A Study of Security Threats and Attacks in Cloud Computing

By

Balachandra Reddy. K,
Research Scholar,
Vels Institute of Science and Te chnology [VISTAS], Chennai, India.
Corresponding Author: kakarla505@gmail.com

Dr. S Meera,
Associate Professor,
Vels Institute of Science and Te chnology [VISTAS], Chennai, India.
Corresponding Author: meeraselvakumar@gmail.com

Abstract

Cloud computing is becoming increasingly popular and widely used. Machine Learning may be used to help protect the Cloud (ML). There are several approaches to identify and prevent attacks and security flaws in the Cloud using ML techniques. We do a literature review on Cloud Security Methodologies and Techniques in this document. For this study, we looked at 63 relevant articles, and the findings can be divided into three key research areas: (i)The diverse types of Cloud security risks.(ii) The ML algorithms employed (iii) 11 distinct aspects of Cloud security that we've identified. The most prevalent threats include distributed denial-of-service (DDoS) and data privacy.. The purpose of this study is to investigate the several components of CC as well as contemporary security and privacy problems. This paper presents a comprehensive overview of the security threats associated with different cloud computing factors. A new taxonomy of developing security solutions in this sector is also proposed in this study.. This survey also showed a variety of security vulnerabilities that put cloud computing at risk, as well as unresolved issues and promising directions for the future.. Security issues that cloud service providers, data owners, and end users all face are the topic of this paper.

Keywords: Privacy, Attacks, Data Owner, Security, Data Storage, Cloud User, Service Provider.

1. Introduction

With the rise of cloud computing as a distributed computing paradigm, the users now have access to a huge pool of shared computing resources such as storage, memory, networks, applications, and processing power. When there is a high demand, they may give and release resources as needed while only paying for the resources they use. It aims to provide computer services to people in the same way that electricity and water are public utilities. Cloud computing architecture is divided into two parts: the Front-end and the Back-end. The Front-end refers to the customers who utilise cloud services, such as individuals, companies, and apps. Data centres, system programmes, and data storage systems make up the back-end, which is made up of a big number of them.

Several important benefits have made cloud computing more popular in recent years. They are as follows: the user may access the data from anywhere at any time, free of the burden of storage management and without the need for initial investment in software, hardware, and people maintenance, etc., making it an important study subject in both business and academia. Three service models and four deployment models are included in this computing model [1-3].

Modern technology has led to an increase in cybercrime and assaults. A company's integration of cloud computing services is far-fetched without adequate protection against such threats. For example, according to Milkovich (2020), human error is to blame for 95% of cybersecurity breaches, and in 2019, 88% of organisations suffered a spear-phishing assault. An increase in assaults and exploitation on enterprises that rely on Cloud Computing makes understanding and taking preventative steps against such risks imperative. A number of the most frequent and bothersome network exploitations may have a substantial effect on enterprises with insecure network settings, including DDoS Phishing, Brute Force, Man in the Middle, and SQL Injections.

The use of cloud computing and a digitalized system is the most prevalent business trend now being used by numerous enterprises. However, many firms who are embracing cloud computing solutions are completely uninformed of the dangers that lurk there waiting to be exploited by an attacker. Cloud computing security is currently implemented by the majority of enterprises with shoddy physical and logical safeguards. Identifying and implementing countermeasures to possible network hazards is critical for businesses looking to deal with these threats. The main objective of this study is to identify the types of attacks in cloud ecosystem and review the studies contributed addressing various classes of attacks and to identify scope for further research in cloud security domain.

Security Issues in Cloud Ecosystem

Defending against harmful and illegal access and use of internet-based services is part of cloud computing security, which also refers to safeguarding the cloud computing environment itself (Tadapani, 2020). For example, internal and external threats, shared cloud computing services, insufficient backups, phishing and social engineering, service assaults and system vulnerabilities may all arise while utilising cloud computing services. The beginning of cloud computing may be dated to the mid-1990s, and Amazon and Ali Baba were among the first to use cloud computing services. Due to cloud computing's rising reliability, organisations now need to safeguard cloud-driven services with secure settings that protect online data (Jathanna & Jagli 2017). As a result of Cloud Computing's increased usage and dependability, customers have reported higher reliability, huge scalability, and lower corporate growth costs. In addition to automating their regular business procedures and needs, cloud computing technologies have given big organisations the ability to construct a readily accessible control mechanism by leveraging an Most firms find cloud computing to be both versatile and cost-effective in their day-to-day company operations, according to research done by Hashizume, Rosado, Fernandez-Medina, and Fernandez (2013) Additionally, the researchers spoke on the safety of cloud computing data, compliance, and the prevention of exploitation (Hashizume et al., 2013). While implementing Cloud Computing services for any firm, this research identifies important weaknesses and obstacles such as "Cloud Storage Misconfiguration, “Insecure APIs," and "Theft of Intellectual Property”.

Major Security Threats in Cloud Ecosystem.

The following are the major security concern in cloud computing environment:

- **Lock-In Vendor:**When a customer is reliant on a single cloud provider, an issue of inflexibility occurs. This is known as a Lock-In Vendor. A lock-in vendor is a problem when services cannot be easily mobilised or transferred between other service providers and vendors online (Opara-Martins, Justice, Reza, & Feng, 2018).

- **Malicious Insiders:**An further problem with cloud computing is malicious insiders, who may take advantage of the carelessness and little mistakes of company personnel to compromise the system and get unauthorised access (Saxena et al., 2020).
- **Compliance Challenges:** Challenges in compliance emerge when implementing cloud computing solutions for any company that adheres to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in order to secure unique health data privacy and security (Yimam & Fernandez, 2016).

- **Denial of Service Attacks (DoS):** As a prevalent danger to online computing services, denial-of-service attacks (DoS) use an unreasonable number of ping connections sent from a separate computer to overwhelm the victim's system. A denial-of-service attack often causes the system to go down with many ping requests (Srinivasan at al., 2019). Using these requests, cloud computing services are offered to users for usability, management, and engagement with the system to minimise cyber dangers and exploitations that need to be appropriately provided, managed, orchestrated, and monitored For example, Odun-Ayo and coworkers (2018)

- **Data Loss or Leakage :**Data loss or leakage is a concern for organisations using cloud computing since it requires adequate encryption and protocol assignments to prevent hackers and data loss during internet communication. For instance, in Tahboub and Saleh (2014)
- **Natural Disasters and Availability:**Natural disasters and availability may be disastrous for a company that relies only on a single system and does not have a backup server integrated, perhaps resulting in the loss of vital data and information without the company even realising it (Ujjwal at al., 2019).
- **Licensing Risk:**When using cloud computing at the IAAS and PAAS levels, Licensing Risk is more of a concern since users aren't in charge of managing or controlling the infrastructures, however with cloud-deployed services, specific capabilities are granted. To comply with the rules for least risk when licencing online services, most major suppliers like Amazon and other cloud-based organisations follow a tight licence (Neicu at al., 2020).
- **Types of Security attacks in cloud environment**

The widespread use of cloud computing services has led to the need to safeguard the cloud-deployed system against many sorts of network assaults, such as DDoS, Man in the Middle, Brute Force, and Data Breaches. Hacking into a cloud network or the internet is often used to get access to sensitive data and information that are protected by stringent security measures (Chou, 2020). Users using cloud platforms may be seriously harmed if hackers get access to the system, allowing them to modify or control the cloud services they utilise. This assault is focused on exploiting cloud system vulnerabilities, stealing intellectual property belonging to the cloud users and performing a harmful insider attack. Cloud computing `services may be divided into three levels: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are three primary levels of cloud server service: the SaaS level, IaaS level, and PaaS level. Attacks against the security of cloud computing may be divided into three categories: SaaS, PaaS, and IaaS, as shown in Figure 1.

