Cloud Computing Security Issues and Techniques: A Systematic Review

Dr. Brinitha Raji

Abstract: *Cloud computing has become increasingly well-liked and successful as a result of improvements in the way information and communication technologies (ICT) are used. For corporate customers, cloud computing offers benefits and chances to move and take advantage of the scalability of the pay-as-you-go pricing model. The adoption of cloud implementation and services has become crucial due to security and privacy concerns raised by outsourcing data and business applications to the cloud or a third party. To address the current security issues, researchers and impacted enterprises have put forth several security strategies in the literature. This systematic review of the literature aims to examine the current research on cloud computing security, dangers, and difficulties. According to the study's findings, 50 publications were chosen and examined after meeting the requirements. With the help of a systematic literature review, we were able to identify a sufficient number of obstacles and solutions that are currently and in the future employed in cloud computing. Future research and cloud users/business organizations might benefit from having a general understanding of the risk elements in a cloud environment and deliberately use this technology to map their indigenous requirements.*

Keywords: Virtualization; Service Level Agreements; Data access; Multifactor authentication; Encryption; Cryptography; Security solutions; Vulnerability

1. Introduction

Large rooms and massive quantities of power have played a major part in the history of technology; therefore, they are commonly utilized to produce just a small quantity of processing output. Smaller and more efficient computers have increasingly replaced large (in some cases, room-size) computers during the previous few decades. Contrary to common belief, both the amount of data needed, and the number of social media users have increased dramatically over the past decade. Data access via conventional computing is also unavailable wherever and at any time due to the infrastructure's increased cost and management complexity. As a result, it has become clear that the external storage system is crucial for maintaining data. Traditional computers cannot keep up with the rising number of internet users on networking websites, social media, information in any manner, etc. Since the number of people using the Internet has steadily increased throughout the world, a brand-new idea known as cloud computing has emerged. The IT business may undergo transformation thanks to the cloud computing environment, which is considered a great breakthrough in computing. This increases the IT sector's consumer appeal and utility while also influencing how IT products are produced and bought (Michael Armbrust et al., 2009). Besides, it would alter peoples' ways of living and working. A combination of grid and utility computing that combines creates a group of dynamically networked computers is one description of cloud computing. They gave the impression of being more unified computing resources. Its foundation consists of service-level agreements (SLA). Cloud computing offers fresh technologies to companies because it is still a young and developing sector. In cloud computing, application types such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IAAS) are specified. The SaaS concept allows users to create software and other programmes in the cloud. By using a SaaS solution, internal applications, storage systems, and administration support are not required. Again, for SaaS resources they use, businesses must pay per user (K. Jamsa,2012). PaaS is a cloud computing solution that allows users to build their own cloud-based services and applications and manages the entire software life span (T. Dillon et al., 2010). Programmers and developers don't need to purchase their own hardware; instead, they use intermediary hardware and offer the programmes they develop to customers online. IaaS stands for a platform-based cloud technology service that is provided in a virtual environment (A. Bouayad et al., 2012). Clients are not needed to acquire servers, data centers, network infrastructure, or space (e.g., Amazon EC2). The main differences between cloud computing and traditional computing are its elasticity, scalability, and the ease with which its users can provision resources for scaling. Additionally, it offers its consumers services at different levels.

Security is a major factor in whether cloud computing services are used more widely. (C. Vidal and K.-K. R. Choo, 2017). It is important to first comprehend the cloud setup presented in the next paragraphs in order to have a better knowledge of security concerns. A cloud business is composed of resources that are devoted to demands. Threats and risk to cloud customers and cloud providers are the main topics of the classification. A cloud consumer is an individual or company that makes use of cloud services. In actuality, a cloud user can select the most suitable services by carefully reviewing the services offered by cloud providers and concluding a contract. To complete this contract and establish the technical performance, a service-level agreement (SLA) between a cloud consumer and a cloud provider must be executed. SLAs (as an agreement) encompass issues including service quality consistency, security, and performance failure prevention. A cloud user can pick providers with better prices and more beneficial services; though. A cloud provider is a person or organization which provides a service available to a cloud user. The cloud provider arranges and distributes cloud software by purchasing and managing the cloud infrastructure. When using SaaS, the cloud provider deploys, configures, maintains, and updates the software applications to deliver services at desired service levels. According to the limited administrative uses of the cloud, SaaS providers are primarily responsible for managing and regulating the infrastructure and applications. In PaaS, the cloud provider administers the platform's computer infrastructure while cloud software

Paper ID: SR23701110417 DOI: https://dx.doi.org/10.21275/SR23701110417

provides its product's elements. In IaaS, the cloud provider purchases the physical computer resources, including servers, networks, storages, and other hosting infrastructure. It is up to a cloud auditor to objectively review the cloud services. In order to determine if standards have been met, the auditor looks at several objective data. The performance, security precautions, privacy implications, and other features of cloud storage offerings may all be assessed by cloud auditors. Cloud consumers buy the cloud services through some kind of cloud broker rather than dealing with the cloud provider directly since coordinating the interoperability of cloud services is too complicated for them. Actually, the cloud broker is in responsible for managing interactions between cloud providers and clients as well as cloud provision of services, performance, and utilization. A cloud carrier serves as a middleman between cloud providers and their clients to deliver cloud services. Cloud carriers may contact clients via networking and other access tools. As was already indicated, through establishing SLAs with such a cloud carrier, the cloud provider may deliver services to cloud users that are in compliance with SLAs. In addition, the cloud carrier is responsible for assigning trustworthy connections to cloud users and providers.

