A Comprehensive Survey on Security Threats and Countermeasures of Cloud Computing Environment

Abeer F Alotaibi[a], Mohammed A. AlZain[a], Mehedi Masud[a], and NZ Jhanjhi[b]

[a]College of Computers and Information Technology,Taif University, Al-Hawiya, 21974, KSA
[b]School of Computer Science and Engineering, SCE, Taylor's University, Malaysia

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: Cloud computing technology is one of the biggest breakthroughs in technology and business boom. This technology is service oriented that focuses on reducing costs, minimizing devices and paying for used service only. This paper surveys recent research on security threats and countermeasures of cloud computing environment. It begins by explaining cloud computing definition with its layers. In addition, it provides a brief explanation of the common characteristics of cloud computing service models and deployment models. Authentication and access control in cloud computing will be given at end of this work.

Keywords: Cloud computing, security threats, cloud security.

1. Introduction

Cloud computing is one of the fastest evolving technologies, while everyone in various fields use cloud computing on a daily basis, such as Microsoft Office 365, Gmail Dropbox, Gmail, etc (P. R. Kumar,2018) Data stored on the servers which can be accessed by an easy and simple authentication by the internet, can use it anywhere in the worl(L. Malhotra,2014). Reflecting the concept of the cloud, a distributed system consisting of multiple virtual machines is dynamically provisioned in order to meet and fulfill the customer's variable resource requirements as the entire base of this customer and cloud relationship are subject to the service level agreement (SLA)(S. Basu,2018; R. Buyya,2009). Although cloud computing has comprehensive and well-understood characteristics, there are shortcomings in its security situation. From this aspect, it is still complex and must be properly addressed in order to be able and to take benefit of cloud services with more performance and efficiency(N. Amara,2017). Cloud service suppliers and providers must meet the myriad of regulatory concerns in order to offer cloud services with minimal risks. The cloud is a central data that authorizes the user to store and retrieve the data in the cloud and perform operations on it to modify, save and delete at any time(C. Modi,2013). The concept of the cloud reduces the continuous essential to maintain an internal data center. The main concept of cloud is relocation the company or organization data to a remote site on the provide cloud site(C. Modi,2013). The cloud led to the minimum investment, reducing costs and rapid deployment of the main factors. The factors that lead to benefit from cloud services and make it important and a priority for many institutions proved that 91% of institutions in Europe and the United States have reduced the cost which was the main reason for migrating it to the cloud(C. Modi,2013; J. Che,2011). In 2007 October Google and IBM have been cooperated which led to that cloud computing has become famous and more attentive(S. M. Hashemi,2012). Cloud computing implements in several forms and models, such as public cloud, private cloud, community cloud and hybrid cloud(T. Diaby,2017).

The remainder of this paper is organized as follows: second section discusses cloud computing layers with its models. Third section discusses Cloud computing threats, attack, data protection techniques as well as authentication and access control in cloud computing model. Section four will conclude the paper.

2. Cloud computing layers

In Cloud computing, many computers access services from the Internet. As the cloud computing offers many reliable services to the customer. Cloud computing offers different services to users such as hardware, software, information access and capacity. It is divided into three layers as it includes the first layer Cloud Computing Deployment models which contains public cloud, private cloud, community cloud and hybrid cloud(A. Panah,2012). The second layer cloud computing characteristics which are On-demand self-service it's based on nature of cloud computing releasing depend on user request. Then broad network access, Resource pooling which are establish resources that could be infrastructure, storage, platform, or data. The rapid elasticity that's provide the flexible provisioned(F. F. Moghaddam,2013). The measure service and finally cloud computing delivery models which it's are Software as a Service (SaaS), The Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Figure2.1. Shows the Cloud Environment Architecture could be.

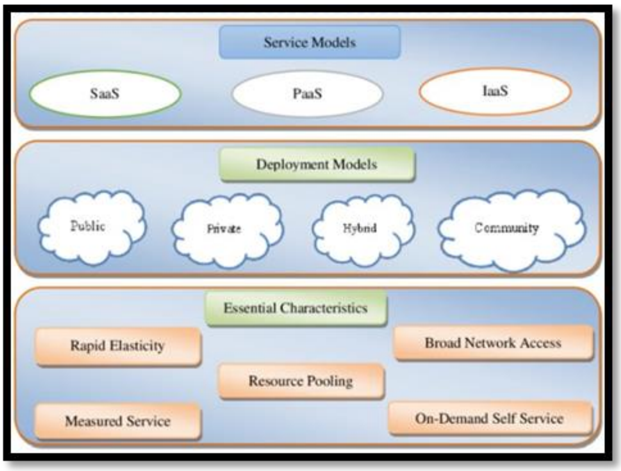


Figure 1.Cloud Environment Architecture adopt from NIST (Y.-C. Lee, H. 2012)

2.1 Cloud computing deployment models

This section will discuss in detail the categories of cloud deployment, as there are four categories of cloud computing deployment, each of which will be explain as follows

- **Private cloud**

This form works privately on behalf of the company and that means that this type cannot be accessed by the public. The private infrastructure provides the cloud for the private and specific use of the company or institution and is used only by members of the same organization or company, as it cannot be accessed by Any other institution**.** Among its features are some services such as reliability, flexibility, data security, and scalability , The organization's network must be the administrator of a service provider for the data center due to virtualization and also distributed computing to supply all members.