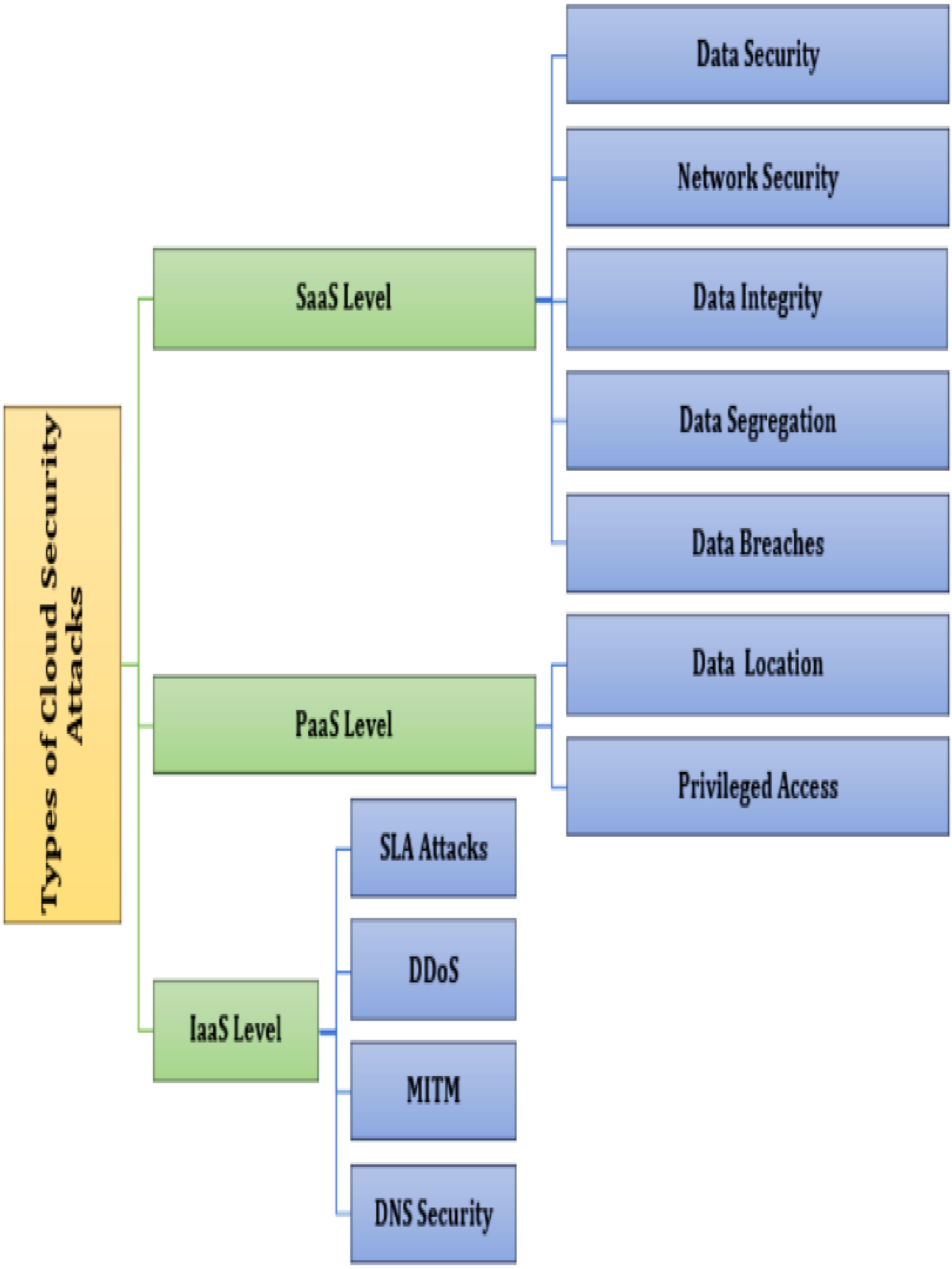

Figure1: Most Common Security attacks in Cloud Eco System

SaaS is a subscription-based licensing and delivery model for software that makes use of internet technologies. It is possible to outsource users' IT infrastructure over the cloud by using IaaS or HAS, two levels of the cloud computing platform (Rani & Ranjan, 2014). This layer of cloud computing offers application developers with a platform on which to construct their systems and apps. Using software as a service (or SaaS), which stands for "software as a service," allows users to pay a monthly fee in exchange for access to a hosted version of the application. SaaS data breaches may be prevented by encrypting data and preventing user credentials from being stolen by phishing and malware attacks that can be used to obtain passwords. In order to utilize SaaS cloud services effectively, it is necessary for the end user to be aware of different network attacks and threats, as well as the potential rewards and losses associated with each (Rani & Ranjan, 2014). The most common SaaS-level risks to cloud security have been identified and described in this article.

PaaS, or application platform as a service, is a cloud computing service that allows users to design, create, operate, and manage their own cloud computing services. Data security, vendor lock-in, customization to legacy systems, and runtime issues are just a few of the dangers associated with PaaS services.

Data partitioning, data locations, data security, and backup and scalability may be used to categorize IaaS as an online service based on high-level APIs from the network architecture. The most common IaaS risks are listed here.

Cloud Security attack Classification

Internal attacks are usually caused by the negligence of employees and workers associated with a certain company. Employee sabotage and theft, unauthorised access by employees, weak cyber security measures, and unsafe practises are the most prevalent causes of this sort of assault (Javaid,2013). Insider assaults have been highlighted in the following list. Human mistake is the most common cause of data loss in the cloud, with hardware or software failures and malfunctions the most common cause. When executing a data migration, a loss of data is possible. When employees and workers of a business use out-of-date software and services, there is a risk of web browser bugs (NSA, 2020). As a result of a lack of encryption, unsecured end points, and insufficient authentication, cloud computing APIs might be vulnerable (Ariffin, Ibrahin, & Kasiram, 2020). In order to deceive cloud monitoring systems, the migrant assault uses many resources to launch a denial-of-service attack on cloud virtual machine migration shames (Chandrakala & Rao, 2018). Insiders need risk profiling to comprehend and access risk incidence, impact, and future cure measurements (Tadapaneni, 2020). Harmful insiders might be ex-employees, contractors, or business acquaintances who have access to the system and use malicious software and computer viruses to tear it down (Duncan, Creese, & Goldsmith, 2012). Cyber-attackers may employ the VM Rollback attack to run virtual machines from a prior snapshot without the user's knowledge or consent (Almutairy, 2019).Intrusion detection system for identification of the black hole attacks in networks ,here to perform the scalabiliy and security of the networks by using different algorithms(S.Sridevi and R.Anandan,2019).

