunmaktadır. Bu yüzden bulut sağlayıcılarının veri depolama ve korumada ne gibi tedbirler aldığı, uçtan uca şifreleme gibi bazı özelliklerin var olup olmaması, ne gibi yedekleme mekanizmalarının kullanıldığı gibi belli başlı güvenlik tedbirlerinin araştırılması gerekmektedir

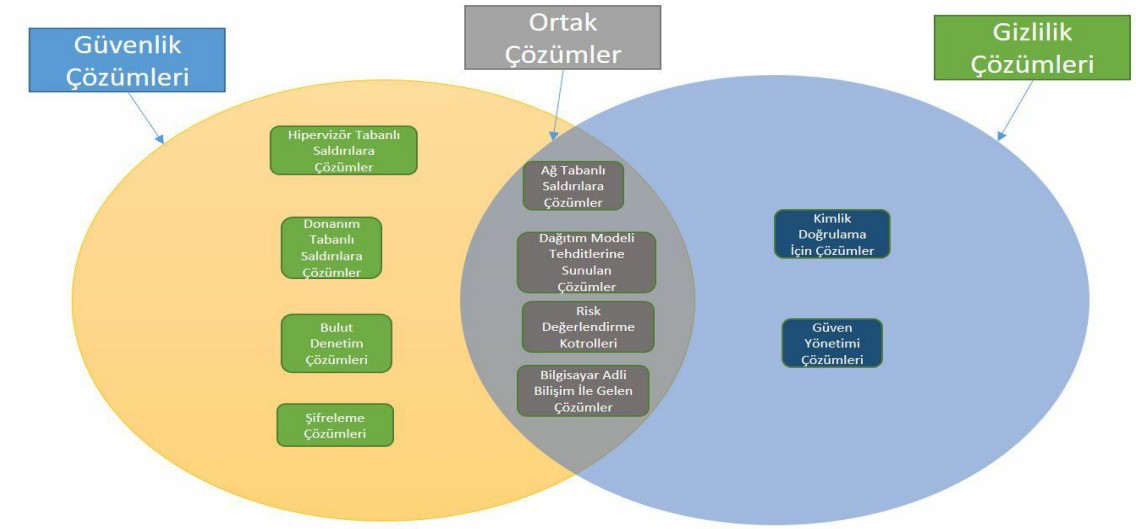
3 BULUT BİLİŞİMDE GÜVENLİK VE GİZLİLİK

Bulut bilişimde güvenlik ve gizlilik konularıyla alakalı birçok tehdit, saldırı ve zafiyet bulunmaktadır.



Şekil 3.1. Bulut bilişimde yer alan sorunlar[37].

Bu saldırılara karşı birçok çözüm bulunmaktadır.



Şekil 3.2. Bulut bilişimde yer alan sorunlara karşı çözümler[37].

3.1 Güvenlik Konuları

Bulut bilişim sistemleri genel itibariyle esnek, uygun maliyetli, her yerden erişime olanak veren, yönetim, raporlama, bakım ve onarım işlerini kolaylaştıran, verilerin olağanüstü durumlarda kaybolmasını engellemek adına yüksek güvenlikli olarak birkaç farklı yerde depolanan ve yedekleme mekanizmasına sahip ve ölçeklenebilirlik özellikleriyle kişi ve kurumların son zamanlarda sıkça kullandığı ve sistemlerini bu altyapıya geçirmeye başladığı önemli bir teknolojidir.

Bulut bilişim getirdiği bunun gibi birçok avantajın yanında dezavantajları da bulundurmaktadır. Bu dezavantajlar bulut kullanıcıların asıl endişesi olan güvenlik sorunlarıdır. Bulut altyapısını kullanan bir kurumun en çok düşündüğü şeylerden biri şüphesiz verilerinin saklanma biçimi ve bu konuda bulut sağlayıcısının aldığı tedbirlerdir. Çünkü bulut bilişimde kontrol tamamen bulut kullanıcısında olmadığından verilerin nerelerde ve nasıl saklandığı önemli bir soru işareti haline gelmektedir.

Bulut bilişim sistemlerinde verilerin yedekleme işlemi kuruma yakın coğrafik yerlerde depolanmak yerine bulut üzerinde yapılmaktadır. Bazı işletmeler hala kendi sahibi olduğu disklere yedekleme yapmakta veya veri yedeklerini yakındaki bir tesis dışı konumda depolamaya çalışmaktadır. Yangın, deprem gibi olağanüstü felaketler olduğunda bu yöntem yedeklenen verilerin de kaybolmasına neden olabilir. Bulut sistemlerinde ise veriler uzak konumlardaki yerlerde depolanmaktadır. Bu sayede verilerin kaybolması sorunu önlenmiş ve olası veri kaybı tehlikesi bertaraf edilmiş olur. Fakat bu yöntemdeki asıl sıkıntıda verilerin nasıl saklandığı ve verilerin kimler tarafından erişildiğinin tam olarak bilinmemesidir.

3.1.1 Bulut Bilişim Güvenlik Sınıfları

Bulut bilişimde güvenlik kimlik ve erişim yönetimi, altyapı güvenliği, yazılım güvenliği, ağ güvenliği, bilgi güvenliği altında kategorilere ayrılmaktadır.

3.1.1.1 Ağ Güvenliği

Kuruluşlar ağlarını şirket içerisinden bulut üzerine taşımaktadır. Bu da verilerin artık kurum içinde değil üçüncü taraf bir bulut sağlayıcı tarafından sağlanan bulut ortamında depolanacağı anlamına gelmektedir ve bu verilerin korunması, güvenliğinin her noktada sağlanması gerekmektedir. Ancak bulut bilişim, güvenliği zorlaştırabilecek yeni zorlukları da beraberinde getirmektedir. En önemli zorluklardan biriside bulut ortamında sağlanması gereken ağ güvenliğidir.

Ağ Güvenliği, bulut bilişim için temel gereksinimler arasında yer almaktadır. Ağ güvenliği, temel ağ altyapısını yetkisiz erişimden, yanlış kullanımdan, arızadan, değişiklikten, imhadan veya uygunsuz ifşadan korumak için fiziksel ve yazılımsal önlemler almayı bunun sayesinde de bilgisayar, kullanıcı ve programların izin verilen kritik operasyonları belirli bir sistem içinde yerine getirmeleri için güvenli bir platform oluşturmayı sağlayan bir bileşen olarak tanımlanmaktadır[61].

Bulut ortamlarındaki değişim hızı bulutta yer alan ağların güvence altına almanın önemli zorluklarındandır. Otomatik ölçeklendirme ve sunucusuz bilgi işlem gibi teknolojiler, bir bulut ağındaki varlıkların sürekli olarak görünüp kaybolduğu anlamına gelmektedir. Yapılan güvenlik açığı taramaları gibi geleneksel önlemleri yeterli bulunmamaktadır. Bunun nedeni de güvenlik açığı bulunan bir varlık kötü niyetli bir aktörün onu bulup kullanması için fazlasıyla yeterli bir zaman olan birkaç dakikalığına var olmaktadır[62].

Bulut bilişim sistemlerindeki dağıtımın kolay olması ve değişimin çok hızlı olması, kurumlardaki güvenlik ekiplerinin bulut ortamlarının eksiksiz bir şekilde korumasını çok zorlaştırmaktadır. Bu, hassas bilgilerin farklı sistemlerde depolandığı ve farklı güvenlik araçlarıyla korunduğu hibrit ortamlarda yani hem şirket içi hem de bulut ağlarını içeren BT ortamlarında daha da zor bir durum halini almaktadır. Bu ortamlarda, güvenlik ekibinin güvenlik işlevlerini yönetmek için çeşitli sistemler arasında gidip gelmesi gerekir. Birleşik verinin yetersiz kalmasıyla, kuruluşun genel güvenlik durumu hakkında tutarlı bilgi edinmek ya da bulut ve şirket içi ağlar arasında var olabilecek kötü niyetli bileşenleri takip etmek epey zorlaşır[62].

En son olarak bulut sistemlerinde ağ güvenliği ile ilgili en önemli saldırılar da hizmet reddi, ortadaki adam saldırısı, ağ dinleme, bağlantı noktası tarama, SQL enjeksiyon ve siteler arası komut dosyası oluşturma saldırılarıdır[63].

Bu tip saldırıların önüne geçmek için bazı tedbirler alınması gerekmektedir. Hizmet olarak altyapı için ağ segmentasyonu yapılandırılmalı ve ağın izlenmesi, İzinsiz Giriş Tespit Sistemlerini (IDS) ve İzinsiz Giriş Önleme Sistemlerini (IPS) içeren bir yapıya geçilmelidir. Ayrıca web sitesinin önüne sanal web uygulama güvenlik duvarı yerleştirilerek kötü amaçlı yazılımın tespiti ve koruması sağlanır.

İkinci olarak platform olarak yazılımda hizmet sağlayıcı, istemciye uygulamalar oluşturmalarına olanak tanıyan platformu sağlarken, bulut sağlayıcısı, altyapıyı oluşturur ve hizmet verir. Burada ise, IP kısıtlamaları ve günlük kaydı arayıcılığıyla güvenlik sağlanabilir. Ayrıca, dağıtılmış API Ağ Geçitleri ve ilkeleri denetleyen bir Bulut Erişimi Güvenlik Aracısı (CASB) sistemin içinde olması gereken diğer unsurulardır.

Son olarak hizmet olarak yazılım için de hizmet olarak platform ve altyapıda bulunan tedbirler alınmalıdır ve ayrıca yapılabilecek tedbir bulunmamaktadır. Çünkü hizmet olarak yazılım sistemlerinde kontrol sağlayıcıdadır ve güvenlik mekanizmaları sağlayıcı tarafından sağlanmaktadır [64].

3.1.1.2 Altyapı Güvenliği

Yeni ve güncel teknolojileri benimsemek ve bunlara geçiş yapmak kurumların büyümesini sağlamaktadır. Ancak aynı zamanda beraberinde güvenlik sorunları ve veri ihlalleri gibi sıkıntıları da getirir. Bulut teknolojisini benimserken, bulut altyapısının güvenliğini en önemli sorumluluklardan biri olarak karşımıza çıkmaktadır. Bu sorunların hala devam ettiği ve bu sistemlere geçişte kararsızlık içinde olan birçok işletme bulunmaktadır. Örneğin bir çevrimiçi kumarhane grubu tarafından 108 milyondan fazla bahis kaydının bilgileri sızdırıldı. Sızan veriler, müşterilerin kişisel bilgilerinin yanı sıra para yatırma ve çekme işlemlerinin ayrıntılarını içermekteydi. Ayrıca 770 milyondan fazla benzersiz e-posta adresi ve 21 milyon benzersiz paroladan oluşan veri kümesinden oluşan büyük bir veri ihlali meydana geldi ve tüm bu veriler bir bulut depolama hizmetinde olan MEGA'da depolandı. Ünlü bir yemek dağıtım hizmeti sağlayıcısı, tüketicilerin yanı sıra teslimat çalışanlarını da içeren 4,9 milyon kullanıcının verilerini güvenlik açığı oluşturarak veri sızması ve ihlallerine neden oldu. Bu verilen örnekler

bulut bilişim altyapısının güvenliğinin ne kadar önemli olduğunu ortaya koymaktadır[70].

Bulut bilişimde altyapı güvenliği birkaç bölüm halinde ele alınabilir. Bunlardan biri olan altyapıdaki ağ güvenliğidir. Bu kısımda özel bulut kullanıcıları için bir risk bulunmamaktadır. Çünkü veriler zaten kurum içinde depolandığı için dışarı ağa kapalı ve gerekli önlemler alınması bu iyi sonucu doğurmaktadır. Fakat genel bulut kullanıcıları için bazı riskler barındırmaktadır ve bazı yerlerde değişime gidilmesi gerekmektedir. Mevcut ağ topolojisinin bulut sağlayıcının ağ topolojisi ile etkileşim kurma şekli dikkate alınması gerekmektedir. Ayrıca genel bulut kullanımında altyapı güvenliği için kullanılan kaynaklara uygun erişim kontrolünün (kimlik doğrulama, yetkilendirme ve denetim) sağlanması, genel bulut sağlayıcıları tarafından bir kuruluşa atanan internete yönelik kaynakların kullanılabilirliğinin sağlanması, yerleşik ağ bölgeleri ve katmanları modelini etki alanlarıyla değiştirilmesi ve verilerin gizliliği ve bütünlüğünün sağlanması gerekmektedir. Diğer bölüm olan host güvenliğinde ise riskler değerlendirildiğinde tüm bulut tipleri ve dağıtım modelleri ayrı ayrı dikkate alınmalıdır. Hizmet olarak yazılım ve platformda host güvenliği sorumluluğu bulut sağlayıcısında iken, hizmet olarak altyapıda sorumluluk bulut tüketicisi sorumlu olmaktadır[71].

Altyapı güvenliğindeki diğer ana sorunlardan biri de sanal makine güvenliğidir. Sanal makine güvenliğinin görevi, işletim sistemlerini ve iş yüklerini geleneksel fiziksel sunucuları etkileyen yaygın güvenlik tehditlerinden (kötü amaçlı yazılımlar ve virüsler gibi) korumak için bulut merkezli güvenlik çözümlerini kullanmaktır ve bu, bulut tüketicilerinin sorumluluğundadır. Diğer sorunlardan birisi ise sanal makine görüntüleri deposunun güvenliğini sağlamaktır. Fiziksel sunucuların aksine sanal makineler çevrimdışı olduğu durumlarda bile risk altında bulunmaktadırlar. Sanal makine dosyalarına kötü amaçlı kodlar sokularak veya sanal makine dosyalarının kendisi çalınarak sanal makine görüntülerinin güvenliği ihlal edilme tehlikesiyle karşı karşıyadır. Güvenli sanal makine görüntüleri deposu, bulut sağlayıcılarının sorumluluğundadır. Diğer ana sorun SM sınırlarının güvenliğini sağlamaktır. Fiziksel sunucu sınırları ile karşılaştırıldığında, VM'lerin sanal sınırları bulunmaktadır. Aynı fiziksel sunucudaki SM'ler aynı işlemciyi, belleği ve diğer olası tüm kaynakları paylaşır. Böylece SM kaynakları arasında fiziksel bir izolasyon olmadığı anlaşılmaktadır. SM sınırlarının güvenliğini sağlamak, yine bulut sağlayıcısının sorumluluğu altında bulunmaktadır. Bulut bilişimin altyapı güvenliği için son sorun ise Hiper yönetici güvenliğidir. Hiper yönetici

aslında fiziksel kaynaklardan sanallaştırılmış kaynaklara ve sanallaştırılmış kaynaklardan fiziksel kaynaklara eşleyen sanallaştırıcı olarak tanımlanmaktadır. Fiziksel sunucu kaynaklarına SM'ler tarafından yapılacak her türlü erişimde ana denetleyici rolü hiper yöneticiye aittir. Hiper yöneticinin herhangi bir şekilde kötü amaçlı kişiler tarafından ele geçirilmesi, sanal makinelerin güvenliğini ihlal etmektedir. Çünkü tüm sanal makinelerin işlemleri şifreleme mekanizması olmadan izlenmektedir[72].

3.1.1.3 Yazılım Güvenliği

Yazılım güvenliği, bulut bilişimde yer alan en endişe verici güvenlik endişelerinin başında gelmektedir. Günümüzde geliştiriciler her bir yazılım programını kendi takımları arasında ürettiği fikirlerle yazmakta ve farklı programlama dilleri, programlama çerçeveleri (framework) ve kütüphanelerini kullanmaktadır. Bu yazılım uygulamalarını milyonlarca satır koddan oluşabilmektedir. Bu da güvenlik ekiplerinin yazılımdaki güvenliği ölçmesi işini zorlaştırmaktadır. Geliştirici, belirledikleri güvenlik kurallarına göre yazılımı geliştirse de tek bir hata veya açık veri ihlali gibi önemli bir sorun ortaya çıkarabilmektedir.

Bir bulut tüketicisi, hizmet olarak altyapı ve yazılım hizmetlerine internet üzerinden erişmektedir. Kullanıcı ön yüzü, kullanılacak hizmetlerin yönetimi ve izlenmesi gibi özellikleri beraberinde bulundurmaktadır. Kullanıcın sistemdeki yetkilerine göre önyüzde farklı arayüzler görmektedir. Mesela sistemde “admin” olarak kayıtlı olan kişinin arayüz içindeki tüm sayfalara ve özellikle yönetim arayüzüne erişim hakkı olmasına rağmen, sadece kullanıcı yetkisi bulunan kişinin belirlenen yetki mekanizmalarına göre göreceği sayfalar bellidir ve yönetimsel arayüzlere erişimi kısıtlanmıştır. Arayüz bir bulut ortamında varsayılan olarak internet üzerinden erişilen bir ağ geçidi olarak değerlendirilmektedir. Saldırganın saldırılarını gerçekleştirmek için kullandığı bu arayüz buluta girmek isteyen kötü amaçlı kullanıcılar için isteklerini gerçekleştirebilecekleri önemli bir yerdir. Bu arayüzlerin yazılımda yapılan kusurlu konfigürasyonlar, eksik yazılımlar, yetkisiz erişim ve maskelenmiş kodları sistem içine enjekte etmek, sistem güvenlik duvarlarını yıkan önemli sorunlardandır.

Hizmet olarak platform bulut uygulamasının dağıtımı için paylaşım tabanlı platform sağlamakta ve uygulamaların geliştirilmesinde kullanılacak birçok yazılım dilini de desteklemektedir. Fakat sunulan bu platformlar kaynak ölçümü, platform izolasyon

sorunu ve güvenli iş parçacığı sonlandırması gibi bazı güvenlik sorunlarına sahip olmaktadır[73].

Bulut bilişim uygulamalarında yer alabilecek güvenlik tehditleri uygulama kurulumunun yanlış yapılandırılması, yetkisiz erişimi güvenli olmayan API'ler ve hesapların ele geçirilmesidir.

Uygulama kurulumunda yapılacak her türlü yanlış yapılandırma, bulut güvenliğine yönelik en büyük tehdit olmaktadır. Çünkü veri ihlalleri, hizmetlerin genel internete maruz kaldığında meydana gelen olaylardır. Bir web sitesine, sunucuya, hizmete veya başka bir sisteme yetkisiz erişim de üstünde önemle durulması gereken bir başka sorundur. Sistem içinde yetkisi olmadığı yere bir kez yetkisiz kullanıcıların ne yapacaklarını kestirmek mümkün değildir. Güvenli olmayan API'ler ve arayüzler, genel bir IP adresine sahip kurumsal sınırların dışındaki tek varlıklar olduklarından, saldırganların sistemleri ihlal etmeleri için kolay fırsatlar sunmaktadır. Son olarak hesapların ele geçirilmesi çok fazla hassas veri ve kaynak, birçok farklı kullanıcı tarafından paylaşılan cihazlarda saklandığı için ve bu verilerin hesapların ele geçirilmesiyle çok kötü bir biçimde kullanılması olağandır[74].

3.1.1.4 Bilgi Güvenliği

Bulut bilişimde bilgi güvenliği terimi, her alanda olduğu gibi gizlilik, bütünlük ve kullanılabilirliği sağlamak için bilgileri ve bilgi sistemlerini yetkisiz erişimlerden, yetkisiz kullanımlardan, bilginin ifşa olmasından, bilgide herhangi bir kesinti olmasından, değişiklik veya imhadan korumak anlamına gelmektedir[65].

Bilgi güvenliğinde bütünlük, bilgilerin uygunsuz şekilde değiştirilmesine, ekleme ya da çıkarma yapılmamasına veya yok edilmesine karşı koruma anlamına gelmektedir ve bilgilerin reddedilmemesini ve orijinalliğini kaybolmamasını sağlamayı konu edinmektedir. Öte yandan gizlilik, özel ve özel bilgileri korumaya yönelik araçlar da dahil olmak üzere, ifşa ve erişim üzerinde yetkili kısıtlamaların sürdürülmesi anlamına gelir. Örneğin, bulut ortamında saklanan veriye ulaşabilecek kişi veya kurumların belirli olması ve hepsine ayrı ayrı erişim hakkı tanınmalıdır. Kullanılabilirlik veya erişilebilirlik, bilgiye zamanında ve güvenilir bir şekilde erişilmesinin ve kullanılmasının sağlanması anlamına gelir. [65].

Bulut bilişim, maliyet tasarrufu, süreklilik gibi sağladığı avantajlarla dahili altyapıya ihtiyaç duymadan talep üzerine bilgi işlem ve depolama kaynakları sağlamaktadır. Teknolojik gelişmeler hızlandıkça ve bulut bilişim daha popüler hale geldikçe, kurumsal veya kişisel olan hassas verilerin gizliliğini, kullanılabilirliğini ve bütünlüğünü sürekli korumak ve sağlamak için ek bulut bilişim güvenlik önlemleri gerekmektedir[65].

Bunlar için alınacak bazı tedbirlerden ve bilgi gizliliği ve bütünlüğü sorununa uygun bir çözüm olarak bulut sağlayıcısı ve bulut tüketicisi arasında karşılıklı güven sağlamak söylenebilmektedir. Diğer bir çözüm uygun kimlik doğrulama, yetkilendirme sağlayarak bilgiye erişim süreci, kaynakların yetkili kullanımını sağlamak için çeşitli çok düzeyli kontrollerden geçirmek olacaktır. Ayrıca bilgiye erişimde RSA sertifikaları ve SSH tabanlı tünel mekanizmaları gibi güvenli erişim mekanizmaları sağlanmalıdır. Bulutta var olan kaynakların kullanılabilirliğini sağlamak için ise yerel kaynaklar ve yedekleme planları ve farklı bölgelerde yedekleme mekanizmaları kullanılması gerekmektedir. Böylece bir yerde bulunan tüm kaynaklar yok olsa da yedeklemeler sayesinde veriye yine de ulaşılıp kullanılabilirlik sağlanmış olmaktadır[66].

Ayrıca bilgi güvenliğinin bu üç ana unsurunu sağlamak için güçlü şifreleme yöntemleri kullanarak verileri saklamak, depolamak ve sadece kullanıcıya özgü anahtarlarla veriye ulaşılmasını sağlamak diğer önemli çözüm olarak karşımıza çıkmaktadır.

3.1.1.5 Yasal Uyumluluk ve Standartlar

Bulut uyumluluğu, bulutu kullanmak için geçerli olan yasalara ve düzenlemelere uymakla sağlanmaktadır. Kurumlar bazı kanun maddelerinden dolayı buluta geçmekte tereddüt etmektedirler fakat yasa ve kanunlar bulutun kurumlar tarafından benimsenmesini engelleyecek bir unsur değildir. Bulut tüketicilerinin bulut sistemlerine transfer olurken verilerin nerelerde işleneceği, hangi yasaların uygulanacağı, ne gibi etkileri olacağı gibi konular hakkında bilgi sahibi olması ve bunun ardından bunlara uyum sağlamak için risk tabanlı bir yöntem izlemek zorundadır. Veri koruma yasaları, veri yerelleştirme yasaları ve veri egemenliği yasaları gibi birçok farklı türde yasa olduğu için bu tip bilgileri elde etmek karmaşık ve zor bir hal alabilmektedir. Ayrıca, hükümetlerin veya başkalarının buluttaki verilere erişmesini sağlayabilecek müdahale yasalarını veya bilgiye erişim yasalarını da bulut tüketicilerinin dikkate alması gerekmektedir. Bunların

yanı sıra, önemli noktalardan biri de yasanın hangi güvenlik önlemlerini ele almanın gerekliliğini bilmektir[67].

Bulut bilişim kullanılması adına kurum ve kuruluşların birçok küresel düzenlemeye uyumlu olması gerekmektedir. Yasal uyumluluk ve düzenlemelerin başında HIPAA, PCI DSS, GDPR, ISO/IEC 27001, NIST, NERC, Sarbanes-Oxley (SOX) gibi düzenlemeler gelmektedir. Bu konuya genel bulutlar kapsamından bakarsak, en iyi bulut sağlayıcıları, ISO 27001, PCI DSS, HIPAA, FedRAMP gibi birçok uluslararası uyumluluk şartlarını karşıladıklarına dair birçok sertifikaya sahiptir. Ancak bulut uyumluluğu, yalnızca bulut sağlayıcılarına ait bir görev değildir. Amazon Web Services (AWS) ve Azure gibi sektör lideri bulut sağlayıcıları, kurumlara ve kuruluşlara güvenlik kontrolleri üzerinde kontrol sağlar. Kuruluşların, tüm hibrit ve çoklu bulut ağlarının uyumluluğunu sağlamak için ortak bir sorumluluğu vardır[68].

Bulut güvenliğinde önemli başlıklardan biri olan yasal uyumluluk ve düzenlemeler, hem bulut sağlayıcıları hem de bulut tüketicileri için önemli konu olmaktadır ve olmaya devam edecektir. Yukarıda verilen düzenlemelerden örneğin, sağlık sektörü için çıkarılmış olan HIPAA adı verilen bir dizi yasa, belirli hasta sağlığı verileri için katı yönergeleri ve güvenlik protokollerini zorunlu kılmaktadır.

Diğer bir örnek PCI ise Kredi kartı veri güvenliği standardı olarak bilinmektedir. Bu standart American Express, Discover Financial Services, JCB International, MasterCard Worldwide ve Visa Inc. tarafından kurulan PCI Güvenlik Standartları Konseyi tarafından yönetimi sağlanmaktadır ve kredi kart sahiplerinin verilerinin gizliliği ile ilgili düzenlemelere sahiptir[69].

Bu ve buna benzer tüm uyumluluklar bulut tüketicilerinin güvenliğinin nerede korunduğu, kim tarafından erişildiği, korunurken alınan tedbirler gibi endişelerin bir nebze yok olmasını sağlamaktadır ve bulut güvenliğini sağlamaya yönelik önemli adımlardır. Bu yüzden bulut tüketicileri bulut sistemlerini kullanacakları vakit, bu yasal düzenlemeleri ve uyumlulukları dikkatlice inceleyerek bulut sağlayıcılarının hangilerine sahip olduğuna bakarak karar vermelidir ki kullandıkları bulut sistemlerinde verilerin güvenliğini arttırabilmiş olsunlar.

3.1.1.6 Kimlik ve Erişim Yönetimi

Kişisel ve gizli bilgiler içeren uygulamaları, hassas verileri ve dosyalarını giderek daha fazla bulut ortamında depolanması, sistem içinde veri ihlallerine ve veri kaybına yol açmaktadır. Bulut bilişimde kimlik ve erişim Yönetimi (IAM) kullanımıyla bu tip sorunları bertaraf etmek için bulut güvenliği sağlamanın en verimli yöntemlerinden biridir.

Kimlik doğrulama(authentication), yetki yönetimi(authorization) ve birleşik kimlik yönetimi(federated identity management) kullanılarak kimlik ve erişim yönetimini sağlanabilir. Bu güvenlik yollarını kullanarak bulut bilişim sistemlerinde yalnızca yetkili kullanıcıların verilen yetki dairesinde sistemde yer alması ve sistemi kullanması sağlanmaktadır.

Kimlik doğrulama, bir kullanıcının kimliğini doğrulamaya ve kanıtlamaya izin verdiği için bulut güvenliği için çok önemlidir. Günlük hayatta kullanılan kimlik kartı veya diğer kimlik olarak kullanılan belgelerin sanal ortamdaki sunuluş şekli olarak tanımlanmaktadır. Kimlik ve erişim yönetimi sistemleri, bir dizi güvenli kimlik doğrulama mekanizmasıyla ileri seviyede bulut güvenliği sağlar. Çok faktörlü kimlik doğrulama, üçüncü taraf kimlik doğrulama, basit metin şifreleri, 3D şifre nesneleri, grafik şifreler, biyometrik kimlik doğrulama ve dijital cihaz kimlik doğrulaması bu güvenli kimlik doğrulama mekanizmaları sistem üzerinde oturum açma kimlik bilgileri arasındadır. Hatta bu güvenlik kontrollerinin daha da geliştirilmesi adına bazı bulut sağlayıcıları kimlik doğrulama yoluyla yetkisiz erişimi reddeden erişim kartları veya biyometrikler gibi fiziksel güvenlik mekanizmalarını kullanarak bulut tüketicilerinde daha fazla güvenli bir ortam sunmaktadırlar.

Yetkilendirme, bulut bilişim sistemlerinde bir sisteme giriş yapan varlıkların, hangi işlemlere yetkisi olup olmadığın tanımlanması ve denetlenmesi sürecidir. Tanımlanan varlıkların yalnızca yetkisi bulunduğu görevleri yerine getirme yeteneğine sahip olmasını sağlar. Yetkilendirme, bir varlığın hangi erişime sahip olduğunun doğrulanmasına da izin vermektedir.

Veri güvenliğinden ödün vermemek adına bulut bilişim sistemlerinde farklı varlıklar için farklı yetki düzeyleri belirlenerek yetkisiz erişim önlenmektedir. Ayrıca başarılı kimlik doğrulama işleminden sonra yapılan yetkilendirme yönetimi sayesinde kimliği

doğrulanmış varlığın belirli bir uygulama içinde bir fonksiyonu kullanmasına izninin olup olmadığı kontrol altında tutulut[75].

Birleşik kimlik yönetimi, abonelerin gruptaki tüm işletmelerin ağlarına erişim elde etmek için kuruluşun kimlik sağlayıcısını kullanarak kimlik doğrulaması yapmaktır. Birleşik kimlik yönetimi, ortak anahtar altyapısı (PKI) ve sertifikalı ortak anahtarların değişimi yoluyla Web tabanlı uygulamalar ve kimlik sağlayıcılar arasında güven sağlar. Birleşik kimlik yönetimi, kullanıcıların kimliklerini birden çok güvenlik etki alanında birbirine bağlar ve her güvenlik etki alanı kendi kimlik yönetim sistemini destekler. İki etki alanı birleştirildiğinde, kullanıcılar bir etki alanında kimlik doğrulaması yapabilir ve ardından ayrı bir oturum açmaya gerek kalmadan diğer etki alanındaki kaynaklara erişebilir. Birleşik kimlik yönetimi, işletmelere ve ağ abonelerine ekonomik avantajların yanında bazı kolaylıkları da beraberinde getirmektedir. Örneğin, birden fazla işletme tek bir uygulamayı paylaşarak, maliyet tasarrufu ve kaynakların güçlendirilmesini sağlamış olur. Tek oturum açma (Single Sign-On (SSO)), birleşik kimlik yönetimi ile aynı şey olarak düşünülse de birleşik kimlik yönetiminin sadece önemli bir bileşenidir[76].

3.1.2 Saldırılar, Zafiyetler ve Tehditler

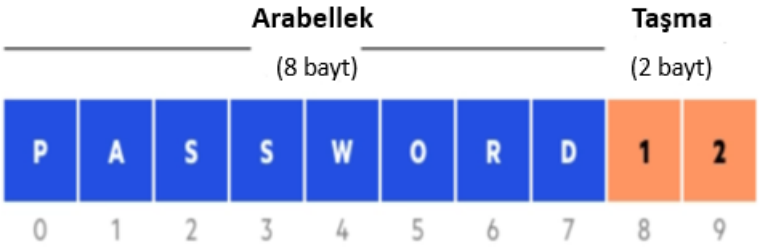
3.1.2.1 Arabellek Taşma Saldırısı

Bilgisayar üzerinde kullanıcıların yaptığı herhangi bir işlem SSD veya HDD gibi sabit disklere veya ilgili depolama birimine yazılmaktadır. Bazen bu yazma işlemleri sabit diskler veya depolama birimleri yerine bellek üzerinde geçici olarak konumlandırılmış alanlarda tutulabilmektedir. Bu geçici konumlandırılmış alanlara tampon(buffer) veya ara bellek denilmektedir.

Arabellekler sabit diskler kadar olmasa da kendisine ait boyutlara sahiptir. Bu arabelleklere saldırganlar tarafından veya yazılım esnasında yapılan hatalardan kaynaklı kendi boyutunun üzerinde yük ile yüklenebilmektedir. Bu boyutunun üzerinde yükün gelmesiyle birlikte veriler bitişik depoya taşarak arabellek taşması meydana gelmektedir. Bu arabellek alanının taşması da verilerin bozulmasına hatta program ve uygulamaların çökmesine neden olabilmektedir.

Bir saldırgan örneğin web üzerinden hizmet veren bir bulut sağlayıcısının

websitesine zararlı yazılımlar kullanarak alabileceği yükten fazla yük yüklemeye çalışarak arabellek taşması sorunlarından yararlanmak ister. Bu hedefe ulaşıldığı takdirde arabellekte taşma meydana gelir. Bu taşan kısımda olan kodlar direkt olarak çalıştırılabilir duruma gelir. Saldırgan dışarıdan eriştiği bölgeye zararlı yazılımı enjekte ederek uzaktaki bilgisayar veya sunucunun içerisinde yönetimi ele alabilmektedir. Hatta saldırganların programın bellek düzenini bildikleri durumlarda, arabelleğin depolayamadığı girişi istekli bir şekilde besleyerek ve yürütülebilir kodu tutan yerlerin üzerine kendi kodlarını yazarak istedikleri değişiklikleri yapabilirler.



Şekil 3.4. Buffer overflow örneği[77].