Confidential information is typically maintained on servers in apps. Data security is always of utmost significance. There are so many difficulties with security. Today, many computing systems fail due to data leaks that are secret. Despite the fact that virtualization and cloud computing offer a wide range of range of methods, security concerns are frequently viewed as a big issue in the cloud, which discourages users from using the technology. Here, some of the security issues with the cloud are covered along with integrity, availability, and confidentiality. Integrity makes ensuring that the information kept in a system correctly represents the careful selection and hasn't been changed by a trusted third party. While any software is running on a server, backup procedures are set up to be safe in the event of a loss of data occurring. Typically, the data is backed up to any portable medium on an even schedule and then kept off-site (C. C Ragin, 1997). According to Jun Feng and Yu Chen (2010), availability ensures that destructive behaviors won't result in the loss of data processing resources. When a user tries to access something, it is an obvious sign that it is available. This is crucial for systems that are mission-critical (Jun-Ho Lee, Min-Woo Park, 2011). Business Continuity Plans (BCPs) must be implemented by organizations to ensure the availability of these systems (B. Lagesse, 2011). Data privacy ensures that private information is not disclosed to unauthorized parties. Confidentiality is compromised when data is accessible to anybody with unauthorized access. You might lose confidentiality physically or digitally. Actual sensitive information is lost due to social engineering. Electronic secrecy is lost when customers and servers refuse to encrypt their communications. (Brenner Michel and Wiebelitz 2011). For purposes such as resource allocation, memory and storage sharing, and distributed computing, multi-tenancy is constructed. It offers good hardware component utilization (Chang Jie Guo et al., 2007) and has very low maintenance costs. It provides the distribution of resources, services, and applications among different components at service providers using the same physical or logical platform. As a result, it violates data confidentiality and causes information leakage, which increases the risk of assaults. The service provider offers a multitenant approach called cloud computing. Information leaking thus becomes a concern for the organization. For recruiting cloud workers, there are no regulations. As a result, a third-party provider may simply hack into a company, making it impossible for that company's data to remain secure. It causes user information loss and compromises security, confidentiality, and integrity. As of yet, there is no known way to defend against this attack (Naresh Vurukonda and B. Thirumala Rao, 2016). One of the main issues of a company is external attacks. Data are stored on servers, and this is publicly accessible private information of a company. Because there are several interfaces in clouds, they vary from private networks. One drawback is that hackers and attackers can break connections by taking advantage of API vulnerabilities. Numerous firms store their data on servers in a cloud environment, however, there are security gaps in the cloud infrastructure. Privacy breaches, concerns with information integrity, and problems with authentication occur. To avoid the loss of sensitive information or other vulnerabilities, any data or services flowing across the network must be protected from attackers throughout the resource pooling process (C. Hong,et al, 2010). It is one of the most often found cloud vulnerabilities and is a direct outcome of XML Signature wrapping Attack and languages and programmes that act as Trojan horses or malware. Malware and Trojan horses are illegal programmes that are embedded or introduced by a malevolent user inside legitimate programmes to carry out unintended and unauthorized functions. It does not multiply itself as viruses do. These kinds of attacks target protocols like SOAP that transmit service requests in XML format. In this attack, the original SOAP message body is transferred to a newly added wrapping element that is written within the SOAP header attack.

The remainder of the SLR is organized as follows. The basic information on the main security services and the main approaches taken to deliver each service is presented in Section 2. The Review of Literature includes an analysis of the advantages and disadvantages of the existing security and privacy in cloud computing. The systematic evaluation and thorough comparison of the examined publications are provided in Section 3. The comparison table lists the most recent threat mitigation strategies put forth by different academics, along with performance metrics, benefits, and drawbacks. Section 4 presents the conclusion of the discussion. The most efficient method, which is appropriate for cloud security advancements, is summarized in the conclusion section. It will emphasize more research as well.

2. Literature Review

It might be challenging to identify security issues, threats, and suitable mitigating techniques in the setting of cloud services. A qualitative research technique was used in this study to offer a complete knowledge of the cloud computing phenomenon, its forerunners, difficulties, dangers, and defense mechanisms. A systematic literature review (SLR) is conducted to gather the most recent knowledge. The main objective of this study is to investigate security vulnerabilities with cloud computing services. The approaches for risk reduction from significant prior research projects are the main topic of this paper.

The existing literature is mostly concerned with implementing security policies and various technologies. The later study presented further criminological assaults on the cloud environment. The suggested defense for the cloud against these current attacks is based on criminal notions. Research by N. Khan and A. Al-Yasiri (2018) found a number of security flaws that have an impact on cloud computing features. The same study makes solutions to the issues with cloud security that has been found. The research-developed security guide makes security risks known to cloud user companies. Utilizing cloud computing services results in security issues and challenges. Currently, cloud computing paradigms are the major culprit behind these challenges and hazards. Hackers exploit the weakness of cloud models to get access to sensitive consumer data by attacking computer systems' processing power. The "Autonomous Cloud Intrusion Response System" (ACIRS) has recently been proposed as a solution to the aforementioned problem (H. A. Kholidy,2016). Prior to this study, the "Network Intrusion Detection and Countermeasure Selection System" (NICE) (C.-J. Chung, 2013) researched the optimum safeguards to lessen the dangers to cloud virtual networks. ACRIS is better to NICE in terms of lowering the risks and challenges that networks face. The usage of cloud computing (CC) in the information technology field is widespread. Several service owners still are unwilling to fully deploy the CC due to the immaturity of the pertinent security technology. Research shows that service providers should invest in the security of CC- associated devices as a result (J.-Y. Park, 2017).

