CHAPTER 7

ATTACK, VULNERABILITY AND DEFENSE APPROACHES IN CLOUD SECURITY

Nafiz ÜNLÜ[1]

INTRODUCTION

Today, everyone, individuals and organizations, uses the cloud services on a certain level. The pay-as-you-go model makes it available for users of every economic scale (Seyrek, 2011). While individuals are using the cloud services for data storage, data backups, e-mails, etc., organizations tend to use it for virtual desktops, software development, data backups, data storage, data recovery, computing power, and strong security tools (Sarıtaş & Üner, 2013). While big organizations need bigger cloud services and resources, individuals only require a small amount of resources. Some of the biggest organizations may need data centers at multiple locations around the world, to deliver their services (Çelik, 2021). Cloud providers solve this problem with their secure big data centers around the world. These data centers also help the enterprises to open their business in other places and grow faster (Ersever et al., 2017). As an example to the use cases of cloud, gaming industries were using cloud for delivering their product to users in the past and today big companies are working on a new system that will enable the users to open games or programs their hardware can not open. With the help of the cloud's computing power and a strong Internet connection any device that satisfies the needs of cloud application will be able to open applications that normally with its hardware it could not (Göv & Erdoğan, 2020).

Cloud computing brings many benefits. Because it uses a "pay-as-you-go" model, it is cheaper in most cases than creating your own data center and physical server (Kavzoğlu & Şahin, 2012; Uslu et al., 2021). The cloud being globally scalable, fast and having easy access to a broad range of technologies increases performance and therefore productivity of customers. Third party cloud providers ensure strong security for the customer's work, customer and their service and therefore themselves. Also, data backup and disaster recovery provides reliability (Dokuz & Çelik, 2017).

[1] Assist. Prof. Dr., İstanbul Technical University, Informatics Institute, nafiz.unlu@gmail.com

We must also know that not all cloud computing systems are the same, they are separated into three different categories depending on the deployment methods. Public clouds are owned and managed by a trusted third-party cloud provider. It delivers the resources chosen by the customers (servers, storage, etc.) over the Internet. Private clouds are cloud computing resources which are dedicated to a single organization. Private clouds can physically exist on the organization's building or data center. Hybrid cloud integrates both these cloud services and brings them together with a technology which allows data and applications to be shared between these services.

Since the cloud contains services companies need to work on, necessary or confidential data etc., it becomes an important target for adversaries. So many important services depending on the cloud, makes it even more important to provide security (Tayaksi et al., 2016).

It is observed today that the developing technology has begun to affect the classical production processes. One of the most up-to-date technologies, Cloud Computing, combined with the classical production process, adds the concept of Cloud Production to the network-based production family. The concept of Cloud Production uses Cloud Computing, Internet of Things (IoT), advanced computing, virtualization and service-oriented technologies as infrastructure and is supported by other advanced production systems.

General Services of Cloud and Some of the Defense Mechanisms

Cloud security may refer to a sequence of policies, applications, technologies and controls used for protecting virtualized IP, data, services and applications. Different cloud services may require different sets of security precautions. Therefore, it is important to know some of the cloud services, what they are used for, how they work to understand why it is so important to provide security for it (Aksakallı, 2019).

Cloud computing services fall into four major groups (Figure 1): IaaS, PaaS, SaaS and serverless (Özdemir & Gökgöz, 2018; Andi, 2021).

In Infrastructure as a Service(IaaS), IT infrastructures (servers, storages, networks, OSs and VMs) can be rented by customers from a cloud provider on a pay-as-you-go basis. In IaaS, clients are responsible for keeping their data safe, controlling user access and application security. Unencrypted data, configuration mistakes, shadow services(rogue cloud accounts), user role-based permissions may cause security issues. To fix these issues, cloud security gateways (provides user activity monitoring, cloud malware detection, data loss prevention and en-