An outsider may get access to and exploit the cloud system via the usage of internet connections (Usman Awwalu, & Kamil, 2016). Destructive assaults from the outside on the cloud system may result in system failures that adversely affect normal business operations. The firm adopting the cloud system may suffer considerable financial losses as a consequence of external attacks. Service Unauthorized access to a system through the cloud puts cloud computing services at risk of hijacking (Tirumala, Sathu, & Naidu, 2015). As a result of malware being introduced into an organization's online system, cloud computing faces an additional external threat (Watson et al., 2015). Unlike a DDoS assault, a botnet attack uses a huge number of computers to attack the same target, causing the system to become unstable and finally break down (Anwar et al., 2014). Another horrible kind of attack develops a similar-looking application and fools an authorized user with a phoney application that obtains important information such as the user's credentials and personal data (Basit at al., 2020).

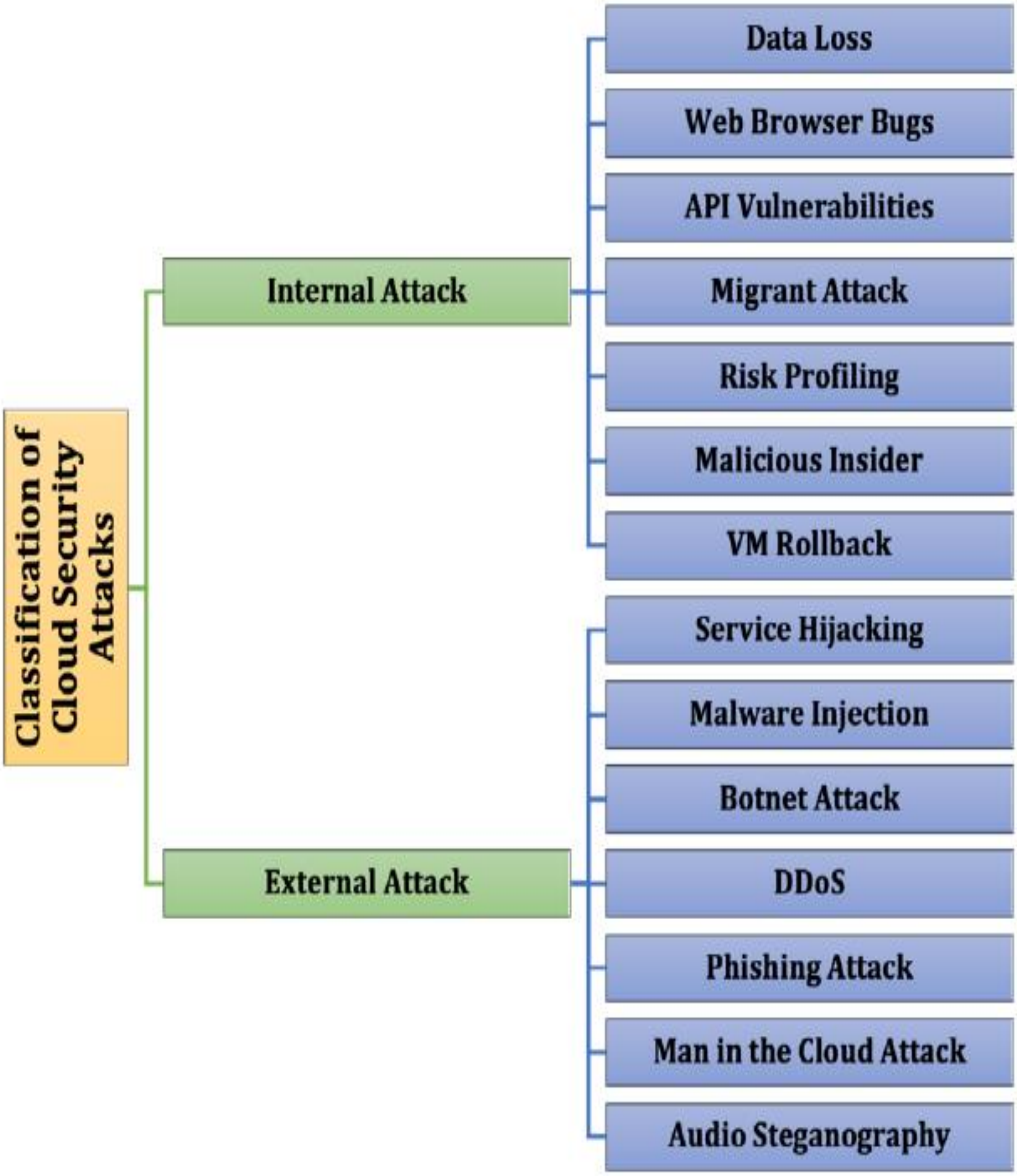

Figure 2: Classification of Security Issues in Cloud

Review of Studies based on Cryptographic algorithms in Cloud

Using a linear arrangement of homomorphic linear authenticator labels, Prakash et al. (2018) proposed a multi-sector public auditing method. To reduce auditing computation, the proposed method performed many auditing jobs at once without attempting to recover the whole file. The proposed methodology was shown to be superior in terms of data security, communication, and computing overheads when compared to the present auditing method. Algebraic signature qualities may be used to identify cloud storage systems, according to a paper by Sookhak et al. (2017). Communication and computing expenses were minimal. Divide and Conquer Table (DCT) was a revolutionary data format that significantly supported dynamic data operations, such as append and insert. For large-scale data storage, the suggested data structure might be advantageous since it would be less computationally costly. In a comparison of the recommended strategy with more complex RDA methods, this method was shown to be safe and exceptionally effective in reducing the computational and communication expenses on the server and auditor.

"Dynamic Data Encryption Strategy" was developed by Kanmani and colleagues in 2018 to ensure the privacy of users' data (D2ES). Data might be encoded selectively and privacy categorization methods could be used under time limitations. A selective encryption strategy was used to maximise privacy protection within the required execution time constraints of this approach.For multimedia files, Kumar et al. (2018) created a three-tier security system that included access control, encryption and signature verification. An enhanced method of dynamic auditing that could properly store data in the cloud was proposed as a result. TPA and combiner could both verify the integrity of the data they were receiving from each other in the proposed structure. Consequently, the proposed improved dynamic auditing technique was safe and effective against various conspiracy attempts. "

A data-centric framework for cloud storage was presented by Jin et al. (2018), which is a generic framework for cloud storage. Action records were created to keep track of any data-related access activity, and to identify any potential misdeeds that may have occurred. Because of replay threats, the research used signature exchanges to ensure that both parties could verify and preserve separate metadata signatures verified by the other side. Additionally, they build an arbitration system to resolve disputes about data content or access records in a fair and fast manner, and to identify the cheating party. Our prototype's cryptography cost, storage overhead, and throughput were found to be realistic and acceptable by conducting an experimental test.For the objective of enhancing the verification of sensor nodes in the system,Thangarasu et al. (2018) developed an ECC-based encryption protocol for secure session keying among users. As a result, the intruder was transformed into a linear deduction problem in Abelian group theory in order to determine how difficult it is to identify intruders inside the system. As a result of this, the complexity of producing a secure message broadcast was reduced and the likelihood of identifying intruders was increased. It was found that the proposed ECC authentication method achieved lower computing costs and improved identification of attackers inside the system throughout the inquiry. As a result, the technique looked to be active and may be beneficial in real-world situations when additional ECC processes fail while running it in real time.

