A Comprehensive Survey of Security Threats, Solutions, and Future Directions in Cloud IoT security

Ramya K M[1], Rajashekhar C Biradar[2]

[1]School of Computer Science and Engineering, Research Scholar, REVA University, Bangalore, India

[1]Assistant Professor, Dept. of CSE, B.M.S. College of Engineering, Bangalore.

[2]School of Electronics and Communication Engineering, Pro Vice Chancellor, REVA University, Bangalore, India

ABSTRACT

In response to the increasing adoption of cloud computing across various industries, the demand for effective cloud security measures has grown exponentially. This survey paper provides a comprehensive examination of existing trends, vulnerabilities, threats, and challenges within the realm of cloud computing. Furthermore, we provide an in-depth evaluation of current countermeasures, frameworks, and best practices, highlighting their strengths, limitations, and effectiveness in safeguarding cloud environments. By synthesizing insights from diverse security solutions and best practices, this survey identifies key challenges that remain unresolved, offering a roadmap for future research and development in cloud security. Moreover, this paper discusses the intricate interplay between regulatory compliance, organizational policies, and technical implementations, emphasizing the critical need for a holistic approach to securing cloud infrastructures. Our insights aim to empower researchers, practitioners, and organizations to design and implement robust security strategies that effectively protect cloud environments, ensuring the integrity, confidentiality, and availability of critical data while supporting seamless business operations. By providing actionable guidance, this paper seeks to contribute to the development of secure, resilient, and future-ready cloud systems.

KEYWORDS: Cloud Computing, Robust security strategies, Cloud Security, Cloud infrastructures, Vulnerabilities.

1 INTRODUCTION

The information technology industry has seen tremendous revolutions in recent years and has grown to be an essential part of peoples' daily lives. The amount of data generated has increased significantly as a result of today's advanced computer technology. The scope of this investigation encompasses data generated by several technologies, including mobile devices, cloud computing, and Internet of Things devices. Massive volumes of data can now be efficiently processed, stored, and managed online thanks to the development of cloud computing. Through cloud computing, users may access a wide range of easily accessible and expandable resources.

The broad field of cloud services includes processing, applications, Internet-based services, and other services [1]. The requested service must be delivered by the cloud service provider. Because cloud computing enables users to access shared resources from anywhere at any time, it eliminates all limitations related to cost, space, or resource availability. The pricing, cost-effectiveness, scalability, and flexibility of cloud computing services set them apart. Cloud computing has become widely recognized and employed by enterprises of all sizes in today's technologically advanced world [2]. Figure 1 shows the cloud based IoT (Internet of Things) context.

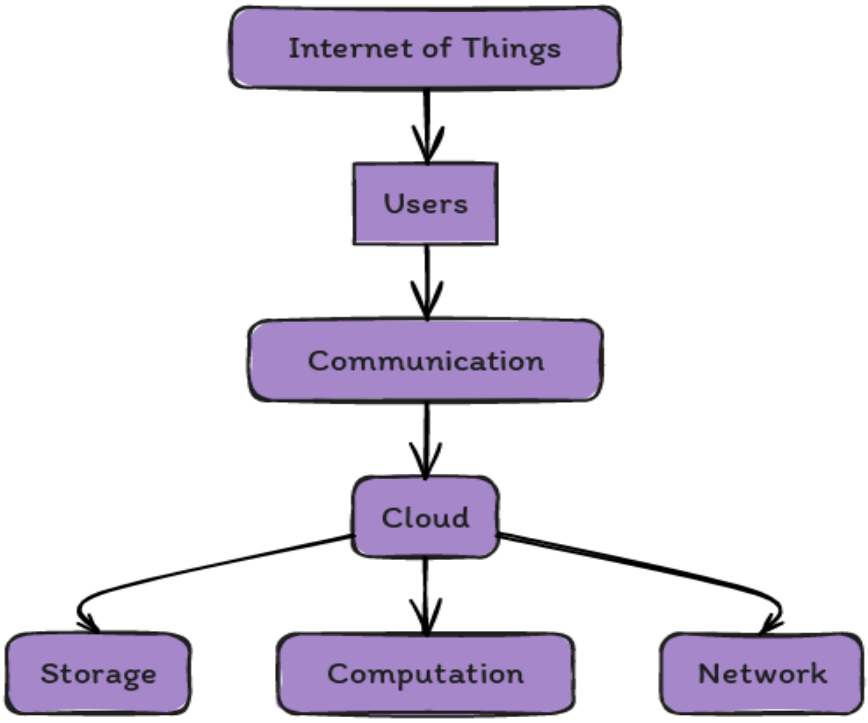

Figure 1 Cloud-based IoT context.