Arabellek taşması saldırıları stack ve heap tabanlı, tamsayı ve unicode olmak üzere dört çeşittir. Stack tabanlı arabellek taşmaları daha yaygındır ve yalnızca bir işlevin yürütme süresi sırasında var olan yığın belleğinden yararlanır. Heap tabanlı saldırılar stack tabanlı arabellek taşma saldırılarına nazaran uygulanması daha zor olan bir türdür. Heap tabanlı saldırı bir programa ayrılan bellek alanının, mevcut çalışma zamanı işlemleri için kullanılan belleğin daha üzerine çıkarak taşma meydan geldiği durumlarda gerçekleşmektedir. Bir tamsayı taşmasında ise bir aritmetik işlem esnasında sonuç için ayrılan tamsayı alanının yeterli olmayıp sonucu belleğinde tutamayıp taşması sonucunda meydana gelmektedir. Unicode taşması ise unicode karakterlerin ASCII olarak gösteriminde meydan gelmektedir[77]. Arabellek taşması saldırıları genellikle c veya C++ programlama dilleriyle yazılan uygulamalarda karşımıza çıkmaktadır. Bu programlama dilleri belleklerdeki verilere erişime ve verilerin üzerine yazılması konusunda herhangi bir yerleşik korumaya sahip olmadıklarından dolayı bu saldırılara daha fazla hassas ve elverişlidir.

Arabellek taşması saldırılarına bazı yöntemler kullanılarak önlem alınabilmektedir. Bunlardan bazıları aşağıdaki gibi sıralanmıştır[78].

- Arabellek taşması saldırılarına karşı hassas olmayan bir dil tercih edilmelidir.
- Arabellek denetimi yapmayan metotlar kullanılmamalı onların yerine alternatif çözümler kullanılmalıdır. Örneğin C programlama dilinde get() metodu yerine fgets() metodu gibi
- ASLR (Address space layout randomization) programda yer alan veri alanlarının rastgele şekilde düzenlenmesini sağlamak
- Fonksiyonların random bir şekilde yapılandırılması
- Adres karıştırma(Obfuscation) yöntemi kullanılması
- Güvenli olmayan hataları belirleyebilecek derleyiciler kullanılması
- Arabellek taşmalarını önlemeye yardımcı olabilecek bir koruma değeri olan Canaries'i kullanılması. Stack'te return adresinde önce eklenip ona erişilmeden önce kontrol edilirler. Program, kanarya değerinde bir değişiklik görürse işlemi iptal olmasını sağlayarak saldırganın arabellek taşması saldırısına engel olur. Bu değer rastgele veya üzerine yazılması imkânsız olan karakterlerden oluşmaktadır.

3.1.2.2 Bulut kimlik doğrulama saldırıları

Kimlik doğrulama, bulut bilişim üzerinde veya her sanal hizmette önemli bir konudur ve çok sık saldırganların hedefinde olmaktadır. Bir kullanıcının ne bildiğine, sahip olduğuna veya ne olduğuna bağlı olarak, kullanıcıların kimliğini doğrulamanın pek çok yolu vardır. Kimlik doğrulama sürecini güvence altına almak için kullanılan mekanizmalar ve yöntemler çoğunlukla saldırganlar tarafından takip edilmektedir. İnternet üzerinde arayüzler aracılığıyla hizmet veren bir bulut hizmetinde herhangi bir kimlik doğrulama mekanizmasının yüksek güvenlikli olmasının yanı sıra arayüzün kolay kullanımını da sağlaması böylece kullanıcıların hizmeti hareketli ve rahat kullanması sağlanmalıdır.

Günümüzde internete bağlı olan ve bulut bilişimde de kullanılan cihazların artmasıyla kullanıcılar hizmetlere her yerden erişim sağlamaktadırlar. Bunun sonucu olarak bulut bilişim erişilebilirlik konusunda geniş bir yelpaze sunarken güvenlik konuları daha çok gündeme gelmekte ve daha da önemli bir hal almaktadır. Bulut hizmeti sağlayıcıları bu nedenle, bulut ortamı için yüksek güvenlikli bir kimlik doğrulama mekanizması geliştirmek için özgünlüğe ve ilgili kimlik doğrulama saldırılarını önleme tekniklerine yönelik derinlemesine bir bilgi birikimine sahip olması ve önlemleri

uygulamalarında işletmesi gerekmektedir. Bulut ortamında kimlik doğrulama tehditleri ve saldırıları aşağıda sıralanmıştır[79-80].

Şekil 3.5. Kimlik doğrulama saldırı çeşitleri[79].

- Gizli dinleme saldırıları: Bir saldırganın iki kullanıcı veya iki cihaz arasındaki iletişim kaynağını dinlemesiyle başlatılan bir saldırıdır. Bir saldırgan bir bulut sunucusuna bir bit kod yükleyerek bulutta aktarılan verileri pasif olarak durdurma işlemini gerçekleştirerek veya bir bulut tüketicisi ile bulut sağlayıcı arasında gidip gelen verileri dinleyerek ve yasal olmayan bir mesaj kopyası oluşturur. Saldırgan, geçerli kimlik bilgilerini almak için bu yasa dışı olarak toplanan verileri kullanır. Burada bahsedilen geçerli kimlik bilgileri yetkili bir kullanıcının kimliğine bürünerek saldırganların saldırı başlatmasına yardımcı olmaktadır. Bulut sağlayıcısı ve tüketicisi iletişimde veriler iletilmeden şifrelenip imzalandığında saldırganın hedefinde olan verilerin bütünlüğünü ve gerçekliğini sağlamaya yardımcı olur. Bulut hizmeti kullanıcısı ve doğrulayıcı sistem arasında kimlik bilgilerinin iletilmesi gereksinimini azaltan ve gizliliği artıran protokollerin uygulanması, gizli dinleme saldırılarını engellemek adına gerekli bir diğer adımdır.

- Tekrarlama(Yeniden oynatma) saldırıları: Orjinal kaynak yerine farklı bir kaynaktan gönderilen mesajın tekrarı yapılarak saldırı gerçekleştirilir ve erişim hakkı elde edilir.

Kısaca özetlemek gerekirse Alice kimliğini Bob'a kanıtlarken Bob Alice'ten şifre bilgisini ister, Alice bu şifreyi özetini alarak Bob'a gönderir. Bu işlem esnasında saldırgan iletişimi dinler ve şifre veya özetlenmiş şifreyi ele geçirir. Daha sonra Alice ve Bob arasında yapılan işlem sonlandığında saldırgan Alice gibi davranarak çaldığı bilgiyi Bob'a kimlik kanıtı olarak sunar ve erişim hakkı elde eder. Böylece saldırı gerçekleşmiş olur. Yeniden oynatma saldırılarına önlem almak adına birkaç çözüm bulunmaktadır. Yukarıdaki işlemde Bob Alice'e tek seferlik bir token gönderir ve Alice bunu alarak kendi şifreyi dönüştürme işlemini Bob ise kendisi için ayrı işlemi yapar ve bir değer ortaya çıkar iki tarafında değeri aynıysa iletişim başlar. Ayrıca tek seferlik parolalar, tek kullanımlık sayılar ve zaman damgaları da kullanılarak bu saldırılar önlenmektedir.

- Oturum ele geçirme saldırısı: İki bilgisayar arasındaki geçerli TCP iletimini ele geçirme olarak tanımlanmaktadır. Kimlik doğrulama için TCP oturumu başladığı durumda saldırganın makineye erişimini sağlamaktadır. Saldırgan kurulmuş TCP oturumlarındaki tüm trafiği dinleyip kimlik, bilgi hırsızlığı, dolandırıcılık yapar. Saldırgan geçerli oturum bilgisini çalıp sunucuya kendini doğrulatmak için kullanmaktadır. Güvenli olmayan iletişim protokolleri ve şifrelenmemiş veriler gibi boşluklardan yararlanan bu oturum ele geçirme saldırıları, HTTPS gibi güvenli bir iletişim protokolü kullanarak, kullanıcı veya yönetici oturum açma bilgilerini vb. depolayan dosyaları şifreleyerek önlenmektedir. Bu tür saldırıları önlemek için bir bulut ortamında, yetkisiz kimlik doğrulama olasılığını ortadan kaldıran güçlü bir kimlik doğrulama mekanizması ve oturum anahtarları gibi hassas verileri koruyan veya bu verilerin saklanmasını önleyen mekanizmalar sağlanması gerekmektedir. Ayrıca bu saldırılar oturum anahtarlarının iletişim kanalı üzerinden aktarılmasından kaçınılarak hafifletilebilir.

- Çerez zehirlenmesi: Çerezler bir web sayfası ziyaret edildiğinde tarayıcı tarafından kullanıcıların bilgilerin depolandığı küçük dosyalar olarak tanımlanmaktadır. Bu çerezler kullanıcının sabit diskinde depolanarak kullanıcın ziyaret ettiği siteler için kimlik doğrulaması, web sitesi içerisinde kullanıcı giriş gibi işlemleri kısa bir sürede yapılmasını ve kullanıcın kişiselleştirilmesini sağlar. Güvenlik önlemlerinin etkisiz ve az olduğu sistemlerde saldırganlar bu çerez bilgisini çalabilir. Saldırganlar çerez zehirlenme saldırılarında kullanıcı hakkında yetkisiz olarak bilgileri elde ederek bunları değiştirir. Bu bilgileri o kullanıcı gibi görünerek yeni hesaplar açmak için veya

kullanıcın sahip olduğu tüm hesaplara erişmek için kullanır. Çerez zehirlenmesi saldırılarına önlem almak adına oturum tanımlayıcıların iletiminde şifreleme kullanılması zorunludur. Web uygulamaları için web uygulama duvarı(WAF) da önlem olarak kullanılabilecek diğer bir seçenektir. Bu yüzden bulut bilişim sistemlerinde verilen hizmetlerin oturum güvenliğinin en iyi düzeyde sağlanması ve bulut tüketiciye güvenli bir ortam sağlanması için bu adımlar gerçekleştirilmelidir.

- Omuz Sörfü saldırısı: Bu saldırı tekniği temelini sosyal mühendislikten almaktadır. Saldırgan bu saldırıyı gerçekleştirme adına kurbanın yakınlarında bulunmakta ve kurbanın hassas yapıya sahip PIN, şifre gibi gizli ve hassas kişisel bilgilerini cihazlara girdiği tuş kombinasyonlarını izleyerek elde etmeye çalışmaktadır. Bu saldırılar casus kameralar kullanılarak da başlatılıp gerçekleştirilmektedir. Bu saldırının bazı durumlarda tam olarak gerçekleşmese bile kısmen gerçekleştiği durumlarda örneğin saldırganın kurbanın herhangi bir şifresinin uzunluğunu saptadığında bu bilgiyi farklı saldırı tekniklerinde kullanabilmektedir. Bunun sonucunda kurbanın bilgilerini açığa çıkararak verilerini ihlal etmesine ve bunlara erişim sağlayabilmektedir.

- Bu saldırıları önlemek için sistemsel olarak iki faktörlü kimlik doğrulama mekanizmaları kullanılması saldırıyı engellemeye yardımcı olmaktadır. Ayrıca cihazların eğilimini sağlamak, herhangi bir kişiden bu kişi çok yakın biri olsa bile bunu engellemek ve herhangi bir kişinin görüş alanının dışında konumlanmak saldırıyı engelleyebilecek diğer önlemlerdir.

- Parola keşif saldırıları: Bu saldırı türü içinde birçok türü barındırmaktadır. Bunlar kaba kuvvet saldırısı, keyloger saldırısı, sözlük saldırısı, tahmin etme saldırısı, oltalama saldırıları ve video kayıt saldırılarıdır[81-82].

Kaba kuvvet saldırısı parola keşif saldırılarında en yaygın kullanılan yöntemdir ve bir saldırgan için en kolay gerçekleştirilen yöntemdir. Kaba kuvvet saldırısında saldırgan kullanıcının hesabında olası tüm parola kombinasyonlarının küçük yazılımlar kullanarak oturumu açmaya çalışır. Ayrıca, bu saldırıyı yaparken sosyal mühendislik kullanılarak kullanıcın belirleyebileceği kolay şifreler denenerek başlar.

Keylogger, klavye vuruşlarını bir günlüğe kaydederek bir kullanıcının bilgisayar üzerinde yapacağı tüm işlemleri kaydeden casus bir yazılımdır. Saldırganlar, şifreler ve

kredi kartı numaraları gibi bu tip hassas verilere erişim sağlamak ve bu bilgileri çalmak için için keylogger yöntemlerini kullanır. Bir parola saldırısında, keylogger yalnızca kullanıcı adı ve parolanın yanı sıra bu kimlik bilgilerini ve diğer hassas bilgileri kullanan web sitelerini ya da uygulamaları da kaydeder. Keylogger saldırıları hem donanım hem yazılım tabanlı yapılmaktadır. Fakat donanım tabanlı saldırıların gerçekleşmesini için ekstra iş, yük ve zaman gerekli olduğundan bu saldırının yazılımsal tarafıyla deneme yaparlar. Bunu bir kullanıcıyı kötü niyetli bir bağlantıya tıklamasını sağlayarak kullanıcı bilgisayarına kötü amaçlı yazılım yüklemeye çalışarak yapmaktadırlar. Ayrıca bu tür saldırılar kullanıcıların yamalı yazılım yüklemesi ve kullanmasından da kaynaklanmaktadır.

Sözlük saldırıları, bir tür kaba kuvvet parola saldırısı olarak önümüze çıkmaktadır. Bu saldırı türünde sık kullanılan parolaların yanı sıra yaygın olarak kullanılan sözcüklerin ve ifadelerin bir listesi barındırılmakta ve saldırıda kullanılmaktadır. Saldırganlar, olası parolaların uzun bir listesini kırmak zorunda kalmamak için listeyi sözlük kelimeleri olarak bilinenlere daraltır. Bu kelimeler sözlükteki gerçek kelimelerle kısıtlanmayıpbilinen evcil hayvan isimlerini, film karakterlerini, akla gelebilecek kullanılan tüm yağın kelimeleri de içermektedir. Bunun yanı sıra kullanıcılar şifre seçiminde bildiği bu kelimeleri çoğu hesaplarında değiştirerek kullanmaktadır. Örneğin bir hesabında 123Rabbit. olarak kullandığı parolayı başka bir hesabında Rabbit.123 diye kullanabilmektedir. Bu saldırıda sona eklemeler yapılarak denemelerle başlanmaktadır.

Tahmin etme saldırısında kullanıcıların çoğu zaman bu saldırıya karşı savunmasız hale getiren hatırlaması kolay şifreler kullanması en önemli faktördür. Saldırgan, şifreyle ilgili bazı bilgileri sosyal mühendislik veya başka yöntemlerle gözler ve tahmin yürütmeye çalışır ve ardından erişim elde edene kadar birden çok kez giriş yapmayı deneyerek doğrular. Çevrimdışı senaryoda, yaptığı deneme sayısında herhangi bir kısıtlama olmadığı için saldırganın doğru şifreyi tahmin etme şansı yüksektir. Ancak çevrimiçi tahmin senaryosunda, sistemler belirli sayıda oturum açma denemesinden sonra kullanıcıyı engellediğinden dolayı bu saldırının başarı şansı bir hayli düşüktür.

Oltalama saldırıları genellikle saldırganlar tarafından meşru ve bilinen hizmetler gibi görünen, şüpheli olmayan e-postalar olarak kullanılarak yapılmaktadır. Saldırganlar bu tip saldırılarda çok bilinen bankaların sayfalarının taklitlerini yaparak kurban

kullanıcılara istedikleri web sitesine yönlendirmektedirler. Daha sonra bu zararlı siteye girişten sonra girilen tüm bilgilerin çalınma durumu çok yüksektir.

Ayrıca, kullanıcıları kandırmak için işyerinin sosyal kurallarını kullanarak yapılan oltalama saldırıları bir tür sosyal mühendislik saldırısı haline gelebilir. Bu. Bilgisayar korsanları, BT ekibi gibi davranarak kullanıcılardan şifrelerini isteyebilir.

Video kayıt saldırısı ise halka açık yerlerde yapılmaktadır. Saldırganlar kameralı cep telefonları veya minyatür kameralar yardımıyla kurbanın şifresini girerken şifreyi ele geçirmeye çalışmaktadır.

- Müşteri dolandırıcılığı saldırısı: Bulut bilişim sistemlerinde kullanıcıların dahil olduğu saldırı türlerinden biridir. Müşteri dolandırıcılığı saldırısında kullanıcı kimlik doğrulama bilgilerini kasıtlı bir şekilde tehlikeye atarak veri ihlali oluşturmaya çalışır. Bu tür atakları önlemek için kimlik doğrulayıcısının kullanıcın hem kurban olduğu hem de kullanıcının hatası olduğunu ilk önce kanıtlaması gerekmektedir. Bulut bilişim sistemlerinde bir kere kullanılabilir parolalar veya kimlik doğrulama protokollerinde yer alacak rastgele oluşturulmuş nonce değerleri kullanılarak hafifletilebilmektedir. Her oturum açıldığında kullanılacak bu değerler doğrulayıcıdan kullanıcıya güvenli bir kanaldan iletilmek zorundadır.

- Ortadaki adam saldırısı: Bu saldırı türü de parola keşif saldırıları gibi birden fazla tür saldırıdan oluşmaktadır. Bunlar taşma saldırısı, tarayıcı saldırısı, kimliğe bürünme saldırısı ve SSL saldırılarıdır.

Taşma saldırısında saldırgan, bilgi işlem kaynaklarını taşma oluşması için meşgul tutarak yanlış istekler kullanır ve bu nedenle bulut ortamındaki diğer istemcilerden gelen isteklere yanıt veremez. Bu tür saldırılar, veri iletim kısıtlamaları, hatasız kimlik doğrulama mekanizmaları ve yanlış istekleri filtreleme mekanizmaları aracılığıyla engellenebilir ve önlenebilir.

Bir tarayıcı saldırısında, saldırgan, Web tarayıcısı ile Web sunucusu arasındaki SOAP mesajı dönüştürme işleminde imzayı ve şifrelemeyi yok ederek verileri çalar, böylece tarayıcı, saldırganı yetkili bir kullanıcı olarak kabul eder ve tüm isteklere yanıt

verir. Bu saldırıya önlem almak adına web sunucu güvenliği mekanizmaları kullanıcı tarayıcılarında etkinleştirilmelidir. web sunucu güvenliği, SOAP mesajlarında mesajların dinlenmesini önleyen uçtan uca şifreleme sağlamak için web tarayıcılarının şifreleme kullanmasına izin vermektedir.

Kimliğe bürünme saldırısında, saldırgan meşru bir sunucu veya kullanıcı gibi davranır ve geçerli bir varlığa kimlik doğrulama bilgilerini ifşa etmesi için başvurur. Bu tür saldırılara örnek olarak aslında parola keşif saldırılarında bulunan oltalama saldırıları örnek olarak verilebilmektedir. Çünkü oltalama saldırılarında saldırgan bir yolla meşru bir kimlikle kullanıcı veya sunucuyla iletişime geçmeye çalışmaktadır. Bu saldırılara önlem açısından iki faktörlü doğrulama veya çok faktörlü kimlik doğrulama mekanizmalarının etkinleştirilmesi gerekmektedir.

SSL katmanı, istemci ve sunucu arasında iletilen verileri şifreleyerek herhangi bir verinin çalınmasını engellemeye yönelik yapılandırılmış temel bir güvenlik mekanizmasıdır. SSL, iletişim taraflarının kimliklerini doğrulayarak bulut hizmetleri için kimliği doğrulanmış bir ortam sağlamaktadır. SSL saldırılarından SSL çıkarma saldırılarında, saldırganlar kullanıcın kullandığı web sitesinde https olan güvenli siteyi ssl katmanının sıyırarak sadece http üzerinde kullanıcının sistemi kullanmasını sağlamaya çalışır. Bunu başardığında ise kullanıcıların trafiği düz metin gibi görüneceğinden kolayca veri çalma işlemini gerçekleştirebilmektedirler.

Buna örnek olarak bir kullanıcın ödeme yapacağı vakit ödeme esnasında SSL sıyırma gerçekleştirildiğinde kullanıcın bilgileri düz metin halinde görüneceğinden saldırgan bu verileri kullanarak istediği işlemi yapabilmektedir. Bu saldırılara önlem olarak websitesi üzerinde http olan anahtar kilidi bulunmayan siteleri ziyaret etmemek işlemler esnasında kontrollü geçişler yapmak gerekmektedir.

3.1.2.3 Zararlı Yazılım Enjekte Etme Saldırıları

Bulut bilişim sistemlerinde güvenlik ile alakalı en önemli sorunlardan biri de zararlı yazılım enjekte etme saldırılarıdır. Bu saldırı türünde saldırgan, kötü amaçlı hizmetleri, kodları veya sanal makineleri bulut ortamına enjekte etmeye çalışır. Bu, bulut sistemlerine kötü amaçlı yazılım enjeksiyon saldırılarına yol açar. Saldırgan, kendi kötü

niyetli hizmet olarak yazılım veya platform uygulama modelini veya hizmet olarak altyapısı olan sanal makine örneğini oluşturarak bu hizmetini bulut ortamına eklemeye çalışmaktadır. Saldırganların amacı, hizmet uygulamalarının bulut sistemi tarafından geçerli bir örnek olarak ele alınmasını ve kötü amaçlı yazılımın yürütülmesi için trafiğin kötü amaçlı hizmete yönlendirilmesini sağlamaktır. Saldırgan başarılı olduğu takdirde gizlice dinleme, veri değiştirme, bulut kaynaklarına yetkisiz erişim, kullanıcı kimlik bilgisi sızıntısı, işlevsellik değişiklikleri ve hizmet engelleme gibi birçok yasa dışı işlemleri gerçekleştirebilmektedir.

Bulutta kötü amaçlı yazılım yerleştirme saldırılarıyla uğraşmanın zorluklarından biri, yalnızca saldırının gerçekleştiğini tespit etmek değil, aynı zamanda saldırgan tarafından kötü amaçlı hizmet uygulaması için hangi sanal makine örneklerinin kullanıldığını belirlemektir. Kötü amaçlı yazılım yerleştirme saldırıları genellikle virüslü bir FTP sunucusu aracılığıyla yapılır. Kötü amaçlı yazılım, FTP parolalarını dinleyerek yakalamaya çalışır ve bu parolaları saldırgana geri gönderir. Saldırgan daha sonra sitenin web sayfasına kötü amaçlı kod eklemek için FTP kimlik bilgilerini kullanır ve bu da siteye erişen diğer ziyaretçilere bulaşır. Bulut tabanlı bir sistemde, bir web istemcisinin isteği, kimlik doğrulama ve yetkilendirmeye dayalı olarak yürütülür. Bu yetkilendirme ve doğrulama işlemi sırasında, web sunucusu ve web tarayıcısı arasında büyük miktarda meta veri alışverişi yapılır. Saldırgan bu meta verilerden yararlanarak saldırısında kullanmaktadır. Düşman kötü niyetli hizmet veya kod enjekte etmeye çalışarak kötü amaçlı yazılım enjeksiyon saldırısının başka bir türünü gerçekleştirmiş olur. Bu saldırıda, bulutta çalışan hizmetlerin geçerli bir örneği enjekte edilen kötü amaçlı hizmet veya koddur. Saldırgan yapmış olduğu saldırıda amacına ulaşırsa, bulut hizmeti gizli dinlemelere ve ihlallere karşı savunmasız hale gelir. Daha sonra yasal bir kullanıcıyı, kullanıcı tarafından oluşturulmayan herhangi bir aktivitenin tamamlanması için zorla bekletir. Bu saldırıya meta-veri sızdırma saldırısı da denmektedir[83].

Tüm kötü amaçlı yazılım enjeksiyon saldırıları arasında, SQL enjeksiyonu ve siteler arası komut dosyası çalıştırma (XSS) saldırıları en iyi bilinen örnekler arasındadır[84-85].

SQL enjekte etme saldırısında saldırganlar kullanıcın sisteme giriş yaptıkları esnada arka tarafta tutulan veritabanına odaklanırlar. Bu saldırı birkaç adımdan oluşmaktadır. İlk

olarak kötü niyetli kullanıcı, bulut sağlayıcısına geçerli bir bulut kullanıcısı olarak kimliğini kanıtlar. Daha sonra satın alınan hizmetlere korumasız olarak kendini doğrular. Bir sonraki aşamada satın alınan hizmete SQL sorguları enjekte ederek gerekli tüm veritabanı bilgilerini toplar. Böylelikle bulut bilişim hizmetine abone olmadan, kurban olan kullanıcıyla ilgili tüm hassas bilgileri ve verileri görüntüleyebilmekte ve kullanabilmektedir.

SQL enjekte etme saldırılarına önlem almak adına birkaç çözüm bulunmaktadır.

Bunlar;

- Eksiksiz bilgi dezenfeksiyonu kullanılmalıdır. Hizmet veren web siteleri, tüm istemci girişlerini kanalize ederek kontrol etmelidir. Bulut tüketicilerinin harika bir ortamda hizmeti kullanabilmesi adına kullanıcı bilgileri yapılabilecek tüm ayarlar için ayrılmalıdır. Örneğin, e-posta gönderimleri, bir e-posta adresinde yalnızca izin verilen karakterlere izin verecek şekilde elenmeli, telefon numaraları, yalnızca bir telefon numarasında izin verilen karakterlere izin vermek için ayrılmalıdır.

- Ayarlar kullanılarak veritabanı avantajlarını sınırlanması gerekmektedir. Kullanım koşulları için faydanın temel boyutları ile çok sayıda veritabanı kullanıcı hesabı yapılmalıdır. Örneğin, bir oturum açma sayfasının arkasındaki kod parçacığı, yalnızca ilgili sertifikalar tablosuyla sınırlı bir kayıt kullanarak veritabanını sorgulamalıdır. Böylece, bu kanalda bir kırılma tüm veri tabanı üzerinde etkileşim için kullanılamaz.

- Kullanıcı girişiyle SQL sorguları geliştirmekten kaçınılmalıdır. Kullanılan ilgi dezenfeksiyon programları hatalı çıkabilmektedir. Düzenlenmiş artikülasyonlar veya yerine koyma sistemleri ile SQL değişken resmi kullanmak, tam sorgular oluşturmaktan çok daha güvenlidir.

- Yazılım esnasında veritabanı için parametreli sorgular kullanılmalıdır. Parametreli sorguların kullanımı ile, tüm yazılım geliştiricilerine veritabanı sorgularının nasıl yazılacağının öğretilmesi gerekmektedir. Yazmaları basittir ve dinamik sorgulardan daha kolay anlaşılır. Parametreli sorgular, geliştiricinin önce tüm SQL kodunu tanımlamasını ve daha sonra her parametreyi sorguya geçirmesini olanak sağladığı bir yöntemdir. Bu kodlama stili, hangi kullanıcı girişi sağlanırsa sağlansın veritabanının kod ve veri arasında ayrım yapmasına olanak tanır. Parametreli sorgu,

saldırgan SQL komutları eklediği durumlar oluşsa da, saldırganın sorgunun amacını değiştirememesini sağlar. Kullanıcı girişi otomatik olarak alıntılandığı ve sağlanan giriş sorgunun amacını değişmesine neden olmadığından dolayı bu kodlama stili bir SQL enjeksiyon saldırısını azaltmaya yardımcı olur.

- SQL enjeksiyon saldırılarını belirlemeye yönelik en iyi uygulamalardan biri, bir web uygulaması güvenlik duvarını sisteme entegre etmektir. Web sunucularının önünde çalışan bir web uygulama güvenlik duvarı web sunucularına giren ve çıkan trafiği izler ve tehdit oluşturan kalıpları belirler. Aslında web uygulaması ile internet arasına konulan bir engel mekanizmasıdır.

- Web uygulama güvenlik duvarı, tanımlanmış özelleştirilebilir web güvenlik kuralları aracılığıyla çalışmaktadır. Bu kurallar ve politikalar, web uygulaması güvenlik duvarına hangi güvenlik açıklarının ve trafik davranışlarının aranacağını söyler. Böylelikle kötü niyetli trafiği bulmak ve engellemek için daha özel çözüm geliştirilmiş olur. Ayrıca web uygulama güvenlik duvarı sql enjeksiyonu saldırılarının yanı sıra Siteler arası komut dosyası çalıştırma (XSS), oturum çalma, dağıtılmış hizmet reddi (DDoS) saldırıları, çerez zehirlenmesi gibi saldırıların önlemi için de kullanılmaktadır.

- Parametreli sorgulara benzer şekilde, saklı yordamların kullanılması da değişken bağlama gerektirir. SQL'i azaltmaya yönelik hazırlanan deyimler yaklaşımının aksine, saklı yordamlar veritabanında bulunur ve web uygulamasından çağrılır. Fakat dinamik SQL oluşturma kullanılıyorsa, saklı yordamlar da güvenlik açıklarına karşı bağışık değildir.

Diğer zararlı yazılım enjekte etme atak türü ise siteler arası komut dosyası çalıştırma (XSS) saldırısıdır. XSS saldırısıyla, kötü niyetli saldırgan HTML tabanlı istemcideki belgelerin veri bağlamına enjekte ederek sunucudaki hassas bilgilere erişim kazanır. Bu yöntem kullanılarak saldırgan, küçük kod parçasını veya betiğini kurbanın web tarayıcısında çalıştırabilir. OWASP tarafından yapılan sınıflandırmada XSS saldırıları, depolanan ve yansıtılan olarak ikiye ayrılmaktadır. Saldırıların neredeyse %13'ünün web üzerindeki XSS ile alakalı olduğu da belirtilmiştir. XSS tabanlı varyete saldırılarında neredeyse sınır bulunmamaktadır.

XSS saldırıları kendi içerisinde 3 farklı çeşit bulundurmaktadır. Bunlar Yansıyan XSS Saldırıları, DOM Tabanlı XSS Saldırıları ve Kalıcı/Depolanmış XSS Saldırılarıdır[86].

En basit XSS saldırı türü olarak bilinen yansıtma XSS saldırılarında, kötü amaçlı komut dosyaları doğrudan HTTP isteklerine enjekte edilir. Daha sonra komut dosyası, sunucudan gelen HTTP yanıtına yansıtılır ve en sonda kullanıcının tarayıcısında yürütülür.

DOM tabanlı saldırılar, sunucu ile etkileşim gerektirmeyen XSS türüdür. Tarayıcı tarafı komut dosyası güvenlik açığının sebebidir. Web uygulamaları, kötü amaçlı komut dosyasını doğrudan bir sorgu dizesinden okur ve böylelikle yansıyan XSS saldırılarına benzerlik göstermektedir.

Kalıcı veya depolanmış XSS saldırıları, siteyi ziyaret eden her kullanıcıyı etkileme potansiyeline sahiptir. Bu sebepten ötürü en tehlikeli saldırı olarak bilinmektedir. Bu tür bir saldırıda formlar kullanılarak komut dosyaları bir veritabanına enjekte edilir ve saldırı gerçekleşir. Bundan sonra komut dosyası süresiz olarak web sitesinin veritabanında saklanır ve web sitesine giren her kullanıcı, oturumlarının ele geçirilmesine karşı savunmasız kalır ve saldırı başarıyla sonlandırılmış olur.

XSS saldırıları için şu adımlar bulunmaktadır.

- Bulut sağlayıcısına karşı, kötü niyetli bir kullanıcı, kimliği doğrulanmış kişi olarak kimliğini doğrular.

- Kötü niyetli kullanıcı, korumasız bir web uygulamasına erişim içim girişiminde bulunur.

- Kötü niyetli kullanıcı, web uygulamasını kendi tarayıcısına yükler.

- Bir URL aracılığıyla, kötü niyetli kullanıcı tarafından bir saldırganın sunucusundan bir kötü amaçlı yazılım enjekte edilir.

- Gönderme işleminden sonra sunucu tarafında içerikler güncellenir. Daha sonra bulut sağlayıcısına karşı, kurban kimliğini doğrulanmış bir kişi olarak doğrular.

- Kötü niyetli kullanıcı tarafından erişilen web uygulamasına kurban tarafından erişilebilmektedir. Ancak kötü amaçlı kod, kurbanın tarayıcısına yüklenir.
- Tarayıcı aracılığıyla, saldırganın sunucusu, kötü amaçlı yazılım tarafından ayıklanabilecek hemen hemen her ayrıntıyı alır.

XSS saldırılarını önlemek adına aşağıdaki önlemlerin alınması gerekmektedir.

- Bulut sağlayıcısında alınan yazılım hizmetin her zaman güncel olarak tutulması gerekmektedir. Yeni gelen güncellenmiş yama ile birlikte var olan hata ve riskler en aza indirgenmiş olur ve sistem performansının da yükseltilmiş olması bir diğer avantajdır.

- Giriş alanları, XSS saldırı komut dosyaları için en yaygın giriş noktasıdır. Bu nedenle, veri alanlarına yapılacak herhangi bir girişin her zaman taranması ve doğrulanması gerekmektedir. Bu, yansıyan XSS saldırılarına karşı koruma sağlamak için veriler HTML çıktısı olarak dâhil edilecekse özellikle önemlidir.