ID-based authentication schemes for mobile client–server environments have been presented by Mo et al. (2018), which considers security considerations. A session key agreement between the client and the server was also obtained with the proposed structure. The suggested protocol was shown to be safe against security threats after a thorough formal security verification under the random oracle model. The informal security assessment found that the proposed structure was able to withstand well-known threats and protect user privacy. The suggested system was shown to outperform and be more suited for actual implementation in mobile client-server scenarios after a series of tests and comparisons.

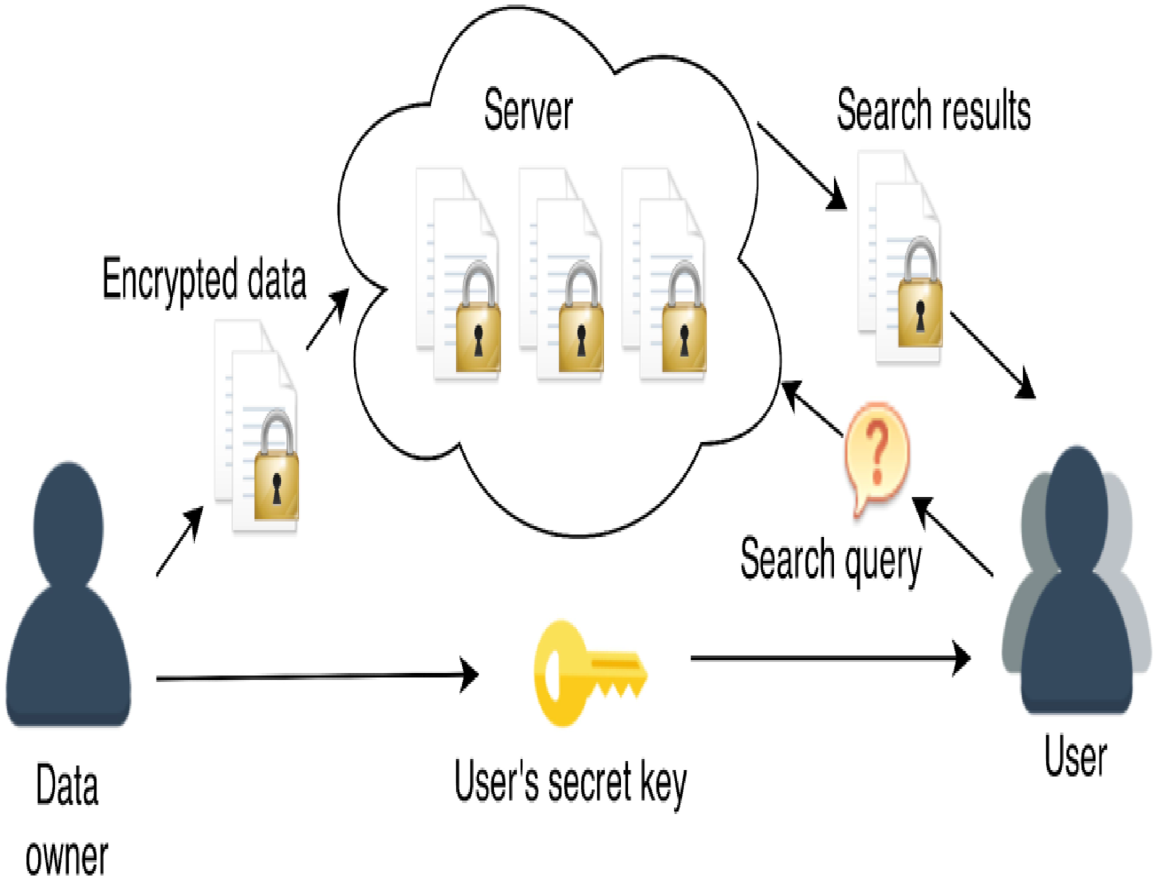

Figure 3: *Workflow for Cryptographic based Algorithms*

On the basis of various limitations, Pharkkavi et al. (2018) examined and compared the performance of numerous current cloud computing security approaches. Additionally, it would be beneficial to discover and implement a unique technique for cloud data storage security enhancement. There is a novel hybrid approach for cryptography that uses two algorithms, according to Abd Elminaam and his colleagues in 2018. (AES and Blowfish). Symmetric and Symmetric encryption techniques were combined in the new method. Everyone has their own private key, which may be used by several people at the same time for decryption, and the combination of symmetric and symmetric techniques provides the highest level of security. Using MD5's hashing function for the key has also helped the approach, since hashing the key in the encryption and decryption processes has been made easier. In addition to enhancing the security of the key, utilising hybrid cryptography would raise the level of security.

Qiu et al. (2018) identified a problem and proposed a technique that uses Attributed-Based Access Control (ABAC) in conjunction with a data self-deterministic system to protect the private information of financial customers. Known as P2DS (Proactive Dynamic Secure Data Scheme), the proposed approach attempted to ensure that the private information was protected from unauthorised access by third parties. According to our research, the study had three primary needs. The first step was to design a semantic mechanism for restricting data access. It was also advised that customers' data should be protected against unexpected cloud procedures through a user-centric way. As a result, the proposed structure has a greater degree of secure sustainability since it can cope with dynamic dangers, such as emerging and upcoming hazards. The proposed structure performed admirably in accordance with their anticipated goal.