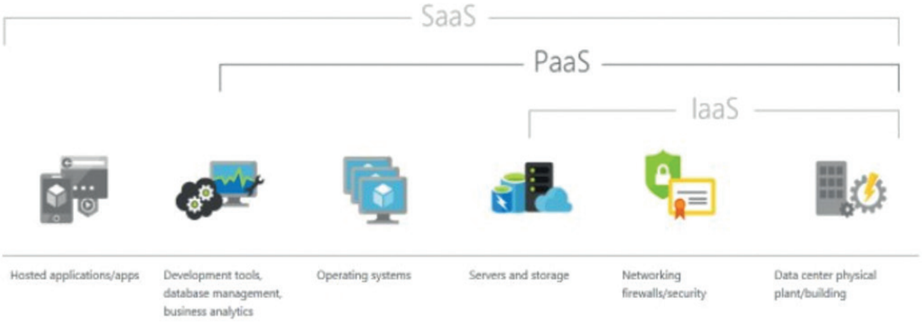
SaaS
PaaS
IaaS
Hosted applications/apps
Development tools, database management, business analytics
Operating systems
Servers and storage
Networking firewalls/security
Data center physical plant/building

Figure 1. Cloud computing services

cryption), cloud workload protection platforms (discovers workloads and containers, applies malware protection, and manages workload instances and containers that if any left unmanaged and cause damage), virtual network security platforms (includes network intrusion detection and prevention -NIDS) and cloud security posture management (audits cloud environment for security and compliance issues) are being used by the cloud providers (Paşaoğlu & Cevheroğlu, 2020).

Platform as a Service (PaaS) provides an environment for developing, testing, delivering and managing software applications. Using threat modeling, checking for software vulnerabilities, implementing improved access controls, managing out of use accounts and taking advantage of resources given by providers (guidelines for platforms) ensures an enterprise's data and application security in the cloud. Using security gateways, workload protection platforms and necessary security managements are used as a security solution. In addition, enterprises can use third party security applications to protect their data and applications against attackers,too (Giessmann & Stanoevska-Slabeva, 2012).

Software as a Service (SaaS) is a method for delivering software applications over the Internet, on a subscription basis. Cloud providers host and manage the software applications inside the infrastructure. They handle any maintenance situations like software upgrades and security patches (Tsai et al., 2014).

In SaaS, providers handle the security processes for cloud services against attacks like phishing and ransomware. Providers are responsible with securing the platform, network, applications, OS and physical platform. Providers are not responsible for securing customer data or user access because these are the responsibilities of the customer (Tang & Liu, 2015).

Detecting untrusted services and compromised accounts, applying identity and access management, encrypting cloud data, enforcing data loss prevention, monitoring collaborative sharing of data are some of the security methods used by the providers. In addition, services like malware prevention, data loss prevention are also used for providing security.

Serverless computing's main interest is building app functionality without spending time on repeatedly managing the cloud servers. The system provider handles the setup, necessary planning, and server management for customers. Serverless architectures are event-driven, only using resources when a specific situation happens. Within this structure, more potential points of attack exist. The providers handle OS, runtime, security and patching.

Vulnerabilities and Attack Vectors on Cloud

As discussed early on in the previous parts, cloud has access to many different applications and services which people use to build their business on. They run servers, use it's data centers for storage and even use it's own security applications for security. When all these come together, or even when they are observed separately, the cloud becomes a target for malicious intended people or organizations. To maintain sustainability, cloud providers care about security more and more. While cloud providers try to fix the loopholes, adversaries try even more

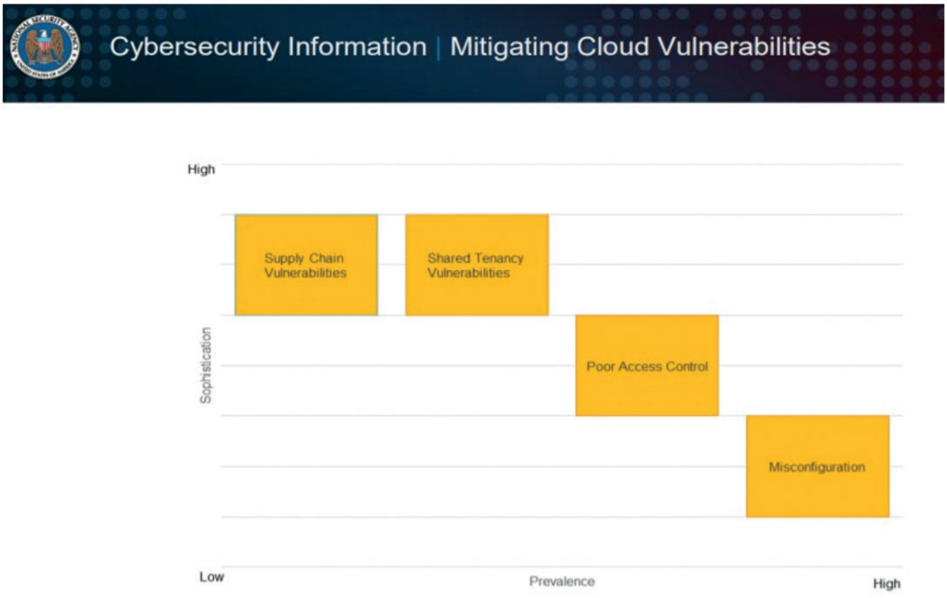

Figure 2. Cloud Vulnerabilities

to find some vulnerability and get what they want. This little attacker-defender cycle causes security systems to grow better and provide better service to their customers.