Businesses should use a variety of network security measures, including physical and virtual firewalls, intrusion detection and prevention systems, gateways, deliberate workload limitations, and cloud application controls. In addition, 66% of respondents claimed that over the previous two years, cyber security had a negative impact on their business operations. These consequences included delays in IT initiatives as well as disruptions to routine company operations and service delivery.

A taxonomy of attacks in virtualized systems has been proposed by (Sgandurra and Lupu, 2016) taking into account the targets at multiple stages, the origin, and the attackers' goals. They truly aim to show how risks grow in virtualized systems at several layers, including the hardware, operating system, and application, as well as how these risks are related to security and trust presumptions.

The security issues with cloud computing were explored by (Kaur and Singh ,2015). In this study, the issues related to data location, storage, security, accessibility, and authenticity have been discussed. In reality, the main topic of this study is one of the primary security problems, however, it's important to point out that the writers just discuss security risks without going into alternative remedies.

(Kumar et al., 2018) had provided a solution to address security concerns in a multi- tenant system as well as other kinds of data security concerns in cloud computing. This paper's whole subject matter is data security concerns, and it provides methods for securing data and upholding user privacy.

The following is a survey of studies on concerns about security and privacy with cloud computing (Khalil et al., 2014). This document categorizes a wide range of well-known security concerns and attacks as well as different types of cloud vulnerabilities. This review effort also analyses potential future security risks and examines the flaws in the current remedies.

The review study by Bashir and Haider (2011) outlines the security risks associated with cloud computing. By examining alternative security models and solutions, this review effort also considers the primary security concerns presented by providers and end users in connection to cloud computing.

(Ryan, 2013) offer a survey with crucial points for future study, such as a technique for data protection that attempts to safeguard data in the cloud infrastructure providers. Additionally, a browser key translation technique is described in this work that enables a software-as-a-service application to offer confidentiality services.

Cryptography is the most used technique of user authentication. The most effective method for ensuring high levels of data storage and transmission security is cryptography. Traditional symmetrical and asymmetrical patterns have certain drawbacks. This problem was addressed by introducing a novel hybrid approach by Chinnasamy, P. et al. in the year 2021. In this article, a hybrid method is constructed by merging ECC with Blowfish.

Between interacting systems, authentication is provided through cryptography (D. Feng et al., 2011). One of the most popular methods of user authentication is passwords. Another method of authentication is a security token or a biometric, such as a fingerprint. Traditional identity management techniques are insufficient for the cloud context. When an organization makes use of several cloud service providers (CSPs). Identity information synchronization in this case is not scalable. When converting from a traditional approach to cloud-based, infrastructure is another major concern. Checking for illegal activity is a challenging task. Users that save their data in the offered cloud do not know where the data is kept; instead, the data is stored on a server. Therefore, the cloud service provider must offer consumers inspection tools so they can check and manage how various policy implementations are carried out.

Hyperelliptic curve cryptography is suggested as an effective solution for protecting cloud data by Nagendran et al. (2018). (HECC). The suggested cryptographic method provides efficient cloud-based data encryption and decryption. A protected key agreement, encryption, decryption, and signature mechanism are all offered by the proposed hyperelliptic cryptography system. Comparing the HECC system to other cryptosystems, it uses less power, bandwidth, and storage. HECC also employs smaller key sizes, ranging from 50 to 80 bits, and is effective in bringing down algorithm complexity.

(Ferrer and colleagues, 2019), This research intends to make a new impact by helping in the recognition of their connections and established advancements as possible impact to the further evolution of the Decentralized Cloud concept, using an SLR of appears to work in the disciplines of Mobile Cloud Computing, Mobile Ad hoc Computing, and Edge Computing.

Sensitive information can be transferred securely without danger of loss or alteration by an unauthorized person while using an insecure channel. Many encryption algorithms have been employed in diverse situations to secure data. Numerous cryptosystems were active at various eras and evolved through time. Khan, I. A., and R. Qazi (2019). Primarily on asymmetric encryption, often referred to as public key encryption or holomorphic encryption. Due to the large key size, asymmetric encryption is primarily used for key exchange instead of data encryption. Because the key being used elliptic curve cryptography has become so small, this study uses it to encrypt data on the cloud. The Elliptic Curve uses the least amount of computing resources due to its small key size. This study demonstrates how elliptic curve encryption may safeguard data quickly, more effectively, and with less processing resources in a cloud computing environment.

Simulation software is a crucial tool for planning, setting, maintaining, and assessing the performance of a system due to the ubiquity and complexity of computer systems that are only growing. In pay-as-you-go (PAYG) scenarios, Simulators for cloud computing have been helpful in evaluating the trade-offs between cost and performance. In order to give an overview of simulation tools suited for cloud systems, (Bahwaireth et al., 2016) set out to do just that. There are several tools described, including CloudSim, CloudAnalyst, CloudReport, CloudExp, iCanCloud, and GreenCloud. The author said that iCanCloud is a superior platform when contrasting the various simulators since it operates on Java Virtual Machine and offers complete GUI support to the user. It is also created especially for cloud simulation.