Table 1: List of Cryptographic Algorithms

S.No	Encryption Algorithm	Stream/ Block Cipher	Key space	Vulnerability	Number of Rounds	Structure
1	Camellia	Block cipher (128 bits)	128, 192, or 256 bits	Algebraic attack	16	Nested Feistel Network
2	Serpent	Block cipher (128 bits)	128, 192 or 256 bits	Linear cryptanalysis and Rectangle algebraic attack	32	Open-source algorithm
3	Rijndael	Block cipher (128 bits)	128, 192 or 256 bits	Related Key Attack, Algebraic attack	10,12,14	maximal size of the input file is 2,097,152 bytes
4	Skipjack	lock cipher (64 bits)	80 bits	Slide attack	32	unbalanced Feistel Network Structure
5	AES	Block cipher (128 bits)	128, 192, 256 bits	Known plaintext, Side-channel attack	12	Substitution- permutation network
6	RC-6	Block cipher (128 bits)	128, 192, 256 bits	Known plaintext, chosen cipher text	20	Feistel network,
7	SEED	Block cipher (128 bits)	128 bits	Chosen plaintext, Known plaintext	16	Nested Feistel Network
8	Two fish	Block cipher (128 bits)	128 256 bits	Truncated differential cryptanalysis	16	Feistel Structure.
9	CAST-256	Block cipher (128 bits)	128 160 192 224 256 bits	Known plain text and ciphertext	48	Feistel Network Structure
10	XTEA	Block cipher (64 bits)	128 bits	The related key differential attack, chosen plaintexts	Variable	Variable rounds. Nested Feistel Network
11	**RC-2**	**Block cipher (64 bits)**	**8-128 bits (64 bits)**	**The related key attack, Chosen plaintext**	**18**	**Feistel Network Structure**
12	CAST-128	Block cipher (64 bits)	40 to 128 Bits	Chosen ciphertext and Known plain text	16	Feistel Network Structure
13	RC-5	Block cipher (32,64,128 bits)	0 to 2040 bits (suggested 128bits)	Differential attack	12	Feistel-like network
14	TEA	Block cipher (64 bits)	128 bits	The related key attack, Chosen plaintext	Variable	Feistel Network Structure
15	Blowfish	Block cipher (64 bits)	32-448 bits	The second-order differential attack, Weak key	16	Feistel Structure.
16	IDEA	Block cipher (64 bits)	128 bits	Weak keys,	8.5	Feistel Network Structure
17	TDES	Block cipher (64 bits)	12 or 168 Bits	Theoretically possible, Known plaintext, chosen-plaintext	48	Feistel Network Structure,
18	DES	Block cipher (64 bits)	56 bits	Differential & Linear Cryptanalysis, Brute- force attack	16	Feistel Structure,

Encryption time was linearly increased when the number of characteristics was increased, according to a method presented by Panchal et al. 2018. Thus, the cypher text storage as well as the encryption time was saved. Because to this, clients may convert all authorization files by just calculating a secret key once. As a result, if the user needed to convert many files, the time cost of decryption was also safeguarded. Many security issues have been addressed in the cloud computing area, according to the study results. Outsourced data might benefit from the ability to have scalability and flexibility while maintaining data confidentiality and fine-grained management Fine-grained access to encoded information was provided by Ling et al. (2018), which was seen as an improvement over ABE and identity-based approaches. The research had a two-fold impact. Server-aided predicate encryption (SR-PE) was validated with rigorous explanations and security principles in the first step of this process. As a non-trivial variant of Cui et

a investigation .'s into the PE backdrop, the present model might be considered. Next, propose a lattice-based implementation of SR-PE, as before. Secure cross-domain access control (RACS) was presented by Punithasurya et al. (2013) as a novel role-based access control strategy (RACS). To ensure cross-domain access and security, a novel approach to access control has been developed by the researchers. A combination of domain identification and role-based access control was used to reduce the time restrictions and geographical constraints of the challenge. A user's domain ID, data, responsibilities, and permissions are all protected by domain identification. Using this approach, the roles and permissions of each user, as well as the time they logged on, were specified. In this case, the time efficiency and location identification were considerably enhanced by the use of this strategy.

New encryption system proposed by Bugiel et al. (2011) provides crucial protection for both unpopular and popular material. A new two-layered encryption approach was proposed for unpopular data that was more secure while still allowing for the deduplication process. For popular material that wasn't very sensitive, standard encryption was used. It was this combination of security and efficiency that resulted in a better trade-off. Key management issues were handled by Li et al. by spreading these keys over various servers before encryption and then deduplication the contents.

Table 2: *Comparative analysis of Studies*

Sno	Authentication mechanism	Authors	Advantages	Disadvantages	Vulnerabilities
1	Attribute based signature	Maji et al.	Anonymity and uniqueness	User revocation is not handled.	Replay attack
2	Plutus	Kallahalla et al.	Secure file sharing	Key distribution overhead and a single point of failure.	Impersonation attack
3	Proxy re encryption	Ateniese et al.	Secure storage and retrieval.	Revoked users may misuse the data.	Collusion attack.
4	Group signatures and CP-ABE	Lu et al	Authentication, verifiability, and confidentiality.	User revocation is not supported.	Forgery attack in case of the trusted arbitrator.
5	KP-ABE	Goyal et al.	Centralized approach	Single point of failure	Impersonation attack
6	Full Disk encryption	Janssen C et al.	The whole disk is encrypted and provides high security.	It slows the process and increases business costs.	Cold boot attack and Evil maid attack.

7	Broadcast encryption	A.Fiat et al.	An authorized subset of users can decrypt the data.	Computation overhead.	Pirate evolution attack.
8	Identity based remote user authentication	Chen et al.	It provides remote user authentication.	Clock synchronization problem.	Offline password guessing attack &Key compromise impersonation attack.
9	File storage on untrusted server	E.Goh et al.	Provides Authenticated access and verifies users using access control.	User revocation is not provided.	-----
10	OAuth and ABE	Anuchart et al.	Credential protection, Lightweight encryption.	Adversaries may update or delete the information as well as issue faked contents.	Impersonation attack.
11	Privacy-preserving authenticated access control	Zhao et al.	Supports anonymity & Authorized access.	Single KDC may be a point of failure.	Impersonation attack.
12	Trusted identity-based authentication	Elbaz et al.	Less computation time and no need for a certificate.	Consumption of network bandwidth.	-----
13	Fast dynamic extracted honey pots	Sebestia et al.	Impact of the detected ongoing attack can be monitored and vulnerability-ties analyzed while sensible data is secure.	Honey pot VM is not fully synchronized with the original VM. Attacks can be delayed for a small amount of time.	-----
14	Privacy-preserving access control	Nabeel et al.	It is single layer encryption, provides user privacy.	High Communication cost and computation overhead.	-----
15	Privacy preserving delegated access control	Nabeel et al.	Preserves confidentiality and user privacy.	Huge I/O cost.	-----

Review of Studies on Machine Learning Algorithms for Cloud Security

This study examined the security of machine learning in Android malware detection via a learning-based classifier using API calls extracted from the tiny files. Furthermore, evasion attempts based on several degrees of attacker capacity were shown to properly test the security of the classifier. A comprehensive secure-learning paradigm was suggested and shown that it could increase system security against a broad range of evasion tactics, allowing it to successfully defeat these assaults. Anti-spam and fraud detection might also be easily implemented using the suggested paradigm.

To better understand the accuracy and detection rate of four distinct types of attacks under varied percentages of normal data, Chourasiy and colleagues (2018) developed a Machine Learning approach. The goal of this suggested technique is to effectively classify abnormal and normal data utilising a very big data set and to identify intrusions even in huge datasets with minimal training and testing durations. High accuracy for a wide range of assaults and a low false alarm rate are achieved using the suggested strategy. In this study, an Azure ML-based attack categorization model was presented. An technique called Multicast Decision Forest was used to train the classifier. The suggested classifier was shown to be more accurate in the assessment findings. An experiment was conducted using a multicast decision forest and an ensemble approach. It performed better than a reference point in tests. For multi-class classification issues, the suggested study might give a possible training and testing method for huge data.