- **Public cloud**

The public cloud is one of many deployment models which is the infrastructure and computing resources existing for public over the Internet (W. A. Jansen 2011). Where it can be accessed by the general public as it is characterized by being on a large scale. Public cloud services are provided by a provider and there are two ways to use as pay or it can be offered as a free to consumer (L. Malhotra, 2014; A. Singh, 2012). An external vendor is someone who maintains and manages the resources at the physical location of the service provider (L. Malhotra, 2014; S. M. Hashemi 2012). The services of these cloud vendors, for example: Amazon EC2, Salesforce.com, Microsoft Azure, Google App Engine and Microsoft Azure (T. Dillon, 2010).

- **Community cloud**

Community cloud defined as group between the public cloud and the private cloud, as it can be used by a group of institutions or partnerships for specific and private purposes (M. Odeh, 2017; G. Briscoe 2009) . It is possible to put the community cloud either on hypothesis or outside the hypothesis in addition to that the responsibility of building, managing, and operating the community cloud is by one or several organizations or a third party or a grouping of the three.

- **Hybrid cloud**

The hybrid cloud is an assembly of two or three clouds, which may be private, public, or community, which remain a unique structure, but have shortcomings, through standard technology or may be owned by enabling data and the application to be able to move. Hybrid cloud has more flexibility and strength than private cloud and public cloud. Figure2.2. Shows Cloud Computing Deployment. Whereas Table 2.1 shows overview of cloud model.

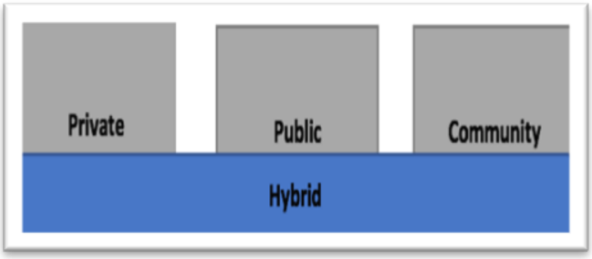
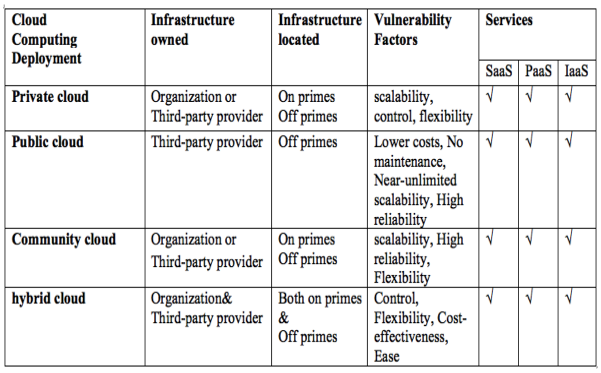


Figure 2. Cloud computing deployment model

Table 1: Overview of Cloud Model



Cloud Computing Deployment	Infrastructure owned	Infrastructure located	Vulnerability Factors	Services		
				SaaS	PaaS	IaaS
Private cloud	Organization or Third-party provider	On primes Off primes	scalability, control, flexibility	√	√	√
Public cloud	Third-party provider	Off primes	Lower costs, No maintenance, Near-unlimited scalability, High reliability	√	√	√
Community cloud	Organization or Third-party provider	On primes Off primes	scalability, High reliability, Flexibility	√	√	√
hybrid cloud	Organization& Third-party provider	Both on primes & Off primes	Control, Flexibility, Cost-effectiveness, Ease	√	√	√

2.2 Characteristics of cloud computing

There are five basic characteristics of Cloud Computing According to the NIST definition of cloud computing as following

- **On-demand self-service**

It is the provision of resources at the request by the user. That is, a self-service that allows users to use computing capabilities, such as applications as well as time and network storage. For the user does not need an official or support to meet the request manually. Demand and execution are automated, so provides this feature to the service provider as well as its consumer.

- **Broad network access**

It is the access to resources through networking or through available internet any time by consumer platforms such as mobile phone, laptop and desktop computers.

- **Resource pooling**

A multi-tenant model is used where the users computing resources are collected and served by a multiple user service provider, so resources assigned dynamically to a user that's after the user finishes it. then provided according and specifically to the user's request.

- **The rapid elasticity**

It is the capability and ability to provide computing resources quickly and also with high flexibility as the issuance may be automatic in order to expand externally and internally. there is advantage that allow consumer to customize in terms of quantity and time. This scale is suitable for customer demand.

- **The measure services**

It is the ability of the cloud to monitor the use of resources and prepare reports, control the cloud system and improve it automatically. It is also a measurement capacity that is used as an abstraction of a phase as it works as appropriate for the specific type of service. Full transparency is provided to each provider and user.

2.3 Cloud computing delivery models

This section shows three types of the delivery model in cloud computing model .

- **Software as a Service (SaaS)**

In this service, the cloud service provider provides software services which provides the ability to consumers using applications that run the cloud infrastructure. As consumers do not need to manage the software architecture and also maintain the programs and basic infrastructure. That means it is a software licensing model. A consumer requests to license the software on a subscription basis and is then hosted centrally on the cloud. As the consumer owned different devices, they can access applications through client interfaces, for example, browsers page (web-based, e-mail, etc.).

- **Platform as a Service (PaaS)**

It is a central layer in the cloud services, it's layer above IaaS. The programming environment is for the consumer to access and use the application. The application is provided by the providers as the providers provide the development environment and the tool kits. Development a set of tools are presented in the cloud and the clients used by browser for example "Google Search Engine". It is provided by the providers from planning, design, build applications and then deployment, and finally testing, maintenance. The platform is a layer as a cloud service. It works like IaaS, but the difference is that it provides an additional level of "rented" functionality.