According to a survey, cloud computing is being implemented by nearly 96% of IT (Information Technology) companies due to its numerous benefits [3]. The architecture of cloud computing encompasses various deployment and service delivery methods. The classification of cloud deployment models can be divided into three categories: private, hybrid, and public. The classification of a cloud is determined by the deployment environment in which it is deployed. Access to the public cloud is available to all users, regardless of their affiliation with any specific company. Access to the private cloud is limited to individuals who are affiliated with the corresponding organization. The term "hybrid cloud" is used to describe a computer environment that combines both private and public cloud services. The service delivery models are categorized based on the type of service provided to customers. The classification encompasses Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Software as a Service (SaaS) enables cloud users to conveniently access a wide range of software applications through the internet.

This service allows users to utilize software applications without the need for local installation or maintenance [4-5]. The Platform as a Service (PaaS) concept enables customers to access a diverse range of platforms and resources online. The creation of apps requires this step to be performed. The concept of Infrastructure as a Service (IaaS) simplifies application development and deployment for cloud customers by offering the necessary hardware and infrastructure as a service. Cloud computing, despite its rapid growth and high demand, is susceptible to specific security vulnerabilities. Consideration must be given to security issues related to cloud computing. The loss of user control over their data occurs when it is made accessible within the domain of cloud service providers, thereby giving rise to security concerns. The user's data is accessible to multiple applications and users. The responsibility for implementing the necessary security measures lies solely with the cloud service provider. The cloud computing environment introduces new security vulnerabilities due to its shared and untrusted nature. Concerns regarding the cloud computing environment have been expressed by users, and the adoption of cloud computing has not yet reached widespread usage [6-10]. Figure 2 shows the security access control in cloud computing.