The stochastic gradient descent technique to gradient descent was used by Mohassel et al. (2017) to construct privacy-preserving machine learning for training neural networks and logistic regression models. Data owners now employ a two-server paradigm, which uses secure two-party computing to train multiple models on integrated data from two non-colluding servers (2PC). When the suggested system was implemented in C++ it gave MPC-friendly alternatives to nonlinear functions such as sigmoid and softmax that were better than past attempts. arithmetic operations on shared decimal integers According to the experiments undertaken, privately-preserving linear and logistic regressions can analyze millions of data samples with thousands of characteristics in a fraction of the time needed by current methods. Finally, the first secure neural network training system was built.

In the cloud, He Z. et al. (2017) advocated a DOS attack detection solution that relies on machine learning techniques at the source side, S.Sridevi.et al.(2020). In order to prevent network packages from being transferred to the external system, this system uses statistical data from the hypervisors of both cloud servers and the VMs. The performance of nine machine learning techniques was carefully compared. More than 99.7 percent of four types of DOS assaults were detected throughout the examination. The suggested method does not affect performance and can be easily extended to a larger DOS assault without any difficulty. The following is a breakdown of the work's suggested structure.They focused on hybrid classifiers as a way to study various machine learning methods that have been offered for recognising interruptions. To assess their strengths and limitations, as well as their potential for growth, is the goal. For the authors, recognising the difference in developing an effective intrusion detection system that had yet to be examined is an important takeaway from the evaluation.

Founded in April 2011, Hido et al. (2012) is an online/machine learning platform that is distributed and implemented in real-time. In addition to stream processing and online learning, Mahout (TM) has a follow-up stage. With every new data sample that arrived through quick and memory-intense methods, the model was constantly updated. Only model mixing was required, no data storage or exchange. Regression based on Passive Aggressive (PA), Confidence Weighted Learning (AROW), Nearest Neighbor (LSH, MinHash, Euclid LSH), recommendation, anomaly detection (LOF based on NN), and graph analysis were all retained (shortest path, PageRank). Jubatus triggered updates on local models in order to allow online learning more effectively, and then each server transmitted its model difference back to all servers.

Case Study

We're presently analyzing the cloud service provider's security measures. Amazon Web Services (AWS) CC platform provides users with the flexibility to construct a broad variety of applications because of its high availability and stability. AWS's success on on the safety, integrity, and always-on accessibility of its customers' systems and data. Enterprises may install apps on AWS, which is a complete cloud service platform. Utilize AWS Self-Service to address internal strategies and respond to external enquiries.

General Security Measures

AWS incorporates security into its services in accordance with best practises and documentation on how to use the safety features. AWS security features must be used by the client to provide a secure application environment. The maintenance of AWS's trust and confidence is a priority for the company. There are a number of precautions taken by AWS to ensure the safety of its cloud infrastructure.

With several Type II audits in the past, AWS has successfully published the Service of the Organization Controls 1 (SOC 1) report in accordance with requirements set out by both SSAE 16 and ISAE 3402. AWS has only begun making the audits public. Additional certifications include PCI Level 1 certification and successful validation as Level 2 PCI compliance (DSS). It has been approved by the US General Services Administration (GSA) as a FISMA Moderate-level certification platform for public services, and it also serves as an application platform for the Defense Information Assurance and Accreditation Program (ATOs) (DIACAP).

When it comes to physical security, Amazon has been designing and operating large data centres for many years. The AWS infrastructure is housed in Amazon-owned data centres throughout the globe. Amazon restricts the placement of its data centres to those with legitimate commercial interests. There are a variety of configurations in place in data centres to thwart unauthorised access.

Users may safeguard their data and applications by encrypting it in the AWS cloud and ensuring that backups and redundancies are in place to help them do so**.**

AWS Infrastructure Security

Customers and AWS establish a shared responsibility paradigm when they migrate IT infrastructure into AWS. As AWS maintains, manages and supervises the host OS and virtualization components, this shared paradigm may save operational expenses. In order to meet more stringent compliance standards, users may strengthen security by deploying basic home firewalls, host-based IDS, and encryption.

Security Best Practices

A multi-tenant arrangement has everyone on edge. Security should be integrated at every level of the cloud application architecture. Another benefit of the cloud is that it takes care of physical security. It is the user's responsibility to keep their network and applications safe from hackers. This section focuses on particular AWS cloud application security tools, features, and recommendations. We propose that these tools and features be used to provide basic security, and then further safety best practises may be applied using normal procedures.

Protect data in transit

The server instance uses the secret data and configures SSL. A certificate is required by a third-party certifying body, such as Entrust. Using the certificate's public key, the browser verifies the server and generates a shared session key to encrypt data both ways.

Protect stored data

If consumers are concerned about the security of their cloud data, they should encrypt it before uploading it. For example, you may use any PGP-based open source or commercial solution to encrypt your data before saving it to Amazon S3 objects. This is a common best practise for developing HIPAA-compliant apps that contain confidential health information (PHI). Amazon EC2's operating system dictates how files are encrypted. It is impossible to encrypt data at rest, no matter what operating system or technology a user chooses. If the user loses the keys or the keys are compromised, the user's data is at jeopardy. In order to prevent the loss of keys, it is important to check the key management capabilities of any offered items.

Protect AWS credentials

It's possible to use both AWS and X.509 security credentials on Amazon Web Services (AWS). A secret access key and a key identifier are both part of the AWS access key. The REST or Query APIs need users to provide their secret access key in the authentication request in order to generate a signature. To avoid disrupting flights, all inquiries should be made through HTTPS.

Manage multiple users with IAM

AWS Identity and Access Management (IAM) allows customers to establish numerous users and manage the permissions of each of these users in the AWS account. Security credentials (AWS Accounts) are unique to each user and may be used to access AWS services. By eliminating the requirement for password and key sharing, IAM lets administrators activate or disable user access as required. Users of an AWS account with IAM are able to implement optimal security practises such as the lowest privilege level by using a single set of login credentials for all users on the account and restricting access to just the most basic AWS services and resources.

Secure Applications

Each Amazon EC2 instance has a security group, a named rule set that specifies which network traffic the instance should be allowed to receive from the internet. Ports, ICMP types, code, and source addresses for TCP, UDP, and other protocols may all be customised by the user. Security groups give the bare minimum in firewall protection for running instances. Over time, software issues are discovered and fixes need to be implemented. For all pre-cloud security criteria, such as correct coding practises, the isolation of sensitive data is still relevant.

Discussion and Open Issues

Multi-tenant enterprises are increasingly relying on cloud computing as a platform for their infrastructure and services. Every key area of security has been handled in previous chapters, so you don't have to worry about missing anything important. Our document contains all of the application-level issues that we've encountered. Embedded innovation includes clustering computers, businesses, a data warehouse, and the kernel itself. This is a game-changer. However, traditional issues such as managing data without administration or constructing a virtual machine without a hypervisor become more crucial and sensitive. conventional challenges. In spite of cloud technology's widespread use, academics and observers have consistently highlighted the cloud's issues and difficulties. There will be a quick review of all the parts learnt from this investigation, and full, confident safety solutions will be offered.