The authors of (Mollah, M.B et al., 2017) provide a thorough analysis of the security and privacy issues faced by MCC as well as their security solutions. First, give a general history of MCC. Then talks about the MCC's possible privacy and security issues. Present very recent related works after that, followed by a summary of the security solutions.

Distributed cloud storage features a blockchain-based security architecture that has been proposed (Jiaxing Li et al., 2018).In terms of security and network transmission latency, the suggested design has been contrasted with two other conventional architectures. According to the simulation assumptions utilized in this study, the recommended performs on average better than the other two conventional designs. The network performance of the traditional distributed architecture has been improved by a revised evolutionary algorithm that reduces the expenses related to replica scheduling and transmission. Additionally, compared to the other two standard structures, the suggested architecture has lower transmission latency. Comparative simulation results demonstrate the remarkable security and network performance of the proposed architecture.

A revolutionary integrated safe and intelligent architecture for the Internet of Things and Cloud Computing is offered by (T.D.P. Bai, S.A. Rabara, 2015). Regardless of the underlying technologies in a smart environment, the public may access a variety of smart apps and services dispersed in the cloud using this one-of-a-kind intelligent architecture from anywhere, at any time, on any device, and over any network. Through a cutting-edge IP/MPLS (Internet Protocol/Multiprotocol Label Switching) core, the cloud services are connected and integrated. To provide total defense against security concerns including confidentiality, integrity, privacy, and authentication, elliptic curve cryptography (ECC) is utilized. With improved performance and the elimination of ambiguity, this model accomplishes the goal of "one intelligent smart card for any applications and transactions." By setting up a test bed in a simulated environment, the performance of the suggested design is evaluated, and the findings are presented.

The application of CoT in the context of smart healthcare is examined by (M.M. Mahmoud et al., 2018), along with CoT designs and platforms. Explains several relevant CoT concerns, such as the absence of uniformity, in the following. Additionally, it emphasizes energy efficiency and provides a thorough examination of the most pertinent suggestions found in the literature. There is still a need to increase energy efficiency, particularly with regard to QoS and performance, according to an analysis of all the energy efficiency solutions examined in this study.

The CoT presents a novel flexible communication paradigm for secure communication (V. Vasic et al., 2017). The author of this research suggests a general approach that offers the required building blocks (i.e., operations) for safe communication in the CoT with the goal of offering adaptable communication mechanisms that can fit well to the resource and context of a CoT environment. The experimental evaluation of the suggested technique reveals encouraging runtime performance for a variety of security scenarios and devices in the CoT, and as a consequence, it greatly advances the state of the art, especially in terms of practical implementations.

3. Comparison of Recent Techniques

One of the biggest issues facing large companies today is security. Examples include banking, supply chain management (SCM), electronic health data, and smart apps. Users' data is encrypted by cloud service providers using a robust encryption method (William Stallings, Cryptography and Network Security Principles and Practic); yet, in some cases, encryption errors can render data utterly unusable, and encryption is extremely challenging. Given the difficulty of the undertaking, the cloud provider must show that the encryption method was developed and thoroughly examined by an authority with the necessary expertise and experience.

A cutting-edge framework is suggested by research (P. Velmurugadass et al., 2020) to follow the actions taking place at the specific data evidence. This data proof is composed of SHA-256 Cryptographic Hash Algorithm-based information and user signatures. A cloud- based "software - defined network" (SDN) is comprised of a Blockchain controller, a cloud server, and an Authentication Server (AS) that all function in concert. The researchers advise that all customers connect with the AS in order to obtain the secret key. The

"Elliptic Curve Integrated Encryption Scheme" (ECIES) approach is used in this suggested framework to encrypt data packets before transferring them to a cloud server. The experimental findings showed that higher performance had been reached in regard to throughput, reaction time, reliability, and general change security features. Both academics and industry face difficult challenges with resource allocation and job scheduling. Security has been regarded as a key factor for customizing cloud services for job scheduling in a distributed computing environment. A. Wilczynski and J. Koodziej (2020) claim that by combining blockchain technology with cloud clusters, it is possible to access application and data codes and conduct safe cloud transactions. According to a recent study, a special blockchain scheduler outperforms more established cloud scheduling techniques. The simulation used in the suggested research, which might be quite realistic but isn't entirely relevant to real-world case studies, is one of its shortcomings. As a result, while developing a multi-cloud system in future works, researchers can take into account plausible situations involving various cloud clusters and cloud technologies. The bulk of research investigations (P. Velmurugadass et al., 2020; A. Wilczynski and J. Koodziej, 2020; J. Cha et al., 2021, H. Huang et al., 2020; Y. Ren et al., 2020; J. Li et al., 2020) have been centered on using blockchain technology to secure cloud data. Utilizing blockchain technology effectively adds an additional degree of security to data stored in clouds while maintaining user confidence in the outsourcing of the data. A valid user obtains the necessary data. Electronic medical records (EMRs) are data exchange systems that make it easier for users to obtain medical records and effectively retain patient information (D. C. Nguyen, 2019). In the cloud computing environment, data transfers also take place between mobile devices that are linked. Still, future research projects will need to address privacy and security issues with blockchain technology. Identity protection for users is crucial.

(N. Eltayieb et al., 2020) offer a blockchain-based attribute-based verifiable outsourced signcryption system that makes it possible to store and share EHRs securely on the cloud. The suggested approach fulfills the requirements of fine-grained access control, secrecy, unforgeability, verifiability, privacy protection, and non-tampering and benefits from attribute-based signcryption, blockchain, and cloud storage. Additionally, our plan makes use of outsourced computing technologies to let CS do the majority of the computations, which lessens the user's computing load. In the conventional model, our approach has also been shown to be secure. Performance study demonstrates that the suggested plan has high efficiency and is practicable as a result.