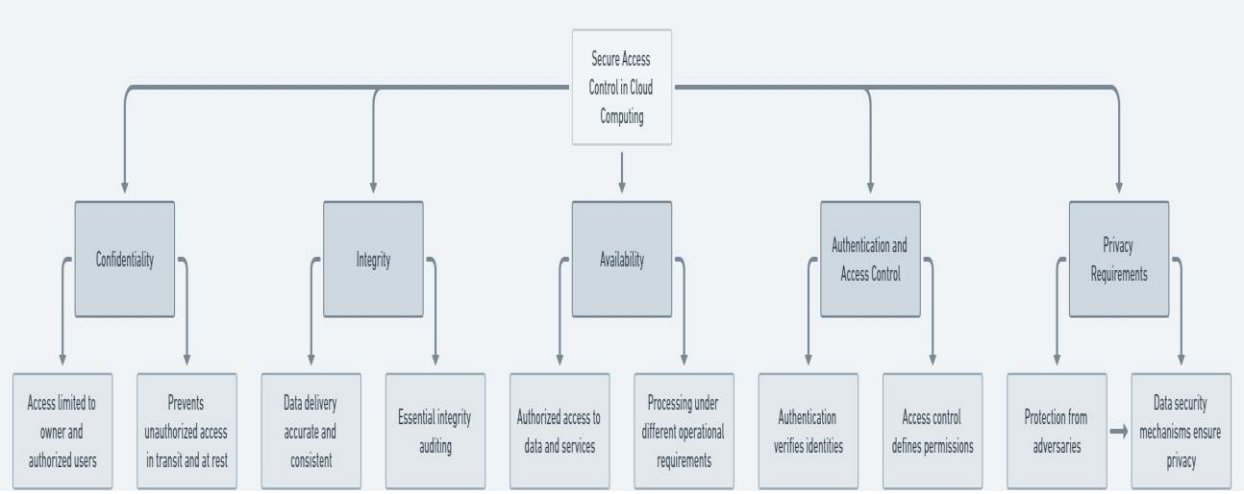

Figure 2 security access control in cloud computing

- **Privacy and security:** The foundation of the cloud architecture is comprised of virtual machines. Within the domain of cloud computing, the efficient and secure management of data resource access has emerged as a significant challenge [11]. Upon verification of the requester's identity, the access control system restricts their access to the data. The aforementioned procedure is commonly employed to ensure the protection of invaluable data assets and prevent unauthorized individuals from gaining access to or modifying them.
- **Confidentiality**: Confidentiality is a fundamental requirement in edge computing to ensure that only the data owner and authorized user(s) can access private information. The transmission, reception, storage, and processing of users' private data across edge or core network infrastructure, as well as its storage or processing in edge or cloud data centers, serves to prevent unauthorized access to the data.
- **Integrity**: The integrity of data ensures that it is delivered to authorized users in a precise, consistent, and unaltered manner. The lack of integrity auditing procedures can have an impact on the privacy of users.

- **Availability**: Availability in the context of edge computing guarantees that cloud and edge services are accessible to all authorized users wherever they are needed. The statement implies that various operational criteria can be followed in managing user data stored in ciphertext format in cloud or edge data centers.
- **Authentication and access control**: An essential step in the user verification process, authentication confirms users' identities by requiring proof of identity and confirming that identities are permitted. In a control strategy, the access control mechanism serves as an essential link between different security and privacy needs. It establishes user authentication, their rightful access to resources, and the allowed actions—like writing and reading—that guarantee confidentiality and integrity.
- **Privacy requirement:** The execution of security protocols ensures the privacy of all user data, location, and personal identity, shielding it from possible enemies who could have good intentions yet try to get unauthorized access. Additionally, by putting in place different data security mechanisms including access control, integrity audits, encryption, and authentication, privacy may be protected. Figure 3 shows the cloud security challenges.

Figure 3 Cloud security challenges

A thorough hold of [12-16] the intricate security issues at hand is necessary to solve cloud security concerns in an efficient manner. In order to mitigate cloud security risks, the following steps must be taken: This study aims to provide a thorough investigation of many aspects associated with cloud security. This test aims to cover a wide range of security-related subjects, including recognizing vulnerabilities, evaluating risks, comprehending attack models, and examining possible threats. It is critical to specify the precise requirements in terms of availability, integrity, confidentiality, and transparency while thinking about cloud security requirements. In the cloud ecosystem, a variety of organizations, including customers, service providers, outsiders, and insiders, are involved in the attack-defense cycle [17-18]. It is essential to comprehend and be able to recognize each party's specific responsibilities. Gaining a comprehensive understanding of the differences in security aspects across public, community, private, and hybrid cloud deployment models is the aim. This paper's main contribution is a comprehensive study of cloud computing security issues [19]. The topic covers a wide range of people who are engaged in cloud computing, such as service providers, end users, and independent contractors. The application, transport, and IP layers are among the network layers that are examined in this study [20]. The security implications of computer infrastructure and data centers are also examined in this study. This essay's goal is to do a detailed review of the privacy and security issues related to cloud computing. An overview of the common dangers, weaknesses, and threats related to cloud computing is given in the next section. In addition, this study looks at other types of assault and examines the connections and interdependencies between them. Furthermore, the study looks at certain attacks and compares the effectiveness of widely used responses [21-25].

In today's rapidly evolving technological landscape, cloud security has become more than just a best practice; it's an essential strategy for ensuring business continuity, customer trust, and regulatory compliance. By prioritizing cloud security, organizations can effectively protect sensitive data, prevent unauthorized access, and maintain the integrity of their systems. As the reliance on cloud services grows, so does the importance of safeguarding these environments. Implementing robust cloud security measures is a proactive step that not only minimizes risks but also fosters innovation and confidence in digital transformation [26-28]. Ultimately, investing in cloud security ensures that organizations can embrace the full potential of the cloud while remaining resilient in the face of emerging cyber threats. Together, let's build a secure and thriving future in the cloud.