- **Infrastructure as a Service (IaaS)**

It is only one cloud layer for the tenant where the resources allocated to the cloud computing resource are only shared with contracted consumers in exchange for a fee per user. As a result, it greatly minimizes necessary huge investments in computing devices like server or network devices. In addition, it allows varying the flexibility of functional doesn't exist in internal data centers or even with clustering services, the resources of computing can be entered or released faster with cost-effectively compared to an on-premises data center or with an aggregation service. Users can dynamically expand and contract these computing resources on request. A lot of renters exist on the same infrastructure resources, for example amazon EC2 and Microsoft Azure Platform. Figure2.3. illustrates summaries of three types of service providers.

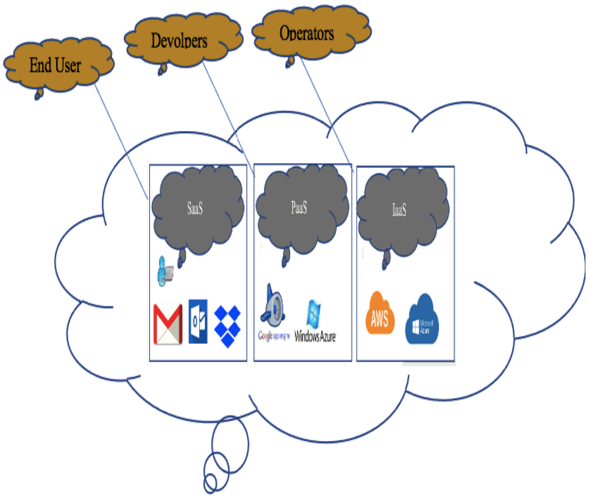


Figure 3. Summaries of three types of service providers.

3. Cloud computing security

Security is a guarantee that the data will not be damaged, lost or violated, as it can only be accessed by these authorized users. Losses of Confidentiality, Integrity, and Availability (CIA) can have a substantial impact on a cloud computing business and it is the data that is a fundamental component of any business. The key goals of Cloud computing is data confidentiality. Confidentiality is through encryption and reliance on the key distribution. Cloud computing may face some problems that may relate to the key and how the key can be accessed and exchanged safely. In addition, the Platform as a Service (PaaS) requires application keys for all APIs as well as service calls from any other application. Therefore, access to these applications and data must be secure and encrypted(M. Almorsy,2016). Integrity is one of the most essential principles of the cloud computing security.

Data that uploaded to the cloud cannot be modified by unauthorized access(P. Ora,2015). Availability determines the time in the system and the absence of interruptions or slow down (Z. Chaczko,2011).

3.1 Cloud threats

This section is about the most important problems and threats that face cloud computing environment. There are many issues in cloud security even with the development of technology researches and mechanism. These issues cause many concerns. So, the insufficient solutions to fill the gaps and protect information from any risk that may be posed it, loss, disclosure or modification, Security is a major concern that always essentials to be considered. The absence of this feature or the presence of a defect affecting it will constitute this negative influence on it of the original model of computing and there may be serious consequences that lead to moral, personal and financial harm (N. Subramanian,2018).

3.2 Cloud Security Alliance (CSA)

CSA list the most important twelve threats that may lead to severe consequences and destroy data. These threats are among the most important security problems that affect and penetrate data(N. Subramanian,2018). Threats indicate that hackers are exploiting vulnerabilities.

3.3 Top 12 threads name by Cloud Security Alliance (CSA)

3.3.1 Data breaches

A data breach its unauthorized access and attempt to get and recover data. It is one of the most important and highest species. Security breaches that you want to sabotage or disclose important and sensitive data or display it and offer it for sale or illegal sites. Both disclosure, modification, or collection of data, whether by intent or unintentionally, directly or indirectly by user or attacker, that considered as data breach crimes(R. Barona,2017)

3.3.2 Compromised credentials and broken authentication

Authentication management is always difficult for organizations to confront and find solutions to fill loopholes and attackers inability to access permissions.

3.3.3 Hacked interface and Application Program Interfaces

The cloud service providers use application program interfaces (APIs) to provide different services to consumers, as a result of which there are no complications and a strong policy to limit access or exploit vulnerabilities increases the chances of risks and exploitation of attackers and the ability to access. The attacker manipulates, responds, eavesdropping and a lot of attacks that may harm the victim.

3.3.4 Exploited system vulnerabilities

Attackers exploit software weaknesses or break the firewall barrier and enable it to gain access to systems. This is one of the biggest faults and security holes in the cloud

3.3.5 Account hijacking

It is the process that make attacker stole accounts, which is the ability of the attacker to access data and steal the account and may perform actions and activities such as eavesdropping and stealing the e-mail of an individual, organization, or any account linked to the computer, and then steal login data. The attacker can manipulate the data, modify and launch various attacks such as phishing, fraud, exploitation of software vulnerabilities.

3.3.6 Malicious insiders

People who have the ability and authority to access the systems and exploit the trust granted to them to intrusion and try to access confidential and sensitive files to damage the institution that’s by firewall or Intrusion Detection System (IDS).

3.3.7 The Advanced Persistent Threat (APT) parasite

The attacker's infiltration and access to the systems and the establishment of an infrastructure that enables the attacker to steal information. These types of attacks are difficult to detect because they develop and reach in advanced stages through several techniques such as direct piracy, phishing, penetration across the network and the use of insecure programming interfaces.

3.3.8 Permanent data loss

Data loss is the result of natural causes, such as natural disasters such as floods, or a human reason such as unintentionally or intentionally deleting data, viruses or power outages.