In order to safeguard the users' identification, research (Q. Su et al., 2020) suggested an attribute-based solution. The suggested method has an attribute master key and an attribute signing key and is based on the KUN odes. Using the KUNodes technique, it is simple to revoke these properties. The suggested method is collision-resistant, unforgeable, and security- preserving.

The drawbacks of cloud-centric computing are numerous. The problems brought on by the unilateral test is one of them. This is the case in a cloud environment when an application is assigned to a user. When a single point of failure happens, cloud-centric computing cannot scale (Y. He et al., 2020). To solve these issues, numerous Internet of Things (IoT) scenarios employ decentralized computing. Applications and services may be easily accessed since linked devices can be locally handled rather than needing third-party services. The resource allocation to clients is optimized via blockchain technology. The proper distribution of computer resources to the real buyers is ensured via auction algorithms. The broker idea was developed in research (Z. Li et al., 2019) as a means of controlling and altering the trading market. The suggested research also combines edge-cloud computing and blockchain technology to address the issues of real-time computing and resource allocation. In the proposed study, the resources of buyers and sellers are competing in a trading economy. Before properly distributing resources, an adaptive auction schema first collects the demands of the purchasers. Security and trust are major issues for IoT Big Data. Trust issues have been resolved by recommending the blockchain network to manage data retrieval and store and prevent data manipulation from internal users and outside attackers (M. Zhaofeng et al.,2019). The entire ledger continues to function and offers users security and trust even if data on some partial nodes is altered because tampering cannot reach and be successful at all. The proposed technique still has security vulnerabilities despite exposing the key for encrypting data at the user layer. Cloud computing, IoT devices, and fog nodes can communicate privately and securely thanks to blockchain technology. As a result of the fact that the study is still ongoing (S. Algarni et al., 2021), it was not entirely successful. The recommended framework from the subsequent study has not been used in a real-world situation. This is due to the issue with big heads in the blockchain topology. This subject is still up for debate. Another critical issue for those involved in blockchain technology is the necessity for latency. The proposed blockchain architecture and smart contracts are assessed using several scenarios (T. M. Fernández-Caramés et al., 2019). The delay must be maintained to a minimum when communication and processing power are carried close to the sensor nodes. In order to enable scalability, mobility, and location awareness, the linked devices in physical surroundings must have the smallest latency feasible. Latency is hence helpful for cloud computing users. Transfer of data on distributed data storage now has an extra degree of security thanks to blockchain technology. By using a smart contract, the correctness or fairness of data flow may be verified without the need of a trustworthy third party. The cost of sending data to cloud storage is decreased by the study that is suggested in (Y. N. Li., 2020). Blockchain technology, however, has problems transmitting the identical data claims made by the purchasers. A hacker might use alternative channels to sell the data privately. Summarized and provided the suggested solutions for cloud computing-related data security problems. Data security has been a top priority as cloud computing with big data has expanded significantly over the past few years. For the various services, there are contradictory limitations on cloud service availability. Financial services in clouds are acquired using a Semantic-Based Access Control (SBAC) technique. The suggested method gives customers access to a variety of materials on numerous platforms. Additionally, it complies with MDB regulations and safeguards sensitive data.

It is desired to give clients the ability to check the accuracy of their data in the cloud given the popularity of outsourcing archival storage to the cloud. In a multi-server environment, (Henry C. H et al., 2013) develop and implement a workable data integrity protection (DIP) strategy for the functional minimum-storage regenerating (FMSR) codes. The authors create FMSR-DIP codes that maintain the fault tolerance and traffic-saving capabilities of FMSR codes. They also use testbed experiments to evaluate the running time overhead and mathematical modeling to analyze the security strength. The findings demonstrate how different parameter settings affect how FMSR-DIP codes balance performance and security.

A formal examination of potential fine-grained data update types was put out by (Chang Liu et al., 2013), along with a proposal for a system that can completely handle both permitted audits and fine-grained update requests. A change that can significantly lower communication overheads for verifying tiny updates was also proposed, based on the aforementioned technique. Theoretical analysis and experimental findings have shown that the proposed scheme can provide big data applications with a lot of frequent small updates, like those in social media and business transactions, significantly lower overheads in addition to improved security and flexibility.

The literature has a variety of categorization approaches that categorize data in social networks or other application areas. In 2015, (Rizwana Shaikh et al.) established a set of criteria for classifying data in the cloud. It is used to provide security levels based on accessibility and type of material. Giving cloud storage the level of security necessary to maintain the data's requisite confidentiality and access limitations have examined a few data points and categorized them using the suggested parameters. The content and access control criteria can be used to categorize all of the items that are stored in cloud storage. On the basis of that, categorization provisions for storage and communication integrity, encryption, and access control methods may be made. Additionally, a regular backup strategy for disaster recovery can be used. The strength is significantly strengthened by data security or quality standards.

(Sandeep K. Sood et al. 2012) suggested a method that enables data protection, integrity verification, and authentication while adhering to the best available industry techniques Furthermore, it provides the user with added flexibility and ability to meet the increasing needs of today's modern complex and diverse networks, as well as the ability to retrieve files saved in the cloud by searching encrypted data. In Table 1, we have various comparisons that may be practiced and used in future efforts.