- Doğrulama, ek bir önlem olarak hem istemci tarafında hem de sunucu tarafında yapılmalıdır. Böylelikle verilerin sunuculara gönderilmeden önce doğrulanması, kalıcı XSS komut dosyalarına karşı da koruma sağlayacaktır.

- Bir web uygulaması güvenlik duvarı (WAF), XSS saldırılarına karşı koruma sağlamak için güçlü bir yöntemdir. Yukarıda da bahsedilen web uygulama güvenlik duvarları XSS saldırıları içinde olmazsa olmazlardandır. Web uygulama güvenlik duvarlarının filtreleme özelliği sayesindebir saldırıya etki edebilecek kötü amaçlı etkinlikler tespit edilebilir. Saldırılar daha sonra herhangi bir komut dosyası yürütülmeden önce engellenebilir.

- Her türlü çıktı kodlanmalıdır.

- Son olarak hala meydana gelen XSS güvenlik açıklarının önem derecesini azaltmak için İçerik Güvenliği İlkesi(CSP) kullanılmalıdır. CSP bir web sitesinin gerçekleştirmesine izin verilen işlevleri tanımlayabilmektedir.

3.1.2.4 Güvensiz uygulama programlama arayüzleri (API)

Bulut bilişimde güvenlik sorunlarıyla alakalı en önemli konulardan biri güvensiz uygulama programlama arayüzleridir. Uygulama Programlama Arayüzü (API), yazılım uygulamalarının oluşturulması esnasında uygulanan protokol ve bileşenelerin bütünü olarak tanımlanmaktadır. API'ler, bulut sağlayıcıları ve yazılım geliştiricileri tarafından, bulut tüketicilerinin bulut hizmetlerinden etkileşim kurmasına, veri çekmesine ve yönetmesine kısacası hizmette yer alan çoğu işlevi yerine getirmesine olanak sağlamak için kullanılır. Hizmet Olarak Altyapı API'leri, ağ ve VM'ler dâhil olmak üzere altyapı kaynaklarına erişmek ve bunları yönetmek için kullanılır. Hizmet Olarak Platform API'lerinin kullanılma amacı depolama gibi hizmetlere erişimin sağlanmasıdır. Hizmet olarak Yazılım API'leri ise bulut altyapısı ile yazılım uygulamalarını birbirine bağlamak için kullanılmaktadır[87].

API'ler, saldırganların için bir kurum ağının ihlali için ana hedeflerden biridir. Bunun nedeni uygulamaya erişebilmek için arayüze erişilmesinin gerekliliğidir. Kullanıcılar bulut bilişim sistemlerinde alacağı hizmetleri arayüzler tarafından almaktadırlar. Fakat API kullanımıyla bulut bilişim süreçlerinin kolaylaştırılması amaçlansa da API'lerde yer alacak kimlik doğrulama, yetkilendirme ve şifreleme hataları ve yetersizliği kötü niyetli kullanıcılara açık kapılar sağlamaktadır. Bu da üçüncü taraf kötü niyetlilerin bulut bilişimde yer alan güvenlik anahtarlarına ve hassas verilere erişmesine ve bulut bilişimde güvenlik sıkıntılarını güvensiz API'ler arayıcılığıyla tekrar gündeme getirilmesine neden olmaktadır. Ayrıca Gartner'a göre 2022 yılına kadar API'lerin kurumsal uygulama verilerini içeren saldırılarda en sık kullanılan saldırma türü olacağını tahmin etmektedir.

Siber suçluların bulut API'lerini kullanarak saldırı gerçekleştirmesinin nedeni BT altyapılarında kuruluşların çoğu iş ortaklarının ve harici geliştiricilerin yazılım platformlarına erişebilmesi için API'leri kullanmakta ve halka açık olarak servis etmektedir. Bu da beraberinde API'lere olan bağımlılığı arttırmaktadır. Bu bağımlılığın artması da saldırganların burada oluşabilecek zafiyetleri sömürmesine yol açmaktadır.

Bulut bilişim sistemlerinde güvensiz API'ler aracılığıyla yapılan atakların en önemli nedenleri yetersiz kimlik doğrulama ve açık kaynak yazılımların verilen hizmet içerisinde kullanılmasından kaynaklanmaktadır. Bazı durumlarda yazılım geliştiricileri, kimlik

doğrulaması olmadan bazı API'ler oluşturur. Sonuç olarak, bu arayüzler tamamen internete açıktır ve herkes bunları kullanarak kurumun sistemlerine ve hassas verilere erişmek için kullanabilir. Diğer yandan yazılım geliştirmeye bileşen tabanlı bir yaklaşım, BT dünyasında yaygın hale geldi. Zaman kazanmak için birçok geliştirici, açık kaynaklı yazılımı kullanarak kodlarını geliştirmektedir. Bu tür açık kaynak yazılımlarında var olan hata ve zafiyetler otomatik olarak bu açık kaynak kodu kullanan bulut bilişim hizmetinin de tehditlerle ve saldırılarla baş başa kalacağının göstergesidir[88].

API'ler arayıcılığıyla oluşabilecek tüm zafiyetlerin önüne geçmek adına bazı önlemler alınması gerekmektedir.

- Bulut bilişim hizmeti veren kurumun yazılım takımının kimlik doğrulama, erişim kontrolü, şifreleme ve etkinlik izleme göz önünde bulundururarak API tasarımını yapması gerekmektedir. API anahtarları güvenli bir şekilde saklanmalıdır.

- Güvenlik kısımları güzelce göz önünde bulundurulmuş standart API çerçeveleri kullanılmalıdır.

- API tasarımına yönelik kapsamlı politikalar bazen güvenlik sorunlarını tamamen yok etmeye yetmeyebilir. Bu yüzden güvenlik ekiplerinin API güvenlik risklerini hızla belirleyip ele alabilmesi için ağ algılama ve yanıt gibi tam görünürlük sağlayan çözümleri kurumlarında kullanması gerekmektedir.

3.1.2.5 İçeriden gelen saldırılar

İçeriden gelen saldırılarda kötü niyetli kişi sistemdeki ayrıcalıklarını kötü niyetli amaçlarla kullanan mevcut veya eski bir çalışan, yüklenici, ağ, sistem veya verilere erişim yetkisi olan iş ortağı olma ihtimali bir hayli fazladır. Bu tip saldırılarda içerideki kötü niyetli kişinin amacı intikam, finansal kazanç, casusluk veya zorlama ile saldırıda bulunmaktır.

Özellikle, ağ güvenlik duvarları ve sisteme giriş tespit sistemlerinde yetkilerinin bulunduğu düşünüldüğünde içeriden birinin faaliyetlerini kaçırabilir. Bulut bilişimde bulut kaynaklarına erişimi olan kötü niyetli kişiler normal saldırılardan çok daha fazla

hasara neden olabilir, çünkü esas olarak bulut bilişimde içeriden birinin saldırısı yalnızca saldırganın kendi kuruluşunu değil çok sayıda bulut müşterisini de etkileyebilir. Bu saldırıların gerçekleşmesi durumunda içerideki kötü niyetli kişi kurumun markasına büyük zarara uğratabilmekte, sistemlerin düzgün bir şekilde çalışmasını engellemekte, ticari sır veya kurumun fikri mülkiyet haklarını çalıp satmakta, kötü amaçlı yazılımları kendi amacı doğrultusunda kullanabilmekte hatta siber düşmanların sistemlere veya hesaplara erişimini sağlayabilmektedir.

İçerinde gelen saldırıları bulut bilişimde ikiye ayrılmaktadır. Bunlar bulut sağlayıcısındaki içeriden gelen saldırılar ve dış kaynak bulut sağlayıcısındaki içeriden gelen saldırılardır[37].

Bulut sağlayıcısındaki içeriden gelen saldırılarda kötü niyetli kişi bulut sağlayıcısında hali hazırda çalışmaktadır veya bulut sağlayıcısının eski bir çalışanı konumundadır.

Bu tip saldırılarda hem bulut sağlayıcısı hem de bulut tüketicileri ciddi zararlara uğrayabilmektedir.

Dış kaynak bulut sağlayıcısındaki içeriden gelen saldırılarında kötü niyetli kişi bulutta bilişim altyapısının bir kısmını veya tamamını dış kaynak olarak kullanan kuruluşun çalışanı konumundadır. Bu tip saldırıların engellenmesi için saldırı tespit sistemleri(IDS) veya saldırı önleme sistemleri(IPS) kullanılmalıdır.

İnsan unsuru kurum ve kuruluşlar için bulut bilişim sistemlerine geçmede önemli bir nedendir. Bu nedenle, bulut hizmetleri bulut tüketicilerinin ve bulut sağlayıcıların kötü niyetli içeriden gelen tehdidi tespit etmek ve bunlara karşı savunmak için ne yaptığını anlamaları çok önemlidir. Tehdit veya saldırılar aşağıdakiler uygulanarak bertaraf edilmelidir.

- Bulut hizmetlerine ve verilere erişimi sınırlamak veya ayrıcalıkları belirlemek
- Uyumluluk raporlaması
- İhlal durumlarında bildirimlerin aktif halde bulunması
- Güvenlik ve yönetim süreçlerinde şeffaflığın artırılması

- Güvenlik duvarı kullanımı
- Hassas verilerin maskeleme ve şifreleme ile güvende tutulması
- Veri kaçağı önleme(DLP) sistemlerinin kullanımı
- Kullanıcı davranışlarını izleyen ve potansiyel risk durumunda makine öğrenmesi kullanılarak uyarı yapan sistemlerin kullanılması
- Veritabanlarının izlenmesi yönetimi ve raporlanması
- Yedekleme mekanizmaları kullanmak
- Güçlü parola ve çok faktörlü kimlik doğrulama kullanılması

3.1.2.6 Dağıtılmış hizmet reddi saldırıları (DDoS)

Dağıtılmış hizmet reddi saldırıları, bulut bilişim sistemlerinde yer alan güvenlik risklerinin en önemlilerindendir. Bunun en önemli nedeni bulut sistemlerinde kaynakları birçok kullanıcı tarafından paylaşılarak kullanılmasıdır. Dağıtılmış hizmet reddi saldırılarında saldırgan sistem kaynaklarını aşırı miktarda gerçek olmayan trafikle doldurarak sistemin kullanılmaz hale gelmesini hedeflemektedir. Yani saldırgan hedef web kaynağına birden çok istek yollayarak sistemin işlem kapasitesinin aşılmasını ve böylece hizmetlerin ve kaynakların erişiminde ve kullanımında sıkıntılar yaşanmasını sağlamaktadır.

Ağ iletişimini veya bulut bilişim hizmetlerine erişimi engelleyerek son kullanıcılar için erişilemez hale getirmek amacıyla bellek, CPU veya ağ bant genişliği gibi her kaynağı tüketmesini sağlamak DDoS saldırılarındaki asıl gayedir. Bulut sistemlerindeki tüm katmanlarda DDoS saldırılarını bertaraf etmek saldırganın istekleriyle gerçek ve meşru kullanıcıların isteklerini ayırt etmenin zor olmasından dolayı önemli bir zorluktur.

DDoS saldırıları, bulut sisteminin hizmet olarak platform, altyapı ve yazılım olmak üzere tüm hizmet sınıflarında meydana gelebilmektedir. Bulut sisteminin dışından başlayan bulut tabanlı harici bir DDoS saldırısı bulut tabanlı olan bütün servislerin zarar görmesini hedefler. Bu saldırı sonucunda, hizmetlerin kullanılabilirliğini zarar görür. Bulut sistemleri içinde gerçekleşen DDoS saldırıları ise hizmet olarak platform ve altyapı katmanlarında yar alır. DDoS saldırıları birçok türden meydana gelmektedir. Bunlar IP sahteciliği saldırısı, SYN flood saldırıları, smurf saldırıları, Ping of Death saldırılarıdır[89-90].

IP sahteciliği saldırılarında saldırgan IP adresini hedefteki sisteme farklı bir şekilde göstererek amacına ulaşmaya çalışır. Bu saldırıdaki amaç ip tabanlı kimlik doğrulama kullanan sistemleri atlamak için kullanılır.

Normal durumlarda istemci ve sunucu arasında 3 adımlı el sıkışma olarak da adlandırılan TCP bağlantısı kurulacağı zaman aralarında bir iletişim başlar. İlk olarak istemci sunucuya SYN mesajı göndererek bağlantı kurulmasını sağlar. Daha sonra sunucu da bu SYN isteğine karşılık olarak SYN-ACK mesajı döner. En sonda istemci ACK mesajı göndererek bağlantının kurulmasını ve başlamasını sağlar. SYN flood saldırısında, bir saldırgan sistemin yasal trafiğini isteklere cevap veremeyecek duruma getirmek için yeterli sunucu kaynaklarını tüketme girişiminde bulunarak, hedef alınan sisteme art arda farklı IP'lerden SYN istekleri gönderir. Sunucu da gelen bu isteklere bellekte yer açarak SYN-ACK paketiyle cevap vermeye başlar. Fakat bir süre sonra bellek taşar. Bu taşma sonunda artık sunucu sadece SYN-ACK paketi yolladığı isteklerden ACK paketi bekler ve sistemin durmasına yol açar. Bu saldırılara önlem olarak hizmet olarak altyapı katmanında filtreleme, güvenlik duvarı ve aktif izleme sistemlerinin kullanılması gerekmektedir. Hizmet olarak platform katmanında ise SYN cache yaklaşımı, gelen SYN isteklerinin zamanının azaltılması ve SYN savunma çerezi yaklaşımları kullanılmalıdır.

Smurf saldırılarında hedeflenen makinenin IP'sini elde etmek ve tüm yanıtları orijinal kullanılan ağ bant genişliğinden daha büyük bir bant genişliği ile kaynak makineye geri göndermek için ICMP protokolü kullanılır. Smurf saldırılarına önlem olarak bulut sistemlerinde yer alan hizmet olarak platform katmanında sanal makinelerin doğru bir şekilde ayarlanması gerekmektedir.

Ping of death saldırılarında saldırgan basit bir ping komutu yardımıyla hatalı bir

şekilde biçimlendirilmiş ya da büyük boyutta ping paketlerini kullanarak kurban olan bulut sistemini kullanılamaz hale getirmeye çalışır. Fakat bu saldırı türü güncel işletim sistemlerinin aldığı önlemler sayesinde tarihe karışmıştır. Bu saldırıya önlem almaya gerek yoktur. Çümkü yapılması günümüzde mümkün değildir.

Genel DDoS saldırılarına çözüm olarak sıralayacak olursak, sunucuların belli zaman aralıklarında kabul edilecek istek sayısını sınırlaması bu saldırılara önlem alınabilecek önemli bir noktadır. Web uygulama güvenlik duvarlarının da kullanılması bu saldırıları hafifletebilmektedir. Ayrıca kullanıcıların güncel sistemleri kullanması, antivirüs programlarının kullanılması da gerekmektedir. Fakat şu unutulmamalıdır ki DDoS saldırıları kolay bir şekilde gözlemlenmesi bir hayli zordur.

3.1.3 Veri Güvenliği Çözümleri

3.1.3.1 Donanım Tabanlı Saldırılara Çözümler

Bulut bilişim sistemlerinde yazılımsal saldırıların yanı sıra donanım tabanlı saldırılar da mevcuttur. Bir bilgisayar donanımı saldırganlara açık kapı bırakabilecek bazı anormal davranışlara veya arızalara sahip olabilmektedir. Donanım tabanlı saldırılar bulut bilişim tüketicileri için yüksek öneme sahiptir. Bulut sağlayıcılarındaki yöneticilerin kötü niyetli bir şekilde hareket etmeleri durumunda sistemin fiziksel güvenlik mekanizmalarının etkinliğinin azalmasına ve veri ihlallerinin gerçekleşmesine neden olmaktadır.

Donanım tabanlı saldırılar birkaç türden oluşmaktadır. Yan kanal saldırıları, önbellek tabanlı saldırılar, flush + yeniden yükleme saldırıları, çekiç saldırıları ve donanım tehdit saldırılarıdır[37, 91].

Bulut bilişimde hizmet olarak altyapı katmanında bilgisayarlar, sanal makineler, uygulamalar ve kaynaklar bulunmaktadır. Yan kanal saldırıları genel olarak bu katmanda devreye giren saldırılardır. Saldırgan bulut sistemin içerisindeki sanal makine içerisine bir şekilde kendisini sokar. Daha sonra bu sanal makine yardımıyla sistemdeki gizli bilgilere erişmeye çalışır.

Bulut bilişim sistemlerinde hassas verilerin neden çok iyi bir kriptografik algoritmayla korunması gerektiğinin önemi bu tür bir atakta vurgulanması gereken bir noktadır. Yapılacak şifreleme sayesinde yan kanal atak saldırısı başarılı olsa bile verilerin şifreli bir şekilde tutulmasıyla saldırgan istediklerini elde edemeyecektir.

Yukarıda da bahsedildiği gibi hassas verilerin şifreli bir şekilde depolanarak ve şifreli kanallar aracılığıyla iletilerek yetkisiz erişime tedbir alınabilmektedir. Fakat hassas verilerin şifresinin çözülmesi bazı yerlerde bir zorunluluktur. Saldırganlar, bellek veri yolu, disk veri yolu ve şifresi çözülmüş verileri ve AES, DES, RSA gibi iyi bilinen algoritmaların kriptografik anahtarlarını bulabilecekleri veri ve önbellekleri gibi fiziksel kaynaklara erişim elde etmek için sanal makine örneklerinden veya çok kiracılı ortamdan yararlanabilmektedir. Önbellek tabanlı saldırı, hiper yönetici katmanı tarafından sağlanan izolasyondan sıyrılır ve iki tür kötü niyetli aktör tarafından başlatılabilir Bunlar sistemin içerisinde var olan sistemdeki ayrıcalıklarını kötü niyetli bir şekilde kullanan bulut çalışanları veya kötü niyetli müşterilerdir.

Bulut bilişimde rakip bulut sağlayıcısı sanal ortamlarda bulunan kaynak paylaşımı özelliklerinden yararlanarak hiper yöneticide sanal makinelere karşı flush + yeniden yükle saldırısında bulunabilmektedir. Ayrıca bellek denetleyicilerinin de zamanlama kanalları olarak bellek parazitlerinden yararlanabilecek Flush + Yeniden Yükleme Saldırılarına karşı zafiyetleri bulunmaktadır. Bu tür saldırılarda truva atı ve casuslar İşlemci Dalı Tahmin Birimlerini(Processor Branch Prediction Units) tehlikeye atmak için kullanılmaktadır.

Bir (DDR) bellek bankasının belirli bir satırı, DRAM yenileme aralığı içinde sürekli olarak etkinleştirilir ve önceden şarj edilirse, fiziksel olarak bitişik DRAM satırlarında yanlış bir değere bir veya daha fazla bit çevirme gerçekleşir. Buna rowhammer saldırısı denmektedir.

Bir saldırgan, Rowhammer saldırılarını kullanarak bir bilgi işlem cihazının DRAM'ini tehlikeye atabilir. Geleneksel güvenlik yazılımı kullanılarak dağıtılan savunma mekanizmalarından ve bellek bozulması saldırısını yapmak için genelde bellek yalıtımı gibi özelliklerden kaçınılmasıyla gerçekleştirilir. Bu saldırı sonucunda sistem belleğinin kirlenmesi, hassas verilere erişim hatta sistemin kontrolünün saldırganın eline geçmesi gibi tehlikeli durumlarla karşılaşılabilmektedir.

Bu saldırıların hafifletilmesi adına aşağıdaki tedbirler alınmalıdır. Bunlar aşağıda sıralanmıştır.

- Sistemde güçlü kriptografik algoritmalar kullanılmalıdır.

- Bilgi işlem, depolama ve ağ güvenliği uygulama ve izlemesini içeren savunma stratejisi kullanılmalıdır.

- Bulut sağlayıcıların aynı bulutta çalışan diğer kiracıların işlemlerinin etkilenmemesi adına sağlam bölümlendirme dağıtımı yapması gerekmektedir. Böylece kiracılar birbirlerinin verilerine veya ağ trafiğine erişim sağlayamayacaktır.

- Veri yedekleme yapılmalıdır.

- Kimlik yönetimi mekanizmaları kullanılmalıdır.

- Erişim kontrollerinin sağlanması gerekmektedir.

- Önbelleği bölümleme ve bölüm kilitli önbellek (PLC) kullanılmalıdır. Bu sayede önbelleğin bir kısmı yalnızca korumalı bir süre içerisinde tahsis edilerek bilgi sızıntısı önlenmiş olur.

- Önbellek ısıtması(cache warming) yapılmalıdır.

- Önbellek S-Box erişimleri kapatılmalıdır.

- Arama tablolarından kaçınılmalıdır.

3.1.3.2 Hipervizör Tabanlı Saldırılara Çözümler

Hipervizör, bulut sistemlerinde sanal makineleri yönetmekten sorumlu olan sanal makine monitörüdür. Hiper yönetici, sanal makineler arasında kaynak paylaşımını yöneten yazılımın bir parçasıdır ve yetkisiz sanal makinelerin bulut bilişime erişmesini engelleyen bir bileşendir. Hipervizörlerin ana işlevleri, sanal makineleri oluşturmak, sonlandırmak, taşımak ve kaynakları tedarik etmektir.

Hipervizörler native ve hosted olmak üzere iki türe sahiptir. Yerel hiper yöneticide, işlemin yürütülmesi yalnızca işletim sistemi olarak ana bilgisayar sisteminin

donanımında yürütülür. Buna ek olarak kaynaklar doğrudan ana sistemle iletişim kurarak sanal makinelerin zamanlanması ve planlanması yapılır. Bu türe örnek olarak XEN ve VMWare ESX verilebilir. Hosted Hipervizörde işlemlerin yürütülmesi ana bilgisayar sisteminin işletim sistemindeki diğer işlemlere benzer niteliktedir. KVM, VMWare GSX ve Kullanıcı Modu Linux bu türün örnekleri arasında yer almaktadır[92].

Hipervizör tabanlı saldırılarda, saldırganlar hipervizörler üzerinde erişilebilirliğe ve yetkiye sahip olmasına izin veren hiper yöneticinin güvenlik açıklarından yararlanmaktadır. Ayrıca harici saldırı olarak kategorilendirilmiştir. Başlangıçta, saldırganlar belirli bir sanal makineye saldırı başlatır. Daha sonra kötü niyetli sanal makine ile hipervizör arasında takas gerçekleştirilir. Ardından, saldırganlar güvenliği ihlal edilmiş hipervizör altında çalışan tüm sanal makinelere yönelik saldırıları çoğaltma fırsatını yakalar. Sonuç olarak tüm sanal makineler, güvenliği ihlal edilmiş hipervizör altında bulunacağından yüksek etkiye maruz kalır. İşletim sistemi dosyaları saldırganlar tarafından değiştirilebilmesi veya kaldırılabilmesi örnek olrak verilebilir. Bu örnek saldırganların sanal makinenin dizin geçişinden kaynaklanan güvenlik açığı bulmasıyla sonuçlanırsa gerçekleşebilmektedir. BluePill, DKSM ve SubVirt hipervizör saldırılarının en bilinen örnekleri arasında yer almaktadır.

Bu saldırılara önlem olarak sanal güvenlik duvarı veya saldırı tespit sistemi türlerinden biri kullanılmalıdır.

Sanal güvenlik duvarı, ağ güvenlik duvarı hizmetlerinden oluşan sanallaştırılmış bir ortam olarak adlandırılır. Sanal güvenlik duvarı, sanal makineler ve dağıtılmış sanal anahtarlarla çalışan veri paketlerini izleyerek ve filtreleyerek saldırıları azaltmaktan sorumludur. Genel olarak, sanal güvenlik duvarı ağ paketlerinin hedef IP'si, protokolleri ve kaynakları, erişimlerini geçip geçmedikleri veya sonlandırdıkları denetimini yapmaktadır. Sonuç olarak, aktarılan paketler önceden belirlenmiş prosedür ve politikalara göre filtrelenip eşleştirilir. Daha sonra kabul veya ret işlemi yapılır. Ayrıca sistemler arası aktarım sırasında sanal güvenlik duvarı, sanal makine üzerinde güvenlik ilkeleri uygulayacaktır. Bu nedenle, sanal güvenlik duvarı, sanal makine ile nakledilebilecek bir güvenlik politikası uygulayabilir. Ayrıca, daha düşük tedarik maliyetlerini elde etmek için, belirli donanım dağıtımı gereksinimi sanal güvenlik duvarı sayesinde gerekmemektedir.

Güvenlik duvarı, kötü niyetli saldırıları tespit etmeyi ve bulut bilişimin güvenliğini korumayı garanti etmemektedir. Çoğu saldırı tespit sistemine güvenlik cihazları denir ve bu kötü niyetli saldırıları izlemek ve kontrol etmek için makine öğrenimi kavramını kullanırlar. Ayrıca, makine öğrenimi metodolojileri kullanan saldırı tespit sistemlerinin tekli öğrenme metodolojisine kıyasla daha verimli olduğunu kanıtlanmıştır. Genellikle izinsiz giriş tespit sistemi, anormallik ya da imza tespiti veya her ikisini içermektedir. Anormallik tespiti konusu ele alındığında saldırı tespit sistemlerinin bulut bilişimdeki ağ trafiğinin davranış modeli aracılığıyla kötü niyetli faaliyetleri tanımlamakta ve denetlemektedir.

Birçok saldırı tespit sistemi bulunmaktadır. Bunlar saldırı tespit ve önleme sistemi (IDPS), ağ tabanlı saldırı tespit sistemi (NIDS), ana bilgisayar tabanlı saldırı tespit sistemi (HIDS), Hipervizör Tabanlı saldırı tespit sistemi ve (VMHIDS)sanal makine hipervizör tabanlı saldırı tespit sistemidir. Hipervizör tabanlı saldırılara önlem olarak yukarıda anlatılan yöntemlerin en kuvvetlisi sanal makine hipervizör tabanlı saldırı tespit sistemidir. Diğer yöntemler bulut bilişimde diğer saldırılar için daha uygun olabilmektedir. Sanal makine hipervizör saldırı tespit sisteminde hipervizör tabanlı IDS sisteminden farklı olarak, şüpheli olmayan saldırıların daha doğru bir şekilde tespit edilmesini sağlamak için hipervizöre ve sanal makinelerine yerleştirilir. Bu yöntem, hipervizörleri ve sanal makineleri bulutun içinden veya dışından gelen saldırılara karşı koruyabilir.

3.1.3.3 Bulut Denetim Çözümleri

Bulut bilişim sistemlerinde güvenlik için denetim, bir kurumun politikalarını, operasyonlarını, uygulamalarını ve teknik kontrollerini değerlendirmeyi ve uyumluluk, tespit, güçlendirme ve adli tıplarını değerlendirmeyi amaçlar. Düzenli güvenlik denetimleri çok önemli bir çözümdür ve bu bu yüzden, bir bulut müşterisinin önemli varlıklarını korumada güvenlik kontrollerinin, süreçlerinin, prosedürlerinin ve operasyonlarının yeterliliğini ve uygulanabilirliğini değerlendirmek için hem olaylar meydana geldiğinde reaktif denetimlere hem de yürütülen proaktif denetimlere ihtiyaç duyulmaktadır[37].

Bulut bilişimde bir güvenlik denetimi için iki önemli konu mevcuttur. İlk başta, bulut hizmeti sağlayıcılarının, bulut müşterilerine uyguladığı güvenlik denetim prosedürlerini

şeffaf bir noktaya getirmesi gerekmektedir. İkinci olarak, kullanılan güvenlik kapsamının büyüklüğü, bulut hizmeti sağlayıcısının denetlediği bir dizi çeşitli ve geniş kapsamlı bilgi varlığını göz önünde bulundurarak yasal, düzenleyici ve sertifika talepleriyle uyumlu olmalıdır[37].

Bulut bilişim sistemlerinde denetim yapılırken birçok önemli engel bulunmaktadır. Bunlar operasyonel esneklik, tedarikçi yönetimi, yönetim politika ve süreçleri, yasal uyumluluklardır[93].

Operasyonel esneklik, hizmeti sürdürmenin anahtarıdır. Mevzuat ve yasal gereklilikleri karşılamanın yanı sıra müşterilere hizmet sağlamak için etkin operasyonel esneklik gerekmektedir. İç denetimin, gereken esneklik düzeyini ve bulut sağlayıcısının bu gereksinimleri nasıl karşıladığı dikkate alınması gerekenlerdendir.

Tedarikçi yönetimi ve hizmetin sürdürülmesindeki rolü iç denetçilerin, işletim modelinin nasıl çalıştığını anlaması gerekmesidir. Yönetim politika ve süreçleri için kuruluş çapında bir bulut politikası oluşturulmalıdır. Diğer yandan bulut tedarikinin hem düzenleyici hem de yasal gerekliliklere uyması gerekmektedir.

3.1.3.4 Şifreleme Çözümleri

Bulut bilişimde güvenliği arttırmak için bazı gelişmiş şifreleme algoritmaları uygulanmalıdır. Bunlar kimlik tabanlı kriptografi, nitelik tabanlı kriptografi, homomorfik kriptografi çözümleridir. Bu konular bir sonraki ana bölüm olan Bulut Bilişimde Kriptografi bölümünde ayrıntılı olarak açıklanmıştır.

3.2 Veri Gizliliği ve Mahremiyet Konuları

Bulut bilişimin maliyet etkinliğinin yanı sıra, verilerin gizliliği ve mahremiyeti sağlandığında bulut hizmetlerinin kullanımının arttığı görülecektir. Yani, müşterilerin bir bulut bilişim sağlayıcısının verilerinin gizliliğini sağladığına olan inancı, bulut bilişim hizmetlerine olan güvenlerini artırır ve bu hizmetlerin kullanımında artışın görülmesini sağlar. Birbirleri arasında yakın bir ilişki olan gizlilik ve mahremiyet terimleri çok sık yanlış şekillerde kullanılmaktadırlar. Ayrıca bu iki terimi eş anlamlı olarak kabul edenler bile bulunmaktadır. Gizlilik, kişisel bilgilerin korunması veya kişisel bilgilerin kontrol edilmesi açısından tanımlanabilir. Bu nedenle, iki terimi de aslında içinde barındırmaktadır. Bir taraf, diğer tarafın hassas veya özel verilerini koruyacağına

güvenerek, veri sahibinin isteklerine karşı ifşa edilmesini önler. Bu nedenle, mahremiyet, bir bireyin bilgilerinin açıklığı üzerinde yalnızca içsel ve seçici kontrolü içerirken, gizlilik, bilgilere yetkisiz kişiler tarafından erişilmesinden koruyan dışsal güçleri içeren terim olarak nitelendirilebilir[37].

Bulut bilişim, çoklu kiracılığı ve bilgi paylaşımını gibi özellikler barındırdığından dolayı gizlilik ve mahremiyet ihlali risklerini de beraberinde getirmektedir. Kullanıcılar verilerini genel buluta koyduğunda, artık bu verilerin gizliliğini kontrol edemezler. Bu, bulut bilişimin gizlilik için ideal olmadığını gösteriyor çünkü bazı kuruluşlar kendi hizmetlerini geliştirmeyi ve verilerini gizli tutmayı tercih ediyor. İş yükleri paylaşılan altyapıya taşınırken, kullanıcıların özel bilgileri yetkisiz erişim ve ifşa riski altındadır. Kuruluşlar, verilerini ve uygulamalarını şirket içi veri merkezlerinin dışında bulunan sistemlerde depolamaktan rahatsızlık duyduklarını belirttiği yazılar ve söylemler bulunmaktadır. Bu, hassas kişisel ve şirket bilgilerini açığa çıkarabilir ve böylece verilerin depolanması veya taşınması için yasal ve düzenleyici gereklilikleri etkileyebilir[37].

Bu bölümde bulut bilişimde gizlilik ile alakalı bozuk kimlik doğrulama ve oturum yönetimi sorunları ve veri ihlalleri, konumu ve sahipliği ile ilgili problemler ve bulut bilişimde gizliliğe etki eden sanallaştırma teknolojisinin kullanımında yer alan sorunlar ve bu sorunlara getirilebilecek olası çözümlerden bahsedilecektir.

3.2.1 Saldırılar, Zafiyetler ve Tehditler

3.2.1.1 Bozuk Kimlik Doğrulama

Veri ihlalleri ve diğer saldırılar genellikle eksik kimlik doğrulama, zayıf parola ve anahtar veya eksik sertifika yönetiminden kaynaklanır. Kuruluşlar, her kullanıcı rolüne ayrı izinler verirken genellikle kimlik yönetimi sorunlarıyla karşılaşır. Daha da önemlisi, bazen bir işin içeriği değiştiğinde veya bir kullanıcı kuruluştan ayrıldığında kullanıcı erişimini kaldırmayı unuturlar. Saldırganların çalınan parolalarla oturum açmasını zorlaştıran tek seferlik parolalar, telefon tabanlı kimlik doğrulama ve akıllı kartlar gibi çok faktörlü kimlik doğrulama sistemleri bulut hizmetlerini korumaktadır[94].