3.3.9 Inadequate diligence

The companies use the services provided by service providers without prior knowledge and sufficient experience in the cloud, in addition to that without knowledge of the consequences and risks of the cloud.

3.3.10 Cloud service abuses

Service providers provide consumers with unlimited computing, storage capacity, and trial periods, where anyone can start using cloud services where malicious code authors and criminals may be able to misuse the cloud and initiate unethical and harmful attacks and activities. Cloud services provided by Twitter, Amazon and Facebook.

3.3.11 Denial-of-Service (DoS) attacks

The attacker's attempt to make the services unavailable or block the services, by sending several requests without a response to make the service be an excess of unanswered requests and try to begin slow down and eventually stop, by launching UDP flooding, SYN flooding, ICMP flooding attacks, buffer overflow attacks.

3.3.12 Shared technology, shared dangers

In a multi-sectoral framework, problems occur in technology. Service delivery is on demand by shared infrastructure, which is the access of different users to the same virtual machine. Table2.3 summarizes the 12 threads according to CSA.

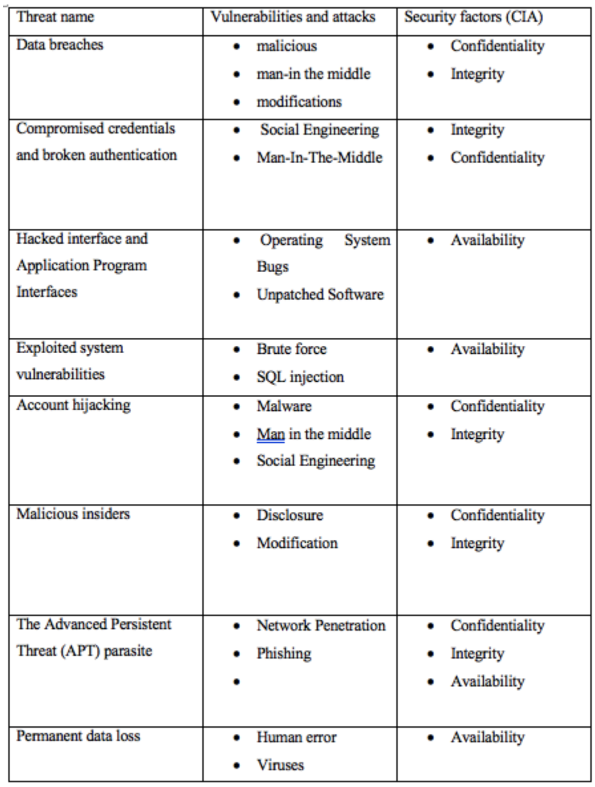
In cloud computing, the security is view as major threats, these can be represented in many factors like access management which contain two fundamental keys. The first is a hard access policy, the second one is a group of authentication and identification kits. This is high target value from an employee, a high number of data cracks have been caused of human error, then there are data cracks, this is further to threat in the cloud systems. In short way the huge sum of data flowing that's happened with the employees and the systems of cloud, which can be stopped by attackers attempts to find the weaknesses. To prevent data cracks by encryption application to all data flowing between network and add certificates SSL/TLS. Then there is data loss in another issue on cloud computing that the amount of data is flow and difficult for backup and costly. So, for in case not performing regular backups is occurs a major of threat because rise of virus, malicious and ransomware attacks, this makes the attacker target to encryption the cloud storage, extortion and demand payment for data return. Misconfigured Cloud Storage, this can made data being missing unsecured. Some corporations keep the security settings of the cloud storage on default state. Others leave the data available without protection, as it is very easy to access it without permission or request(N. J. King,2013).

Some examples of data breaches happened in 2019:

Capital One Breach of more than 80 thousand Bank Account numbers and 140 thousand that's in social Security numbers, 1 million Canadian Social Insurance Number, on this attack a former Amazon software engineer was behind the attack of capital one data breach, which amazon didn't erase his access credentials or neither denied, this flaw caused a major review on cloud computing community, this shouldn't have be occurred how did he get access to client personal information.(The New York Times), this could be prevented by adding a discovery system for monitoring process hierarchy.

Another example from data breach on Facebook, which happened in 2019 there was breach of 540,000 Records, those files covered data for profile users in details and included all sensitive data which put Facebook user high risk information at jeopardy by an unsecured leaked from cloud computing environment.

Table 2: summarize the 12 threads



Threat name	Vulnerabilities and attacks	Security factors (CIA)
Data breaches	• malicious • man-in the middle • modifications	• Confidentiality • Integrity
Compromised credentials and broken authentication	• Social Engineering • Man-In-The-Middle	• Integrity • Confidentiality
Hacked interface and Application Program Interfaces	• Operating System Bugs • Unpatched Software	• Availability
Exploited system vulnerabilities	• Brute force • SQL injection	• Availability
Account hijacking	• Malware • Man in the middle • Social Engineering	• Confidentiality • Integrity
Malicious insiders	• Disclosure • Modification	• Confidentiality • Integrity
The Advanced Persistent Threat (APT) parasite	• Network Penetration • Phishing •	• Confidentiality • Integrity • Availability
Permanent data loss	• Human error • Viruses	• Availability

3.4 Cloud Attacks

Cloud Computing may face multiple attacks from hackers and saboteurs to unheroized access. Some of the attacks that occur include:

- **Denial of Service (DoS) Attacks**

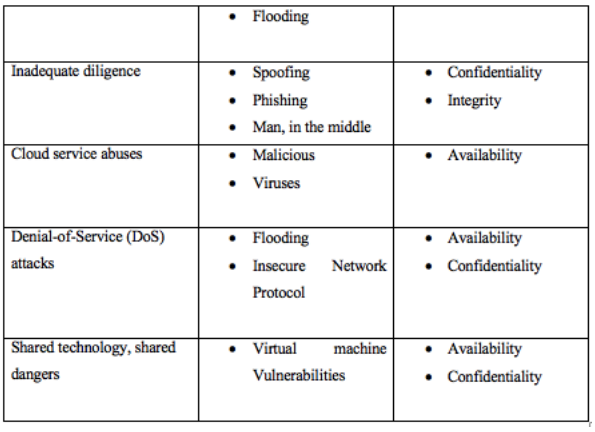
The cloud is further vulnerable to denial-of-service attacks because it is distributed with a lot of clients. Which is that the cloud computing operating system causes a large load on the service. As it will begin providing a lot of computational power, which mean the increase of virtual machines and also added cases of service to deal with overtime workload. Consequently, the server hardware limits for the maximum workload are no longer able to withstand this burden and in trying to work against this attack, but in fact it tries to damage the availability of the service and overwhelm the server.

- **Cloud Malware Injection Attack**

An attempt to introduce a system attack with a malware service application or a virtual machine in the cloud. The malware works by eavesdropping and modifications. This attack needs the opponent to make own malware service execution unit Software as a Service (SaaS) or Platform as a Service (PaaS) Enabled Virtual Machine Instance (Infrastructure as a Service) and add it to the cloud. Then, the cloud system is deceived as the cloud system automatically sends the user's valid requests to the malware service execution. In terms of classification, this attack is a exploitation of the cloud service attack surface.

- **Authentication Attacks**

Authentication is one of the most important weaknesses of hosted services that are targeted by the attacker. Currently, there is a lot services using a traditional type of authentication depend on a username and password, but some exceptions financial institutions that may use various forms of secondary authentication such as security questions and biometrics. These some of attacks launched by the attacker.



	• Flooding	
Inadequate diligence	• Spoofing • Phishing • Man, in the middle	• Confidentiality • Integrity
Cloud service abuses	• Malicious • Viruses	• Availability
Denial-of-Service (DoS) attacks	• Flooding • Insecure Network Protocol	• Availability • Confidentiality
Shared technology, shared dangers	• Virtual machine Vulnerabilities	• Availability • Confidentiality

- Brute Force Attacks: It is the attacker's attempt to guess all possible passwords to crack the password.

- Shoulder Surfing: This attacks its spy that's mean attacker spying and monitoring the user's movements in order to obtain his / her password. As the attacker watches the victim how to enter the password, that is, monitoring the entry of the keyboard keys that the user pressed.

- Replay Attacks: Called reflection attacks, they are a method of attacking a user's authentication mechanism.

- Phishing Attacks: It is redirecting the user to a bogus website so that the attacker can obtain the user's passwords.

Key Loggers: It is a program that monitors user activity by recording every key that the user presses.

- **Man-In-The-Middle Attacks**

It's an attack in which the attacker intercepts messages between the sender and the recipient in key exchange. the attacker replaces his key with the requested key, since the sender and receiver are still communicating with each other. The attacker is in full control of the connection. Some of the types of MIM attacks are address Resolution Protocol Communication (ARP), ARP Cache Poisoning Spoofing, and Session Hijacking.

- **Side Channel Attacks**

The attacker tried to penetrate the cloud system by malware virtual machine that places it near to a cloud server system to target an attack on a side channel.

4. Data protection techniques

To enhance and achieve better protection and security in cloud, a combination of protection techniques must be used, to maintain and prevent attacks or data loss. It is very important for vendors and organizations to use known algorithms as mentioned by NIST. Protection strength is evaluated on an annual basis for used keys and algorithms. Businesses or organizations using cloud technology It is very important to understand the security controls associated with data in a multi-tenant cloud environment. Hardware security modules or HSMs are preferred for storing keys. The cloud has three main types of end-user SaaS, PaaS, and IaaS services. In service models, there is security levels provided in the cloud computing environment(K. Jakimoski,2016). For securing data in cloud computing, there is forms to be ensure data and privacy requirements such as application of confidentiality, creation a catalog of data assets, availability and integrity well as an authentication and access management device. Each algorithm and protection technology has advantages and disadvantages and a distinct role to play in data security. Encryption is the process of encrypting and hiding data to keep it confidential and protected from users and unauthorized access. There are many encryption algorithms that provide excellent security features in terms of speed and high processing, less memory space during implementation, such as Advanced Encryption System (AES), RSA, and also blowfish, using AES in developing this system instead for the following reasons: (NIST) express for electronic data encryption and decryption required by AES .Because the type of information may change, for example the image instead of the content, so it was discovered that AES has a suitable site on RC2, Blowfish , RC6, with regard to time. Another concept of encryption called functional encryption, feature-based encryption was presented by Sahai and Waters in 2005 .A broader class of cryptography is used identity-based encryption (IBE). There are two main types of feature-based encryption: the first is KP-ABE and the second is the encrypted text policy. Attribute-based encryption is defined by an algorithm in which the user's secret key and either of its encrypted text algorithms depend on a specific feature such as location and account type. The ciphertext cannot be decrypted if the attributes of the customer's key match those of the ciphertext (CP-ABE). One of the advantages of encryption based on the policy feature of the encrypted text over the encryption based on the main policy feature is that it enables and supports data users at the same time, but provided that the access policy is specified with the user. Table2.4 below shows advantages base on algorithms:

Table 3: advantages base on algorithms CP-ABE& KP-ABE

Advantages	CP-ABE	KP-ABE
Data confidentiality	Yes	No
Scalability	Yes	No
Security	average	Low
Performance	Efficient(high)	low
Reliability	Yes	Yes(slow)
Accuracy	High	Average
Privacy	High	High
Robustness	Yes	Yes

Another concept of cryptography is called CloudX encryption it's made the cloud platform more secure by using these ABE and AES encryption. AES has a robust security protocol so that data is shared securely outside of the platform(M. Ezema,2020). Another way to protect is to use token encryption salts and decryptions into all layers of cloud computing, but this have some impact on performance which is not efficient, if the cloud computing makes less encryption, the data come vulnerable and can be easy captured. So they Implemented supplement layer of security like access key and secret key the generation of user token which is a time to live token(ttlt), this is can be very secured but if as your access token & secret key is fixed this cloud be easily get access to the others access if there is flaw breach, this could have major impact so to protect the cloud vendor ask for change the secret key and access key every month or weeks, so we know this works temporary there is another method and that is using certificate which have heavy layer of security inside of cloud computing resources(M. Ezema,2020).

4.1 Authentication and access control in cloud computing

Authentication and access control are one of the ways that provide a high level of security for the company's resources and data, in addition to privacy and protection of information, by imposing rules and policies on users by means of many different technologies. Whereas cloud computing authentication involves verifying the identity of the user or systems. For example, verifying the authenticity of a request to access information served by another service.

In terms of delivery models which are Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) architecture, just IaaS offer information defense and encryption data. The most appropriate solution in data connection security Cloud computing is IaaS architecture.

Most user-face services to this day use traditional type of authentication such as username and password. Some exception such as financial institutions using a various forms of authentication such as keyboards, keys, the default location, also common confidentiality questions and other forms, to make Slightly more difficult for phishing attacks. There are possible solutions against Authentication attacks for example Delayed response it's means stop attacker to check a lot of attempts password in a reasonable time. Account locking that's mean after unsuccessful login attempts locked accounts. Biometrics its image-based authentication system in which are signature verification, fingerprints, voice, face, speech.

In addition, the literature available by the authors, further, in express the security and privacy issues in the mobile cloud computing for the location services, and real time video transferring to the cloud. The other security and issues related to the cloud enabled healthcare are elaborated . The authors in discussed about the security and resource management for the cloud at virtual machine migrations, and the role of load balancing with the security issues.

5. Conclusion

There is a lot of issues in cloud computing related security. The main goal of this paper was analyzing the cloud computing security threats, attacks and the data protection techniques in the cloud computing which defined the important side that's enhance the authentication and access control in cloud.

Until this moment, security challenges are numerous thus that providing a lot of chance for attacker be able to break the authentication level and get the data. Because of the urgent need for cloud computing and the demand of many companies for it, and their confidence in computing and raising their data. Computing constantly invokes the enhancement of security, the increase in the level of security, and an attempt to stop all kinds of cyber-attacks on it.

References

1. A. O. Albadrany and M. Y. Saif, Review on security challenge faced organization based on-cloud computing, International Journal, 7 (2018).
2. A. Almusaylim, Z., Jhanjhi, N. Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. Wireless Pers Commun 111, 541–564 (2020). https://doi.org/10.1007/s11277-019-06872-3
3. A. Goyal and S. Dadizadeh, A survey on cloud computing, University of British Columbia Technical Report for CS, 508 (2009), pp. 55-58.
4. A. Panah, A. Panah, O. Panah and S. Fallahpour, Challenges of security issues in cloud computing layers, Rep. Opin, 4 (2012), pp. 25-29.
5. Aroulanandam, V.V., Latchoumi, T.P., Balamurugan, K., Yookesh, T.L. (2020). Improving the energy efficiency in mobile Ad-Hoc network using learning-based routing. Revue d'Intelligence Artificielle, Vol. 34, No. 3, pp. 337-343. https://doi.org/10.18280/ria.340312
6. A. Singh and D. M. Shrivastava, Overview of attacks on cloud computing, International Journal of Engineering and Innovative Technology (IJEIT), 1 (2012)
7. B. A. Khalaf, S. Mostafa, A. Mustapha, A. Ismaila, M. Mahmoud, M. A. Jubaira and M. Hassan, A simulation study of syn flood attack in cloud computing environment, AUS journal, 26 (2019), pp. 188-197.
8. Balamurugan, K., Uthayakumar, M., Sankar, S., Hareesh, U.S. and Warrier, K.G.K., 2018. Effect of abrasive waterjet machining on LaPO 4/Y 2 O 3 ceramic matrix composite. Journal of the Australian Ceramic Society, 54(2), pp.205-214.
9. Balamurugan, K., Uthayakumar, M., Sankar, S., Hareesh, U.S. and Warrier, K.G.K., 2018. Modeling and surface texturing on surface roughness in machining LaPO4–Y2O3 composite. Materials and Manufacturing Processes, 33(4), pp.405-413.
10. Balamurugan, K., 2020. Metrological changes in surface profile, chip, and temperature on end milling of M2HSS die steel. International Journal of Machining and Machinability of Materials, 22(6), pp.443-453.
11. C. Modi, D. Patel, B. Borisaniya, A. Patel and M. Rajarajan, A survey on security issues and solutions at different layers of Cloud computing, The journal of supercomputing, 63 (2013), pp. 561-592.
12. C. Pedigo, The Biggest Cloud Breaches of 2019 and How to Avoid them for 2020, Biggest Cloud Breaches, 2019.