Table 1: Comparison of Cloud Computing Security Issues and Techniques

Author	Methodology	Advantages	Disadvantages	Remarks
J. Cha et al.	Cloud architecture enabled by blockchain	personal information security; faster and safer transactions	Issues with scalability in a big, scalable environment	Additional expansion for numerous applications in smart cities
H. Huang et al.	Blockchain-based eHealth (BCE) system	Each transaction's permanent record, such as a valid query	Tempered data is a liability. The proposed strategy's design needs to be improved	combining different EHR types to improve the precision of disease diagnosis
Y. Ren et al.	Identity-based proxy aggregate signature (IBPAS) scheme	Data availability, reliability, and integrity are all guaranteed.	Blockchain storage efficiency compression	Cloud could be used as a transitional stage.
Henry C.H et al.	Regeneration coding-based method.	The approach can be used to analyze random subsets for data integrity checks.	As security key and block size increase, efficiency in terms of computation overhead and running time deteriorates.	Probability and Length of Time
Chang Liu et al.	The public auditing makes use of fine- grained updates.	The cost of communication is lower for small data.	Improved server- side quality of service should be used to improve data security from a confidentiality and availability perspective.	Fewer data was retrieved in terms of percentage, storage, and proof size.
Rizwana Shaikh et al.	A data classification technique is created to enhance cloud security.	Depending on the need, data security is enhanced.	The strength of the encryption, integrity, and access control mechanisms need to be significantly increased.	The method's strength and quality are improved
Sandeep K. Sood et al.	A combination of techniques is used to increase security	The method is highly adaptable and capable of handling intricate structures.	Due to data leakage, retrieving files from the cloud is more complicated than searching for encrypted data.	Data security and worth (in Tera bytes)
J. Li,et al.	new procedures for Public auditing	Protecting against harmful activity	limits the ability to detect malicious activity at a higher rate.	Services for secure blockchain- based auditing
N. Eltayieb et al.	integrating blockchain and attribute-based signing	secure data sharing in the cloud	Mutual trust is still a problem that needs to be fully resolved.	deployment of smart contracts on Ethereum
D. C. Nguyen et al.	Blockchain technology in EHRs	EHRs are shared securely	does show an evaluation of the proposed on different cloud	the possibility of utilizing multiple clouds
Q. Su et al.	an attribute-based signature scheme	unalterable, immune to collusion, and protecting private	still needs to be evaluated remains	Analyze the extensive EMR data.
Y. He et al.	edge computing based on the blockchain framework	The efficient distribution of the edge computing resources	does not display activity related to a public blockchain network	expansion of a private blockchain network to a public one

4. Conclusion

In this SLR, we started by reviewing the literature on several cloud computing topics, including cloud security concerns, and associated mitigating strategies. We discovered several security problems with cloud computing. All of the core components of computation, including end-user hardware, communications systems, access control strategies, and cloud infrastructures, are part of a new paradigm known as cloud computing. Additionally, with the emergence of new phenomena such as the 5G Network, the Internet of Things (IoT), and intelligent buildings, cloud technology would play a larger role in storing and processing more data than ever before. The diversity of the modern business environment has increased the spectrum of security risks and vulnerabilities. It has recently become more challenging for organizations to recognize and address rising security problems since they are unaware of the amount and whereabouts of information and workloads stored. Without a profound comprehension of the cloud architecture, security organizations are failing to deal with issues including duplication of data, the inability to identify attacks in a timely way, a loss of supervision of access to data, and the protection required to meet legal standards. To achieve complete cloud security, the information and cloud technology must be protected from both known and unknowable threats. Numerous research have attempted to tackle the security concerns in the context of clouds. There are still many unresolved issues that must be addressed in order to establish a secure cloud infrastructure. Traditional issues with networking, data protection, app, and online platform security are present at the beginning of cloud computing. Multi-tenancy, virtualization, and sharing pool resources are some examples of innovative security issues. In a cloud-based computing environment, there are many services and resources available, but the value and sensitivity of those resources determine how secure they are. However, no operations are made just on encrypted data in the storage. The bulk of calculations required data in plain text. Attackers may target the external or internal processor's memory, which is utilized to gather temporary data. Research is being conducted in this area to provide a comprehensive approach that maintains privacy throughout calculating time. Additionally needed in cloud technology is a security mechanism for insider danger. Numerous options continue to function using the cloud. However, the available alternatives cannot adequately address the insider threat. One of these incidents that still need examination is the identification of insider attack in cloud computing. In this instance, a sign is made to help identify insider attacks. This signal will increase the chance of safeguarding the cloud system. Another significant concern in the context of cloud computing is how difficult it is to discern between trustworthy users and malicious users. A growing number of security products now use AI and machine learning to automate operations and provide more intelligence to differentiate between internal and external assaults. This comprises an analysis of user activity, which is employed to identify potential security risks by establishing a baseline of usage over time and identifying unusual cloud activity. Too many companies hesitate to admit the identified gaps in cloud computing security and the ongoing popularity of cloud computing. Most of the data that is stored is encrypted. They significantly underestimate the risks of today, leaving themselves vulnerable to data breaches and cloud account thefts that might cause them serious financial and reputational harm. It is evident that the best way to automate defenses and enforce data governance norms is to invest in cloud cyber security solutions that leverage automated and artificial intelligence to supplement scarce human resources. Enterprises may more readily detect and categories potential threats by using provided skills to automate the collecting and analysis of existing network data, which also increases efficiency.