Kimlik doğrulama, uygulamadaki bilgilere ve ayrıcalıklara yalnızca doğrulanmış bir kullanıcının erişebilmesini sağlamaktadır. Bir saldırgan kimlik doğrulama işlemini atladığında veya uygulamada kullanıcıyı taklit ettiğinde saldırı başarılı olmuş olur. Bu

saldırıdaki zayıflıklar, genel olarak zayıf oturum yönetimi ve zayıf kimlik bilgisi yönetimi olmak üzere iki kategoride sınıflandırılmaktadır.

Doğrulanmış oturum kimlikleri, kullanıcı kimliklerini taklit ederek ele geçirilmektedir. Bir kullanıcı ortak bir bilgisayardan oturumu kapatmayı unuttuğu zaman, başka bir kişi, daha önceki kullanıcı için oluşturulan oturum kimliğini kullanarak bu oturuma devam edebilir. Bunun sonucunda bozuk kimlik doğrulama saldırısına gerçekleşebilmektedir. Oturum kimliği web sitesi URL'sinde görünür ve URL'ye kablolu veya kablosuz bir ağ üzerinden erişen saldırgan, kullanıcının kimliğini taklit etmek için bunu kullanabilir. Bilgisayar korsanları, kullanıcıların şifrelenmemiş kullanıcı şifrelerini içeren bir veritabanına erişim sağlar ve genellikle şifrelerin geçerli ve işlevsel olup olmadığını belirlemek için bazı yöntemler kullanır. Bu saldırıya kimlik bilgisi doldurma saldırısı denmektedir. Parola püskürtme saldırısında, güvenli hesaplara erişmeye çalışan bir saldırgan tarafından en yaygın ve zayıf parolaları kullanarak oturumu ele geçirmeye çalışır. Kimlik avı saldırılarında saldırganlar kullanıcıların oturum açma kimlik bilgilerini açıklamalarını sağlamak için herhangi bir gerçek web uygulamasının temasına benzeyen bir web sitesine bağlantılar göndererek kimlik avı yaparlar. Bu tip saldırıların tümünü engellemek için aşağıdaki önlemlerin alınması gerekmektedir[95].

- Oturum süresinin düzenlenmesi: Web uygulaması, kullanıcının gereksinimlerinin türüne bağlı olarak belirli bir süre kullanılmadığında web oturumlarını sonlandırılmalıdır.

- Oturum yönetimini iyileştirilmesi: Web uygulaması, her başarılı kimlik doğrulamasından sonra yeni bir oturum kimliği vermelidir. Kötüye kullanımı önlemek adına bu kimlik bilgileri, oturumun sonlandırılması sonrasında geçersiz olarak nitelendirilmelidir.
- Çok faktörlü kimlik doğrulama mekanizmaları kullanılmalıdır.

- Kullanıcıların, kimlik bilgilerinin çalınmasını önlemek için özel karakterler, harfler ve sayılar içeren belirli bir uzunlukta parolaların kabul edilmesi gerekmektedir. Böylece, gerekli karmaşık ve uzunluğu bulunan parolalar kabul edilmiş olur.

- Parolaları ele geçirilen kullanıcıların hesaplarını, parolayı doğrulayıp yenisiyle değiştirene kadar kilitleyen, ihlal edilmiş bir parola koruma mekanizması

kullanılmalıdır.

- Kimlik bilgilerini kurtarma işlemi katı olmalıdır ve bu kurtarma seçeneklerinin saldırganlar tarafından kötüye kullanılmaması için birden fazla doğrulama yapılmalıdır.

- Parolalar şifrelenmiş vaziyette saklanmalıdır.

- Bulut uygulamalarında, kaba kuvvet ve kimlik bilgisi doldurma saldırılarını önlemek için belirli bir IP adresinden kullanıcının oturum açma istekleri için bir sınır belirlemelidir. Bu sınırı aşan herhangi bir kullanıcının başka bir girişimde bulunmasına izin verilmemelidir.

3.2.1.2 Veri İhlalleri

Veri ihlali, bulut kullanıcılarının hassas veya korunan verilerinin yetkisiz bir kişi tarafından görüntülenmesi, çalınması veya kullanılması durumuna verilen addır. Veri ihlallerine hırsızlık gibi çeşitli sebepler neden olmaktadır. Bulut bilişim çağında, veri ihlalleri kullanıcıların kafasında bulunan en önemli güvenlik endişelerinden biridir. Bilgi işlem tarihinde ve bulut bilişimin son dönemlerinde buna benzer birçok örneğe rastlamaktayız. Bulut bilişim, altyapı, yazılım ve platformlarla ilgili isteğe bağlı hizmetler sunan bir teknoloji olmasından kaynaklı çeşitli veri ihlallerine karşı savunmasız olabilmektedir. Güvenlik mekanizmalarına sahip olmanın güvencesi olmadıkça, veri sahipleri, verilerini genel buluta dış kaynak sağlamak için güvenlik endişelerini ifade eder. Bulut hizmeti sağlayıcıları, bulut sağlayıcılarının verilerinin korunmasını sağlamaya yönelik çalışmalar yapsa da, bulut ekosisteminde çoğu bilinen şirket için sorun yaratan veri ihlalleriyle ilgili yeterli sayıda olay yaşandığı gözlemlenmiştir[96].

Bu olaylardan bazıları CapitalOne bankası, Docker Hub ve AutoClerk vakalarıdır.

CapitalOne bankası AWS kullanan dünyadaki en büyük bankalardan biridir. Web uygulama güvenlik duvarının yanlış yapılandırılmasından yararlanan saldırganlar müşteri veri kümelerini içeren 700 klasörü sızdırmayı başarmıştır. Diğer saldırıda konteyner kullanıcıları 190 bin hesabın açığa çıkmasından epeyce etkilenmiştir. Bu saldırıda Docker, finansal olmayan kullanıcı verilerini depolayan Docker Hub veritabanlarından

birine yetkisiz erişim olduğunu açıklamıştır. Otel rezervasyon yönetim sistemi olan Autoclerk, AWS'de yüz binlerce rezervasyon yayınlayan güvenli olmayan bir Elasticsearch veritabanı için host olarak görev yapmıştır[97].

Veri ihlallerine maruz kalmamak için aşağıdaki önlemler alınmalıdır[98].

- Herhangi bir bilgisayarda çalışan tüm yazılımları ve bu tür yazılımlarda yapılan tüm değişiklikleri doğrulayan bir mekanizma işletilmelidir.

- Bulut sağlayıcısının yazılım yamalarını ve yapılandırma değişikliklerini otomatik olarak gerçekleştirilmesi, doğrulaması ve ayrıca güvenlik yamalarını proaktif bir şekilde yönetmesi gerekmektedir.

- Verilere veya uygulamalara erişim izni isteme sürecini resmi bir şekilde yapılandırılmalıdır.

- Tüm ağ etkinliğinin izlenmesi ve tüm olağan dışı etkinlikleri günlüğe kaydedilmesi gerekmektedir.

- İzinsiz giriş ve önleme sistemleri kullanılmalıdır.

- İnternete veya herhangi bir harici kullanıcıya maruz kalan tüm yazılımlardaki güvenlik açıkları için ağ düzenli olarak kontrol edilmelidir.

- Tüm hassas verilerin uçtan uca şifrelenmelidir.

- Bulut operatörlerinin iyi bir güvenliği olsa bile (fiziksel, ağ, işletim sistemi, uygulama altyapısı) uygulamaların ve bilgilerin korunması ve güvenliğinin sağlanması için şirket içinde önlem alınmalıdır. Çünkü veri ihlallerin pek çoğu içeriden yapılan saldırılardan oluşmaktadır.

- Tüm kullanıcı etkinliklerini izlenmeli, günlüğe kaydedilmeli ve anormallik tespiti yapılmalıdır.

3.2.1.3 Verilerin Konumu

Bulut bilişim sistemlerinde verilerin konumu, bir kuruluşun bulut bilişimi benimsedikten sonra karşılaştığı en yaygın uyumluluk sorunlarından biridir[37].

Yerel bilgi işlem sisteminde kuruluş, bilgi işlem ortamını, verilerin depolandığı konumu ve verileri korumak için alınan önlemlerin yapılandırmasını yapar. Ancak bulut bilişimde, bir kuruluşun verileri birden fazla fiziksel konumda yedekli olarak depolanır ve kuruluşa verilerin konumu hakkında ayrıntılı bilgi verilmez. Bu yüzden, verileri korumak için yeterli önlemlerin alınıp alınmadığını tespit etmek karmaşık bir hal alır.

Ayrıca, bulut hizmeti tüketicileri, bulut sağlayıcılarının yasal veya düzenleyici gereksinimleri karşılayıp karşılamadığından emin değildir. Bu yüzden kuruluşlar, bulut bilişim sağlayıcılarının verileri belirli yetki alanlarında depolamasını ve işlemesini ve bu yetki alanlarının gizlilik kurallarına uymasını şart koşmalıdır. Veriler, ek teknik ve yasal sorunlara neden olabilecek bir ülkenin sınırları dışında saklanabilir. Her ülkenin değişik yasa, gizlilik ve düzenleyici sistemleri bulunmaktadır. Mesela ABD'de, bir hizmet tüketicisi hakkındaki hassas veriler, şüpheli suç faaliyeti olması durumunda, yetkileri olmadan yasal makamlara sunabilmektedir. Diğer yandan Avrupa ülkelerinin çoğunda, tüketici verilerinin nispeten daha fazla korunmasını sağlayan düzenlemeler getirmiştir.

Hassas verilerin sınır ötesi geçişi ve verilerin korunması için uygulanan koruma önlemleri, ulusal ve bölgesel bir güvenlik ve gizlilik endişesi olmaya devam etmektedir. Verilerin toplandığı yargı bölgesinin yasaları, sınır ötesi veri akışlarına izin verebilir veya bunları reddedebilir. Ancak, veri toplama yasasının geçişten sonra etkili olup olmadığı konusunda sorunlar bulunmaktadır.

Bu problemlere çözüm olarak Puneet Kumar ve Harwant Singh Arri önerdiği aşağıdaki çözüm kullanılmalıdır. Önceliklendirme, kullanıcının bulutta depolanan verilerin veri konumuna ilişkin beklentilerine veya ihtiyaçlarına dayalı olmalıdır. Hangi verilerin hassas ve hassas olmadığı kullanıcı tarafından belirlenmelidir. Veri depolama sırasında kullanıcıya veri hassasiyet seviyesi kontrollerini içeren bir arayüz sağlanması ve verileri kullanıcının veri hassasiyeti isteğine göre saklanması sağlanmalıdır[99].

3.2.1.4 Verinin Sahipliği ve İçeriğin İfşa Olması

Bulut bilişimde veri sahipliği, bilgiye sahip olma ve bu bilgi üzerinde kontrol

hakkının elinde bulundurulması anlamına gelmektedir. Bu kontrol, verilere erişme, oluşturma, değiştirme, paketleme, veri türetme, satma veya kaldırma yeteneğinin yanı sıra bu hakları devretme hakkını bile içermektedir. Verilerin bulut bilişim sistemleri gibi paylaşılan kontrolünün olduğu yerlerde, bu tür verilerden kaynaklanan bir hak talebinde kimin hak sahibi olduğunu bilmek için veri sahipliğiyle ilgili farklı konuların tam olarak anlaşılması gerekmektedir.

Kişi kendi verilerine erişim sağlayamıyorsa, veri sahipliğinin aslında bir değerinin olduğundan söz edemeyiz. Örneğin, bir son kullanıcı bir bulut sağlayıcısından veri taşımak isterse, tüm kullanıcı verilerine erişime izin verdiğinden emin olmalıdır. Abonelik bulut hizmetleri genellikle son kullanıcıların kullandıkları uygulamanın işlevlerine erişmesine izin verse de, bu erişim silindiğinde verilere erişmeye devam edebilmelerini sağlamak da aynı derecede önem arz etmektedir. Bulut tüketicileri ve bulut sağlayıcıları arasındaki anlaşmalar, sözleşmenin sona ermesinden sonra bile, doğrudan veya sağlayıcı aracılığıyla veri dışa aktarma gibi özellikleri sunması gerekmektedir. Bu nedenle, mülkiyet haklarının kaybı, bir iş ortamında hissedar değerini azaltmak veya hatta tehlikeye atmakla kalmaz, aynı zamanda kuruluşun başka bir sağlayıcıya geçme isteğini ve bunu gerçekleştirmesini riske atmaktadır. Pazardaki işletmelerin rekabeti için bulut sağlayıcılarını değiştirme fırsatı ve yeteneği önemli bir etkendir.

Bulut sağlayıcılarına bağlı kalmaktan kaçınmak ve sağlayıcılar arasında geçişi sağlamak için daha düşük maliyetlerle daha iyi hizmet seviyelerini teşvik edecek işlemlerin yapılması zorunludur. Bulut tüketicilerinin bulut sağlayıcılarına sağladıkları verilere sahip olmasını sağlamak önemlidir. Bu amaca ulaşmanın bir yolu, herhangi bir resmi anlaşmada (SLA gibi) tüm mülkiyet haklarını ayrı ayrı ifşa etmek ve resmileştirmektir. [100].

3.2.1.5 Sanallaştırma Sorunları

Ana bilgisayar ve konuk sistemi arasında soyutlama katmanı oluşturma işlemine sanallaştırma denmektedir. Bu soyutlama katmanına sanal makine monitörü (VMM) veya hiper yönetici denir. Başlangıçta IBM, bu teknolojiyi, ek yükü azaltmak ve verimliliği artırmak için tek bir anasistemin birden çok eşgörünümünü çalıştırmak için geliştirdi. Sanallaştırma teknolojisi, her bulut altyapısının önemli bir parçasıdır. Ayrıca sanallaştırma sayesinde bulut altyapısı içerisinde aynı donanım üzerinde çalışan birden

çok örneği soyutlama ve izole etme gibi işlemler yapılabilmektedir. Sanallaştırma, bulut altyapısındaki kaynaklar için güvenlik sağlasa da, yine de geleneksel güvenlik sorunlarından daha yüksek güvenlik sorunlarını gündeme getirir[101].

Sanallaştırma teknolojisinin birden fazla türü bulunmaktadır. Bunlar tam, işletim sistemi katmanı, donanım katmanı, konuk işletim sistemi, uygulama ve kaynak sanallaştırmadır. Tam sanallaştırmada VMM veya hipervizör konuk ve ana işletim sistemi arasında konumlandırılmaktadır. Ana işletim sistemi, donanımla doğrudan etkileşime girmektedir. Bu sanallaştırmadaki performansa bakılırsa donanım üzerinde doğrudan çalıştırmaya kıyasla çok daha düşük seviyededir. İşletim sistemi katmanı sanallaştırma türünde, tüm konuk işletim sistemleri tek bir çekirdek görüntüsü üzerinde çalışmaktadır. Bu türde sanallaştırılan donanım değil işletim sistemidir. Tek çekirdek kullanıldığı için, işletim sistemi sanallaştırıldığından dolayı ana işletim sisteminden farklı bir işletim sistemini konuk olarak çalıştırmak mümkün olmayacaktır. Donanım katmanı sanallaştırmasında, hipervizör doğrudan donanımın üzerinde çalışmaktadır ve konuk işletim sisteminin kaynaklara erişimini kontrol etmekten sorumludur. Misafir işletim sistemi sanallaştırmasında ise diğerlerinden farklı olarak misafir işletim sistemi sanal ortam hakkında bilgilendirilmektedir. Bu sanallaştırma türünde konuk işletim sistemleri, verilen sanallaştırılmış senaryoda verimli çalışacak şekilde geliştirilmektedir. Uygulama sanallaştırma, yalnızca uygulamanın ihtiyaç duyduğu kaynakların sanallaştırıldığı küçük bir sanal ortamda yerel olarak çalışacak şekilde tasarlanmış bir sunucu uygulaması türüdür. Son olarak, kaynak sanallaştırmada, sistemin belirli kaynakları sanallaştırılır.

Bulut bilişimde sanallaştırmayla alakalı saldırılar sanal makineler arası saldırılar, sanal makine geri alma(rollback), ayak basma saldırısı, sanal makine yayılma, kaçma, atlama ve hyperjacking saldırılarıdır. Sanal makineler arası saldırıları, kötü niyetli bir sanal makine, ortak konumdaki sanal makinelere saldırmak için hiper yönetici düzeyinde izolasyondan kaçınılması sonucu gerçekleşmektedir. Hiper yöneticiler çalışma esnasında bir sanal makinenin duraklatılmasını, bellek ve işlemci görüntülerinin yakalanmasını ve sanal makine anlık görüntülerin yakalanmasını sağlayabilmektedir. Bu özellik kullanıldığında sistem sanal makineleri geri alma saldırılarına maruz kalabilmektedir. Ayak basma saldırılarında saldırganın sistemle alakalı bilgi toplaması durumunda meydana gelmektedir. Kurban platformunun güvenlik açıkları sanallaştırılmış bir ortamda çalışır. Bu bilgi sistem üzerinde kötü niyetli faaliyetler gerçekleştirmek için

kullanılabilir. Sanal makine yayılma saldırısı ise aynı ana bilgisayardaki sanal makinelerin sayısı uygun kontrol olmaksızın sürekli arttığında ve bazıları boş durumda olduğunda gerçekleşmektedir.

Hyperjacking saldırısında, saldırgan tüm sanallaştırılmış ortamı kontrol etmek için sanal makine tabanlı rootkitlerin eklenmesini sağlar. Orijinal hipervizör yerine sahte bir hipervizör enjekte eder ve onu değiştirir. Hipervizör sistemde çok büyük ayrıcalığa sahip olduğundan tespit edilmesi bir hayli zordur[102].

Sanallaştırma sorunlarının üstesinden gelmek için aşağıdaki yöntemlerin kullanılması gerekmektedir[101].

- Güvenli programlama: Bulut servis sağlayıcıları ciddi hasara neden olabileceğinden, hata ve güvenlik açıklarından kaçınmak için güvenli programlama yöntemleri kullanılmalı ve ciddi testler yapılmalıdır.

- Güvenli kimlik ve erişim yönetimi: Kimlik ve erişim yönetimi, doğru kişilerin doğru kaynaklara doğru zamanda ve doğru nedenlerle erişmesini sağlamaktadır. Böylece erişimle ilgili sıkıntılar giderilebilir.

- Ağın güvenliği: Güvenli ağ sayesinde bilgi sızıntısını, rastgele kod yürütülmesini, ağ trafiğini yönlendirilmesi ve sanal makinelerin ele geçirilmesini önlemek için gereklidir. Ağlar, SSL ve IPsec gibi güvenli iletişim kanalı kullanılarak güvence altına alınmalıdır.

- Hipervizör ve sanal makinelerin sağlamlaştırılması: Çoğu durumda, saldırganlar hipervizörlerdeki hatadan veya güvenlik açıklarından yararlanmaktadır. Bu yüzden hipervizörün güvenliğini sağlam tutmak önemlidir. En güncel yamalar derhal yüklenmeli, bunun yanında kara kutu saldırılarını önlemek için açıkta kalan terminaller için güvenlik duvarlarının ve antivirüsün uygun şekilde yapılandırılması gerekmektedir.

3.2.2 Veri Gizliliği ve Mahremiyeti Çözümleri

3.2.2.1 Kimlik Doğrulama için Çözümler

Kimlik doğrulamayla ilgili sıkıntıların giderilmesi için genel anlamda bazı çözümler bulunmaktadır. Bunlar kullanıcı merkezli kimlik yönetimi, hesap verilebilir bir sistem, güvenlik onayı biçimlendirme dili(SAML), tekli oturum açma ve çok faktörlü kimlik doğrulamadır[37].

Kullanıcı merkezli kimlik yönetimi çözümünde bulut kullanıcılarının tanımlanmasına ve bu işlemin gerçekleşmesi için tanımlayıcılar ve öznitelik gibi belirleyiciler kullanılmaktadır. Bu yaklaşım hem bireysel hem de kurumsal bulut kullanıcıları için dijital kimliklerini kontrol etmelerini sağlar. Bunun yanı sıra, bulut sağlayıcının kullanıcı merkezli kimlik yönetimi ile ilgili karmaşıklıkları ortadan kaldırarak hizmete odaklanmalarını sağlar. Kullanıcıların farklı yerlerden bulut sağlayıcı tarafından sağlanan hizmetlere erişimi göz önünde bulundurulduğunda kullanıcıların dijital kimliklerini çeşitli dijital cihazlara aktarabilmeleri ve güvenli bir şekilde aktarabilmeleri gerekliliği bulunmaktadır ve belli öneme sahiptir. Ayrıca, kullanıcı merkezli kimlik yönetimi, bulut sisteminin kullanıcıların kimlik bilgisi bağlamının anlamını düzgün bir şekilde sürdürebileceğini, zaman zaman kullanıcıları belirli durumlarda kullanıcılar tarafından sunulan taleplere hızlı ve düzgün cevaplar sunulması açısından epey özellik sağlamaktadır.

Sistem içerisinde hizmetin yanlış kullanımı ve belirli faaliyetlerden sorumlu bileşeni ifşa etmesi için hesap verilebilir bir sistemin sağlanması gerekmektedir. Hizmet veren bulut sistemi tüm faaliyetlerin inkar edilemez kanıtlarını yaratmalıdır. Ayrıca suçlu olmayan tarafın kendisinin suçlanması durumunda savunabilme mekanizması sağlanmalıdır.

Diğer yandan güvenlik onayı biçimlendirme dili (SAML), bir kimlik sağlayıcının kullanıcıların kimliğini doğrulamasına ve bundan sonra kimlik doğrulama belirtecini servis sağlayıcı olarak bilinen başka bir uygulama yazılımına iletmesine olanak tanıyan açık bir standardın adıdır. SAML sayesinde kendisinin iki temel işlevi olan doğrulama ve yetkilendirme işlevleri yerine getirilir. SAML sayesinde parolalar gibi birden çok

konumda birden çok kimlik doğrulama bilgilerini koruma ihtiyacını giderilmiş olur. En önemli özellikleri kimlik hırsızlığı fırsatlarını ortadan kaldıran ek kimlik bilgilerini ortadan kaldırarak güvenliği arttırması, bir kullanıcının bu kullanıcı adı oturum açma formlarından birini kullanarak İnternet üzerinden kaç kez oturum açması gerektiğini ortadan kaldırarak kimlik avı fırsatlarını ortadan kaldırması, kullanım engellerini ortadan kaldırarak uygulama erişimini artırması, ve bu yinelenen kimlik bilgilerini ortadan kaldırarak ve ayrıca bu kaybolan parolaları sıfırlamak için tüm bu ekstra yardım masası çağrılarını ortadan kaldırarak yönetim süresini ve maliyetlerini ortadan kaldırmaktır.

Tekli oturum açma(SSO), kullanıcının kimlik bilgilerini doğrulamaya gerek kalmadan çeşitli hizmetlere erişmek için yalnızca bir kez kimlik doğrulamanın yapıldığı süreçtir. Tekli oturum açmanın dağıtımının ardından, kimlik bilgileri için yinelenen istekler kaldırıldığından, kullanıcının çalışma işlemleri çok daha basit hale gelir. Bu nedenle, bir istemcinin yalnızca bir oturum açması gerekmekye ve her istemcinin ilgilenmesi gereken yalnızca bir kullanıcı adı-şifre çifti bulunmaktadır. Bu verilen hizmetin verimliliğini arttırır. [103].

İki faktörlü kimlik doğrulama yalnızca bir parola ve kullanıcı adı değil, aynı zamanda yalnızca uygun olan başka bir belirteç gerektiren çok faktörlü kimlik doğrulamanın en basit şeklidir. Bu, potansiyel saldırganların kimlik doğrulama alt sistemini atlamasını veya aldatmasını zorlaştırır. İki faktörlü kimlik doğrulamanın kullanılması, İnternette kimlik hırsızlığı ve e-posta kimlik avı vakalarının sayısını azaltmaya yardımcı olabilir. Çünkü suçluların sadece kullanıcı adı ve şifre detaylarına detaylarına değil bundan çok daha fazlasına ihtiyaçları bulunmaktadır. Örneğin kurumun bir mail uygulamasında bir kullanıcıya yapılan saldırı sonucu mail kullanıcı adı ve parolanın çalındığını varsaydığımızda, saldırgan kurban kullanıcının mail hesabına girmesi mümkün olmayacaktır. Bunun nedeni hesaba erişmek için kullanılan belirtecin de ele geçirilmesi gerekmektedir.

3.2.2.2 Güven Yönetimi Çözümleri

Güvenin tanımından başlayacak olursak, güven güvenilen varlığın veya sağlanan hizmetin dürüstlüğüne, doğruluğuna, güvenine, verimliliğine, güvenilirliğine, mahremiyetinin korunması gibi birçok bileşenin bir araya gelmesiyle oluşmaktadır. Bazı araştırmalar, sistem güvenini, varlıkların tanımlanması, bilgi gizliliği, veri bütünlüğü,

yetkisiz erişimin önlenmesi, ürün kalitesi ve güvenilirliği, hizmet kullanılabilirliği ve güvenilirliği, altyapı güvenliği, işlem tahmini süresi, kritik durumlarda risk yönetimi gibi özelliklerin sağlanması temeline dayandırmaktadır. Güven, günümüzde özellikle bulut uygulamalarının seçimini yaparken önemli bir rol üstlenmektedir. Açıkçası, bir varlığa güven varsa, belirli hizmetlere daha fazla erişim için yetki verilmesinde sakıncalar azalmış olur. Güvensizlik ise bir varlığın güvenilir, emniyetli ve güvenilir bir şekilde hareket etme yetkinliğindeki yer alan eksiklik olarak tanımlanmaktadır. Bulut bilişimde güveni birkaç türe ayırabiliriz. Bunlar altyapı, yetkilendirme, hizmet sağlama, varlık sertifikası ve varlık kaynaklarıdır[104].

Altyapı güveni için bulut sağlayıcılarının, iş istasyonları, yerel alan ağı ve yerel sunucular gibi güvenli ve korumalı altyapıyı sağlaması gerekmektedir. Bu şekilde, sistemin altyapısını korumak için güvenlik protokollerini ve diğer koruyucu önlemleri kullanmasını sağlanabilir. Yetkilendirme için bulut sağlayıcılarının, kaynak paylaşımı veya sunulan hizmetler ile ilgili olarak kendi adına kararlar alması için başka bir bulut kuruluşuna güvenmesi gerekebilir. Hizmet sağlama için ise bulut kullanıcılarının bulut sağlayıcılarının, bulut kullanıcıları kaynaklarına erişmek zorunda kalmadan bir hizmet sunmasını ummaktadırlar. Varlık sertifikası türü için üçüncü bir taraf, bu varlığın güvenilirliğine dayalı olarak bir bulut varlığına sertifika sağlayarak işlemi başarıyla gerçekleştirebilir. Varlık kaynaklarında bulut kullanıcıları, bulut sağlayıcılarının sahip olduğu veya kendi kontrolü altındaki kaynakları kullanmasını beklemektedir[104].

Bir bulut sisteminde güven yönetimi sağlamak adına birçok zorluklar bulunmaktadır. İlk olarak güven yönetim sisteminin, bulut hizmeti sağlayıcılarını hizmetlerini ve bulut hizmeti tüketicilerini değerlendirmek, geri bildirimlerini sağlamlaştırmak adına verimli bir şekilde tanımlama yapılması gerekmektedir. Bulut ortamındaki kullanıcıların özel bilgilerinin güvenli bir şekilde saklanması gerekmektedir. Bir saldırının nereden kaynaklandığını tespit etmek bulut ortamının dinamik ve dağıtık yapısı dolayısıyla gereklidir. Ayrıca bulut hizmetinin ne ölçüde ve hangi koşullar altında güvenilir olabileceği belirlenmelidir. Bulut hizmeti sağlayıcıları tarafından dağıtılan yazılım, bileşenlerin sayısını artırarak veya azaltarak ve bilgi işlem kaynaklarını genişleterek veya serbest bırakarak iş yükündeki değişikliklere uyum sağlayabilmelidir. Bu nedenle, ölçeklenebilirlik garanti edilmelidir. Bulut tüketicileri ve sağlayıcıları başlangıçta herhangi bir deneyim olmadan etkileşime girebilir. Her ikisi de alt bulut altyapısını

anlamayabilir. Bu nedenle şeffaf yapılar üzerinde hareket etmelidir. Ayrıca geri bildirim toplamak bulut kaynakları, hizmet sağlayıcılar ve tüketiciler farklı konumlarda yer almasından dolayı ayrı bir zorluktur. Hizmet düzeyi anlaşmaları (SLA'lar), karmaşık bulut ortamlarının tüm yönlerini kapsayamaz. SLA'nın belirsiz ifadeleri ve belirsiz özellikleri genellikle bulut hizmeti tüketicilerinin güvenilir ve uygun bulut hizmetlerini kolayca tanımlamasını engeller [104].

Ayrıca politika tabanlı güven yönetimi, öneri tabanlı güven yönetimi, itibar tabanlı güven yönetimi ve tahmin tabanlı güven yönetimi gibi bazı teknikler kullanılarak bulut ekosistemi içerisinde güven yönetiminin sağlanabilir.

Diğer yandan bulut sistemlerinde güvenin ölçülmesi için bazı kriterlere göre bir değerlendirme yapılmalıdır. Bu kriterler veri bütünlüğü, güvenlik, gizlilik, güvenilirlik, dönüş verimliliği, kullanılabilirlik, inanılabilirlik, uyarlanabilirlik, hizmet düzeyi sözleşmeleri, müşteri desteği ve kullanıcı geri bildirimleridir.

Son olarak güven yönetimin sağladığı avantajların yanı sıra getirdiği bazı dezavantajlar da bulunmaktadır. Bu sistemin bulut sistemine entegre edilmesi halinde sistemin aşağıdaki saldırılara maruz kalabileceği unutulmamalıdır[104].

- Hizmet reddi saldırıları
- Kötü amaçlı hizmet sağlayıcı saldırıları
- Veri kaybı
- Trafiğin ele geçirilmesi
- Güvenli olmayan API
- Kötü niyetli kişilerin içeriden saldırıları
- Hizmetin kötüye kullanımı
- Yan kanal saldırıları
- Kimlik doğrulama saldırıları
- Ortadaki adam saldırıları

3.3 İç içe Geçmiş Güvenlik ve Gizlilik Konuları

3.3.1 Saldırılar, Zafiyetler ve Tehditler

3.3.1.1 Paylaşılmış Ortamların Ele Geçirilmesi

Bulut bilişim en önemli endişelerinden biri gizliliğin sağlanmasıyla alakalıdır. Bütünlük ve gizlilik risklerine yol açan bulut bilişimde kaynakları paylaşmayı ifade eden çoklu kiracılık durumundan kaynaklanmaktadır. Çoklu kiracılık, sanallaştırma ve kaynak paylaşımını kullanarak bulut bilişimde ekonomik açıdan daha düşük faydalar sağlamak için uygulanmaktadır. Hizmet olarak yazılımda çoklu kiracılık, kaynaklara bakılmaksızın iki veya daha fazla kullanıcının bulut sağlayıcısından sağlanan aynı yazılımı veya uygulamayı kullanmasına denmektedir. Hizmet olarak platformda ise çoklu kiracılık, bir platform veya sanal makine iki veya daha fazla kullanıcı arasında paylaşıldığında meydana gelmektedir. Hizmet olarak altyapıda farklı kullanıcılara ait iki veya daha fazla sanal makine aynı kaynakları paylaşırsa çoklu kiracılık ortaya çıkmaktadır[105].

Bulut bilişim sistemleri birden çok yazılım ve donanım bileşeninden oluşmaktadır. Bir bulut mimarisinde kullanılan yazılım veya donanımı belirleyebilen rakipler, buluttaki ayrıcalıkları yükseltmek için güvenlik açıklarından yararlanabilir. Bulut sistemi içerisindeki hipervizörlerde yer alan yazılım, donanım veya konteyner platformlarındaki güvenlik açıkları, bu teknolojilerin bulut mimarilerinin güvenliğini sağlamada ve müşteri iş yüklerini izole etmede oynadığı kritik rol nedeniyle ciddi bir öneme sahiptir. Hiper yönetici güvenlik açıklarını bulmak ve kullanmak zordur ve maliyeti yüksektir, bu da gelişmiş saldırganların kullanımını sınırlar. Önde gelen bulut sağlayıcıları, hiper yönetici kodundaki güvenlik açıklarını sürekli olarak tarar ve hiper denetleyicilerini fuzz testine göndererek güvenlik açıklarını belirler ve bunları düzenler. Ayrıca bulut sağlayıcıları, herhangi bir hipervizör istismarı kanıtı için sistem günlüklerini izlemektedir. Konteynerler, sanallaştırma tarafından sağlanan soyutlama katmanı olmadan paylaşılan bir çekirdek üzerinde çalışır. Çok kiracılı ortamlarda, kapsayıcı platformundaki güvenlik açıkları, bir saldırganın aynı ana bilgisayardaki diğer kiracıların kapsayıcılarının güvenliğini aşmasına izin verebilir[106].

Paylaşılmış ortamların ele geçirilmesine yönelik bazı önlemlerin bulut sistemlerinde alınması gerekmektedir. Bazı çözümler aşağıda sıralanmıştır[107].

- Kullanıcı ve sağlayıcı arasında gidip gelen verileri korumak için şifreleme denetimlerini kullanılmalıdır.