13. D. A. Shafiq, N. Jhanjhi and A. Abdullah, "Proposing A Load Balancing Algorithm For The Optimization Of Cloud Computing Applications," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-6, doi: 10.1109/MACS48846.2019.9024785.
14. D. A. Shafiq, N. Z. Jhanjhi, A. Abdullah and M. A. Alzain, "A Load Balancing Algorithm for the Data Centres to Optimize Cloud Computing Applications," in IEEE Access, vol. 9, pp. 41731-41744, 2021, doi: 10.1109/ACCESS.2021.3065308.
15. D. M. Shawky and A. F. Ali, Defining a measure of cloud computing elasticity, 2012 1st International conference on systems and computer science (ICSCS), IEEE, 2012, pp. 1-5.
16. F. F. Moghaddam, M. B. Rohani, M. Ahmadi, T. Khodadadi and K. Madadipouya, Cloud computing: Vision, architecture and Characteristics, 2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC), IEEE, 2015, pp. 1-6.
17. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger and D. Leaf, NIST cloud computing reference architecture, NIST special publication, 500 (2011), pp. 1-28.
18. G. Briscoe and A. Marinos, Digital ecosystems in the clouds: towards community cloud computing, 2009 3rd IEEE international conference on digital ecosystems and technologies, IEEE, 2009, pp. 103-108.
19. J. Che, Y. Duan, T. Zhang and J. Fan, Study on the security models and strategies of cloud computing, Procedia Engineering, 23 (2011), pp. 586-593.
20. J. Murchinson and C. Haikes, Google and IBM Announce University Initiative to Address Internet-Scale Computing Challenges, News from Google. URL: http://googlepress.blogspot. fi/2007/10/google-and-ibm-announce-university_, 8 (2007).
21. K. Jakimoski, Security techniques for data protection in cloud computing, International Journal of Grid and Distributed Computing, 9 (2016), pp. 49-56.
22. Latchoumi, T.P., Reddy, M.S. and Balamurugan, K., 2020. Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention. European Journal of Molecular & Clinical Medicine, 7(02), p.2020.
23. L. Malhotra, D. Agarwal and A. Jaiswal, Virtualization in cloud computing, J. Inform. Tech. Softw. Eng, 4 (2014), pp. 136.
24. Loganathan, J., Janakiraman, S. and Latchoumi, T.P., 2017. A Novel Architecture for Next Generation Cellular Network Using Opportunistic Spectrum Access Scheme. Journal of Advanced Research in Dynamical and Control Systems,(12), pp.1388-1400.
25. M. A. AlZain, B. Soh and E. Pardede, Mcdb: using multi-clouds to ensure security in cloud computing, 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, IEEE, 2011, pp. 784-791.
26. M. A. AlZain, E. Pardede, B. Soh and J. A. Thom, Cloud computing security: from single to multi-clouds, 2012 45th Hawaii International Conference on System Sciences, IEEE, 2012, pp. 5490-5499.
27. M. Almorsy, J. Grundy and I. Müller, An analysis of the cloud computing security problem, arXiv preprint arXiv:1609.01107 (2016).
28. M. Ezema and C. I. Nwafor, Enhancing Cloud Computing Security in the 21st Century Using Advanced Web Technologies, (2020).
29. M. Odeh, A. Garcia-Perez and K. Warwick, Cloud computing adoption at higher education institutions in developing countries: a qualitative investigation of main enablers and barriers, International Journal of Information and Education Technology, 7 (2017), pp. 921-927.
30. M. H. Sqalli, F. Al-Haidari and K. Salah, Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing, 2011 Fourth IEEE International Conference on Utility and Cloud Computing, IEEE, 2011, pp. 49-56.
31. M. K. Srinivasan, K. Sarukesi, P. Rodrigues, M. S. Manoj and P. Revathy, State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment, Proceedings of the international conference on advances in computing, communications and informatics, 2012, pp. 470-476.
32. N. Amara, H. Zhiqui and A. Ali, Cloud computing security threats and attacks with their mitigation techniques, 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), IEEE, 2017, pp. 244-251.
33. N. J. King and V. Raja, What do They Really Know about Me in the Cloud: A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data, Am. Bus. LJ, 50 (2013), pp. 413.
34. N. Subramanian and A. Jeyaraj, Recent security challenges in cloud computing, Computers & Electrical Engineering, 71 (2018), pp. 28-42.