References

[1] S. Algarni et al., “Blockchain-based secured access control in an IOT system,” MDPI, https://doi.org/10.3390/app11041772 (accessed Apr. 5, 2023).

[2] K. Bahwaireth, L. Tawalbeh, E. Benkhelifa, Y. Jararweh, and M. A. Tawalbeh, “Experimental comparison of simulation tools for efficient cloud and Mobile Cloud Computing Applications - EURASIP Journal on Information Security,” SpringerOpen, https://doi.org/10.1186/s13635-016-0039-y (accessed Apr. 18, 2023).

[3] T. D. P. Bai, V. Profile, S. A. Rabara, and O. M. A. Metrics, “Design and development of integrated, secured and intelligent architecture for internet of things and cloud computing: Proceedings of the 2015 3rd International Conference on Future Internet of Things and Cloud,” Guide Proceedings, https://dl.acm.org/doi/10.1109/FiCloud.2015.23 (accessed Apr. 18, 2023).

[4] Bouayad, A. Blilat, N. E. Mejhed, and M. El Ghazi, “Cloud computing: Security challenges,” *2012 Colloquium in Information Science and Technology*, pp. 26–31, 2012. doi:10.1109/cist.2012.6388058

[5] M. Brenner, J. Wiebelitz, G. von Voigt, and M. Smith, “Secret program execution in the cloud applying homomorphic encryption,” *5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011)*, pp. 114–119, 2011. doi:10.1109/dest.2011.5936608

[6] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, “Blockchain-empowered cloud architecture based on secret sharing for Smart City,” *Journal of Information Security and Applications*, vol. 57, pp. 1–12, 2021. doi:10.1016/j.jisa.2020.102686

[7] C. J. Guo, W. Sun, Y. Huang, Z. H. Wang, and B. Gao, “A framework for native multi- tenancy application development and management,” *The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007)*, 2007. doi:10.1109/cec-eee.2007.4

[8] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, “Efficient data security using hybrid cryptography on cloud computing,” *Lecture Notes in Networks and Systems*, pp. 537–547, 2020. doi:10.1007/978-981-15-7345-3_46

[9] C.-J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, “Nice: Network intrusion detection and countermeasure selection in Virtual Network Systems,” *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 198–211, 2013.

doi:10.1109/tdsc.2013.8

[10] T. Dillon, C. Wu, and E. Chang, “Cloud computing: Issues and challenges,” *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, pp. 27–33, 2010. doi:10.1109/aina.2010.187

[11] T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, and P. Fraga-Lamas, “Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IOT based continuous glucose monitoring system for diabetes mellitus research and care,” *Sensors*, vol. 19, no. 15, p. 3319, 2019. doi:10.3390/s19153319

[12] J. Ferrer, J. M. Marquès, and J. Jorba, “Towards the decentralised cloud,” *ACM Computing Surveys*, vol. 51, no. 6, pp. 1–36, 2019. doi:10.1145/3243929

[13] Hashem *et al.*, “The rise of ‘Big data’ on cloud computing: Review and open research issues,” *Information Systems*, vol. 47, pp. 98–115, 2015. doi:10.1016/j.is.2014.07.006

[14] Y. He *et al.*, “Blockchain-based Edge Computing Resource Allocation in IOT: A deep reinforcement learning approach,” *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2226–2237, 2021. doi:10.1109/jiot.2020.3035437

[15] C. Hong, Z. lv, M. Zhang, and D. Feng, “A secure and efficient role-based access policy towards cryptographic cloud storage,” *Web-Age Information Management*, pp. 264–276, 2011. doi:10.1007/978-3-642-23535-1_24

[16] H. Huang, X. Sun, F. Xiao, P. Zhu, and W. Wang, “Blockchain-based eHealth system for auditable ehrs manipulation in cloud environments,” *Journal of Parallel and Distributed Computing*, vol. 148, pp. 46–57, 2021. doi:10.1016/j.jpdc.2020.10.002

[17] K. A. Jamsa, *Cloud Computing: Saas, Paas, Iaas, Virtualization, Business Models, Mobile, Security and More*. Burlington, MA: Jones & Bartlett Learning, 2013.

[18] J. Li, J. Wu, and L. Chen, “Block-secure: Blockchain based scheme for secure P2P cloud storage,” *Information Sciences*, vol. 465, pp. 219–231, 2018. doi:10.1016/j.ins.2018.06.071

[19] J. Feng, Y. Chen, W.-S. Ku, and P. Liu, “Analysis of Integrity Vulnerabilities and a non- repudiation protocol for cloud data storage platforms,” *2010 39th International Conference on Parallel Processing Workshops*, pp. 251–258, 2010. doi:10.1109/icppw.2010.42

[20] J.-H. Lee, M.-W. Park, J.-H. Eom, and T.-M. Chung, “Multi-level intrusion detection system and log management in cloud computing,” https://www.icact.org/, https://icact.org/upload/2011/0686/20110686_abstract_b.pdf (accessed May 2, 2023).