Here is a chart that shows, according to NSA (National Security Agency-USA), four classes of security vulnerability in the cloud (Bendiek & Schulze, 2021; Figure 2):

Security Vulnerabilities in Cloud

Below, there are some information about some of the major vulnerabilities in the cloud and how to stay protected against them. The importance of using an advanced incident response plan should be noted for each vulnerability (Christen et al., 2020).

Security Vulnerabilities in Cloud

Putting inadequate restrictions to prevent unauthorized access to cloud infrastructure may be riskful. Cloud contains a rich source of data waiting for adversaries to take it. According to a report by a security firm, almost 70 million records were stolen or leaked in 2018 because of misconfigurations (Neto et al., 2021).

1. A Misconfiguration could lead to;
2. Allow an attacker to access a customer's cloud-based servers and cause data exfiltration.
3. Negative impact to brand
4. To prevent Misconfiguration from happening;
5. Cloud storage security configurations should always be checked twice.
6. Specialized tools can be used to check cloud storage security configurations on a routine and give warnings of vulnerabilities.

Insecure APIs

Application user interfaces (APIs) are used for upgrading efficiency of cloud computing and provide convenience. APIs make it easier to share information between two or more applications (Ma et al., 2018).

Insecure APIs could lead to;

1. Adversaries launching DDoS attacks.
2. Inadequate authentication: APIs created without suitable authentication controls can be open to the Internet and cause anyone accessing enterprise data.
3. Insufficient authorization: Sloppy developed APIs do not have suitable authorization controls in place. Backend data becomes compromised.

To prevent Insecure APIs;

1. Designing APIs that has strong encryption, authentication, access control and activity monitoring.
2. Running penetration tests to imitate
3. API attacks.
4. Using strong SSL/TLS encryption on transferred data.

Loss or Theft of Intellectual Property

Intellectual properties are one of the most important assets of an organization. Data stored online is vulnerable against security threats. Data breaches mostly affect small businesses because they do not have the same standard of protection as big global corporations (Morrow, 2012).

L&T of IP could lead to;

1. Data alteration: Changing of existing data and previous backups can result in loss of data integrity.
2. Data deletion: Adversaries could delete sensitive data from the cloud and cause severe damage to an organization's operations.
3. Loss of access: Adversaries can perform a ransomware attack or encrypt data with strong encryption keys until their malicious goal is fulfilled.
4. Regulatory fines and penalties on firms

To prevent L&T of IP;

1. Frequent backups are very important and effective against data loss or theft.
2. Using data loss prevention (DLP) software to detect and prevent malicious activities.
3. Encrypting stored data.
4. Using secure and encrypted servers to retrieve data.
5. Routine security audits to know who has access to data at all times.
6. Having offline backups (especially against ransomware).

Loss of Control Over End-User Actions - Malicious Insiders

Companies have to monitor how their employees use cloud computing systems. If they don't, they can lose control of their data and eventually become vulnerable to threats from within and without. Insiders do not have to break through firewalls, IDSs or other security defenses. Insiders could access confidential data in the cloud without much of a problem (social engineering) (Magklaras & Furnell, 2005).

Loss of Control Over End-User Actions could lead to;

1. Loss of intellectual property (Stolen data)
2. Data alteration and deletion
3. Sabotaging of IT systems

To prevent Loss of Control Over End-User Actions;

1. Integrating surveillance, monitoring, escalation, post-incidence analysis, remediation, investigation and incident response with the company's security plan.
2. Training employees about handling security vulnerabilities (importance of regularly changing passwords or protecting confidential information carried outside with physical devices)
3. Running audits routinely
4. Limiting access to confidential data (employees should not be accessing data they do not need to know)

Compliance Violations and Regulatory Actions

Companies must put unchangeable rules to regulate which user can access which data and limit their actions with it. The "shared responsibility model" given by cloud providers signifys that providers will provide cloud security, but customers must preserve their own data security in the cloud (Bharadwaj et al., 2018).