- Çok faktörlü kimlik doğrulama mekanizmaları kullanılmalıdır.

- Ağ trafiğinin şifreli bir şekilde sağlanması gerekmektedir.

- Gerçek zamanlı uyarı sistemleri kullanılmalıdır.

- Tüketicilerin etkinlikleri günlüklerde tutulmalıdır.

- Gizlilik ve yasal risklerin yer aldığı sözleşmelerin dikkatlice taranması gerekmektedir.

- Şifreli yedeklemeler yapılmalıdır.

3.3.1.2 Doğal Afetler

Doğal afetler, insanların hayatındaki birçok yerde hasar bırakan bazen ani gerçekleşen bazen de tahmin edilebilir olaylardır. Bu olayların yaşanması ani olmasına rağmen bulut sistemlerinde bu tip olaylara karşı acil müdahale yönetimi veya daha önceden sağlanacak bazı önlemlerin alınması elzemdir. Doğal afetler genellikle elektrik hatlarında kesintiye yol açarak bulut bilişim sistemlerinin içerisindeki bazı donanım cihazlarının çalışmasını durdurur ve bulut kullanıcıların verilen hizmetlere erişmesinde sıkıntıya yol açar.

Acil durum yönetimi, bir kurumun hassas varlıklarını afet veya afetlere neden olabilecek tehlike risklerinden korumak ve kurumun planlanan yaşam süresi içinde devamlılığını sağlamak için kullanılan stratejik yönetim süreçleri ile ilgilenen disiplinler arası alan olarak tanımlanmaktadır. Doğal bir afet durumunda, kurumsal veri merkezinde mevcut iş yüklerinin sanal makine görüntüleri oluşturulabilir ve bulut veri merkezinde saklanabilir. İlki başarısız olursa, sanal makine bulutta yeniden etkinleştirilebilen bir kurtarma mekanizması görevi görecektir. Bulut altyapı sağlayıcısı kullanıcı verilerini ve bulut sunucularını birden çok veri merkezinde çoğaltmasından dolayı bulut veri

merkezine zarar verebilecek bir doğal afet durumunda kullanıcı verileri kaybolmaz.

Örneğin, Amazon ve Microsoft'un tüm dünyada on binlerce işlem birimi ve depolama ile veri merkezleri bulunmaktadır. Doğal afet sonrası elektrik kesintilerinde bu sistemleri günlerce hatta haftalarca çalıştırmak için kilometrelerce kabloları, jeneratörleri ve pilleri bulunmaktadır ve birçoğu, doğal afetlerden zarar görmeye daha az duyarlı yerlerde bulunur. Bazı hizmet sağlayıcılar, devasa beton binaların içine yer altında veri merkezleri kurarak hizmetlere ve verilere her zaman erişim sağlanması içindir[108].

Bulut sistemleri doğal afetlere karşı gereken önlemleri alsa da bazı durumlara hassas yaklaşmalıdır. Bunlar[108];

- Bulut sağlayıcı, veri gizliliği, bütünlüğü ve kullanılabilirlik bileşenleriyle alakalı görevleri üstlenmelidir. Kısacası kimlik doğrulama, iletim, işleme, depolama, kurtarma gibi işlemlerin afet sırası veya sonrası gereken tedbirlerin alınması gibi.

- Bulut sağlayıcının isteklerden veriyi nasıl koruyacağı ve üreteceği ile ilgili spesifikasyonlar hazırlanmalıdır. Bu bulut içinde birden fazla sağlayıcıyı kapsama ve diğer bulut tüketicileriyle paylaşılan sistemlerin uyumluluk ve yasal hedeflere göre etkileme durumu bulunmaktadır.

- Kullanımının coğrafi ve mantıksal konumu, gereken minimum ve maksimum seviyeler, kullanımı etkileyebilecek yasalar ve şifrelemenin veri ve tehditleri izleme ve izleme yeteneğini engelleyip engellemeyeceği dikkate alınmalıdır.

- Bulut sağlayıcı, uygun teknik, prosedürel önlemlere sahip olacak bir kriz yönetimi sürecine sahip olmalıdır. Bu, satıcı iflasları, birleşmeler, satın almalar gibi finansal krizlerin yanı sıra hava durumu, jeolojik bozulmalar, salgın hastalıklar vb. gibi geleneksel alanları içerebilir.

3.3.1.3 Kalıcı Veri Kayıpları

Kalıcı veri kayıpları, hem bulut kullanıcıları hem de sağlayıcılar üzerinde daha büyük etkilere neden olduğundan, bulut bilişimdeki ciddi tehditler arasında yer almaktadır. Kötü niyetli saldırganlar verilere erişip sildiğinde, veri sızıntısı kalıcı veri kaybına neden olur. Bulut kullanıcıları ayrıca verilerini yanlışlıkla silebilir. Bu, onların eğitimsiz davranışları

veya bulut hizmetleri ve kaynaklarının nasıl kullanılacağına ilişkin yetersiz bilgilere sahip olduğundan kaynaklanmaktadır. Veri kaybının bir diğer nedeni ise sağlayıcıların verileri yanlışlıkla yok etmesi olabilir. Ayrıca verilerin bir çalışan tarafından harici veya dâhili olarak kötü niyetli olarak silinmesi, değiştirilmesi veya bozulması da veri kaybının nedenleri arasındadır. Diğer yandan üçüncü taraf yazılımların kullanılması sonucu oluşacak bazı bozulmalar neticesinde verilerin kaybolması ihtimali de bulunmaktadır. Ayrıca, yaşanabilecek her türlü doğal afet tarzı felaketlerle altyapıda oluşacak büyük hasarlar veri kaybına neden olabilir[37].

Tüm bu nedenlerden kaynaklanacak olan veri kaybını önlemek adına bazı önlemlerin alınması veya uygulanması gerekmektedir. Bunlar[109];

- Uygulamalardaki her hesap için zor ve benzersiz parolalar oluşturulmalıdır.
- Çok faktörlü kimlik doğrulama mekanizmalarından yararlanılmalıdır.
- Hizmet sözleşmelerinin veri kaybı ile ilgili tüm ayrıntılarının dikkatle incelenmesi gerekmektedir.
- Kaynakların yedeklemelerinin alındığının bilinmesi gerekmektedir.
- Sıklıkla bulut risk değerlendirmesi yapılmalıdır.
- İşlemlerin şifreli olarak yapıldığı bulut sağlayıcılar tercih edilmelidir.

3.3.1.4 Sanal Makine Göç Saldırıları

Sanal makine göç saldırısı, sanal makinenin bir yerden başka bir yere taşınması sırasında ağa yapılan saldırıdır. Bu saldırı, sanallaştırılmış hareketliliğin kullanılmasıdır. İşletmeler sanal makineleri kullanımlarına göre ayrı ayrı yerlere taşımaya devam edeceklerdir. Bunun başlıca sebebi sanal makine imajlarının ağ üzerinden fiziksel makineler arasında rahatlıkla taşınabilmesidir. Örneğin, iptal edilen müşterilerden gelen SM'ler yedek veri merkezine taşınabilir ve bakım gerektiren SM'ler değişiklikler için test veri merkezine taşınabilir. Bu nedenle, sanal makine güvenlik çemberleri arasında ağ

üzerindeyken, bir saldırgan veri merkezine yetkisiz erişim sağlamak ve sanal makinedeki sanallaştırma güvenliğini etkisizleştirmek adına ağ güvenlik açıklarını kullanabilir. Benzer şekilde, saldırganlar, sanal makinelerin arasında gezdiği veri merkezlerine saldırılar düzenlemek için sanal makine görüntülerine kötü amaçlı kod yerleştirerek amacına ulaşabilmektedir[110].

Bu tip saldırılara önlem almak adına geçiş başlatıcısının kimliğinin doğrulanması, geçiş esnasında varlıklar arası güvenin korunması ve yapılacak göçün gizli olarak yapılması gerekmektedir.

Ayrıca canlı göç, bulut veri merkezinde çeşitli güvenlik tehditlerine yol açmaktadır. Güvenli olmayan canlı geçiş, saldırgan tarafından yararlanılabilecek güvenlik açıklarına ve tehditlere yol açabileceğinden güvenlik riskini arttırmaktadır. Canlı geçişe yönelik saldırıları birkaç türe bölebiliriz. Bunlar kontrol düzlemi, veri düzlemi ve göç modülleridir[111]. Kontrol düzleminde canlı geçişin başlatılması ve yönetilmesi gibi tüm işlemler, geçiş sürecini sızdırma saldırılarına ve yeniden yürütme saldırılarına karşı güvenceye almak için uygun kimlik doğrulaması ile sağlanmalıdır. Kimliği doğrulanmış kullanıcı dışında hiçbir kullanıcı taşıma işlemini yapmamalıdır. Bir saldırgan tarafından hedefe çok sayıda sahte geçiş başlatarak hizmet reddi saldırısı gibi birçok farklı saldırı yapılabilmektedir.

Güvensiz veri düzlemi, çeşitli aktif ve pasif saldırılara yol açabilir. Canlı geçişte olduğu gibi, işlemci durumu dâhil tüm durumlar, çekirdek detayları ana sanal makineden hedef sanal makineye aktarılır. Bu nedenle saldırganın pasif gözetleme yapması ve geçiş sırasında aktarılan gizli bilgileri alması mümkün olabilmektedir. Saldırgan ayrıca geçiş verilerinin kontrolünü ele geçirebilir ve değiştirebilir. Ortadaki adam saldırısı, verilerin bulunduğu ortamda oluşabilecek saldırılar için örnekler arasındadır. Bu tür saldırıların tespitinde “wireshark” gibi çeşitli koklama araçları kullanılmalıdır.

Göç modülü, göç ile ilgili tüm işlevlerden sorumlu bir yazılım yardımcı programıdır, geçiş modülündeki güvenlik açığı, saldırı olarak kullanılabilecek güvenlik açığının ardından sanal makinenin tehlikeye atılmasına izin verebilir.

Canlı göç saldırılarına çözüm olarak aşağıdaki işlemler uygulanmalıdır[111].

- Göç ağı izole edilmelidir.

- SSH tünelleme kullanılmalıdır.

- Güvenli sanal makine vTPM göç protokolleri kullanılarak güvenli bir göç işlemi yapılabilir. Bu protokol sayesinde kaynak ve hedef sanal makineler arası kimlik doğrulama yapılır. Daha sonra verinin bütünlüğü kontrol edilir ve şifreli bir şekilde göç işlemi sonlandırılır.

- Ağ Güvenlik Motoru Hipervizör kullanılmalıdır. Bu sayede, dış saldırılara karşı geçişi güvence altına alan ve ayrıca izinsiz giriş için ağı tespit edebilen ve böylece herhangi bir izinsiz giriş tespiti durumunda bir alarm oluşturabilen güvenlik duvarı ve IDS/IPS işlevselliği sağlayarak hipervizöre genişleme sağlar.

- Geliştirilmiş vTPM geçiş protokolleri kullanılmalıdır. Bu sayede veri transferinde güvenli bir kanal oluşturulmuş olur.

3.3.2 İç içe Geçmiş Güvenlik ve Gizlilik Çözümleri

3.3.2.1 Ağ Tabanlı Saldırılara Çözümler

Bir sanal makinenin diğerine güvenli bir şekilde bağlanmasını sağlamak için bulut sağlayıcılarının bulut altyapısındaki ve dışarıdan gelen trafiği etkili bir şekilde korumaları gerekmektedir. Kuruluşlar ve sağlayıcılar tarafından yaygın olarak kullanılan güvenlik duvarları, izinsiz giriş tespit sistemleri, virüsten koruma ağ geçidi, gelen ve giden trafiği izleme gibi teknikler ağ tabanlı saldırılara karşı başlıca çözümler olarak gözükmektedir. Bu önlemler sayesinde sistem kullanılabilirliğini, veri gizliliğini ve veri bütünlüğünü sağlanması asıl amaç olması gerekmektedir. Bulut sağlayıcılarının sunduğu sistemde kullanılabilirlik özelliğinin etkili bir şekilde tedarik etmesi için DOS ve DDOS türü saldırılardan önce, bu saldırılar sırasında ve sonrasında sağladıkları ortamın güvenli olmasını sağlamalıdır[37].

Filtreleme mekanizmaları sayesinde bazı saldırılara önlem sağlanabilmektedir. Bu filtreleme mekanizmalarının bazıları güvenlik duvarı kullanılması, paket, TCP düzeyi ve uygulama düzeyinde filtrelemedir[112].

Güvenlik duvarı, ağ saldırılarını önlemek için en yaygın kullanılan filtreleme aracıdır. Güvenlik duvarı, yerel sistem ile kötü niyetli olarak algıladığı İnternet trafiği arasında bir filtre görevi görür. Güvenlik duvarı, kötü ağ paketlerini güvenli hale getirmek için bırakarak veya değiştirerek veya günlüğe veya denetim izine kopyalayarak ele alır. Bir güvenlik duvarı veya filtre üç farklı seviyede çalışabilir: IP paketi, TCP oturum seviyesi ve uygulama seviyesi.

Paket filtreleme, güvenlik duvarının, bilinen yanlış bir IP adresinden gelen trafiğin hariç tutulduğundan emin olmak için paket adresini ve bağlantı noktası numarasını kontrol etmesi anlamındadır.

TCP düzeyinde filtrelemenin çalışma prensibi, her TCP oturumunda tüm paketleri yeniden birleştirmek ve incelemektir. DNS filtreleme için ve trafik şifreleme amacıyla sanal özel ağ (VPN) işlevleri sağlamak için kullanılabilir.

Uygulama düzeyinde filtreleme, bir veya daha fazla hizmet için proxy işlevi görür ve e-posta filtreleri ve web proxy'leri gibi bileşenler içermektedir. Uygulama düzeyinde filtreler kullanmak, kendi sıkıntılarını da beraberinde getirir. Ayrıca bu filtrelerin kullanılması durumunda özellikle yüksek bant genişliğine sahip web içeriğinde kullanıldığında daha pahalı bir hale gelir.

Ağ tabanlı saldırılara çözüm için sistemin yönetiminin de önemli bir gösterge olduğu unutulmamalıdır. İlk olarak kuruluşlar tarafından kullanılan tüm yazılımlar için yama sürümlerinin düzenli olarak izlenmesini ve yamaların yayımlanır yayınlanmaz uygulanmasını zorunlu kılan politikalar uygulanmalıdır. Daha sonra saldırı yüzeyinin azaltılması adına, bir kuruluştaki tüm bilgi işlem cihazlarından kullanılmayan veya gereksiz uygulamaların ve hizmetlerin kaldırılmasını içeren politikalar uygulanmalıdır. Ayrıca ağı bölümlere ayırmak önemli bir çözümdür. Segmentasyon, kuruluşların ağlarını korumanın en kolay yollarından biridir. Ağı bölümlere ayırmanın en büyük yararı, işletmelere bir saldırı durumunda ek olay yanıt süresi sağlamasıdır. Segmentasyon, kuruluşların hassas verilerin göreceli güvenliğini korumasını ve kritik verilere erişimi kısıtlamasını da kolaylaştırır. Son olarak varsayılan yapılandırmadan güvenli yapılandırmaya geçişin bir an evvel sağlanması gereklidir. Kuruluşlar, kural olarak, yüklü tüm yazılımların güvenlik ayarlarını periyodik olarak izlemeli ve mümkün olan en güvenli yapılandırmaya değiştirmelidir. Yeni yazılımların varsayılan ayarda uzun süre

zarfında kullanılması sonucu birinin ayarları değiştirme zahmetine girmesi durumunda kolayca önlenebilecek ihlallere yol açar[112].

Ağ tabanlı saldırılara en önemli çözümlerden biri de izinsiz giriş tespit sistemleridir. Bu sistemler güvenlik ihlali belirtileri veya gelen spam, sahte IP adreslerinden gelen paketler veya bir botnet denetleyicisiyle bağlantı kurmaya çalışan biri gibi devam eden bir saldırı için tarama yapar ve herhangi bir kötü amaçlı etkinlik olduğunda alarm verir.

Son çözüm olarak ise ağdaki yapılacak şifrelemedir. Ağ şifrelemesi veya bu konudaki herhangi bir şifreleme, verileri, onu görme yetkisi olmayan herkesten gizlemek için yapılan kodlama demektir. Şifrelenmiş verilere erişmek veya şifresini çözmek için şifre çözme anahtarını kullanabilmektedir. Ev ağları genelde WPA veya WPA2 gibi şifreleme algoritmaları ile şifrelenirken, web tarayıcıları ise Güvenli Yuva Katmanı (SSL) protokolünü kullanır. SSL'nin ile kullanılan sertifikalar ile istemci ve sunucu arasında tüm iletiler şifrelenmektedir[112].

3.3.2.2 Servis Modeli Saldırılarına Çözümler

Bulut bilişimde yer alan servis modellerini etkileyen çeşitli güvenlik ve gizlilik sorunları bulunmaktadır. Bu sorunlara yönelik denetimler, diğerlerinin yanı sıra güçlü uçtan uca şifreleme ve bir güven yönetimi organizasyonu gerektirmektedir. Yetkisiz erişimlerin engellenmesi için servis modellerinin genel bir bulutta yetkilendirme yapması gerekmektedir. Bütünlük, yüksek kullanılabilirlik gibi özellikleri bulut bilişimde sağlamak gerekmektedir. Aşağıdaki tabloda servis modellerinde yer alan bazı saldırı ve çözümleri yer almaktadır[37].

Tablo 3.1. Servis modellerinde yer alan saldırı ve çözümleri[37].

Sorun	Etkileri	Etkilenen Servis Modeli	Çözüm
Bulut bilişimin kötüye kullanımı	Doğrulama kaybı, hizmet dolandırıcılığı, tanımlanamayan kayıt nedeniyle daha güçlü saldırı	Hizmet olarak altyapı, Hizmet olarak platform	Ağ durumu gözlemlenmeli, sağlam kayıt ve kimlik doğrulama teknikleri kullanılmalı
Veri kaybı ve sızıntısı	Kişisel hassas veriler silinebilir, yok edilebilir, bozulabilir veya değiştirilebilir	Hizmet olarak altyapı, Hizmet olarak platform, Hizmet olarak yazılım	Denetim yapılandırması ve güvenlik açığı için güçlü kimlik doğrulama ve erişim kontrol mekanizmaları kullanılmalı, Veri depolama ve mekanizmaları sağlanmalı.
Farklı hizmet sunma/alma	Bulut altyapısı üzerinde kontrol kaybı	Hizmet olarak altyapı,	Sunulan hizmetler kontrol altında

modeli		Hizmet olarak platform, Hizmet olarak yazılım	tutulmalı ve izlenmeli
Güvensiz uygulama programlama arayüzü	Uygunsuz kimlik doğrulama ve yetkilendirme, içeriğin yanlış iletimi	Hizmet olarak altyapı, Hizmet olarak platform, Hizmet olarak yazılım	Ağ durumunu gözlemlenmeli, sağlam kayıt ve kimlik doğrulama tekniği kullanılmalı
İçeriden gelen saldırılar	Kuruluş kaynaklarına nüfuz eder, varlıklara zarar verir, üretkenlik kaybı, bir operasyonu etkiler	Hizmet olarak altyapı, Hizmet olarak platform, Hizmet olarak yazılım	Veri iletimi şifreli olarak yapılmalı, güçlü erişim kontrolü ve kimlik doğrulama mekanizması uygulanmalı
Hizmet/Hesap Ele Geçirme	Çalınan kullanıcı hesabı kimlik bilgileri, bulutun kritik verilerine erişerek saldırganın hizmetlerin güvenliğini tehlikeye atmasına olanak tanır.	Hizmet olarak altyapı, Hizmet olarak platform, Hizmet olarak yazılım	Güçlü kimlik doğrulama benimsenmeli
Paylaşılan Teknoloji Sorunları	Hipervizörden ödün vererek bir kullanıcı hizmetini diğer kullanıcı hizmetlerine müdahale etmesine yol açar	Hizmet olarak altyapı	Kullanım sözleşmesi raporlama ve ihlal bildirimleri, güvenlik ve yönetim süreci şeffaf bir şekilde yapılmalı

3.3.2.3 Bilgisayar adli bilişim çözümleri

Adli bilişim, bir siber suç veya dolandırıcılık faaliyetinin ardından mahkemede yasal olarak kabul edilebilir olan dijital cihazlarda yığılmış dijital gerçeklerin tanımlanmasını, çıkarılmasını, muhafaza edilmesini ve sunulmasını ifade eden terimdir. Dijital bilgi manipüle edilebildiği, kopyalanabildiği, yok edilebildiği için son derece kırılgan yapıya sahiptir. Soruşturma sırasında, bu tür verilerin herhangi bir değişikliğe uğramadığı garanti edilmesi gereklidir. Adli bilişim ile alakalı bulut bilişim sistemlerinde birçok zorluk vardır. Bulut bilişimde yapılan araştırmaların bulut modeline göre değişmesi ilk zorluktur. Örneğin, hizmet olarak yazılım ve platformda adli ekipler, güvenliği ihlal edilen sistemin günlük geçmişine anında erişim sağlayabilmekte olmasına karşın hizmet olarak altyapıda bu durum söz konusu değildir. İkinci sorun, fiziksel cihazların erişilebilirliğidir. Adli ekipler yalnızca özel bulut modellerindeki fiziksel cihazlara erişim sağlayabilmektedir. Genel bulutlarda erişim, inceleme ekibinin gereksinimlerine göre sınırlandırılmaktadır.

Üçüncü sorun ise bulut hizmeti sağlayıcısında yer almaktadır. Adli soruşturmanın başarısı, yasal, sözleşmeye dayalı veya kasıtlı olarak soruşturma ekibine suç, dolandırıcılık veya sahtekârlığın izini sürmek için fiziksel ve mantıksal erişim sağlamayı reddedebilecek sağlayıcının işbirliğine bağlı olarak değerlendirilmektedir. Dördüncü konu, incelenen kuruluşun bulutunun veya tedarikçinin bulut sisteminin tehlikeye girme olasılığıdır. İstemci tarafı bilgilerinin, kötü amaçlı komut dosyaları veya tarayıcı uzantıları gibi sosyal mühendislik teknikleri yoluyla ele geçirilebileceği keşfedilmiştir. Mahkeme tarafından kabul edilebilir veriler ihlal edildiğinde, adli işlemler daha sonra

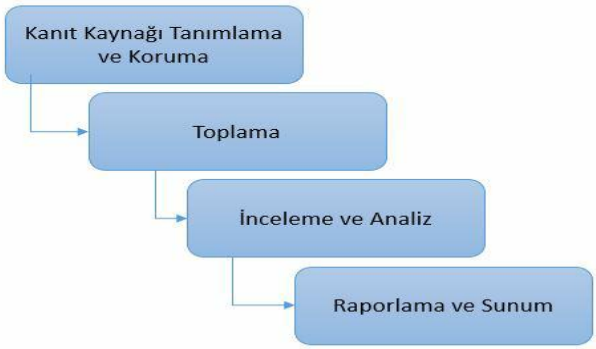
etkilenir. Bunun gibi, yetersiz fiziksel ve mantıksal güvenlik politikaları nedeniyle bulut hizmeti sağlayıcısının sitesi kesintiye uğradığında, inceleme ekiplerinin çalışmaları da kesintiye uğrayacak ve sonuçsuz kalacaktır[33].

Adli bilişim, soruşturma standartlarının verimliliğini artırmak için bulut ortamlarında bazı iş akışlarını takip eder. Bu akış aşağıdaki gibidir[113]:

- Adli tıp gereksiniminin amacını belirlenir.
- Hizmet olarak altyapı, platform ve yazılım gibi bulut hizmetleri türlerini tanımlanır.
- Kullanılan arka plan teknolojisinin türü belirlenir.

  - İstemci tarafı: kullanıcının istemci tarafındaki rolünü belirleme için canlı adli bilişim araçları aracılığıyla müşteri tarafında gerçekleştirilen faaliyetleri toplanır.
  - Sunucu tarafı: kanıtların korunması için bulut hizmeti sağlayıcı ile iletişim kurulur. Bulut hizmeti sağlayıcısından günlükler ve kanıtlar toplanır.
  - Geliştirici tarafı: geliştiriciden kanıtlar toplanır ve verilerin yüklenmesi için kullanılan araçlar tanımlanır.

Bulut bilişim sistemlerinde adli tıp, daha iyi soruşturma için bir dizi yönerge şeması takip etmektedir. Bulut depolamanın varlığını belirlemek ve verileri geri yüklemek için yinelemeli bir süreç için gerekli olan bir dizi öğretim programı kullanılabilir. Bu şema aşağıdaki gibidir[114].



Şekil3.6. Bulut bilişimde adli tıpta kullanılan yönerge şeması[114].

Kanıt kaynağı tanımlama ve koruma: Bu aşama, bir dijital adli tıp araştırmasında

kanıt kaynaklarının belirlenmesi aşamasıdır. İlk yineleme sırasında, tanımlanan kanıt kaynağı bilgisayar veya mobil cihazlar gibi her türlü fiziksel cihazlardan biri olabilir. İkinci yineleme sırasında, bu aşama dolaylı bulut hizmeti veya sağlayıcısı, bulut sağlayıcısında depolanan olası kanıtlar ve bu potansiyel kanıtın depolanması süreci ile ilgilenir. Tanımlanan kanıt kaynağından bağımsız olarak, adli araştırmacılar kanıtların uygun şekilde korunmasını sağlamalıdır.

- Toplama: Toplama: Bu aşama, verilerin fiili olarak yakalanması aşamasıdır. Adli verilerin zamanında korunması kritik öneme sahiptir ve bulut bilişim veri toplamanın zorlukları nedeniyle ikinci yinelemede meydana gelen sunucu verilerinin toplanmasıyla bir istemci cihazına el konulmasını gerekebilmektedir.
- İnceleme ve Analiz: Bu aşama, adli verilerin incelenmesi ve analizi aşamasıdır. Bu aşamada, bulut bilişim kullanımının fiziksel cihazların incelenmesi ve analizine dayalı olarak keşfedilmesi muhtemeldir ve bu, sürecin ikinci (veya daha fazla) yinelemesine sebebiyet verir.
- Raporlama ve Sunum: Bu aşama, toplanan deliller hakkında yasal bir açıklama yapmaktır. Bu aşamada, genel olarak rapor, kullanılan tüm süreçler, araçlar ve uygulamalar hakkında bilgilerin yanı sıra yanlış sonuçlardan kaçınmak için her türlü kısıtlamayı içermelidir.

3.3.2.4 Risk değerlendirme çözümleri

Güvenlik ve gizlilik sorunu vakalarının olasılıkları ve yaygınlığını belirlemede risk değerlendirme yöntemleri kullanılmalıdır. Risk değerlendirmesi, zorluk etkisinden kaçınmak veya azaltmak için tahminler ve zamanında müdahale yaptığından, bulut bilişim sistemlerinde çok büyük öneme sahiptir. Bulut sağlayıcıları, müşterinin bir hizmet sınıfı seçiminden bağımsız olarak, bir hizmet için güvenlik ve gizlilik sağlamaktan sorumlu taraf olarak bilinmektedir. Sonuç olarak, bulut hizmeti sağlayıcılarının risk değerlendirmeleri kaçınılmaz olmalıdır. Bulut hizmetlerinin sağlandığı platformun değerlendirmesini hariç tutarken geçmiş olayları inceleyen masaüstü değerlendirmesi tarafından yalnızca hizmet planı incelenir. Varlıklar, tehditler ve duyarlılıklar gibi üç bileşen genellikle bir bulut hizmetleri sağlayıcısının risk değerlendirmesine dahil edilmektedir. Riski tanımlarken "Risk = Varlık sayısı x güvenlik açığı sayısı x tehdit sayısı" denklemi kullanılmaktadır. Risk değerlendirmesi aşağıda belirtilen aşamalardan

oluşmaktadır[33]:

- Bir buluttaki ortamdaki varlıkların belirlenmesi.
- Tespit edilen varlıklarla ilgili teknik, hukuki ve işle ilgili gerekliliklerin incelenmesi.
- Belirlenen varlıkların değerlendirilmesi. Bu işlem belirlenen teknik, yasal ve ticari ihtiyaçlar ve kullanılabilirlik, mahremiyet, gizlilik ve güven ve bütünlük kaybı nedeniyle oluşan etkiler dikkate alınarak yapılmalıdır.
- Belirlenen varlıklar için olası tehdit ve hassasiyetlerin belirlenmesi.
- Tehdit ve duyarlılık olaylarının olasılığının değerlendirilmesi.
- Risklerin hesaplanması ve daha önce tanımlanan bir risk ölçeği ile karşılaştırılması.

Kuruluş bu risk değerlendirmelerini tamamladıktan sonra, güvenlik ve gizliliğe yönelik olası tehditleri önlemek için uygun şekilde yanıt vermelidir.

3.4 Bulut Depolama Güvenlik Çözümleri

Bulut depolama, verilerin internet gibi bir ağ üzerinden korunduğu, yönetildiği, yedeklendiği ve kullanıcılara sunulduğu uzak depolama sistemlerinde iletildiği ve depolandığı bir bulu bilişim hizmet modelidir. Bulut kullanıcıları genellikle bulut veri depolaması için ücretsiz depolama miktarını aştıklarında tüketim başına aylık ücret üzerinden ödeme yapmaktadır. Bulut depolama, erişilebilir, esneklik ve ölçeklenebilirlik, çoklu kullanım ve ölçülü kaynaklar gibi özellikleri içerisinde barındıran sanallaştırılmış bir depolama altyapısına bağlı çalışmaktadır. Bulut tabanlı veriler, yerel olarak veya bir üçüncü taraf bulut sağlayıcısı tarafından yönetilen bir veri merkezinde bulunan farklı ticari depolama sunucularındaki mantıksal havuzlarda depolanır. Bulut hizmeti sağlayıcısının ana görevleri buluta iletilen verilerin yönetimi güvenliğidir. Kapasiteyi artırmak veya azaltmak için bulutta isteğe bağlı depolama hizmetleri sağlanmaktadır.

Bulut depolamayı tercih eden kurumlar, kurum içi depolama altyapısını satın alma, yönetme ve sürdürme ihtiyacını ortadan kaldırarak bulut tüketicileri için önemli bir yükü kaldırmaktadır. Bulut hizmeti sağlayıcıları, farklı yerlere bulundurduğu büyük veri merkezlerinde verileri depolamaktadır. Bulut kullanıcıları bir bulut sağlayıcısından bulut depolama alanı satın aldıklarında, güvenlik, kapasite, depolama sunucuları ve bilgi işlem kaynakları, veri kullanılabilirliği ve ağ üzerinden teslimat dâhil olmak üzere veri depolamanın birçok yönünü sağlayıcıya emanet ederler. Müşteri uygulamaları, geleneksel depolama protokolleri veya internette bulunan uygulama programlama arabirimleri sayesinde depolanan bulut verilerine erişim sağlar.

Bulut bilişimde, depolamada blok, dosya ve nesne depolama olmak üzere üç tür çalışma mekanizması vardır. Blok depolama sisteminde, büyük miktarda veri blok adıyla tanımlanan daha küçük birimlere bölünür. Ardından, her blok benzersiz bir tanımlayıcıyla ilişkilendirilir ve sistemin depolama sürücülerinden birine yerleştirilir. Blok depolama sistemi hızlı ve verimli olduğundan veritabanları ve yüksek performanslı iş yükleri gibi uygulamaların gerektirdiği gecikme süresini iyi ölçüde düşürür. Dosya depolama sisteminde ise veriler hiyerarşik bir dosya ve klasör sistemi içinde düzenlenir. Bir dosya depolama sisteminde yer alan veriler dosyalarda, dosyalar ise klasörlerde saklanır. Klasörleri düzenlemek ve dosya ve verileri bulmak için dizin kullanılır. Dosya depolama tabanlı bir bulut, bu hiyerarşik formatın kullanıcılara aşina olması ve bazı uygulamalar tarafından gerekli olması ile veri erişimini ve alımını kolaylaştırabilir. Bir nesne depolama sisteminde veriler, üç bileşenden oluşan bir nesne olarak depolanır. RESTful API kullanan nesne depolama protokolü, dosyayı ve ilişkili meta verilerini tek bir nesne olarak saklar ve ona bir kimlik numarası atar. İçeriğin geri alınabilmesi için kullanıcı sisteme kimliğini gösterir ve içerik tüm metadata, kimlik doğrulama ve güvenliği ile birleştirilir. Nesne tabanlı depolama sistemleri, veri erişimini ve analizini kolaylaştırabilen meta verilerin özelleştirilmesine izin verir.