[21] M. Kaur and H. Singh, “A review of cloud computing security issues,” *International Journal of Grid and Distributed Computing*, vol. 8, no. 3, pp. 397–403, 2015. doi:10.14257/ijgdc.2015.8.5.21

[22] Khalil, A. Khreishah, and M. Azeem, “Cloud computing security: A survey,” *Computers*, vol. 3, no. 1, pp. 1–35, 2014. doi:10.3390/computers3010001

[23] N. Khan and A. Al-Yasiri, “Cloud security threats and techniques to strengthen cloud computing adoption framework,” *Cyber Security and Threats*, pp. 268–285, 2018. doi:10.4018/978-1-5225-5634-3.ch016

[24] R. Qazi and I. A. Khan, *Data Security in cloud computing using elliptic curve cryptography*, 2020. doi:10.31221/osf.io/puj5v

[25] H. A. Kholidy, A. Erradi, S. Abdelwahed, and F. Baiardi, “A risk mitigation approach for Autonomous Cloud Intrusion Response System,” *Computing*, vol. 98, no. 11, pp. 1111– 1135, 2016. doi:10.1007/s00607-016-0495-8

[26] P. R. Kumar, P. H. Raj, and P. Jelciana, “Exploring data security issues and solutions in cloud computing,” *Procedia Computer Science*, vol. 125, pp. 691–697, 2018. doi:10.1016/j.procs.2017.12.089

[27] B. Lagesse, “Challenges in securing the interface between the cloud and Pervasive Systems,” *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pp. 106–110, 2011. doi:10.1109/percomw.2011.5766850

[28] Y. Li *et al.*, “A decentralized and secure blockchain platform for Open Fair Data Trading,” *Concurrency and Computation: Practice and Experience*, vol. 32, no. 7, 2019. doi:10.1002/cpe.5578

[29] Z. Li, Z. Yang, and S. Xie, “Computing resource trading for edge-cloud-assisted internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3661–3669, 2019. doi:10.1109/tii.2019.2897364

[30] M. M. Mahmoud *et al.*, “Enabling Technologies on Cloud of Things for Smart Healthcare,” *IEEE Access*, vol. 6, pp. 31950–31967, 2018. doi:10.1109/access.2018.2845399

[31] M. Armbrust *et al.*, “A view of cloud computing,” *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010. doi:10.1145/1721654.1721672

[32] M. B. Mollah, Md. A. Azad, and A. Vasilakos, “Security and privacy challenges in Mobile Cloud Computing: Survey and Way Ahead,” *Journal of Network and Computer Applications*, vol. 84, pp. 38–54, 2017. doi:10.1016/j.jnca.2017.02.001

[33] R. Qazi and I. A. Khan, *Data Security in cloud computing using elliptic curve cryptography*, 2020. doi:10.31221/osf.io/puj5v

[34] N. vurukonda and B. T. Rao, “A study on data storage security issues in cloud computing,” *Procedia Computer Science*, vol. 92, pp. 128–135, 2016. doi:10.1016/j.procs.2016.07.335

[35] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for secure ehrs sharing of mobile cloud based E-Health Systems,” *IEEE Access*, vol. 7, pp. 66792–66806, 2019. doi:10.1109/access.2019.2917555

[36] J.-Y. Park, S.-H. Na, and E.-N. Huh, “An optimal investment scheme based on ATM considering Cloud Security environment,” *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*, 2017. doi:10.1145/3022227.3022319

[37] C. Ragin *et al.*, “Turning the tables: How case-oriented research challenges variable- oriented research,” *Case Studies*, pp. 303–303, 1997. doi:10.4135/9781473915480.n15

[38] Y. Ren *et al.*, “Multiple cloud storage mechanism based on blockchain in Smart Homes,” *Future Generation Computer Systems*, vol. 115, pp. 304–313, 2021.

doi:10.1016/j.future.2020.09.019

[39] M. D. Ryan, “Cloud computing security: The Scientific Challenge, and a survey of Solutions,” *Journal of Systems and Software*, vol. 86, no. 9, pp. 2263–2268, 2013. doi:10.1016/j.jss.2012.12.025

[40] D. Sgandurra and E. Lupu, “Evolution of attacks, threat models, and solutions for virtualized systems,” *ACM Computing Surveys*, vol. 48, no. 3, pp. 1–38, 2016. doi:10.1145/2856126

[41] Q. Su, R. Zhang, R. Xue, and P. Li, “Revocable attribute-based signature for blockchain- based healthcare system,” *IEEE Access*, vol. 8, pp. 127884–127896, 2020. doi:10.1109/access.2020.3007691

[42] V. Vasić, A. Antonić, K. Pripužić, M. Mikuc, and I. P. Žarko, “Adaptable secure communication for the cloud of things,” *Software: Practice and Experience*, vol. 47, no. 3, pp. 489–501, 2016. doi:10.1002/spe.2437

[43] P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand, and V. Vasudevan, “Enhancing blockchain security in cloud computing with IOT environment using ECIES and cryptography hash algorithm,” *Materials Today: Proceedings*, vol. 37, pp. 2653–2659, 2021. doi:10.1016/j.matpr.2020.08.519

[44] C. Vidal and K.-K. R. Choo, “Situational Crime Prevention and the mitigation of cloud computing threats,” *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 218–233, 2018. doi:10.1007/978- 3-319-78816-6_16

[45] A. Wilczyński and J. Kołodziej, “Modelling and simulation of security-aware task scheduling in cloud computing based on Blockchain Technology,” *Simulation Modelling Practice and Theory*, vol. 99, p. 102038, 2020. doi:10.1016/j.simpat.2019.102038

[46] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, “Blockchain-enabled Decentralized Trust Management and secure usage control of IOT Big Data,” *IEEE Internet of Things Journal*, vol.7, no. 5, pp. 4000–4015, 2020. doi:10.1109/jiot.2019.2960526