- **Comprehensive Analysis:** This paper provides a holistic review of cloud security, examining vulnerabilities, threats, risks, and attack models across various cloud deployment models. It also identifies essential security requirements and analyzes the roles of different stakeholders in the security ecosystem.
- **Attack Classification and Insights:** It offers a detailed classification of attack types and their interdependencies, providing a clear understanding of known attacks and common security gaps. The paper further explores existing countermeasures and provides a comparative analysis of some of the most well-established security solutions.
- **Identification of Unaddressed Challenges:** By synthesizing insights from current security solutions, the survey identifies unattended security challenges and outlines areas that require further research, offering a roadmap for future developments in the field of cloud security.

2 RELATED WORK

2 M. K. Sinchana and R. M. Savithramma

Although cloud computing has many uses, it also has some disadvantages too, and the most important is security issue. It has many security-related issues such as identity management, resource management, and integrity control and so on. In cloud computing, if any organization or user wants to store their important data, they should provide it to the utility provider. Therefore, the risk of important information going into the evil hands is high because cloud services are available and accessible by all its users. Hence, there is the most probability of misusage of confidential data or the user data may be altered intentionally by hackers or accidentally by other users. This leads to confidentiality and consistency breach.

By considering all these issues regarding the security of the data, it is considered an important concern in cloud computing. Cryptography is widely approved method for ensuring the information security. This mechanism will secure the information by changing it to the unreadable form.

There are two types of cryptographic algorithm. They are symmetric key algorithm and asymmetric key algorithm. In symmetric key algorithm, one key is used for both encryption and decryption of the data known as private key, and in asymmetric key cryptographic algorithm, two keys are used, namely private key and public key [3]. Here, public key is used for encrypting the information, and private key is used for decrypting the user information. As compared to symmetric key cryptography, asymmetric key cryptography is considered as more secure because here we use two different keys and if in case one key gets leaked cannot cause any harm to the encrypted data.

2 Related Works

Soman and Natarajan [1] proposed an enhanced hybrid data security algorithm for the cloud in order to protect the information that is present in the cloud by using the combination of SHA256, ECDSA, and AES. These methods are used for securely sending and receiving the information or data on the cloud.

Timothy and Santra [4] have proposed a new hybrid cryptography method for security by using RSA, Blowfish, and SHA-2 algorithms. Here, by combining the symmetric and asymmetric algorithm, the efficiency of the proposed system is increased, and by using SHA-2 algorithm, high security is provided to the data transmission.

Kanna and Vasudevan [2] proposed a novel identity-based hybrid encryption (RSA with ECC) to increase the security of the information. Here, the information is encrypted by sender by using the identity-based hybrid encryption algorithm.

Singh and Malhotra [3] have proposed a hybrid two-tier agent-based framework which deploys symmetric and asymmetric key algorithms in combination to provide robust security to user data in the cloud environment.

Chauhan and Gupta [5] proposed a novel parallel cryptographic algorithm where MD5 and Blowfish encryption algorithms are used in order to overcome the problems of symmetric block cryptography and hash function algorithm, which can upgrade the security

2 M. K. Sinchana and R. M. Savithramma

Although cloud computing has many uses, it also has some disadvantages too, and the most important is security issue. It has many security-related issues such as identity management, resource management, and integrity control and so on. In cloud computing, if any organization or user wants to store their important data, they should provide it to the utility provider. Therefore, the risk of important information going into the evil hands is high because cloud services are available and accessible by all its users. Hence, there is the most probability of misusage of confidential data or the user data may be altered intentionally by hackers or accidentally by other users. This leads to confidentiality and consistency breach.

By considering all these issues regarding the security of the data, it is considered an important concern in cloud computing. Cryptography is widely approved method for ensuring the information security. This mechanism will secure the information by changing it to the unreadable form.