Ayrıca günümüz teknolojisi ile birlikte mevcut cihazlarda kullanıcılar her geçen gün daha fazla kişisel veri barındırmak ve saklamak istediği için bu belli başlı disk sorunlara sebep olmaktadır. Bununla birlikte cihazların ve kullandıkları uygulamaların özellikleri, kapasiteleri gittikçe artmaktadır. Tüm bu sorunlara çözüm olarak bulut depolama ortaya çıkarılmıştır. Tüm bu işlemler için, internet ortamında kullanıcılara ve tedarikçilere hard disk, USB gibi donanım cihazlarına gerek kalmadan veri saklama ve depolama kurum ve

şirketler için yazılım, altyapı ve daha birçok özellik sağlamaktadır. Tam da bu noktada düşünülmesi gereken nokta bu verilerin güvenli bir şekilde saklanması olacaktır. Bu noktada ise uygulamalar üzerinde kullanıcıların işlemleri kriptografik algoritmalara dayalı bir şekilde yapılmalıdır. Bunun ötesinde bu algoritmalar kullanılırken kullanıcıların sahip olduğu master anahtarlar bulundurulmalı ve bu anahtarlarla işlemler yürütülmelidir. Bulut depolama için kullanılabilecek birçok platformda hem yazılımsal hem de donanımsal olarak sağlanan birçok anahtar saklama teknolojisi bulunmaktadır.

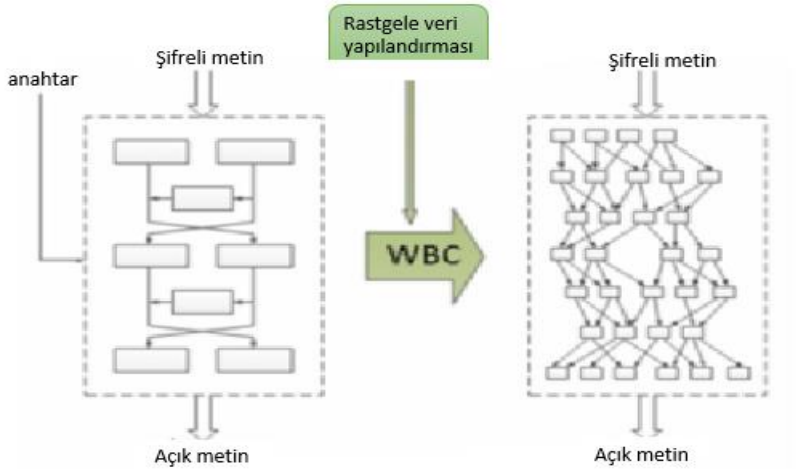
3.4.1 Windows işletim sistemi çözümleri

Windows platformlarında anahtarları saklamanın yazılımsal ve donanımsal çözümleri bulunmaktadır. Donanımsal olarak TPM mekanizması yazılımsal olarak da White-Box-Kriptografi kullanılabilir.

3.4.1.1 White-Box-Kriptografi

White-box kriptografisi, uygulama içindeki anahtarları ve kritik verileri korumak için şifreleme, şaşırtma ve matematiksel dönüşümler kullanır. Yazılım, tersine mühendislik gibi uygulama saldırılarına karşı savunmasız hale getirmek için tasarlanmıştır. Ayrıca White-Box kriptografi yazılım tarafında şifreleme algoritmaları kullanarak gizliliği sağlanması gereken anahtarların güvenliğini whitebox saldırıları yapıldığında bile sağlamaktır.

White-Box kriptografi çalışma mantığı şöyledir. İlk önce şifreleme ve şifre çözme için kullandığımız anahtarlar karartılır veya gizlenir(obfuscation). Anahtar kötü niyetli saldırgan tarafından çıkarılmasın diye anahtar sistemde gömülü bir şekilde kalır ve hafızada açık bir şekilde değil karartılmış bir şekilde tutulur. Bu işlemlerde bütün şifreleme ve şifre çözme işlemleri gözlemlenebilir fakat anahtar açığa çıkarılamaz. Bulut bilişim uygulamalarında White-Box kriptografi kullanılması sayesinde, herhangi bir donanımsal olarak güvenliği sağlayacak cihaz bulunmadığı durumlarda, yazılımsal olarak anahtarların güvenliğini sağlanabilmektedir.



Şekil 3.7. Whitebox çalışma mantığı[115].

3.4.1.2 TPM

Trusted Computing Group adlı yazılımcılar ve büyük şirketlerin de yer aldığı önemli bir grubun karar verip üretilmesinde büyük rol oynadığı donanım tabanlı güvenlik yazılımıdır. Trusted Computing Group 2003 yılında IT endüstrisinde güvenli bilişim standartları oluşturmak amacıyla kurulan bir yapılanmadır. Kritik iş verileri, ticari ve finansal güvenlik, güvenli kimlik doğrulama ve kimlik hırsızlığı başta olmak üzere güvenlik konularında standartlar oluşturmuşlardır. Bu oluşum en büyük destekçileri AMD, Cisco, Dell, HP, Huawei, IBM, Microsoft, Intel, Lenovo gibi büyük şirketlerdir. Windows işletim sistemlerinde donanımsal olarak anahtarları saklamanın en iyi yöntemlerinden biridir.

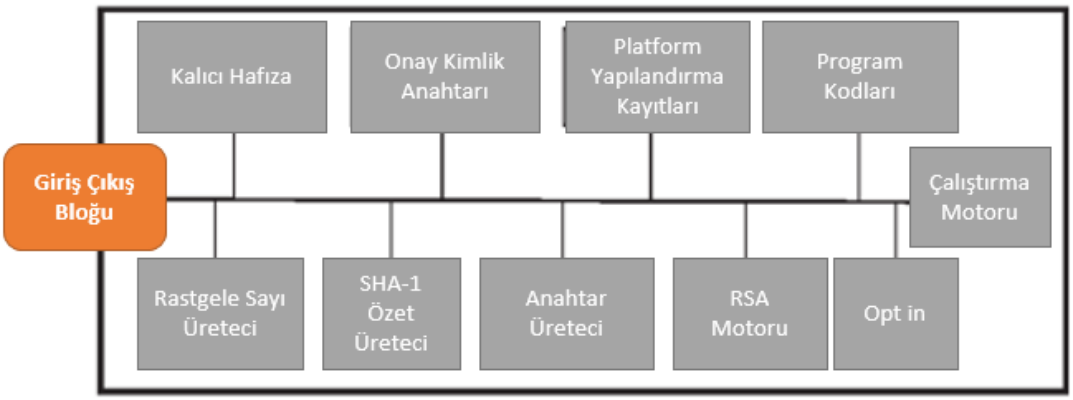
TPM'in özellikleri şunlardır;

- Güvenli Yazılım
- Kök Güvenliği (Root of Trust)
- Kurcalamaya Dayanıklı (Tamper Proof)
- Donanım seviyesinde izolasyon

TPM'in bileşenleri şunlardır;

- Rastgele sayı Üreteci
- RSA anahtar Üreteci

- Özet Fonksiyonu Matematiksel Sonuç(Hash) Üreteci
- İmzalama Motoru
- Onay Anahtarı
- Depolama Kök Anahtarı
- Platform Yapılandırma Kaydı
- Onay Tanımlama Anahtarları
- Depolama Anahtarları



Şekil 3.8. TPM bileşenleri[116].

TPM ile birlikte çalışan işletim sistemlerinde işlemcinin içinde izole bir şekilde kesinlikle fiziksel temasa korunaklı bir yer bulunmaktadır. TPM ile işlemci burada ayrı bir güvenli kanal üzerinden haberleşmeyi sağlamaktadır. TPM'in pratikteki uygulamaları şunlardır;

- Sertifika Üretimi
- Güvenli Kimlik Doğrulama
- Disk Şifreleme ve Çözme
- Anti Zararlı Yazılım

Ayrıca TMP' in 1.2 ve 2.0 olmak üzere iki adet versiyonu bulunmaktadır. TPM 2.0 Windows 8 ile beraber gelmesine rağmen TPM 1.2 versiyonu Windows 7 ile birlikte piyasaya sunulmuştur. Bu iki TPM versiyonunun destekledikleri algoritmalar aşağıdaki görseldeki gibidir.

Tablo 3.2. TPM versiyonları karşılaştırma tablosu[117].

Algoritma Tipi	Algoritma Adı	TPM 1.2	TPM 2.0
Asimetrik	RSA 1024	Evet	Evet
	RSA 2048	Evet	Evet
	ECC P256	Hayır	Evet
	ECC BN256	Hayır	Evet
Simetrik	AES 128	Evet	Evet
	AES 256	Hayır	Hayır
Özet	SHA-1	Evet	Evet
	SHA-2 256	Hayır	Evet
HMAC	SHA-1	Evet	Evet
	SHA-2 256	Hayır	Evet

3.4.2 Mac ve iPhone işletim sistemi çözümleri

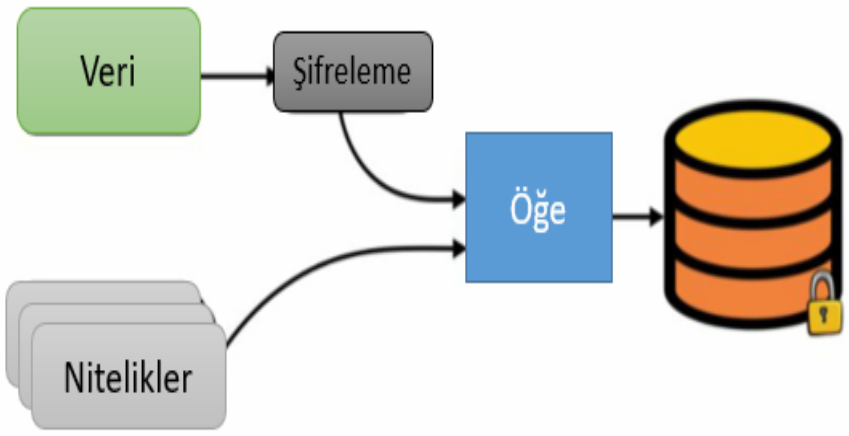
Mac ve iphone platformlarında anahtarları saklamanın yazılımsal ve donanımsal çözümleri bulunmaktadır. Donanımsal olarak Secure Enclave mekanizması varken yazılımsal olarak da Keychain mekanizması kullanılmaktadır.

3.4.2.1 Keychain

MacOS ve iOS işletim sistemlerine özel master anahtar gibi hassas verilerimizi açıkta tutmadan yazılımsal ve donanımsal olarak saklamanın olanakları bulunmaktadır[5]. Keychain' de tam da bu noktada yazılımsal olarak uygulamaların ihtiyaç duyduğu Apple şirketinin yazılımlarından biridir. Eğer kullanılan cihazda donanımsal olarak güvenlik modülü bulunmuyorsa kullanılabilecek en iyi seçenek olarak Keychain göze çarpmaktadır. Ayrıca Keychain'i daha rahat ve kolay bir şekilde kullanabilmek adına sarıcı(wrapper) yazılımlar yani Keychain'in karmaşık metotlarının fazla derinlerine inmeden kullanılabilecek kütüphaneler de mevcuttur. Bunlardan bazıları

“KeychainAccess” ve “KeychainSwift” gibi kütüphanelerdir. Bu kütüphaneler genel olarak MIT lisanslarına sahip olmaktadır ve açık kaynak olarak kullanılabilmektedir.

Keychain mekanizmasının içinde Security adında bir modül bulunmaktadır. Bu modül sayesinde Keychain içinde kriptografik anahtarlar üretebilir, bu anahtarları saklayıp getirme(retrieve) işlemleri yapmaya olanak sağlanabilmektedir. Keychain sayesinde ana anahtar gibi hassas verileri Keychain'e yükleme(store), alma(obtain or retrieve), güncelleme(update) ve silme(delete) işlemleri yapılabilmektedir. Aslında Keychain uygulamalar için veri saklamadaki gerekli tüm işlemleri sağlamaktadır. Fakat Keychain'de bunun dışında yapılabilecek başka işlemler de mevcuttur. Keychain çalışma prensibi aşağıdaki şekildeki gibidir[118].



Şekil 3.9. Keychain çalışma mantığı [118].

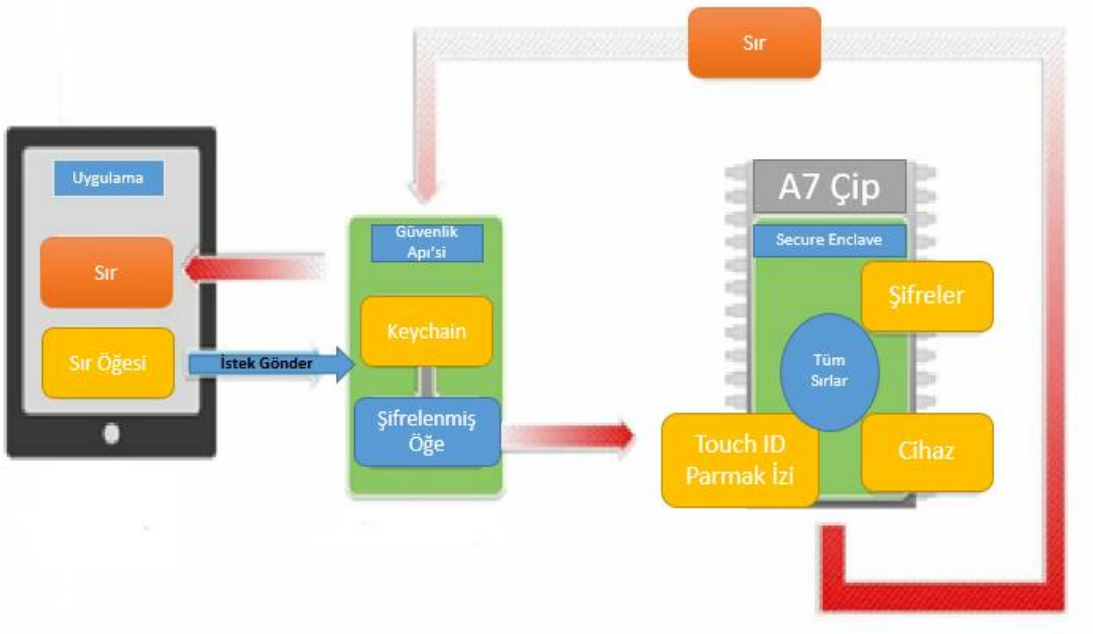
Keychain'de depolanan veriler şifrelenir ve cihazın Keychain’in belirlediği veritabanında tutulmaktadır. Bu hassas verilerin çalışan diğer uygulamalar tarafından erişilmesine olanak verilmemektedir. iOS cihazlarda, kullanıcı cihazın kilidini açtığında Keychain açılır ve cihaz kilitlendiğinde Keychain otomatik olarak kilitlenir. Böylece istenmeyen girişler engellenmiş olur. Ayrıca bir uygulama yalnızca kendi öğelerine veya ait olduğu bir grupla paylaşılanlara erişebilir ve iOS’da uygulamalar sadece bir tane Keychain'e erişimi bulunmaktadır. Diğer yandan MacOS cihazlarda bir uygulamada istenilen sayıda Keychain oluşturma imkanı bulunmaktadır. Buna ek olarak Keychain'i

direkt olarak manipule edilebilmektedir. Örneğin özel olarak sadece uygulamamız için oluşturulan ve diğer Keychain'lerin erişemeyeceği bir Keychain gibi.

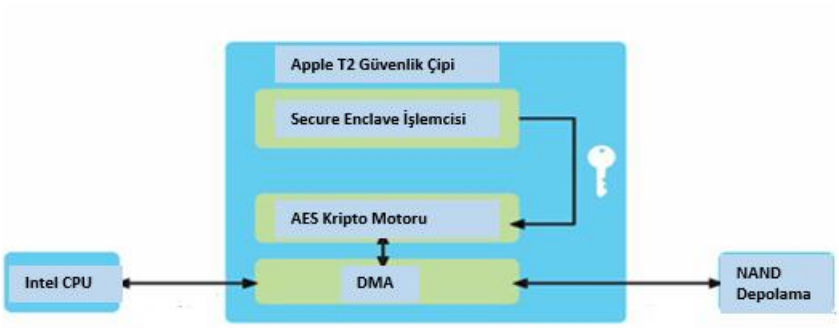
3.4.2.2 Secure enclave

Secure Enclave, ekstra bir güvenlik katmanı daha oluşturma amacıyla oluşturulmuş cihazlardaki ana işlemciden ayrık durumda bulunan donanım tabanlı bir anahtar yöneticisi ile idare edilebilen güvenli bir yardımcı işlemcidir.

MacOS ve iOS sistemlerinde özel, gizli anahtar gibi hassas verilerimizi açıkta tutmadan saklamanın yazılımsal ve donanımsal olarak olanakları bulunmaktadır. Secure Enclave'de tam da bu noktada donanımsal olarak uygulamaların işine yarayabilecek Apple şirketi tarafından geliştirilmiş güvenlik modüllerinden biridir. Secure Enclave yukarıda bahsedildiği gibi ana işlemciden izole edilmiş durumda olduğundan dolayı fazladan güvenlik katmanı sağlamaktadır. Saklanan ana anahtarlar hiçbir şekilde elde edilemez ve kullanılamaz şekilde üretilmiştir. Ayrıca Secure Enclave anahtar oluşturmak ve bu oluşturulan anahtarlar ile bazı işlemler yapmak için de kullanılabilir. Secure Enclave kullanan uygulamalar yapılan şifrelenmiş metin ve kriptografik imza doğrulaması sonucu gibi işlemler sonucunda çıkan sonuca erişebilmektedir. Böylelikle içerideki özel anahtara ait hiçbir veriye ulaşılamamış olunmaktadır.



Şekil 3.10. Secure Enclave iOS çalışma mantığı [120].



Şekil 3.11. Secure Enclave MacOS çalışma mantığı [121].

Temel veriler diskte şifrelenir ve yalnızca uygulamalara veya yetkilendirilen uygulamalara erişilebilir. Secure Enclave kullanmak için bazı kısıtlamalar bulunmaktadır[8].

- iOS cihazlar için sadece A7 ve bundan sonraki A-serisi işlemcisi bulunan cihazlarda bulunmaktadır.

- MacOs cihazlar için sadece Touch Bar ve Touch ID bulunan cihazlarda bulunmaktadır.

- Sadece 256 bitlik eliptic curve özel anahtarlarını tutmaktadır.

- Ayrıca sadece kriptografik imza oluşturmak, kriptografik imzaları doğrulamak ve eliptik curve Diffie-Hellman anahtar değişimi için kullanılmaktadır.,

3.4.3 Android işletim sistemi çözümleri

3.4.3.1 Keystore

Android Keystore sistemi, Android cihazdan çıkarılmasını daha zor hale getirmek için uygulamaların ve geliştiricilerin KeyChain API arayıcılığıyla uygulamalarda master anahtar gibi şifreleme anahtarlarını güvenle saklamasına izin veren bir yazılımdır. Android Keystore kullanmak için, standart KeyStore API'lerinin yanı sıra "KeyPairGenerator" veya "KeyGenerator" gibi sınıflar da kullanmaya ihtiyaç duyulmaktadır[119].

Android sistemlerde anahtar saklamanın zorlukları elbette diğer yazılımlarda da olduğu gibi mevcuttur. Bazı tehdit modelleri bulunmaktadır. Bunlar[120];

A. Cihazda herhangi bir kök izni olmayan başka bir üçüncü taraf uygulaması (Third party application).
B. Bir aygıtı fiziksel olarak ele geçirdikten sonra bilgilere erişen kötü niyetli hacker. Bu tehdit modelinde kötü niyetli taraf aygıta ele geçirir ve aygıttaki bellek veya diğer hassas verileri boşaltabilir.
C. Kötü niyetli kişi veya cihazda çekirdek düzeyinde kök erişim haklarına sahip uygulama.

Android KeyStore sistemi ilk olarak Android 4.0 (Ice Cream Sandwich) sürümünde piyasaya konulmuş, ancak kullanıcı için çok fazla esnek bir yapı sunulmamıştır. Ayrıca Android Keystore yazılım uygulaması yukarıdaki sadece A şıkkındaki tehdit modeline karşı savunma sağlayabilmektedir. Anahtarlar, Keystore'un içine girdikten sonra, dışa

aktarılamayan bir mekanizma sunar[121]. Bu anahtarlar şifreleme işlemleri için güvenle kullanılabilmektedir. Ayrıca, anahtar kullanımı için kullanıcılara kimlik doğrulama zorunluluğu ya da anahtarların yalnızca belirli kriptografik modlarda kullanılmasına kısıtlama getirme gibi anahtarların ne zaman ve nasıl kullanılacağını kısıtlamaya olanak sağlamaktadır.

Ayrıca Android Keystore kullanılarak RSA ve AES anahtarları üretilebilir. KeyStore kullanılarak oluşturulan anahtarlar, Android Keystore dışında kullanılamamaktadır. Uygulamalar yalnızca bu anahtarlara yapılan referanslarla çalışır. Android Keystore tarafından kriptografik işlemler gerçekleştirilebilmektedir. Yalnızca bir yazılım uygulaması olmasından dolayı Android işletim sisteminin kendisinde yerleşik olduğundan, yalnızca uygun uygulamanın temel malzemeye, yani uygulamaya erişebilmesini sağlamak için süreç ayırma ve erişim kontrolünü kullanır veya aynı UUID'ye sahip olan herhangi bir başka uygulama anahtarları ilk başta oluşturup depolamaktadır.

Keystore'un sağladığı özellikler şunlardır;

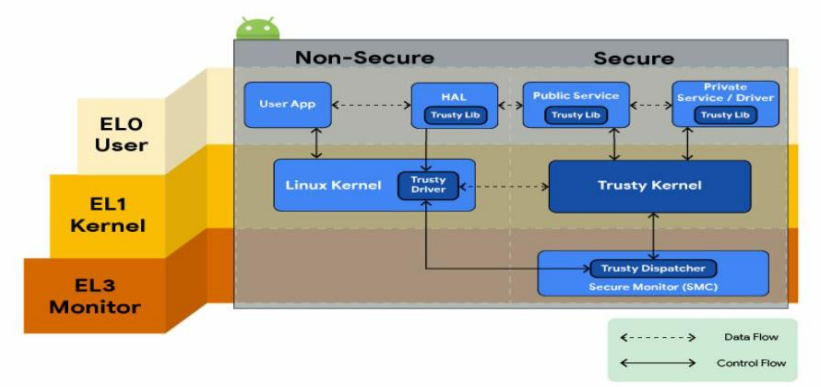
- Kriptografik anahtarları saklama (özel (private), genel (public) anahtarlar)
- Depolanan anahtarları kullanarak kriptografik işlemleri gerçekleştirme (şifreleme, şifre çözme, imzalama, doğrulama vb.)

3.4.3.2 Hardware backed store

Android KeyStore sadece yazılımsal bir uygulama olduğundan dolayı yukarıdaki tehdit modellerinden sadece A şıkkına bir koruma sağlamaktadır. Tehdit modeli B ve C'ye de koruma sağlamak açısından TEE (Trusted Execution Environment) diye genel ifadeyle adlandırılan Hardware Backed Keystore tasarlanıp üretilmiştir.

Hardware Backed Keystore donanım tabanlı bir yazılım olduğundan dolayı tehdit modellerinin hepsine karşı koruma sağlamaktadır[119]. TEE (Trusted Execution Environment) çalıştırılan kodun ve erişimi olan hassas verilerin gizlilik ve bütünlüğü ilkeleri açısından izole bir şekilde korunduğu bir ortamdır. Çevremizdeki birçok cihaz akıllı telefonlar video oyun konsolları ve akıllı televizyonlar da dâhil olmak üzere birçok kullanım alanı mevcuttur. Bu sistemin kullanılmasındaki asıl amaç şifreleme anahtarlarını

ve hassas verileri güvenle donanım tabanlı işlemcilerde saklamak ve anahtar çiftleri üretmektir. Android cihazlardaki Hardware Backed Keystore implementasyonu TEE arayıcılığıyla sağlanmaktadır.

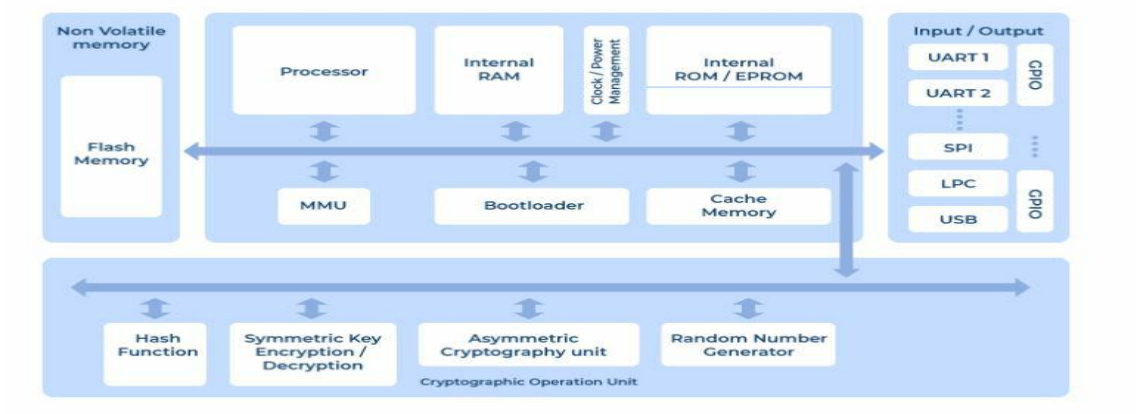


Şekil 3.12. TEE çalışma mantığı [120].

Yukarıdaki TEE çalışma mantığı görselinden anlaşılacağı üzere, TEE çekirdeği Android işletim sisteminden nasıl tamamen ayrıldığı gözükmektedir. TEE ile iletişim Trusty lib adındaki API üzerinden yapılmaktadır. Şifreleme anahtarları, TEE çekirdeğinde üretilir, depolanır ve yalnızca TEE çekirdeğinde düz metin olarak yaşamını sürdürür. Bir geliştirici, kriptografik bir işlem yapacağı zaman, bu işlemi TEE'ye aktaracak olan KeyStore API'yi kullanmaktadır. Hassas veriyi şifrelerken veriler, kullanılması gereken anahtar tanımlayıcı ile birlikte TEE'ye gönderilir, TEE, arayan uygulamanın bu anahtara erişimi olduğunu doğrular. Daha sonra verileri doğru anahtarı kullanarak ve şifreli metnini döndürür. Böylece şifreleme işlemi TEE kullanılarak yapılmış olur[119].

3.4.4 Donanım güvenlik modülü(HSM) cihazları

Depolama ve paylaşım esnasında master anahtar gibi hassas verilerin korunması için kriptografinin kullanımından kaynaklanan ana sorunlardan biri bu anahtarlarının gerçekten güvenli bir şekilde tutulup aynı şekilde üzerinde anahtar üretme, depolama, paylaşım, imha gibi bazı işlemler yapabilmektir[122]. Bulut bilişim depolama uygulamalarında HSM cihazları anahtar üretme ve bu anahtarları şifreleyip kriptografik işlemler yapılması için kullanmaktadır. Donanım güvenlik modülleri(HSM) hassas verileri ve kriptografik anahtarları donanım tabanlı ortamlarda saklamak ve kriptografik işlemleri uygulamalar için yüksek güvenlikli bir şekilde gerçekleştirilmesi için üretilmiş güvenlik donanımlarından biridir. Bu donanımsal cihazlar uygulamaların güvenli bir şekilde hassas verilerle operasyonlar yapmasını sağlarlar ve kullanıcıya güven verirler.



Şekil 3.13. HSM şematik gösterimi[122].

Donanım güvenlik modülleri saldırılara karşı savunma sistemleri sayesinde herhangi bir müdahaleye karşı kendi kendilerini sıfırlama özelliğine sahiptirler. Yani HSM cihazlarının içindeki bilgilerin yan kanal veya başka donanımsal saldırılar karşısında korunması amacıyla temas halinde içerideki bilgiyi yok ederler.

Donanım güvenlik modüllerinin bazı kullanım alanları bulunmaktadır. Bunlar;

- Akıllı kartlar
- Taşınabilir cihazlar
- Kriptografik kartlar
- Bağımsız cihazlar
- Bulut hizmetleri (HSM-as-aService

4 BULUT BİLİŞİMDE KRİPTOGRAFİ

Kriptografi, kendi içerisinde matematiğin ağırlıklı olarak kullanıldığı bir bilimdir. Şifreleme algoritmalarında matematiği kullanır. Şifreleme algoritmaları iki şekilde çalışmaktadır. Birinci kısım şifrelemedir. Bu kısımda düz metin üzerinde bazı işlemler uygulanarak şifreli metin oluşturulur. İkinci kısım ise şifre çözmedir. Bu bölümde şifreli olan metin bazı işlemlerden sonra tekrar düz metin haline çevrilir.

Günümüzde kriptografi simetrik, asimetrik anahtar ve özet algoritmaları olmak üzere üç ana algoritma başlığı altında incelenmektedir. Simetrik anahtar algoritmalarının en önemli örnekleri AES, DES ve Blowfish algoritmalarıdır. Asimetrik anahtar algoritmalarına örnek olarak ise RSA ve Diffie Helman verilebilir. Özetleme algoritmalarına da MD5 SHA-0 SHA-1 algoritmaları örnek olarak gösterilebilir.

Verilerin güvenliği, bütünlüğü, konumu ve yedeklenmesi, ağ trafiği, ve depolama sağlanması esnasında yaşananlar bulut bilişim sisteminde yer alan ana problemlerdendir. Kriptografi doğru bir şekilde uygulandığında tek başına bu sorunları büyük ölçüde çözebilme yetisine sahiptir. Konuk etki alanı ile ana bilgisayar etki alanı arasında veya ana bilgisayarlardan yönetim sistemlerine güvenli bir iletişim için HTTPS, şifreli VPN'ler, TLS, Secure Shell gibi şifreleme teknolojilerinin kullanılması çok önemlidir[123].

Bulut bilişim, bulut tüketicilerine hassas verilerini depolayabilecekleri ve uygulamaları çalıştırabilecekleri bilgi işlem olanakları veya altyapısı sağlamaktadır. Bulut bilişimin birçok avantajı olmasına rağmen, bulut sağlayıcılarına yeni güvenlik sorunları da getiriyor ve tam bir güven gerektiriyor. Güvenlik, verimlilik ve işlevsellik arasında bir denge kurmaya çalışarak, bulut bilişim ortamına uyarlanmış kriptografik temeller ve protokollerin tasarlanıp uygulanması gerekmektedir. Daha açık bir ifadeyle verilerin güvenli bir şekilde saklanması ve işlenmesi, müşteriden gönderilen herhangi bir isteğe yanıt vermek için gerekli süre ve bulut sunucusunda depolanacak şifreli bir verinin boyutu gibi işleme özelliklerine sahip modern bir kriptografi yaklaşımın kullanılmasını gerekmektedir.

Bulutta kriptografi kullanmanın temel amacı, kullanıcının verilerini bulut sağlayıcısına göndermeden önce şifrelemektir. Bu durumda, müşterinin verileri üzerinde her çalışması gerektiğinde, şifresi de çözülür. Bunun sonucunda maalesef zaman kaybı ve yedekli bilgi işlem gibi bazı sıkıntılar baş göstermektedir. Bu nedenle, bulut sağlayıcısının şifrelenmiş veriler üzerindeki işlemleri şifrelerini çözmeden yürütmesine izin vermek ve bu işlemlerin daha hızlı yapılabilmesi adına homomorfik şifreleme temelli şifreleme sistemlerini kullanmak gerekmektedir[124].

4.1 Kriptografinin Temelleri

4.1.1 Simetrik Anahtar Algoritmaları

Simetrik anahtar algoritmaları, verileri şifrelemek ve şifresini çözmek için aynı anahtarın kullanıldığı daha geleneksel bir yöntemdir. Blowfish, DES, AES gibi algoritmalar simetrik anahtar algoritmalarının önemli örneklerindendir. Her algoritma, verileri şifrelemek ve şifresini çözmek için farklı bir yöntem kullanır. Bunun yanı sıra her biri sabit bir veri boyutunu bir blok ve sabit bir anahtar boyutu olarak şifreler ve böyle de şifre çözme işlemini yapmaktadır. Bu tür algoritmalar sadece alfabelerin, özel sembollerin ve sayısal değerleri düz metin olarak kabul etmektedir. Bu nedenle çıktı (şifreli metin), özel karakterler veya alfabeler veya sayılar şeklinde veya hepsini birleştirerek bir belge olarak üretilmektedir. Simetrik şifrelemede yer alan bileşenler aşağıdaki gibidir[125]:

- Düz metin: Simetrik şifrelemede göndericinin alıcıya göndermek istediği orijinal metin olarak tanımlanmaktadır. Bu veriler şifreleme algoritmasına girecek metindir.

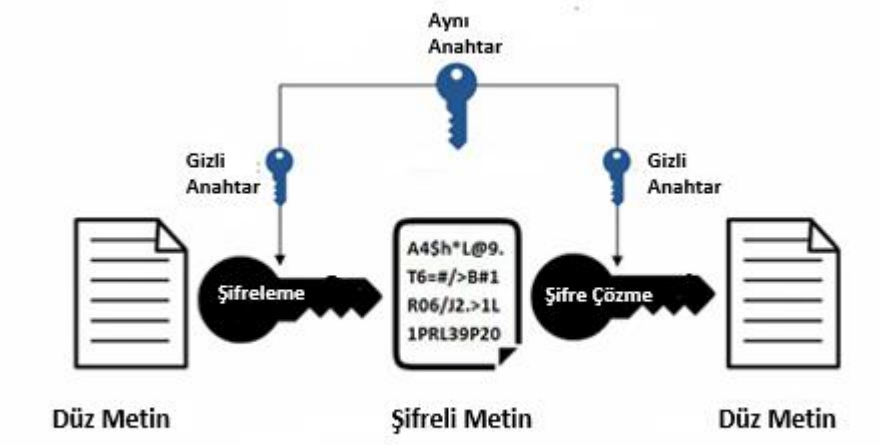
- Şifreleme algoritması: Şifreli metni üretmek için gizli anahtar kullanılarak düz metin üzerinde yapılacak işlemler dizisidir.