Attacks on cloud computing security are on the rise, as is use. Many major attacks impair security and related research, including those that augment or remove access rights or that disapprove of a user's actions (such as a wrapping attack or a hijacking session).

Confidence assaults, such as social engineering and specific insider attacks in cloud storage, such as loss of server control, audit monitoring and security instrument misconfiguration, have not been completely eradicated.

Authorized users who typically have access to a higher security level, such as those who engage in login abuse, are an example of this kind of behaviour. Like a network intrusion, this kind of abuse targets people who have weaker levels of security on a variety of platforms. Multi-user operators expect their cloud service providers to adhere to strict security standards and processes. For the government cloud projects, infrastructure needs including smart cities, smart homes, and IoT prompted the development of their modules. For this reason, only a few cloud projects serve as intermediaries between different CCs and technologies.

Online, the cloud computing business does not face any unique legal issues. Cross-border external services face a wide range of issues, many of which are similar to all external services. This shows that the difficulties of cloud computing development may be dealt with by having a robust legal framework for privacy and data protection.

Many security and research solutions target personal security, encryption, disaster recovery, vitalization solutions, forensic digital tools and cloud technologies. For a complete plan, virtualization takes more attention since VMMs are large and complex systems. Due to the large number of vulnerabilities in VMM code, this is the case.

The major aspect of the Cloud is multi-tenancy, which relates to the utilisation of resources but comes with several risks. The multi-tenant user faces substantial cloud security, privacy, and confidence concerns.. Few efforts are being made to address multi-tenant security issues at this time. However, a number of attempts have been undertaken to develop security measures to address these issues. Sharing pool resources requires an effective security solution to prevent unauthorised access to them Due to the dynamic nature of resources and the variety of services, it is challenging to implement access restrictions. So that auditing and insurance instruments may continue to be used directly by organisations, they should be integrated and mitigated in future endeavours.

If there are concerns about cloud-based legal problems, they should be examined in terms of law in different countries and jurisdictions. We also need to look at our data storage, processing, and use policies. Health insurance records must also be examined for restrictions governing the publication of specific information, such as financial information.

As a last step, the security solution is well worth mentioning, and a security module is made available to both customers and suppliers to fill any remaining gaps in security. There is also an emphasis on time management, cost-cutting, and efficiency in the system. You may save money on your business process by using the business model.

Conclusion

Cloud computing is exposed to a wide range of risks, including phishing and social engineering, shared cloud computing services, and internal/external threats and system vulnerabilities, all of which must be addressed. In this paper, the dangers have been outlined in depth and illustrated with relevant instances whenever possible. A cloud-based system may be used by internet firms to manage their day-to-day operations at all times. IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) are the three main types of cloud computing services that have been shown in this thesis (PaaS). The attacks have been classified and organized in a hierarchical manner in order to provide comprehensive insight into cloud security vulnerabilities. Peer-reviewed sources and real-time examples based on these hot-trending cloud security dangers are the most essential components of this thesis's examination. Studies show that implementing data encryption at rest, two-factor authentication, removing shared accounts, enforcing a clearly defined shared responsibility model, and implementing a Standardized Cloud Assessment may reduce the risk of data in the cloud. It helps to limit risk by providing data security, which necessitates the use of a decryption key to access particular data. Because of government and cybersecurity rules, organizations must encrypt their data. In addition to protecting the cloud-based system, two-factor authentication may make the system more user-friendly. Two-factor authentication has become the usual compliance requirement in today's cloud-based systems, where most of an organization's normal business operations are established on a shared cloud platform using legitimate credentials, which may be abused by an attacker.

References

[1] Aishwarya, C., Sannidhan, M. S., & Rajendran, B. (2014, December). DNS Security: Need and Role in the Context of Cloud Computing. In 2014 3rdInternational Conference on Eco-friendly Computing and CommunicationSystems (pp. 229-232). IEEE.

[2] Ali, M. B., Wood-Harper, T., & Ramlogan, R. (2020). A Framework Strategy to Overcome Trust Issues on Cloud Computing Adoption in Higher Education In Modern Principles, Practices, and Algorithms for Cloud Security (pp. 162- 183). IGI Global.

[3] Aljahdali, H., Townend, P., & Xu, J. (2013, March). Enhancing multi-tenanc security in the cloud IaaS model over public deployment. In 2013 IEEE Sevent International Symposium on Service-Oriented System Engineering (pp. 385- 390). IEEE.

[4] Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET Communications, 14(7), 1185-1191.

[5] Almutairy, N. M. (2019). A taxonomy of virtualization security issues in cloudcomputing environments. Indian Journal of Science and Technology, 12(3), 1- 19.

[6] Amara, N., Zhiqui, H., & Ali, A. (2017, October). Cloud computing security threats and attacks with their mitigation techniques. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 244-251). IEEE.

[7] Anwar, S., Zain, J. M., Zolkipli, F., & Inayat, Z. (2014). A review paper on botnet and botnet detection techniques in cloud computing. Proceedings of the ISCI, 28-29.

[8] Ariffin, M. A. M., Ibrahim, M. F., & Kasiran, Z.(2020). API Vulnerabilities In Cloud Computing Platform: Attack And Detection. In 2020 International Journa of Engineering Trends and Technology(pp8-14).

[9] Aviles, M. E. (2015). The impact of cloud computing in supply chain collaborative relationships, collaborative advantage and relational outcomes (Electronic Theses and Dissertations Graduate Studies, Georgia Southern University)

[10] Awadh, W. A., Hashim, A. S., & Hamoud, A. (2019). A Review of VariousSteganography Techniques in Cloud Computing. University of Thi-Qar Journalof Science, 7(1), 113-119.

[11] Banyal, R. K., Jain, P., & Jain, V. K. (2013, September). Multi-factorauthentication framework for cloud computing. In 2013 Fifth InternationalConference on Computational Intelligence, Modelling and Simulation (pp. 105-110). IEEE.

[12] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2020). Acomprehensive survey of AI-enabled phishing attacks detectiontechniques. Telecommunication Systems, 1-16.

Bendechache, M., Svorobej, S., Takako Endo, P., & Lynn, T. (2020). Simulatingresource management across the cloud-to-thing continuum: A survey and futuredirections. Future Internet, 12(6), 95.

[13] Duncan, A. J., Creese, S., & Goldsmith, M. (2012, June). Insider attacks in cloud computing. In 2012 IEEE 11th international conference on trust, security and privacy in computing and communications (pp. 857-862). IEEE.

[14] Gong, M. (2020). Cloud-Based System for Effective Surveillance and Control of COVID-19: Useful Experiences From Hubei, China. Journal of Medical Interne Research, 22(4), 4-20.

[15] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1-13.

[16] Hourani, H., & Abdallah, M. (2018, July). Cloud computing: legal and security issues. In 2018 8th International Conference on Computer Science and Information Technology (CSIT) (pp. 13-16). IEEE.