Compliance Violations could lead to;

1. Data breach
2. Inside attacks

To prevent Compliance Violations;

1. Keeping track of all users, roles and access permissions.
2. Maintaining strong configuration management

System Vulnerabilities

System vulnerabilities could happen for many different reasons. Integrating insecure third party applications or poorly configured security tools could create security risks (Padhy et al., 2011; Bisong & Rahman, 2011; Figure 3).

To prevent system vulnerabilities;

1. Encrypting data
2. Implementing a strong IDS
3. Deploying a WAF

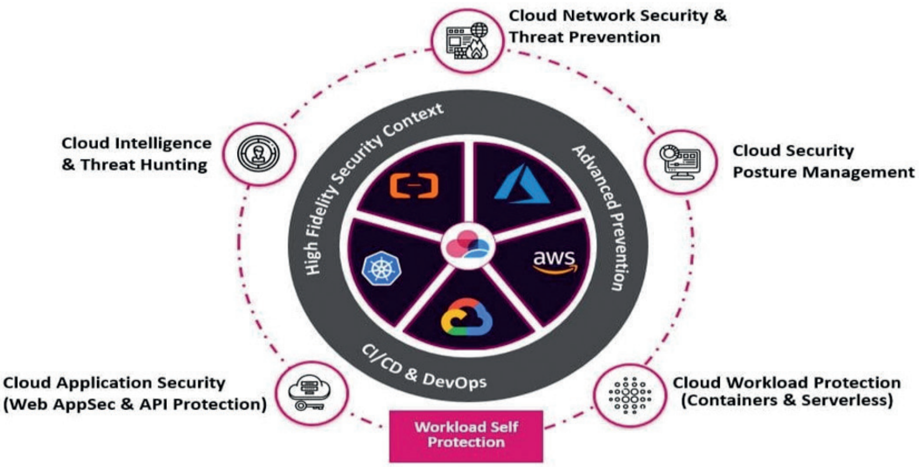
Cloud Network Security & Threat Prevention
Cloud Intelligence & Threat Hunting
Cloud Security Posture Management
High Fidelity Security Context
Advanced Prevention
aws
CI/CD & DevOps
Cloud Application Security (Web AppSec & API Protection)
Cloud Workload Protection (Containers & Serverless)
Workload Self Protection

Figure 3. Above is a cloud security pillars diagram of cloud computing providers

Attack Vectors and Countermeasures

Attackers' main goals with cyber attacks are obtaining access to confidential user data and stopping users from accessing cloud services. Both these situations can lead to major damage to both users and providers (Modi et al., 2013).

Since the attackers are always working on developing more and more improved attacking methods, there are so many alternative ways to attack cloud services.

1. Take advantage of vulnerabilities in the cloud system
2. Stealing confidential data with social engineering
3. Acting as a malicious insider
4. An attacker stealing a user's data and legitimately accessing the cloud system as if he/she is the user.

Usually threats come from either inside or outside of network, but in cloud computing security threats take place in three different levels: application level, network level and user level. Below are some of the example attacks for each different level (Hao et al., 2009).

Application Level Attacks

Application level security issues mean intrusion from attackers because of vulnerabilities of the sharing focused nature of the cloud system (Hao et al., 2009).

Cloud Malware Injection Attack

Malware injections are used for taking control of users' information. To accomplish this goal, a malicious VM instance or an infected service implementation module such as SaaS or IaaS is injected into the cloud, making the cloud think that the new instance is valid. If sucds, the user requests will be sent automatically to the new instance instead of the actual site user wants to access. In the redirected site, malicious code is executed and the attacker begins his/her malicious activities. Some of these activities are manipulating data, altering data, stealing data and eavesdropping attacks. The most seen malware injection attacks are SQL injection attacks and cross-site scripting (XSS) attacks (Gupta & Gupta, 2017).

In an SQL injection attack, an unauthorized person gains access to the database of an application (can read, modify or execute administration operations) by inserting malicious codes into the SQL code. Attackers target SQL servers containing vulnerable database applications. SQL injection could be avoided by using parameterized queries in the code. It is also important to make sure only the privileged users who have permission to access the database can access it.