- Gizli anahtar: Düz metnin şifreli metne dönüştürülmesi için düz metni birleştirmek için kullanılan değerdir.

- Şifreli Metin: Şifreleme algoritmasına konulan orijinal düz metnin çıktısıdır. Düz metne hiçbir benzerliği bulunmamaktadır.

- Şifre çözme algoritması: Orijinal düz metin üretmek için gizli anahtar kullanılarak şifreli metin üzerinde yapılacak işlemler dizisidir.

Simetrik anahtarlı kriptografide şifrelenecek ve şifresi çözülecek metin için aynı anahtar kullanılmaktadır.



Şekil 4.1. Simetrik şifreleme gösterimi[127].

Simetrik anahtar algoritmalarının kullanılması ile birlikte birçok avantaj ve dezavantaj beraberinde bulunmaktadır. Simetrik şifrelemenin kullanılmasının sağladığı avantajlar aşağıdaki gibi sıralanmaktadır[125]:

- Simetrik anahtarın şifreleri, yüksek veri çıktı oranları elde etmek için kullanılmaktadır. Bazı donanım uygulamaları, her saniyede yüzlerce megabaytı şifreleyebilirken, yazılım uygulamaları, aktarım hızı olarak saniyede megabayt elde edebilir.

- Simetrik anahtar algoritmalarında anahtarlar asimetrik algoritmalara nazaran daha kısadır.

- Simetrik anahtarın şifreleri, hesaplama açısından verimli dijital imza şemaları, karma işlevleri ve sahte rasgele sayı üreteçleri dahil olmak üzere farklı şifreleme mekanizmaları oluşturmak için kolayca kullanılabilmektedir.

- Simetrik anahtarın şifreleri, daha güçlü şifrelerin sonucunu verecek şekilde derlenebilir. Üzerinde analiz yapmak ne kadar kolay olsa da zayıf olduklarında karmaşık olmayan dönüşümler, güçlü bir şifre ürünleri oluşturmak için kullanılmaktadır.

Simetrik anahtar algoritmalarının dezavantajları da aşağıdaki gibi sıralanmaktadır[125]:

- Simetrik anahtar algoritmalarında kullanılan gizli anahtarın hem alıcı tarafında hem de gönderici tarafında kesinlikle gizli kalması gerekmektedir.

- Büyük ağlarda birçok anahtar çifti vardır, bu anahtarların uygun şekilde yönetilmesi gerekmektedir. Etkin anahtarın yönetimi, koşulsuz olarak güvenilir bir üçüncü tarafa(TTP) ihtiyaç duyulmaktadır. Kriptografide, güvenilir bir üçüncü taraf (TTP), her iki tarafın da üçüncü bir tarafa güvendiği etkileşimleri kolaylaştıran bir varlıktır. Üçüncü Taraf, sahte dijital içerik oluşturma kolaylığı temelinde taraflar arasındaki tüm kritik işlem iletişimlerini gözden geçirme görevini üstlenmektedir.

- Doğru ve güvenli şifreleme yapmak için anahtarı sık sık değiştirilmesi gerekmektedir.

- Dijital imza mekanizmaları, simetrik anahtar şifrelemesinden geliştirilmektedir ve genel doğrulama işlevi amacıyla genellikle TTP kullanımını veya büyük anahtar boyutuna ihtiyaç duymaktadır.

4.1.2 Asimetrik Anahtar Algoritmaları

Asimetrik anahtar algoritmalarına ortak anahtar algoritmaları da denir. Açık anahtarlı şifreleme yani simetrik olmayan şifreleme, simetrik şifrelemede anahtarın saklanmasının zorluğu, bazı güvenlik sorunlarının meydana gelebilme olasılığı ve anahtarın yönetilememesi gibi sebeplerden dolayı keşfedilip üretilmiştir. Ayrıca asimetrik anahtar algoritmaları anahtar dağıtımı için kullanılmaktadır[124].

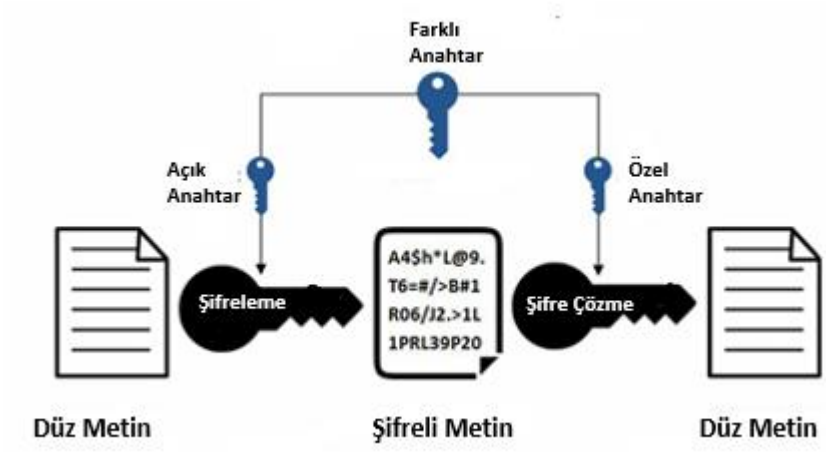
Açık anahtarlı şifrelemede, insanlar hem mesajın şifresini çözmek için özel bir anahtara hem de mesajı şifrelemek için kullanılan açık bir anahtara sahiptir. Açık anahtar, herkese açık bir şekilde tutulurken özel anahtar için durum farklı olup kullanıcı tarafından

bilinmektedir. Bu nedenle iletimden önce anahtarları dağıtımını yapmaya gerek kalmaz.

Yani herhangi bir kişi başka bir kişiye mesaj göndermek istediğinde, alıcının açık anahtarı ile metni şifreler ve bu mesaj sadece alıcının özel anahtarı ile açılabilir. Örnek bir senaryoda Alice'in Bob'a bir mesaj göndermek istediğini varsayalım. İlk önce Alice bu mesajı şifrelemek için Bob'un açık anahtarına ulaşmalıdır. Bu açık anahtarlar sertifikalar arayıcılığıyla alınabilmektedir. Alice bu anahtarı elde ettikten sonra mesajı bu anahtar ile şifreler. Daha sonra Bob kendine ait olan özel anahtar ile bu mesajın orijinal halini şifreyi çözerek ulaşır.

Açık anahtar şifrelemesinin sağladığı bazı avantajlar aşağıdaki gibidir[124];

- Güvenilmezlik, kimlik doğrulama ve sağlanan gizlilik.
- Anahtar dağıtımı çok kolaydır ve sistemde anahtar kalabalığı yoktur.
- Anahtarın çalınma olasılığı daha düşük olduğu için simetrik anahtardan daha güvenlidir.
- Açık anahtar şifrelemesinde yer alan bazı dezavantajlar aşağıdaki gibidir[124];
- Simetrik şifrelemeden çok daha yavaştır.
- Sistemde daha fazla CPU kullanımına yol açar.



Şekil 4.2. Ortak anahtar kriptografi gösterimi[127].

Açık anahtar algoritmalarının en önemlileri Diffie-Helman, RSA, ElGamal şifreleme algoritması, Eliptik Eğri Kriptografi ve Dijital İmza Algoritmasıdır(DSA). Aşağıdaki tabloda bu algoritmların avantajları ve dezavantajları yer almaktadır[126].

Tablo 4.1. Açık anahtar algoritmaları avantaj ve dezavantajları tablosu[126].

Algoritma	**Avantajları**	**Dezavantajları**
Diffie-Helman	Özel anahtar hiçbir zaman kanal üzerinden iletilmemektedir. Ayrıca bu algoritmada kullanılan ayrık logaritmayı çözmek çok zor bir işlemdir.	Kimlik doğrulama eksikliği bulunmaktadır. Üstel işlemler çok sistemler için büyük bir yüktür.
RSA	Yüksek güvenlik	İşlemlerin yavaş olması
ElGamal	Uzun mesajlar için genelleştirilmiş şifrelemesi çok hızlıdır.	Şifreli metin, düz metnin iki katı uzunluğundadır.
Eliptik Eğri Kriptografi	Daha fazla esneklik sağlamaktadır ve daha küçük anahtar boyutları ile aynı güvenliği vermektedir.	Daha küçük anahtar boyutları üzerinde hiper eliptik şifreleme yapılması müşteriye açıklanmasını zorlaştırmaktadır.
Dijital İmza Algoritması	Kimlik doğrulama, bütünlük sağlar. Ayrıca belgede sahtecilik veya yanlış bilgi yer almamaktadır.	Maliyet, Eğitim ve sorun giderme, Gereklilik, Teknolojik Uyumluluk, Güvenlik Endişeleri, Hukuki Sorunlar, İnkar Edilemezlik.

4.1.3 Özetleme Algoritmaları

Bir kriptografik hash fonksiyonu özet işlemi, mesaj adı verilen rastgele uzunluktaki bir girdiyi sabit uzunlukta bir çıktıya yani mesaj özetine eşleştiren bir dönüşümdür.

Kolayca hesaplanabilecek şekilde tasarlanmıştır ve belirli güvenlik özelliklerini sağlaması gerekmektedir. Kriptografik hash fonksiyonu, özgünlük, dijital steganografi, zaman damgası, imza gibi birçok güvenlik hedefine ulaşmak için kullanılan kriptografi alanındaki en önemli araçlardan biridir[128].

Kriptografik hash fonksiyonları iki türe sahiptir. Bunlar anahtarlı ve anahtarsız hash fonksiyonlarıdır. Anahtarlı hash fonksiyonları gizli anahtar kullanırken anahtarsız hash fonksiyonları gizli anahtar kullanmamaktadır. Anahtarsız veya kısaca hash fonksiyonları ek özelliklere bağlı olarak OWHF (Tek Yönlü Hash Fonksiyonları), CRHF (Çarpışmaya Dayanıklı Hash Fonksiyonları) ve UOWHF (Evrensel Tek yönlü Hash Fonksiyonları) olarak sınıflandırılmaktadır[129].

Kriptografik hash fonksiyonları sağladığı birçok güvenlik hizmetleri bulunmaktadır. Bunlar aşağıdaki gibi sıralanmaktadır[129]:

- Bütünlük ve kimlik doğrulama
- Etkili dijital imzalar
- Bilgisayar sistemlerinin yer alan kullanıcıların kimlik doğrulaması
- Dijital zaman damgası
- Rastgele sayı üreteci
- Oturum anahtarı türevleri
- Blok şifrelerin yapıları
- Hash tablolarında veri indeksleme
- Parmak izi alma
- Dosyaların benzersiz bir şekilde tanımlanması
- Yanlışlıkla bozulan verilerin tespiti

Birçok farklı hash algoritma türü bulunmasına rağmen dosya bütünlüğü kontrolleri için kullanılan en yaygın özet fonksiyonları MD5, SHA-2 ve CRC32'dir[130].

- MD5: Bu hash fonksiyonu bir dizi bilgiyi kodlar ve kodlanmış diziyi 128 bit parmak izine kodlar. MD5 genellikle veri bütünlüğünü doğrulamak için kullanılır. Bununla birlikte, MD5'in birçok farklı güvenlik açıklarına sahip olduğu bilinmesine rağmen, hala dünyada en yaygın kullanılan algoritmalardan biridir.

- SHA-2: Ulusal Güvenlik Ajansı (NSA) tarafından geliştirilen SHA-2, SHA-1'e kıyasla birçok farklılığa sahiptir. SHA-2 ailesi, 224, 256, 384 veya 512 bit olan özetlere hash değerlerine sahip SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA -512/256 olmak üzere altı özet fonksiyonundan oluşmaktadır.

- CRC32: Döngüsel artıklık denetimi (CRC), verilerde yanlışlıkla yapılan değişikliklerin tespiti için sıklıkla kullanılan bir hata tespit eden koddur. Aynı veri dizisini kodlamak için CRC32 kullanmak her zaman aynı karma çıktıyı üretecektir. Bu nedenle, CRC32 bazen dosya bütünlüğü kontrolü için bir karma algoritma olarak kullanılır.

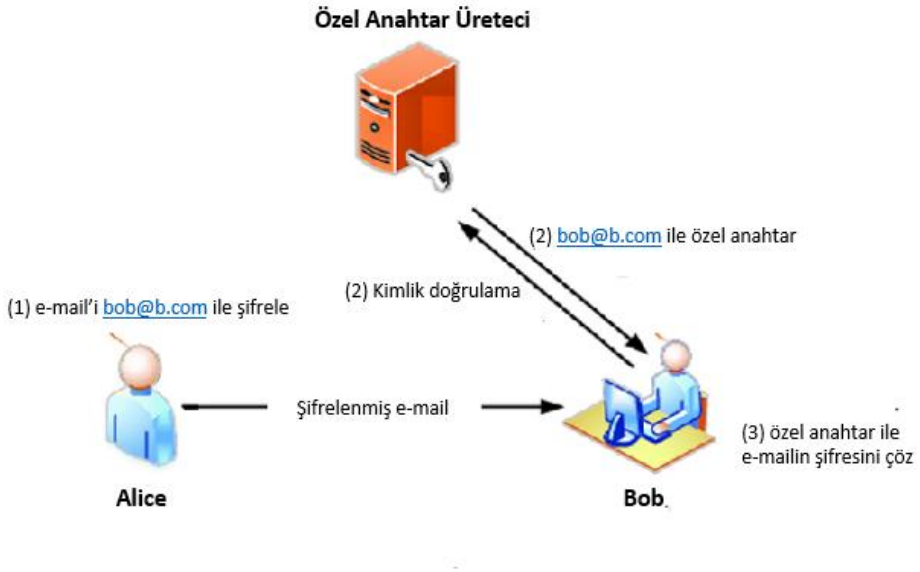
4.2 Kriptografik Mekanizmalar

Bulut bilişimde ve birçok farklı dalda bazı kriptografik mekanizmalar kullanılmaktadır. Bunlardan en öne çıkan türler kimlik tabanlı kriptografi, nitelik tabanlı kriptografi ve homomorfik kriptografidir.

4.2.1 Kimlik Tabanlı Kriptografi

Kimlik tabanlı şifrelemede kullanıcıların benzersiz bir tanımlayıcı varlığa ihtiyaçları bulunmaktadır. Algoritmaya göre her adım bu benzersiz tanımlayıcıyla beraber gerçekleştirilmektedir. Bu benzersiz tanımlayıcı e-mail parmak izi ya da telefon numarası gibi bileşenler olmaktadır. Kimlik tabanlı şifreleme kısaca bu benzersiz tanımlayıcıdan genel anahtarın oluşturulduğu ve güvenilir bir üçüncü taraf sunucusu tarafından genel anahtar kullanılarak buna karşılık gelen özel anahtarı oluşturulduğu bir genel anahtar şifreleme türü olarak tanımlanmaktadır. Bu şekilde, şifreli veri alışverişi yapmadan önce ortak anahtarları dağıtmaya gereksinim ortadan kaldırılmaktadır. Gönderici, bir genel anahtar oluşturmak ve verileri şifrelemek için alıcının benzersiz tanımlayıcısını

kullanmaktadır. Alıcı, güvenilen üçüncü taraf sunucusu olan özel anahtar üreticisinin (ÖAÜ(PKG)) yardımıyla karşılık gelen özel anahtarı ulaşabilir[131].



Şekil 4.3. Kimlik tabanlı kriptografi gösterimi[131].

Bu şifreleme şemasını çalıştırmak için, ÖAÜ önce bir genel anahtar yayınlar ve ilgili ana özel anahtarı sisteminde tutar. Ortak anahtar verildiğinde, herhangi bir taraf, ortak anahtarı e-posta adresi veya telefon gibi bilinen benzersiz bir kimlik değeriyle birleştirerek bir kimliğe karşılık gelen ortak anahtarı hesaplayabilir. Karşılık gelen bir özel anahtarı elde etmek için, genel anahtarı oluşturmak için kullanılan kimliğin sahibi, ilgili özel anahtarı oluşturmak için özel anahtarını kullanan ÖAÜ ile iletişime geçer.

Kimlik tabanlı şifrelemenin sağladığı birçok fayda bulunmaktadır. Bunlar[132]:

- Alıcı taraftaki kişi herhangi bir şifreli mesaj alması için hazırlık yapmasına gerek yoktur.
- Ortak anahtar altyapısının yönetilmesi gereksinimi bulunmamaktadır.
- Yalnızca belirlenmiş alıcının imzasının geçerli kılınacağı bukalemun imzaları sağlar.

ÖAÜ kullanıcılar için tüm kriptografik işlemler yürüttüğünden ötürü istemci tarafının herhangi bir kurulum yapmasına gerek yoktur.

Kullanıcıların özel anahtarını almasını gerektirmeyen durumlarda yüksek güvenlikli ÖAÜ özel anahtarları saklayabilir.

Kimlik tabanlı şifrelemenin dezavantajları ise şunlardır[132]:

- Özel anahtarın kaybolması halinde şifreleme anahtar emaneti kullanıcılarda bulunacağından dolayı inkâr edilmezlik özelliği sağlanamayabilir. Bu özellik kimlik tabanlı kriptografi ile ortak anahtar altyapısı arasındaki en önemli farklardan biridir.
- Güvenli anahtar verme durumunda ana anahtarlar birden çok ÖAÜ'ye yayılması halinde güvenlik artmasına rağmen performans düşüklüğüne sebep verir.
- Anahtar iptal mekanizması bulunmamaktadır. Yukarıdaki resimdeki Bon'un özel anahtarının ele geçirildiğini varsaydığımızda, anahtar Bob'un e-posta bilgisiyle ilişkilendirildiği için Bob'un e-posta adresini değiştirmesi gerekmektedir. Bu sorunun biraz sınırlandırılması maksadıyla benzersiz kimlik bileşeninin zaman damgasının bulundurulması gerekmektedir.
- ÖAÜ'nin yüksek düzeyde güvenlik sağlaması gerekmektedir. Tüm özel anahtarlar burada depolandığından ötürü sistem birçok endişeyi beraberinde getirmektedir.
- Ayrıca ÖAÜ kullanıcılarla olan bağlantısı her zaman açık olması gerekmektedir. Böylece kullanılabilirlik özelliği sağlanmış olur

4.2.2 Nitelik Tabanlı Kriptografi

Nitelik tabanlı kriptografi ilk olarak Sahai ve Waters tarafından şifreli erişim kontrolü için yeni bir araç olarak tanıtılmıştır[132]. Nitelik tabanlı kriptografide, geleneksel açık anahtar şifrelemesine benzer şekilde şifreli metinlerin belirli bir kullanıcıya şifrelenmesi gereksinimi yoktur. Bunun aksine, hem kullanıcıların özel anahtarları hem de şifreli metinleri, bir dizi nitelik veya nitelikler üzerinde bir politika arayıcılığıyla ilişki kurulur. Kullanıcı, sadece kendi özel anahtarı ile şifrelenmiş metin arasında bir eşleşme bulunduğu takdirde şifreli metnin şifresini çözebilme imkânına sahiptir[133].

Nitelik tabanlı şifrelemenin en önemli yönleri esneklik, ölçeklenebilirlik ve ince taneli erişim kontrolü sağlamaktır. Klasik modelde bunun sağlanması, yalnızca kullanıcı ve sunucu güvenilir bir etki alanının oluşması durumunda gerçekleşir. Kimlik tabanlı şifreleme gibi geleneksel açık anahtar şifrelemesinden farklı olarak, Nitelik tabanlı şifreleme şifreli metinlerin belirli bir kullanıcı için mutlaka şifrelenmediği birden çok sayıda şifreleme için uygulanmaktadır. Ayrıca birden fazla sayıda kullanıcı için de

uygulanabilmektedir. İlkelerin şifreleme algoritmasının kendisinde belirlendiği ve uygulandığı nitelik tabanlı şifreleme mevcut şemaları iki tiptir. Bunlar Anahtar-Politika NTŞ (KP-ABE) şeması ve Şifreli Metin-Politika NTŞ (CP-ABE) şemasıdır[134].

- Anahtar-Politika nitelik tabanlı şifreleme: Nitelik tabanlı şifrelemenin klasik modelinin değiştirilmiş halidir. KP-ABE modelini keşfederken, nitelik politikaları anahtarlarla ve veriler niteliklerle ilişkilendirilir. Yalnızca ilkeyle ilişkili anahtar (ilişkili verilerin öznitelikleri tarafından karşılanacak olan) verilerin şifresini çözebilir. Anahtar-politikası niteliğine dayalı şifreleme şeması, bire çok iletişim için tasarlanmış bir açık anahtar şifreleme tekniğidir.
  Veriler ayrı ayrı ortak anahtarlarla tanımlanmış niteliklerle ilişkisi kurulur. Verileri şifreleyen, bir ortak anahtarla şifreleyerek, veri veya mesaja ilişkin nitelikler kümesiyle ilişkilendirilir.

  Kullanıcılara veride yer alan özniteliklere dayalı bir erişim ağacı yapısı ataması yapılır ve bu ağacın düğümlerine de eşik kapsı denmektedir. Bu ağaç yapısında yer alan her yaprak düğümü bazı niteliklerle ilişkilendirilir. Erişim ağacı yapısına benzemiş bir şekilde kullanıcıların gizli anahtarı tanımlanır. Bu nedenle, kullanıcı, ancak ve ancak veri öznitelikleri erişim ağacı yapısını karşılıyorsa, şifreli metin olan mesajın şifresini çözebilir. Şifreli metinle ilişkili nitelikler erişim ağacı yapısını sağladığında, kullanıcı şifreli metnin şifresini çözebilir. Bulut bilişimde etkin iptal için KP-ABE tabanlı bir erişim kontrol mekanizması ve yeniden şifreleme tekniği birlikte kullanılmaktadır. Bu teknik sayesinde veriye sahip olan varlıkğın sunuculara doğru yaptığı hesaplama iş yükü azaltılması sağlanır.

  KP-ABE çözümü, hassas erişim kontrolü sağlar. Her dosya veya mesaj, KP-ABE'deki bir dizi özniteliğe karşılık gelen bir ortak anahtarla şifrelenen simetrik bir veri şifreleme anahtarı ile şifrelenir ve bu ortak anahtar aynı zamanda bir erişim ağacı yapısına karşılık gelir. Şifrelenmiş veri dosyası, ilgili özniteliklerle ve şifrelenmiş veri şifreleme anahtarıyla depolanır. Dosyaların veya mesajların şifresini çözmek için de kullanılan bu sistemde yalnızca bulutta depolanan dosyanın veya mesajın karşılık gelen öznitelikleri kullanıcı anahtarının erişim yapısını karşıladığında, kullanıcı şifrelenmiş veri şifreleme anahtarının şifresini çözebilir.

- Şifreli metin–politika nitelik tabanlı şifreleme: CP-ABE şemasında, öznitelik politikaları ile verilerin, öznitelikler ile de anahtarların arasında bir ilişki kurulur. Verilerin şifresini çözmek adına ancak ilişkili özniteliklerin verilerle ilişkili politikayı karşılaması gerekmektedir. CP-ABE çalışma mantığı, KP-ABE şemasının tam tersi yönünde olan CP-ABE'de şifreli metin bir erişim ağacı yapısıyla ilişkilendirilir ve her kullanıcı gizli anahtarı bir dizi niteliğe sahiptir.

  Şifre çözme işlemi ancak yetkili kullanıcılar şifre çözme algoritmasını çağırdığı takdirde gerçekleşir. CP-ABE'de kullanıcılar ile bazı öznitelikler arasında bir ilişkilendirme yapılır ve gizli anahtarlar da niteliklerine dayalı bir şekilde meydana getirilir.

  Şifreleme esnasında, şifreleyen özniteliklere eşik erişim yapısını bildirir. Bu erişim yapısına göre mesajlarda şifreleme işlemleri yapılır. Şifrenin çözülmesi için sadece nitelikleri erişim yapısına uygun olması zorunluluğu vardır. CP-ABE sayesinde şifrelenmiş verilerin gizliliği sağlanarak bazı olası saldırıların önüne geçilmiş olur.

4.2.3 Homomorfik Kriptografi

Kriptografide homomorfik şifreleme, bir bulut hizmeti sağlayıcısının veriler şifrelenirken veriler üzerinde belirli hesaplama işlevlerini çalıştırmasını sağlayan bir şifreleme şeması olarak tanımlanmaktadır. Geleneksel şifreleme şemaları, sağlayıcının şifrelenmiş veriler üzerinde çalışmasına izin verememektedir ve müşterilerin bulut hizmetlerini kullanmak için veri güvenliklerinden ödün vermesi gerekir. Bu nedenle, hala şifrelenmiş haldeyken şifrelenmiş veriler üzerinde hesaplama işlemlerinin gerçekleştirilebileceği bir şemanın var olması gerekmektedir. İşlemler homomorfik şifreleme ile gerçekleştirilerek verilerin şifresi çözülmeden işlemler gerçekleştirilmekte ve bu sayede çözüme ulaşma hızı artırılarak veri gizliliği sağlanabilmektedir. Genel olarak bulut kullanıcısı ile bulut sağlayıcı arasında, sunucunun hiçbir şekilde orijinal veriyi görmeden işlem gerçekleştirdiği bir veri hesaplama süreci aşağıdaki gibi özetlenir[124]:

- İstemci: a ve b verilerini Enc (a) ve Enc (b) olarak şifreler ve ardından Enc (a) ve Enc (b) şifrelenmiş verileri sunucuya gönderilir.

- Sunucu: Enc (a) ve Enc (b), şifreli metne belirli bir işlemi belirten f-işlevi uygular ve istemcinin hesapladığı şifreli sonuç (Enc (a), Enc (b)) istemciye gönderilir.

- Müşteri: İstenen hesaplama sonucunu gizli anahtarı ile şifreler, bu sayede verilerin veya işlemin sonucunun gizliliğini ve güvenliğini sağlar.

Homomorfik şifreleme içerisinde tanımlanan üç ayrı şema bulunmaktadır. Bunlar kısmen, biraz ve tam homomorfik şifreleme şemalarıdır[135].

- Biraz Homomorfik Şifreleme (SWHE)

İlk kullanılabilir FHE piyasaya sürülmeden önce bazı pratik SWHE örnekleri bulunmaktaydı. SWHE şemalarından bazıları FHE şemalarını oluşturmak için kullanılır.

SWHE, yalnızca sınırlı sayıda tekrar için hem toplama hem de çarpma işlemlerini gerçekleştirebilmektedir. Bu sınırlamaya, şemanın homomorfik işlemlerle ilişkili şifreli metinlerin şifresini doğru bir şekilde çözmesi denmektedir. Genel olarak, homomorfik şifreleme şemasının şifreli metni bir gürültü parametresine sahiptir ve bunun şifresini düzgün bir şekilde çözmek için gürültünün belirli bir sınırdan az olması gerekir.

Bir SWHE şeması, şifrelenmiş veriler üzerinde hem toplamalı hem de çarpımsal homomorfizm gerçekleştirebilir. Fakat bunun sonucunda her işlemde üretilen homomorfik şifreli metindeki gürültü artmış olacaktır. Gürültü parametresini olabildiğince küçük tutmak için, SWHE şemaları yalnızca sınırlı sayıda işlemi gerçekleştirebilmektedir[135].

SWHE içerisinde birkaç tür şema bulunmaktadır. 2005 yılına kadar, önerilen tüm homomorfik şifreleme şemaları, yalnızca toplama veya çarpma işlemiyle sınırlıydı. Boneh-Goh-Nissim (BGN) şemasında bir çarpmayı ve sınırsız sayıda eklemeyi ve sabit boyutlu bir şifreli metni desteklemektedir. BGN şemasında anahtar oluşturma algoritması aşağıdaki gibidir[135]:

Anahtar oluşturma:

G ve G1, $n = q_1q_2$ düzeyindeki döngüsel grupların olduğu, q_1 ve q_2 iki farklı büyük asal sayı olduğu ve e çift doğrusal harita olduğu, $e : G \times G \rightarrow G_1$ durumda (n, G, G_1, e,

g, h) açık anahtardır. Varsayalım ki g ve u adında G'nin iki tane rastgele üreteç seçildi ve $h = u^{q2}$ olduğu durumda h, G'nin alt grubunun q_1 sıralı rastgele bir üretecidir. Gizli anahtar ise q1'dir.

BGN'de m adlı mesajı şifrelemek için $r \in \{0, 1, \ldots n\}$ r için rastgele bir değer alınır g ve h kullanılarak aşağıdaki algoritma ile şifreleme işlemi yapılır[135]:

Şifreleme:

$E(m) = g^m h^r = c \in G$

BGN'de q^1 gizli anahtarı kullanılarak c adlı şifreli metni çözmek için $h^{q1} \equiv 1 \pmod n$ olduğu durumda

Şifre çözme:

$c^{q1} = (g^m h^r)^{q1} = (g^{q1})^m$ kullanılır. Daha sonra m adlı mesajı çözmek için de

$D(c) = \log_g q1(c^{q1}) = m$ algoritması kullanılır[135].

Diğer önerilen SWHE şemalarına bakacak olursak Melkor ve arkadaşlarının[136], bazı homomorfik özelliklere sahip bazı iyi bilinen şemalara bağlı olarak, sabit derinlik devre homomorfik değerlendirmesini destekleyen bir şifreleme şeması sunduğu, Sander, Young ve Yung [137] ise, birçok AND kapısına sahip yalnızca bir OR/NOT kapısını destekleyen bir şema sunmuştur. Şifreli metin boyutu her OR/NOT kapısı değerlendirmesiyle birlikte büyüdüğünden dolayı devre derinliği değerlendirmesi sınırlıydı.

- Kısmi Homomorfik Şifreleme (PHE), ya yalnızca toplamsal işlemleri destekleyen bir eklemeli homomorfik şema veya yalnızca şifrelenmiş veriler üzerinde çarpımsal işlemleri destekleyen bir çarpımsal homomorfik şema olarak tanımlanmaktadır. PHE için birçok türde şema bulunmaktadır. Bunlar RSA, Goldwaser-Micali, Elgamal, Benaloh ve Pailier'dir. Bu şemaların içerdiği algoritmalar aşağıdaki tabloda listelenmiştir[135].

Tablo 4.2. Kısmi homomorfik şifreleme türlerinin algoritma tablosu[135].

PHE Şemaları	**Algoritma**
RSA	$(m^e_1 \ (mod\ n)) * (m^e_2 \ (mod\ n)) = (m1 * m2)^e \ (mod\ n)$
GM	$y^2_1 x^{m1} (\text{mod } n) * (y_2{}^2 x^{m2} (\text{mod } n)) = (y_1 * y_2)^2 x^{m1+m2} (\text{mod } n)$
Elgamal	$(g^1_x, m_1 h^{x1}) * (g^{x2}, m_2 h^{x2}) = g^{x1+x2}, m_1 8 m_2 h^{x1+x2})$
Benaloh	$(y^{m1} u^{r1} (\text{mod } n)) * (y^{m2} u^r_2 (\text{mod } n)) = y^{m1+m2} (u^1 * u^2)^r (\text{mod } n)$
Pailier	$(g^{m_1} r_1{}^n (\text{mod } n^2)) * (g^{m_2} r_2{}^n (\text{mod } n^2)) = g^{m1+m2} (r^1 * r^2)^n (\text{mod } n^2)$

Aşağıda ise kısmi homomorfik şifreleme türlerinin özellik grafiği bulunmaktadır[135].

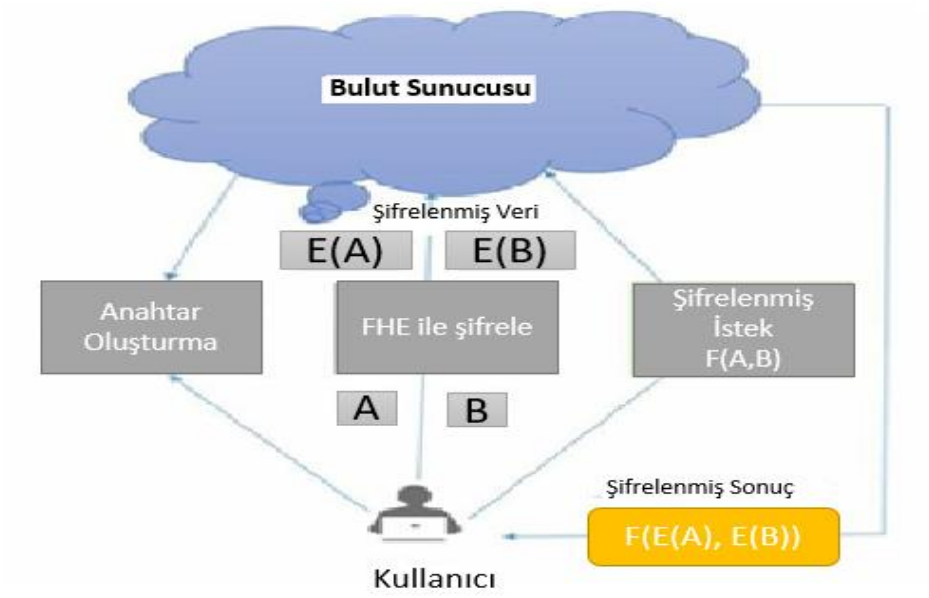
Tablo 4.3. Kısmi homomorfik şifreleme türlerinin özellik tablosu[135].