35. O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, E. A. Naeem, M. A. AlZain, J. F. Al-Amri, B. Soh and F. E. Abd El-Samie, Investigation of Chaotic Image Encryption in Spatial and FrFT Domains for Cybersecurity Applications, IEEE Access (2020).
36. O. S. Faragallah, W. El-Shafai, A. I. Sallam, I. Elashry, E.-S. M. EL-Rabaie, A. Afifi, M. A. AlZain, J. F. Al-Amri, F. E. Abd El-Samie and H. S. El-sayed, Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication, Journal of Ambient Intelligence and Humanized Computing (2021), pp. 1-25.
37. P. R. Kumar, P. H. Raj and P. Jelciana, Exploring data security issues and solutions in cloud computing, Procedia Computer Science, 125 (2018), pp. 691-697.
38. P. R. Kumar, P. H. Raj and P. Jelciana, Exploring security issues and solutions in cloud computing services–a survey, Cybernetics and Information Technologies, 17 (2017), pp. 3-31.
39. P. Princy, A comparison of symmetric key algorithms DES, AES, Blowfish, RC4, RC6: A survey, International Journal of Computer Science & Engineering Technology (IJCSET) ISSN (2015), pp. 2229-3345.
40. P. Mell and T. Grance, The NIST definition of cloud computing, (2011).
41. P. Ora and P. Pal, Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography, 2015 International Conference on Computer, Communication and Control (IC4), IEEE, 2015, pp. 1-6.
42. P. Chouhan and R. Singh, Security attacks on cloud computing with possible solution, International Journal of Advanced Research in Computer Science and Software Engineering, 6 (2016).
43. P. Ganapathi, A Review of Machine Learning Methods Applied for Handling Zero-Day Attacks in the Cloud Environment, Handbook of Research on Machine and Deep Learning Applications for Cyber Security, IGI Global, 2020, pp. 364-387.
44. P. Suryateja, Threats and vulnerabilities of cloud computing: a review, International Journal of Computer Sciences and Engineering, 6 (2018), pp. 297-302.
45. Ranjeeth, S., Latchoumi, T.P. and Victer Paul, P., 2019. Optimal stochastic gradient descent with multilayer perceptron based student's academic performance prediction model. Recent Advances in Computer Science and Communications. https://doi. org/10.2174/2666255813666191116150319.
46. Ranjeeth, S., Latchoumi, T.P. and Paul, P.V., 2020. Role of gender on academic performance based on different parameters: Data from secondary school education. Data in brief, 29, p.105257.
47. R. Creutzburg, The strange world of keyloggers-an overview, Part I, Electronic Imaging, 2017 (2017), pp. 139-148.
48. R. Barona and E. M. Anita, A survey on data breach challenges in cloud computing security: Issues and threats, 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), IEEE, 2017, pp. 1-8.
49. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg and I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation computer systems, 25 (2009), pp. 599-616.
50. S. A. Almulla and C. Y. Yeun, Cloud computing security management, 2010 Second International Conference on Engineering System Management and Applications, IEEE, 2010, pp. 1-7.
51. S. Basu, A. Bardhan, K. Gupta, P. Saha, M. Pal, M. Bose, K. Basu, S. Chaudhury and P. Sarkar, Cloud computing security challenges & solutions-A survey, 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2018, pp. 347-356.
52. S. R. Choudhury, Capital One data breach, Capital One data breach, 2020.
53. S. Ali et al., "Towards Pattern-Based Change Verification Framework for Cloud-Enabled Healthcare Component-Based," in IEEE Access, vol. 8, pp. 148007-148020, 2020, doi: 10.1109/ACCESS.2020.3014671.
54. S. K. Pande, S. K. Panda, S. Das, K. S. Sahoo, A. K. Luhach et al., "A resource management algorithm for virtual machine migration in vehicular cloud computing," Computers, Materials & Continua, vol. 67, no.2, pp. 2647–2663, 2021.
55. S. M. Hashemi and A. K. Bardsiri, Cloud computing vs. grid computing, ARPN journal of systems and software, 2 (2012), pp. 188-194.
56. S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of network and computer applications, 34 (2011), pp. 1-11.
57. S. Rachana and H. Guruprasad, Emerging Security Issues and challenges in cloud computing, International Journal of Engineering Science and Innovative Technology, 3 (2014), pp. 485-490.
58. S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar and A. V. Vasilakos, On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services, IEEE Access, 5 (2017), pp. 25808-25825.

59. S. Kansal and M. Mittal, Performance evaluation of various symmetric encryption algorithms, 2014 International Conference on Parallel, Distributed and Grid Computing, IEEE, 2014, pp. 105-109.
60. T. Diaby and B. B. Rad, Cloud computing: a review of the concepts and deployment models, International Journal of Information Technology and Computer Science, 9 (2017), pp. 50-58.
61. T. Dillon, C. Wu and E. Chang, Cloud computing: issues and challenges, 2010 24th IEEE international conference on advanced information networking and applications, Ieee, 2010, pp. 27-33.
62. T. Islam, D. Manivannan and S. Zeadally, A classification and characterization of security threats in cloud computing, Int. J. Next-Gener. Comput, 7 (2016), pp. 268-285.
63. W. A. Jansen and T. Grance, Guidelines on security and privacy in public cloud computing, (2011).
64. M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, On technical security issues in cloud computing, 2009 IEEE International Conference on Cloud Computing, Ieee, 2009, pp. 109-116.
65. X. Xu, X. Zhao, F. Ruan, J. Zhang, W. Tian, W. Dou and A. X. Liu, Data placement for privacy-aware applications over big data in hybrid clouds, Security and Communication Networks, 2017 (2017).
66. Y.-C. Lee, H. Tang and V. Sugumaran, A deployment model for cloud computing using the analytic hierarchy process and BCOR analysis, (2012).
67. Z. Mahmood, Cloud computing: Characteristics and deployment approaches, 2011 IEEE 11th International Conference on Computer and Information Technology, IEEE, 2011, pp. 121-126.
68. Z. A. Almusaylim, N. Zaman and L. T. Jung, "Proposing A Data Privacy Aware Protocol for Roadside Accident Video Reporting Service Using 5G In Vehicular Cloud Networks Environment," 2018 4th International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 2018, pp. 1-5, doi: 10.1109/ICCOINS.2018.8510588.
69. Z. Chaczko, V. Mahadevan, S. Aslanzadeh and C. Mcdermid, Availability and load balancing in cloud computing, International Conference on Computer and Software Modeling, Singapore, 2011, pp. 134-140.