In the cross-site scripting attacks (XSS), attackers add malicious scripts (Flash, JavaScript, etc.) to a vulnerable web page. An attacker can use XSS to send a malicious script to an unsuspicious user. The target's browser does not know that the script is malicious and then executes the script (thinking it is coming from a trusted source). The malicious scripts can access any cookies or sensitive information held by the browser. These malicious scripts could change the contents of the HTML page, too (Gupta & Gupta, 2017).

ARP Poisoning Attack

Address Resolution Protocol (ARP) is a protocol used in network communications. ARP translates IP addresses to MAC addresses. In ARP poisoning attacks, ARP is exposed to MitM attack. The attacker intercepts communications between devices in the network. Then, the attacker could alter communications or perform session hijacking (Bruschi et al., 2003).

Using VPNs, static ARP, packet filtering may minimize the effects of this attack.

Cookie Poisoning Attack

Cookie poisoning or session hijacking, is an attack type, in which the attacker obtains unauthorized access into a webpage or an application by stealing or changing the substances of the cookie. In the SaaS model, cookies hold user information which lets the applications authenticate the user identity (Prapty et al., 2020).

Using proxy data inspection and encrypting cookie data may prevent cookie poisoning attacks.

Malicious Insider Attacks

Insider attacks are caused by a legitimate user (someone who works for the firm) acting malicious, intentionally, knowing what he/she is doing. The attacker could be currently working for the firm (employee), working with the firm (client). It could be someone who worked for or with the firm in the past, too. The common point of all this possible person is that they use their in company privileges for malicious intent and activities. They could cause any kind of damage to the enterprise by violating security policies (Khan et al., 2019).

To prevent or at least reduce the harms of insider attacks, cloud architectures containing different authorization levels could be designed. With such designs, employees can not access the data they do not need to know. Also strict security policies in the building should be applied since physical security is as important as digital security.

Backdoor Attack

The backdoor is a hidden access to an application. Backdoors may be created intentionally (malicious) or unintentionally (carelessness) by developers at the coding stage (Ohm et al., 2020).

Attackers can use backdoors to pass security measures and lurk around undetected doing their malicious activities.

Network Level Attacks

Cloud computing services work depends on network infrastructures. Therefore, security threats which originate from vulnerabilities caused by these network infrastructures may occur (Almorsy et al., 2016).

Domain Name System (DNS) Attacks: DNS attacks are caused by attackers using vulnerabilities of DNS. These attacks directly focus on DNS infrastructure. These attacks may render the DNS as unavailable. Since DNS is used by network based applications such as e-mail, web browsers, e-commerce many different type of attacks could happen. Such as network floods, subdomain attacks, cache poisoning etc. DNS attacks may be used combined with some other attacks, too.

Denial of Service Attack: In DoS attacks, the attacker floods the target machine with a massive number of requests. Since the target machine can not handle this much request in such a short time, it gets overloaded and becomes unavailable. The cloud system begins to provide more computational power for the extra process demand coming from the system. Providing more computational power slows down the cloud system too and people begin to have trouble accessing their cloud system. Because of the unique characteristics of this attack, it is not possible yet to create an absolute solution to this high level threat.

Man in the Middle Attack: MitM attack is an intrusion, where intruder remotely interrupts a conversation or data transfer between two entities and either stealing data, altering data or doing both unnoticed. The intruders may install a packet sniffer to analyze network traffic for insecure communications.

To reduce the harm and efficiency of MitM, packet filtering, static code analysis, firewalls and manual penetration tests can be used.

User Level Attacks: The user level attacks are a malicious attempt to steal user identity information. One of the most common examples for user level attacks is phishing attacks. Phishing attacks work by sending an email which contains a link leading the attack victim to a fake website. This website looks almost the same as the original one, except for a few minor changes, for example a few different letters in domain name. All the contents of this site are malicious and when a user tries to log in as they usually do with the original website, their username and passwords get stolen by the attacker. Other than this, attackers may send an email imitating legitimate corporations or enterprises. If user gets deceived, attackers may get username and password information for so called reasons.

Updating email policies, planning for ID theft after a data breach, regularly updating OSs and applications, implementing message authentication, using spam filters, giving basic level security training to users are some of the countermeasures against phishing attacks.