PHE Şemaları	**Simetrik**	**Asimetrik**	**Olasılıksal**	**Deterministik**	**Toplamsal**	**Çarpımsal**
RSA		✓		✓		✓
GM		✓	✓		✓	
Elgamal		✓	✓			✓
Benaloh		✓	✓		✓	
Pailier		✓	✓		✓	

- Tam Homomorfik Şifreleme (FHE), analitik işlevlerin doğrudan şifrelenmiş

veriler üzerinde çalıştırılmasına ve işlevler düz metin üzerinde çalıştırılmış gibi aynı şifreli sonuçların verilmesine olanak tanıyan bir şifreleme şemasıdır.

FHE şemaları sayesinde bulut sisteminde depolanan verilerin güvenliğinin sağlanması daha kolay olmaktadır. Bunun için, buluta gönderilmeden evvel tüm verilerin bu şemayla şifrelenmesi gerekmektedir. İlk olarak, kullanıcı oturum açar ve gizli anahtarı oluşturmak için sunucu tarafından sağlanan anahtar oluşturmayı kullanır ve kullanıcı bu gizli anahtarın tek sahibi konumunda olur. Daha sonra bulut sistemine gönderilmesi arzu edilen veriler şifrelenir. İletim sırasında, dijital imza gibi diğer kriptografik teknolojilerin uygulanmasıyla bütünlük ve inkar edilemezlik garanti edilmiş olur. Kullanıcı, sunucunun bu şifreli veriler üzerinde bazı hesaplamalar yapmasını istediğinde bulut sunucusuna şifreli istek gönderebilir. Sunucu kendisinin sorumlu olduğu görevleri tamamlayarak şifrelenmiş sonucun kullanıcıya iletilmesini sağlar. Son olarak kullanıcı, doğru sonucu elde etmek için gizli anahtarıyla verilerin şifresini çözer. Aşağıda FHE'nin bulut sistemlerinde nasıl kullanıldığı gösterilmektedir[138].



Şekil 4.4. FHE'nin bulut sistemlerindeki kullanım grafiği[138].

5 SONUÇ VE ÖNERİLER

Bulut bilişim sistemlerinin hayatımıza girmesiyle birlikte kişiler ve kurumların günümüzde yer alan birçok akıllı cihazla istediği yerden internet aracılığıyla bilgilere erişim, paylaşım, depolama gibi birçok özelliği kullanması kolaylaştı. Bununla birlikte bulut bilişim platformlarıyla diğer sistemlere nazaran daha az maliyetli ve daha az kullanışlı, erişilebilir, ölçeklenebilir, esnek ve güvenli bir ortam sağlanmış oldu. Ayrıca bulut bilişim ortaya koyduğu başta altyapı, platform ve yazılım hizmetleri sayesinde kurumlara daha az emek ile daha hızlı uygulamaların oluşturulmasına, daha az donanım cihazıyla güvenli, maliyetsiz ve ölçeklenebilir sistemler kurulmasına katkı sağlamaktadır. Bunun yanında bulut bilişimde yer alan dağıtım modelleri sayesinde hassas verilerin ve sistemlerin gizli, dışarıya kapalı ve daha güvenli bir yapıda yer almasının yanı sıra istenildiğinde herkesin erişebileceği platformlar, yazılımlar ve uygulamalar geliştirilmesine büyük olanak sağlanmaktadır.

Bulut bilişim kullanan veya kullanmaya başlayan her kurum ve kuruluş bulut bilişimin ne kadar güçlü bir yapısı olduğunu ve bunun kendilerine ne kadar yarar sağladığını görebilmektedir. Her geçen gün artışını sürdüren yüksek veriler, bu verilerin bakımı, yönetimi ve bunlar için gerekli personeller ve geleneksel BT altyapısının sunamadığı diğer önemli özellikler, kurumları bulut bilişim altyapısına doğru yönlendirmektedir. Bunun en büyük nedeni ise bulut bilişimin düşük maliyet, esneklik, erişilebilirlik, yönetim, raporlama, yedekleme, depolama, bakım, performans ve ölçeklenebilirlik gibi birçok avantajının bulunmasıdır. Fakat her teknoloji beraberinde birçok avantajla geldiği gibi kendisinde dezavantajları, riskleri ve endişeleri beraberinde getirmektedir. Bulut bilişimin de üzerinde önemle durulup düşünülmesi gereken hizmet sağlayıcıya bağımlılık, sabit internet ve yüksek bant genişliği gerekliliği, verilerin kontrol ve konumu ile güvenlik ve gizlilik konuları gibi birçok dezavantajları bulunmaktadır. Bu dezavantajlar sistemin doğru bir şekilde öğrenilip gerekli önlemlerin alınmasıyla bertaraf edilebilmektedir.

Bulut bilişim, gelecek nesil BT uygulamaları için umut vadeden ve hala gelişimini sürdürmekte olan bir teknolojidir. Bulut sistemini kullanan kullanıcılar verilerini güvenli bir ortamda depolayacağı, sahip oldukları altyapıları daha az maliyetle kuracağı, müşterilerine sundukları platformları ve uygulamaları her yerden ve her zaman erişilebilir ve sürekli olarak sağlayacakları, bu uygulama ve platformların geliştirilmesinde

kullanılan tüm donanım ve yazılım personel gereksinimlerinin en az maliyetle oluşturacağı ortamın bulut sistemleri olduğunun farkına varmışlardır. Fakat bulut bilişimin hızlı büyümesinin ve tüketicilerin bu sayılan işleri yapma isteğinin önündeki engeller, veri güvenliği, gizlilik ve mahremiyet ile ilgili problemlerdir. Bulut sistemler üzerinde kullanıcıların verilerinin nasıl ve nerede saklandığı, bu verilere kimlerin erişim ve kontrol hakkının bulunduğu ile ilgili bir hayli endişeleri bulunmaktadır. Tüm bunlar için ağ, yazılım ve altyapı tarafında gerekli önlemlerin alınması, bilgi güvenliğinde yer alan temel bileşenlerin sistem tarafından garanti edilmesi, kimlik ve erişim yönetimi sistemleriyle uygulamalara kayıt ve girişlerin daha olgun ve güçlü bir yapıda yapılması, yetkisiz bireylerin sisteme girmesinin engellenmesi ve yasal uyumluluk ve standartların takip edilmesiyle kullanıcılar için problem ve endişeye yer bırakmayacak şekilde bir sistem sunulması gerekmektedir.

Bu tez çalışmasının bir başka konusu ise bulut depolamada kullanılan kullanıcı anahtarlarının saklanma yöntemleridir. Bir bulut depolama ürününde kullanıcıların anahtarlarının yazılımsal ve donanımsal olarak saklanması çok önemlidir. Anahtarların donanımsal yerlerde tutulması sayesinde kullanıcıların yaptığı işlemler geri getirilip çözümlenemez ve tüm işlemlerin şifreli bir şekilde kalması sağlanır. Bu yazılımsal ve donanımsal saklanma yöntemlerini bulut bilişim sağlayıcıları kullanıcılar için uygulamalı ve bunları şeffaf bir şekilde kullanıcıya bildirmelidir.

Bulut tüketicilerinin hem kendilerini güvende hissedeceği ve rahatlıkla hassas verilerini depolayacağı hem de ağ üzerinden aldıkları hizmeti kolay ve etkili kullanmaları için bulut sağlayıcılarının sadece verdiği hizmetler değil, bu hizmetleri verirken güvenlik, gizlilik ve mahremiyet açısından ne gibi önlemler aldığı, hangi standartlara uyarak verilen hizmeti daha güvenlir kıldığı, hassas verilerin depolanması esnasında verilerin nasıl ve ne şartlar altında tutulduğu, bilgi güvenliğinin en önemli üç esası olan bütünlük, gizlilik ve erişilebilirlik ilkelerine ne kadar uyum sağladığı dikkatlice incelenmeli ve kendilerine en uygun bulut sağlayıcıyı bu kriterleri ön plana çıkararak belirlemelidir. Ayrıca bulut tüketicileri kendilerini endişelendiren her hususu bulut sağlayıcılarla yaptıkları sözleşmelerde belirtmelidir. Bulut sağlayıcıları ise bulut bilişimin kendini çok hızlı geliştirdiği ve yaygınlaştığı bu dönemde bulut kullanıcılarına sundukları hizmetleri daha güvenli yazılım ve donanımlar kullanarak devam etmelidir. Bunun yanında en önemli güvenlik sorunlarından olan kimlik ve erişim yönetimi ile alakalı daha sağlam standartlar kullanılarak kullanıcılara katı güvenlik önlemlerini uygulatmalıdır.

Bulut bilişim sistemlerinin güvenliğinin sağlanmasında gelecekte ortaya çıkması muhtemel yeni yöntemlerin tartışılacağı ve bunların kapsamlı değerlendirmenin yapılacağı öngörülmektedir. Ayrıca gelecekte bulut bilişim sistemleri üzerinde güvenlik, gizlilik, mahremiyet ve kriptografi için daha fazla yöntemin araştırılıp uygulanması ve literatüre girmesi gerekmektedir. Bulut bilişimde güvenlik, gizlilik ve kriptografi konularının incelendiği bu tez çalışmasının gelecekteki BT yapılarında yer alabilecek teknoloji ve güvenlik sistemleri üzerinde yapılacak çalışmalara ve sistemlere katkı sağlayacağı düşünülmektedir.

Bu tez çalışmasının sonrasında bulut bilişimde bulut sağlayıcıların sunduğu hizmetlerin veri güvenliği, gizlilik, mahremiyet, bütünlük ve erişilebilirlik ve kullanım kolaylığı açısından detaylı karşılaştırmasının yapılarak bulut kullanıcıları için örnek bir seçim modeli oluşturulması doğru bir seçim olacaktır. Oluşturulacak olan bu seçim modelinde hangi bulut sağlayıcının hangi alanda daha verimli hizmetleri barındırdığı, hangi uluslararası standartlar ile hizmetlerin güvenilirliğini sağladığı, hangi kriptografi algoritmaları kullanarak veya saldırıları, zafiyet ve tehditlere karşı hangi önlemleri alarak sistemin daha güvenilir bir yapıya sahip olduğu ve ne gibi metodlar ile kullanıcı dostu hizmetler sağladığı detaylıca anlatılmalıdır.

6 KAYNAKLAR/REFERENCES

[1] Sriram, I. and A. Khajeh-Hosseini, Research Agenda in Cloud Technologies. 2010.

[2] NIST. Final Version of NIST Cloud Computing Definition Published. 2011 [cited 2021 14 Nisan]; Available from: https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computingdefinition-published.

[3] Microsoft. What is cloud computing? [cited 2021 15 Nisan]; Available from: https://azure.microsoft.com/enus/overview/what-is-cloud-computing/.

[4] IBM, Staying aloft in tough times. 2009.

[5] Fellows, W., Partly Cloudy, Blue-Sky Thinking About Cloud Computing. 2008.

[6] Thomas Bittman, D.C., Daryl Plummer, Tom Austin, David Smith, Cloud Computing: Defining and Describing an Emerging Phenomenon. 2008.

[7] Rayport, J. F. and Heyward, A. Envisioning the Cloud: The Next Computing Paradigm. 2009

[8] R. Buyya, C. S. Yeo and S. Venugopal, Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. 10th IEEE International Conference on High Performance Computing and Communications. 2008. pp. 5-13, doi: 10.1109/HPCC.2008.172.

[9] Mcfedries, P. The Cloud Is The Computer. 2008 [cited 2021 16 Nisan]; Available from: https://spectrum.ieee.org/the-cloud-is-the-computer.

[10] Nathaniel S. Borenstein, J.B., Cloud Computing Standards: Where's the Beef?. 2011.

[11] Armburst M. Above the Clouds: A Berkeley View of Cloud Computing. 2009 [cited 2021 18 Nisan]; Available from: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.

[12] E., G. What Is Cloud Computing. 2020 [cited 2021 24 Nisan]; Available from: https://www.pcmag.com/news/what-is-cloud-computing#:~:text=The%20term%20%22cloud%20computing%22%20is,of%20your%20computer's%20hard%20drive.&text=When%20you%20store%20data%20on,called%20local%20storage%20and%20computing.

[13] Wikipedia. Cloud computing. 2021 [cited 2021 25 Nisan]; Available from: https://en.wikipedia.org/wiki/Cloud_computing.

[14] Lillard T. V., Digital Forensics for Network, Internet and Cloud Computing. 2010.

[15] Furth, B. ve Escalante, A., Handbook Of Cloud Computing. 2010.

[16] Mirzaoğlu, A. G., Bulut bilişimin teknik, uygulama ve düzenleme boyutuyla değerlendirilmesi, dünya örnekleri ve ülkemize ilişkin öneriler". 2011.

[17] Hogan, M., Liu, F., Sokol, A. and Jin, T., NIST Cloud Computing Standards Roadmap, Special Publication (NIST SP). 2011; Available from: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909024

[18] Vyas, I. 10 Popular Examples Of SaaS Applications. 2020 [cited 2021 1 Mayıs]; Available from: https://citrusbug.com/blog/saas-application-example.

[19] Chai W., Brush K., Bigelow S. J., What is PaaS? Platform as a service definition and guide. 2021.

[20] Toman, Y. Bulut Bilişim Nedir? 2021 [cited 2021 1 Mayıs]; Available from: https://www.sanalhukuk.net/bulut-bilisim-nedir/#:~:text=Bulut%20bili%C5%9Fim%20hizmeti%20kapsam%C4%B1nda%20hizmet%20sa%C4%9Flay%C4%B1c%C4%B1%20ve%20kullan%C4%B1c%C4%B1%20aras%C4%B1nda%20s%C3%B6zle%C5%9Fme%20yap%C4%B1lmaktad%C4%B1r.&text=Hizmet%20Seviyesi%20Anla%C5%9Fmas%C4%B1%20(Service%20Level,sa%C4%9Flayacak%20hizmet%20seviyesine%20ili%C5%9Fkin%20anla%C5%9Fma.

[21] IDC. Public Cloud IT Infrastructure Revenue Growth Remained Strong in Third Quarter of 2020, According to IDC. [cited 2021 3 Mayıs]; Available from:

https://www.idc.com/getdoc.jsp?containerId=prUS47279621.

[22] Kobilinskiy A., Cloud Service Models: SAAS, PAAS, IAAS - Which Is Better For Business. 2019 [cited 2021 8 Mayıs]; Available from: https://dev.to/artemkobilinskiy/cloud-service-models-saas-paas-iaas-which-is-better-for-business-574k.

[23] Fechter J.(2020), 15 Common Software as a Service (SaaS) Examples to Inspire You. [cited 2021 11 Mayıs]; Available from: https://joshfechter.com/software-service-examples/.

[24] Shim T., Popular Software as a Service (SaaS) Examples. 2021 [cited 2021 14 Mayıs]; Available from: https://www.webhostingsecretrevealed.net/blog/web-business-ideas/saas-examples/.

[25] Watts S., Raza M., SaaS vs PaaS vs IaaS: What's The Difference & How To Choose. 2019 [cited 2021 18 Mayıs]; Available from: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/#:~:text=PaaS%3A%20Platform%20as%20a%20Service,use%20to%20create%20customized%20applications.

[26] Solutions, I. Cloud computing. [cited 2021 19 Mayıs]; Available from: https://icewaresolutions.com/cloud-computing/.

[27] Upadhyay I., 15 Important PaaS Example In 2021. 2021 [cited 2021 22 Mayıs]; Available from: https://www.jigsawacademy.com/blogs/cloud-computing/paas-examples/.

[28] Shim T., 15 Popular Platform as a Service (PaaS) Examples. 2021 [cited 2021 24 Mayıs]; Available from: https://www.webhostingsecretrevealed.net/blog/web-business-ideas/paas-examples/.

[29] Okutucu, B.O., Bulut Bilişim ve Teknolojileri. 2012.

[30] 1. Hou, T. SaaS vs. PaaS vs. IaaS: What You Need to Know. [cited 2021 26 Mayıs]; Available from: https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/#the-three-types-of-cloud-computing-service-models-explained.

[31] Upadhyay I., Hardware as a Service (HaaS): An Easy Guide in 5 Points. 2021 [cited 2021 28 Mayıs]; Available from: https://www.jigsawacademy.com/blogs/cloud-computing/hardware-as-a-service/#:~:text=Hardware%20as%20a%20Service%20(HaaS)%20model%20is%20synonymous%20with%20licensing,owning%20the%20underlying%20hardware%20itself.

[32] Lewis, G. Basics about Cloud Computing. 2010 [cited 2021 1 Haziran]; Available from: http://resources.sei.cmu.edu/asset_files/WhitePaper/2010_019_001_28877.pdf.

[33] Ünlü, Ç., Data Security and Privacy in Cloud Computing. 2019.

[34] Manyando, O., Technologies and Business Value of Cloud Computing: Strategy for the Department of Information Processing 2013.

[35] Citrix. Application Delivery and Security What is Public Cloud. [cited 2021 5 Haziran]; Available from: https://www.citrix.com/tr-tr/solutions/app-delivery-and-security/what-is-public-cloud.html.

[36] Shaptunova Y., 4 Best Cloud Deployment Models Overview

2021 [cited 2021 15 Haziran]; Available from: https://www.sam-solutions.com/blog/four-best-cloud-deployment-models-you-need-to-know/.

[37] Krishnan, Security and Privacy in Cloud Computing. 2017.

[38] Savu, L., Cloud Computing Deployment models, delivery models, risks and research challenges. 2011.

[39] Kalpana P, Laharika M., A Comparative Study of Different Deployment Models in a Cloud. 2013.

[40] T. Dillon, C. Wu and E. Chang, Cloud Computing: Issues and Challenges. 2010.

[41] Tinankoria Diaby, B.B.R., Cloud Computing: A review of the Concepts and Deployment Models. 2017.

[42] Roomi M., 6 Advantages and Disadvantages of Private Cloud | Limitations &

Benefits of Private Cloud. [cited 2021 24 Haziran]; Available from: https://www.hitechwhizz.com/2020/05/6-advantages-and-disadvantages-risks-benefits-of-private-cloud.html.

[43] 1. CtrlS. Private Cloud vs Public Cloud. [cited 2021 2 Temmuz]; Available from: https://www.ctrls.in/blog/private-cloud-vs-public-cloud/.

[44] M.Malathi, Cloud Computing Concepts. 2011.

[45] D, Tucakov. What is Community Cloud? Benefits & Examples with Use Cases. 2020 [cited 2021 8 Temmuz]; Available from: https://phoenixnap.com/blog/community-cloud.

[46] Sacic B., Hibrit Bulut Nedir? 2021 [cited 2021 14 Temmuz]; Available from: https://nttdata-solutions.com/tr/local-blog/hibrit-bulut-nedir/#.

[47] Innova. Hibrit bulut nedir ve nasıl çalışır? 2021 [cited 2021 23 Temmuz]; Available from: https://www.innova.com.tr/tr/blog/dijital-donusum-blog/hibrit-bulut-nedir-ve-nasil-calisir.

[48] Odunayo O. Owopetu, Private Cloud Implementation and Security. 2013.

[49] Blog, R. Hibrit Bulut Teknolojisi Nedir ve Avantajları Nelerdir? 2017 [cited 2021 28 Temmuz]; Available from: https://radore.com/blog/hibrit-bulut-teknolojisi-nedir-ve-avantajlari-nelerdir.html.

[50] Eyüpoğlu Ç., Bulut Bilişim, Geçiş Ve Türkiye'deki Mevcut Durum. 2013.

[51] ARSLAN M. Ş., Bulut Bilişim Uygulamaları ile Veritabanlarına Erişim: Ulakbim ve Üniversite Kütüphaneleri İçin Bir Model Önerisi. 2019.

[52] Henkoğlu T, Külcü Ö., Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme. 2013.

[53] Oyoyo Y. J., Adoption Of Cloud Computing In Government Instutions in Nigeria. 2018.

[54] Kılıç H., Kamuda Bulut Bilişim Kullanımına Yönelik Risk Analizi ve Yönetimi. 2017.

[55] Batı K., Bulut Bilişim Ve Etkileri. 2015

[56] Öz A., Bulut Bilişim Veri Güvenliği. 2013.

[57] Arslan B., Bulut Bilişim'in Avantajları Ve Dezavantajları. 2018.

[58] Dahshan M. M., Data Security In Cloud Storage Services. 2013.

[59] Şişman E. K., Bulut Bilişim Teknolojisi Yakın Gelecekte Vazgeçilmez Olacaktır. 2019.

[60] Öğretmen F. D., Güvenli Bulut Bilişim İçin Saldırı Tespit Sistemi Kullanımı. 2015

[61] Institute, S. Network Security Resources. 2021 [cited 2021 7 Ağustos]; Available from: https://www.sans.org/network-security/.

[62] Rapid7. Cloud Network Security Best Practices. [cited 2021 13 Ağustos]; Available from: https://www.rapid7.com/fundamentals/cloud-network-security/.

[63] Qaisar S., Khawaja K. F., Cloud Computing: Network/Security Threats And Countermeasures. 2012.

[64] DeMuro J. P., What is network security in the cloud computing era? 2010 [cited 2021 22 Ağustos]; Available from: https://www.techradar.com/vpn/what-is-network-security-in-the-cloud-computing-era.

[65] Akter L., Rahman M., Hasan, Information Security In Cloud Computing. 2013.

[66] Gupta G., Laxmi P.R., Sharma S., A Survey on Cloud Security Issues and Techniques. 2014.

[67] Michalsons. Cloud Compliance: What you need to know. 2020 [cited 2021 25 Ağustos]; Available from: https://www.michalsons.com/blog/cloud-compliance/22643.

[68] Algosec. Cloud Compliance. [cited 2021 27 Ağustos]; Available from:

https://www.algosec.com/cloud-compliance/.

[69] AWS. PCI DSS. [cited 2021 1 Eylül]; Available from: https://aws.amazon.com/tr/compliance/pci-dss-level-1-faqs/.

[70] Dutta P., Top 5 Benefits of Cloud Infrastructure Security 2020 [cited 2021 2 Eylül]; Available from: https://www.kratikal.com/blog/top-5-benefits-of-cloud-infrastructure-security/.
[71] Velev D., Zlateva P., Cloud Infrastructure Security. 2010.

[72] Almorsy, M., Grundy, J.C., & Müller, I., An Analysis of the Cloud Computing Security Problem. 2010.

[73] Singh A., Chatterjee K., Cloud security issues and challenges: A survey. 2016.

[74] Fritchen K.(2019), What Is Cloud Application Security. [cited 2021 7 Eylül]; Available from: https://managedmethods.com/blog/what-is-cloud-application-security/.

[75] Institute, I.M. Identity And Access Management For Cloud Security. 2021 [cited 2021 12 Eylül]; Available from: https://identitymanagementinstitute.org/identity-and-access-management-for-cloud-security/.

[76] Rosencrance L., Federated Identity Management. [cited 2021 14 Eylül]; Available from: https://searchsecurity.techtarget.com/definition/federated-identity-management.

[77] Imperva. Buffer Overflow Attack. [cited 2021 15 Eylül]; Available from: https://www.imperva.com/learn/application-security/buffer-overflow/.

[78] Kaczanowski M., What is a Buffer Overflow Attack – and How to Stop it. [cited 2021 15 Eylül]; Available from: https://www.freecodecamp.org/news/buffer-overflow-attacks/.

[79] Sumitra B., Pethuru C.R., Misbahuddin M., A Survey of Cloud Authentication Attacks and Solution Approaches. 2014.

[80] Dhange M., Sajjan R., Ghorpade V., A Survey on User Authentication Techniques and Attack Taxonomy in Cloud Computing. 2017

[81] Canner B., The Top 7 Password Attack Methods (And How to Prevent Them). [cited 2021 21 Eylül]; Available from: https://solutionsreview.com/identity-management/the-top-7-password-attack-methods-and-how-to-prevent-them/.

[82] SailPoint. 8 Types of Password Attacks. 2021 [cited 2021 21 Eylül]; Available from: https://www.sailpoint.com/identity-library/8-types-of-password-attacks/.
[83] Marchioro C. C., Data Security in Cloud Computing. 2019.

[84] Ranjan I., Agnihotri R. B., Ambiguity in Cloud Security with Malware-InjectionAttack. 2019.

[85]Positive Technologies, How to prevent SQL injection attacks. 2019 [cited 2021 4 Ekim]; Available from: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/.

[86] Guercio K., How to Prevent Cross-Site Scripting (XSS) Attacks. 2021 [cited 2021 4 Ekim]; Available from: https://www.esecurityplanet.com/endpoint/prevent-xss-attacks/.

[87] Kazim M., Zhu S. Y., A survey on top security threats in cloud computing. 2015.

[88] Davis R., Insecure API Cloud Computing: The Causes & Solutions. 2020 [cited 2021 10 Ekim]; Available from: https://www.extrahop.com/company/blog/2020/insecure-apis-cloud-computing-cause-solutions.

[89] Darwish M., Ouda A., Capretz L. F., Cloud-based DDoS Attacks and Defenses. 2013.

[90] Abusaimeh H., Distributed Denial of Service Attacks in Cloud Computing. 2020.

[91] Montasari R., Daneshkhah A., Jahankhani H., Hosseinian-Far A., Cloud Computing Security: Hardware-Based Attacks and Countermeasures. 2020.

[92] Dildar M. S., Khan N., Abdullah J. B., Khan A. S., Effective Way to Defend the Hypervisor Attacks in Cloud Computing. 2017.

[93] Icaev. How to audit the cloud. [cited 2021 17 Ekim]; Available from: https://www.icaew.com/technical/business-and-management/strategy-risk-and-innovation/risk-management/internal-audit-resource-centre/how-to-audit-the-cloud.

[94] Sattar S. A., Security Issues in Cloud Services. 2016.

[95] Upadhyay I., Broken Authentication: How to Prevent It, Examples and More. 2020 [cited 2021 24 Ekim]; Available from: https://www.jigsawacademy.com/blogs/cyber-security/broken-authentication.

[96] Mettu G.R., Patil D.A., Data breaches as top security concern in cloud computing. 2018.

[97] Cloud Insights Team, Top Cloud Security Breaches and How to Protect Your Organization. 2021 [cited 2021 28 Ekim]; Available from: https://cloud.netapp.com/blog/cis-blg-top-cloud-security-breaches-and-how-to-protect-your-organization.

[98] Judith S. Hurwitz, Bloor R., Kaufman M., Halper F., How to Reduce Security Breaches in Cloud Computing Networks. 2009 [cited 2021 1 Kasım]; Available from:

https://www.dummies.com/programming/networking/how-to-reduce-security-breaches-in-cloud-computing-networks/.

[99]Kumar P., Arri H. S., Data Location in Cloud Computing. 2013.

[100] Djemame K., Barnitzke B., Corrales M., Kiran M., Jiang M., Armstrong D., Forgó N. and Nwankwo I., Legal issues in clouds: towards a risk inventory. 2013.

[101] Kumar V., Rathore R. S., Security Issues withVirtualization in Cloud Computing. 2018.

[102] Almutairy N. M., Al-Shqeerat K. H. A., A Survey On Security Challenges Of Virtualization Technology In Cloud Computing. 2019.

[103] Topal B., Comparison of Methods of Sign-On. 2016

[104] Monir M. B., AbdelAziz M. H., AbdelHamid A. A., EI-Horbaty E. M., Trust Management in Cloud Computing: A Survey. 2015.

[105] Yancheshmeh A. S., Multi-Tenancy Security in Cloud Computing. 2019.

[106] National Security Agency, Mitigating Cloud Vulnerabilities. [cited 2021 3 Kasım]; Available from: https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF.

[107] Australian Cyber Security Centre, Cloud Computing Security for Tenants. [cited 2021 7 Kasım]; Available from: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-tenants.

[108] Velev, Dimiter & Zlateva, Plamena., Principles of Cloud Computing Application in Emergency Management. 2011.

[109] Virgillito D., What happens when data gets lost from the cloud? [cited 2021 7 Kasım]; Available from: https://cloudcomputing-news.net/news/2015/jan/26/what-happens-when-data-gets-lost-cloud/, .

[110] Zheng M., Virtualization Security in Data Centers and Clouds. 2011.

[111] Pandya T., Bhavsar M., Live Migration in Cloud and Its Security Concerns. 2015.

[112] EthicalHat. Network-based attacks. 2019 [cited 2021 17 Kasım]; Available from: https://www.ethicalhat.com/2019/08/network-based-attacks/.

[113] Yin, L., Study on Computer Forensics in Cloud Computing. Intl. Conf. on Computer Science and Service System. 2012

[114] Martini B. and Choo K.-K. R., Cloud storage forensics: ownCloud as a case study. 2013.

[115] Wyseur B., "white-box cryptography: hiding keys in software", MISC magazine. 2012.

[116] Ezirim K., Khoo W., Koumantaris G., Law R., and Perera I. M., Trusted Platform Module – A Survey. 2012.

[117] Hyper Scalers, Building Secure Clouds with TPM 2.0. [cited 2021 19 Kasım]; Available from: https://www.hyperscalers.com/secure-clouds-tpm-2.0-security-intel-spectre-meltdown-flaw.

[118] Boaro L. (2018), Keychain Services API Tutorial for Passwords in Swift. 2018 [cited 2021 21 Kasım]; Available from: https://www.raywenderlich.com/9240-keychain-services-api-tutorial-for-passwordsin-swift.

[119] Bibek K. (2018), Android Security – Part II: Android KeyStore and cryptography operations. [cited 2021 21 Kasım]; Available from: https://techdroid.kbeanie.com/2018/12/11/android-security-part-ii-android-keystore-and-cryptography-operations.

[120] Incalza D., Cryptographic Key Handling in Android: from software to StrongBox and everything in between. [cited 2021 21 Kasım]; Available from: https://proandroiddev.com/cryptographic-key-handling-in-android-from-software-to-strongbox-and-everything-in-between-b12b80d47cb0.

[121] Android Developers, Android keystore system. [cited 2021 21 Kasım]; Available from: https://developer.android.com/training/articles/keystore.

[122] Acosta D. E. (2021), How does Hardware Security Module (HSM) protect Payment Card Data? [cited 2021 21 Kasım]; Available from: https://www.advantio.com/blog/hardware-security-module-hsm-what-is-it-and-what-is-its-role-in-protecting-payment-card-data.

[123] Chatterjee R., Roy S., Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud. 2017.

[124] Çebi G., Homomorphic Encryption In Cloud Computing. 2019.

[125] Shallal, Qahtan & Bokhari, Mohammad., A Review on Symmetric Key Encryption Techniques in Cryptography. 2016.

[126] Asaithambi.N, A Study on Asymmetric Key Cryptography Algorithms. 2015.

[127] ElBeltagy M. K., StegoCrypt3D: 3D Object and Blowfish. 2019

[128] Sokoowski P., Design and Analysis of Cryptographic Hash Functions. 2016

[129] Sobti, Rajeev & Ganesan, Geetha., Cryptographic Hash Functions: A Review. International Journal of Computer Science Issues. 2012.

[130] Chung C.(2021), Introduction to Hashing and its uses. [cited 2021 25 Kasım]; Available from: https://www.2brightsparks.com/resources/articles/introduction-to-hashing-and-its-uses.html.

[131] Zhang J., Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues

[132] Sahai A., Water B., Fuzzy Identity-Based Encryption. 2005

[133] Kaaniche N., Cloud data storage security based on cryptographic mechanisms. 2015.

[134] Mr. Anup R. Nimje, Prof. V. T. Gaikwad , Prof. H. N. Datir, Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview. 2013.

[135] Wainakh A., In Partial Fulfillment Of The Requirements For The Degree Of Master Of Science In Cryptography. 2018.

[136] Melchor C. A., Gaborit C. A., and Herranz J., Additively homomorphic encryption with d-operand multiplications., in Crypto. 2010.

[137] Sander T., Young A., and Yung M., Non-interactive cryptocomputing for NC1, in Proceedings of the 40th Annual Symposium on Foundations of Computer Science. 1999.

[138] Jabbar I., Najim S., Using Fully Homomorphic Encryption to Secure Cloud Computing. Internet of Things and Cloud Computing. 2016.

[139] Aung T. H., SaaS in Business: Exploring Strategic Benefits and Considerations of Software as a Service (SaaS) Model in Business Organizations. 2014.

[140] Brunzel D. G. T., Cloud Computing Evaluation How it Differs to Traditional IT Outsourcing. 2010.

[141] Osaiasi A. E., Foleti K., Creatıon Of A Private Cloud Infrastructure. 2019.

[142] Owopetu O. O., Private Cloud Implementation and Security. 2013.

[143] Boronin M., Hybrid Cloud Migration Challenges. 2020.

ÖZGEÇMİŞ