[17] Ibidunmoye, O. (2016). Performance problem diagnosis in cloud infrastructures (Doctoral dissertation, Department of Computing Science, Umeå University).

[18] Jabir, R. M., Khanji, S. I. R., Ahmad, L. A., Alfandi, O., & Said, H. (2016, January). Analysis of cloud computing attacks and countermeasures. In 2016 18th International Conference on Advanced Communication Technology (ICACT) (pp. 117-123). IEEE.

[19] Jan, S. U., Ghani, D., A Alshdadi, A., & Daud, A. (2020). Issues and challenges in cloud storage architecture: a survey. , Issues and Challenges in CloudStorage Architecture: A Survey. Researchpedia Journal of Computing, Volume 1, Issue 1, Article 6, Pages 50–65, Jun 2020.Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3630761 accessed: May07 2021

[20] Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. International Journal of Engineering Research and Applications, 7(6), 31-38.

[21] Javaid, A. (2013). Top Threats to Cloud Computing Security.SSRN Electronic Journal.10.2139/ssrn.2325234

[22] Khalil, S., Fernandez, V., & Fautrero, V. (2016, August). Cloud impact on IT governance. In 2016 IEEE 18th Conference on Business Informatics (CBI) (Vol. 1, pp. 255-261). IEEE.

[23] Khan, I. R., & Alam, M. (2017). Cloud Computing: Issues and FutureDirection.
Global Sci-Tech, 9(1), 37-44.

[24] Lee, T., Kim, H., Rhee, K. H., & Shin, U. S. (2013). Design and Implementation of E-Discovery as a Service based on Cloud Computing. Computer Science and Information Systems, 10(2), 703-724.

[25] Majeed, M. G. A. S. S. (2020). Data security in cloud computing. Solid State Technology, 63(6), 7184-7193

[26] Megouache, L., Zitouni, A., & Djoudi, M. (2020). Ensuring user authentication and data integrity in multi-cloud environment. Human-centric Computing an Information Sciences, 10, 1-20.

[27] Megouache, L., Zitouni, A., & Djoudi, M. (2020). Ensuring user authentication and data integrity in multi-cloud environment. Human-centric Computing and Information Sciences, 10, 1-20.

[28] Milkovich, D. (2020, December 23). Cybint. From Cybintsolutions: Available at :https://www.cybintsolutions.com/cyber-security-facts-stats. Accessed: May 13 2021

[29] Neicu, A. I., Radu, A. C., Zaman, G., Stoica, I., & Răpan, F. (2020). Cloud Computing Usage in SMEs. An Empirical Study Based on SMEs Employees Perceptions. Sustainability, 12(12), 4960.

[30] O'Keeffe, D., Vranaki, A., Pasquier, T., & Eyers, D. (2020, April). Facilitating plausible deniability for cloud providers regarding tenants' activities using trusted execution. In 2020 IEEE International Conference on Cloud Engineering (IC2E) (pp. 59-65). IEEE.

[31] Odun-Ayo, I., Ananya, M., Agono, F., & Goddy-Worlu, R. (2018, July). Cloud computing architecture: A critical analysis. In 2018 18th international conference on computational science and applications (ICCSA) (pp. 1-7). IEEE.

[32] Odun-Ayo, I., Geteloma, V., Falade, A., Oyom, P., & Toro-Abasi, W. (2019, December). A Systematic Mapping Study of Utility-Driven Models and Mechanisms for Interclouds or Federations. In Journal of Physics: Conference Series (Vol. 1378, No. 4, p. 042008). IOP Publishing.

[33] Opara-Martins, Justice, Reza Sahandi, and Feng Tian. "Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective." Journal of Cloud Computing 5, no. 1 (2016): 1-18.

[34] Patrick, Z. P. G., & Satyanarayana, K. (2020). optimization of service level agreements (SLAS) within saas cloud it infrastructure. Journal of Critical Reviews, 7(1), 414-420.

[35] Rani, D., & Ranjan, R. K. (2014). A comparative study of SaaS, PaaS and IaaS in cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering, 4(6).

[36] Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9(9), 1460.

[37] Schulze, H. (2020). Cloud Security Report. Cybersecurity Insiders. Available at: https://www.isc2.org/Resource-Center/Reports/Cloud-Security-Report//media/44A81ED54571463997B1DDACE905665F.ashx .Accessed : 04 may 2021

[38] Shankarwar, M. U., & Pawar, A. V. (2015). Security and privacy in cloud computing: A survey. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 (pp. 1-11). Springer, Cham.

[39] Shibli, M. A., Masood, R., Habiba, U., Kanwal, A., Ghazi, Y., & Mumtaz, R. (2014). Access control as a service in cloud: challenges, impact and strategies. In Continued Rise of the Cloud (pp. 55-99). Springer, London.

[40] Srinivasan, K., Mubarakali, A., Alqahtani, A. S., & Kumar, A. D. (2019, February). A Survey on the Impact of DDoS Attacks in Cloud Computing Prevention, Detection and Mitigation Techniques. In Intelligent Communication Technologies and Virtual Mobile Networks (pp. 252-270). Springer, Cham.

[41] Tadapaneni, N. R. (2020). Cloud Computing Security Challenges. International Journal of Innovations in Engineering Research and Technology, 6(7) (pp. 1-6)

[42] Tahboub, R., & Saleh, Y. (2014, January). Data leakage/loss prevention systems (DLP). In 2014 World Congress on Computer Applications and Information Systems (WCCAIS) (pp. 1-6). IEEE.

[43] Tirumala, S. S., Sathu, H., & Naidu, V. (2015, December). Analysis and prevention of account hijacking based incidents in cloud environment. In 2015 international Conference on Information Technology (ICIT) (pp. 124-129). IEEE.

[44] Ujjwal, K. C., Garg, S., Hilton, J., Aryal, J., & Forbes-Smith, N. (2019). Cloud Computing in natural hazard modeling systems: Current research trends and future directions. International Journal of Disaster Risk Reduction, 38, 101188.

[45] Usman, A., Awwalu, J., & Kamil, B. (2016). Security threat on Cloud Computing. International Journal of Emerging Trends & Technology in Computer Science (pp. 18-21)

[46] Watson, M. R., Marnerides, A. K., Mauthe, A., & Hutchison, D. (2015). Malware detection in cloud computing infrastructures. IEEE Transactions on Dependable and Secure Computing, 13(2), 192-205.

[47] Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. Journal of Internet Services and Applications, 7(1), 1-12.

[48]Zafar, F., Khan, A., Malik, S. U. R., Ahmed, M., Anjum, A., Khan, M. I.,& Jamil,F. (2017). A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. Computers & Security, 65, 29-49.

[49] S. Sridevi, R. Anandan (2019). AORA-A Novel Optimized Intrusion Detection System for Identification of the Black Hole Attacks in Wireless Sensor Networks. (IJRTE) ISSN: 2277-3878.

[50] Sridevi, S., Anandan, R.(2020). RUDRA—A novel re-concurrent unified classifier for the detection of different attacks in wireless sensor networks. Advances in Intelligent Systems and Computing, 2020, 1125, pp. 251–259.