Vulnerabilities and Attack Vectors on Cloud

As seen in previous chapters, cloud computing systems are always under risk of being attacked. Therefore, both cloud providers themselves and clients try to keep their application safe. To keep the cloud servers and applications safe, either the options offered by the providers or a third party security application which is chosen by the client can be used. These security applications contain WAFs, Firewalls, IDS and IPS systems (Byrne, 2006). Even if these applications are used for safety, they are not enough on their own. Cloud computing systems always need strong safety policies, too. Below are some of the basic policies and security mechanisms that must be used, followed and done:

Physical Security: Cloud providers must physically secure IT hardware against situations of unauthorized access, interference, etc. (any activity that can be related to social engineering attack). Also must be prepared for natural disaster situations.

Identity management: A strong identity management will have a stronger effect on controlling access to information resources. Therefore, any kind of sensitive data will be safe against attacks that may be because of abuse of power.

Privacy: Providers must make sure that all the confidential data entrusted with them is safe and encrypted. Unauthorized users should not have access to encrypted data..

Penetration Testing: Performing offensive security tests on the system will help to find security weaknesses in it. In this method it is possible to simulate all the possible attack types.

Confidentiality: Other than authorized users should not be able to access sensitive data.

Data must be kept strictly confidential.

Integrity: Data should not be altered. Therefore, backups should be kept in trusted servers or locations (could be online or offline).

Encryption: Encryption is not only used to encrypt critical data but it is also used in communication and end-to-end encryption (for the data uploaded to the cloud).

Security audits: Conducting regular external audits is very important to detect the vulnerabilities before they become a real problem.

Using strong passwords: Using a password manager, protecting all physical devices, creating backups regularly, using IDS and IPS systems, and avoiding accessing critical data on public Wi-Fi are also important.

IDS and IPS systems: IDS and IPS systems are used for detecting and preventing malicious activities. Clients could either accept any IDS/IPS system that is offered by the cloud provider, or they can use any other third party system, too. These systems could either be on the cloud provider's system, or physically exist in the enterprise's building. These systems could be network based (NIDSNetwork Intrusion Detection Systems) or host based (HIDS- Host Based Intrusion Detection Systems). NIDS are used for watching the traffic from the network, analyzing it and checking the traffic for any kind of malicious activity by comparing it with a library of known attacks. HIDS watches every device that is connected to the network and warns the accountable principal.

Conclusion

This study presents the security of the cloud. A brief summary about cloud infrastructures followed by general cloud services. Then, we can see what causes vulnerabilities and how to avoid them with the right security policies. We can see that most of the vulnerabilities are (other than the malicious intended ones) caused unintentionally. Afterwards, we see the attack vectors, how they work, what causes them to happen, are all of them intentional or some of them happen because of negligence. What are their harm to the cloud, cloud provider and the client, how can they be prevented. Finally, in the defense mechanisms part, it is seen that although IDS and IPS applications are very crucial for security, policies are at the center of the security mechanisms. Since even if the strongest IDS/IPS applications are used, without a strong security policy and an advanced incident response plan, we can never say our system is safe.

REFERENCES

Aksakallı, İ.K. (2019). Bulut bilişimde güvenlik zafiyetleri, tehditleri ve bu tehditlere yönelik güvenlik önerileri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 5(1), 8-34.

Almorsy, M., Grundy, J., & Müller, I. (2016). *An analysis of the cloud computing security problem*. arXiv preprint arXiv:1609.01107.

Andi, H. K. (2021). Analysis of serverless computing techniques in cloud software framework. *Journal of IoT in Social, Mobile, Analytics, and Cloud,* 3(3), 221-234.

Bendiek, A., & Schulze, M. (2021). *Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW (No. 11/2021)*. SWP Research Paper.

Bharadwaj, D. R., Bhattacharya, A., & Chakkaravarthy, M. (2018, November). *Cloud threat defense–A threat protection and security compliance solution.* In 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) (pp. 95-99). IEEE.

Bisong, A., & Rahman, M. (2011). *An overview of the security concerns in enterprise cloud computing*. arXiv preprint arXiv:1101.5613.

Bruschi, D., Ornaghi, A., & Rosti, E. (2003, December). *S-ARP: a secure address resolution protocol*. In 19th Annual Computer Security Applications Conference, 2003. Proceedings. (pp. 66-74). IEEE.

Byrne, P. (2006). Application firewalls in a defence-in-depth design. *Network Security*, 2006(9), 9-11.

Christen, M., Gordijn, B., & Loi, M. (2020). *The ethics of cybersecurity* (p. 384). Springer Nature.

Çelik, K. (2021). Bulut Bilişim Teknolojileri. *Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 12(24), 436-450.

Dokuz, A.Ş., & Çelik, M. (2017). Bulut Bilişim Sistemlerinde Verinin Farklı Boyutları Üzerine Derleme. *Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi*, 6(2), 316-338.

Ersever, B., Doğru, İ. A., & Dörterler, M. (2017). Büyük ölçekli veri merkezleri için bulut bilişim kullanarak sunucu sanallaştırma. *Gazi Mühendislik Bilimleri Dergisi*, 3(1), 20-26.

Giessmann, A., & Stanoevska-Slabeva, K. (2012). Business models of platform as a service (PaaS) providers: Current state and future directions. *JITTA: Journal of Information Technology Theory and Application*, 13(4), 31.

Göv, S.A., & Erdoğan, D. (2020). Dördüncü Endüstri Devriminin (Endüstri 4.0) Neresindeyiz?. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi*, 7(2), 299-318.

Gupta, S., & Gupta, B. B. (2017). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management*, 8(1), 512-530.

Hao, S., Syed, N. A., Feamster, N., Gray, A. G., & Krasser, S. (2009, August). *Detecting Spammers* *with SNARE: Spatio-temporal Network-level Automatic Reputation Engine*. In USENIX security symposium (Vol. 9).

Kavzoğlu, T., & Şahin, E. K. (2012). *Bulut Bilişim Teknolojisi Ve Bulut Cbs Uygulamaları.* IV. Uzaktan Algılama ve Coğrafi Bilgi Sistemleri Sempozyumu, Zonguldak.

Khan, A. Y., Latif, R., Latif, S., Tahir, S., Batool, G., & Saba, T. (2019). Malicious insider attack detection in IoTs using data analytics. *IEEE Access*, 8, 11743-11753.

Ma, X., Wang, Z., Zhou, S., Wen, H., & Zhang, Y. (2018, June). *Intelligent healthcare systems assisted by data analytics and mobile computing.* In 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 1317-1322). IEEE.

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. Computers & Security, 24(5), 371-380.

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. *The journal of supercomputing,* 63(2), 561-592.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security*, 2012(12), 5-8.

Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality (JDIQ),* 13(1), 1-33.

Ohm, M., Plate, H., Sykosch, A., & Meier, M. (2020, June). *Backstabber's knife collection: A review of open source software supply chain attacks.* In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 23-43). Springer, Cham.

Özdemir, A., & Gökgöz, B. (2018). Bulut bilişimde felaket kurtarma tekniklerinin incelenmesi. *Internatıonal Symposium on Innovative Approaches in Scientific Studies,* 3, 202-213.

Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2011). Cloud computing: security issues and research challenges. *International Journal of Computer Science and Information Technology & Security (IJCSITS),* 1(2), 136-146.

Paşaoğlu, C., & Cevheroğlu, E. (2020). Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması. *Bilişim Teknolojileri Dergisi*, 13(2), 183-195.

Prapty, R. T., Md, S. A., Hossain, S., & Narman, H. S. (2020, April*). Preventing session hijacking using encrypted one-time-cookies.* In 2020 Wireless Telecommunications Symposium (WTS) (pp. 1-6). IEEE.

Sarıtaş, T., & Üner, N. (2013). Eğitimdeki yenilikçi teknolojiler: Bulut teknolojisi. *Eğitim ve Öğretim Araştırmaları Dergisi*, 2(3), 192-201.

Seyrek, İ. H. (2011). Bulut Bilişim: İşletmeler için Fırsatlar ve Zorluklar. *Gaziantep University Journal of Social Sciences,* 10(2). 701-713.

Tang, C., & Liu, J. (2015). Selecting a trusted cloud service provider for your SaaS program. *Computers & Security*, 50, 60-73.

Tayaksi, C., Ada, E., & Kazançoğlu, Y. (2016). Bulut Üretim: İşlemler Yönetiminde Yeni Bir Bulut Bilişim Modeli. *Ege Academic Review*, 16, 71-84.

Tsai, W., Bai, X., & Huang, Y. (2014). Software-as-a-service (SaaS): perspectives and challenges. *Science China Information Sciences*, 57(5), 1-15.

Uslu, B., Eren, T., & Özcan, E. (2021). Bulut Bilişim Güvenliği Etki Düzeylerinin Değerlendirilmesi. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 7(1), 47-60.