There are two types of cryptographic algorithm. They are symmetric key algorithm and asymmetric key algorithm. In symmetric key algorithm, one key is used for both encryption and decryption of the data known as private key, and in asymmetric key cryptographic algorithm, two keys are used, namely private key and public key [3]. Here, public key is used for encrypting the information, and private key is used for decrypting the user information. As compared to symmetric key cryptography, asymmetric key cryptography is considered as more secure because here we use two different keys and if in case one key gets leaked cannot cause any harm to the encrypted data.

2 Related Works

Soman and Natarajan [1] proposed an enhanced hybrid data security algorithm for the cloud in order to protect the information that is present in the cloud by using the combination of SHA256, ECDSA, and AES. These methods are used for securely sending and receiving the information or data on the cloud.

Timothy and Santra [4] have proposed a new hybrid cryptography method for security by using RSA, Blowfish, and SHA-2 algorithms. Here, by combining the symmetric and asymmetric algorithm, the efficiency of the proposed system is increased, and by using SHA-2 algorithm, high security is provided to the data transmission.

Kanna and Vasudevan [2] proposed a novel identity-based hybrid encryption (RSA with ECC) to increase the security of the information. Here, the information is encrypted by sender by using the identity-based hybrid encryption algorithm.

Singh and Malhotra [3] have proposed a hybrid two-tier agent-based framework which deploys symmetric and asymmetric key algorithms in combination to provide robust security to user data in the cloud environment.

Chauhan and Gupta [5] proposed a novel parallel cryptographic algorithm where MD5 and Blowfish encryption algorithms are used in order to overcome the problems of symmetric block cryptography and hash function algorithm, which can upgrade the security

2 M. K. Sinchana and R. M. Savithramma

Although cloud computing has many uses, it also has some disadvantages too,

and the most important is security issue. It has many security-related issues such as identity management, resource management, and integrity control and so on. In cloud computing, if any organization or user wants to store their important data, they should provide it to the utility provider. Therefore, the risk of important information going into the evil hands is high because cloud services are available and accessible by all its users. Hence, there is the most probability of misusage of confidential data or the user data may be altered intentionally by hackers or accidentally by other users. This leads to confidentiality and consistency breach.

By considering all these issues regarding the security of the data, it is considered an important concern in cloud computing. Cryptography is widely approved method for ensuring the information security. This mechanism will secure the information by changing it to the unreadable form.

There are two types of cryptographic algorithm. They are symmetric key algorithm and asymmetric key algorithm. In symmetric key algorithm, one key is used for both encryption and decryption of the data known as private key, and in asymmetric key cryptographic algorithm, two keys are used, namely private key and public key [3]. Here, public key is used for encrypting the information, and private key is used for decrypting the user information. As compared to symmetric key cryptography, asymmetric key cryptography is considered as more secure because here we use two different keys and if in case one key gets leaked cannot cause any harm to the encrypted data.

2 Related Works

Soman and Natarajan [1] proposed an enhanced hybrid data security algorithm for the cloud in order to protect the information that is present in the cloud by using the combination of SHA256, ECDSA, and AES. These methods are used for securely sending and receiving the information or data on the cloud.

Timothy and Santra [4] have proposed a new hybrid cryptography method for security by using RSA, Blowfish, and SHA-2 algorithms. Here, by combining the symmetric and asymmetric algorithm, the efficiency of the proposed system is increased, and by using SHA-2 algorithm, high security is provided to the data transmission.

Kanna and Vasudevan [2] proposed a novel identity-based hybrid encryption (RSA with ECC) to increase the security of the information. Here, the information is encrypted by sender by using the identity-based hybrid encryption algorithm.

Singh and Malhotra [3] have proposed a hybrid two-tier agent-based framework which deploys symmetric and asymmetric key algorithms in combination to provide robust security to user data in the cloud environment.

Chauhan and Gupta [5] proposed a novel parallel cryptographic algorithm where MD5 and Blowfish encryption algorithms are used in order to overcome the problems of symmetric block cryptography and hash function algorithm, which can upgrade the security

While cloud computing has many benefits, there are some disadvantages as well, the most significant of which being security issues. The system is linked to a number of security-related problems, including integrity control, resource management, and identity management. It is advised that individuals or businesses weigh the possible advantages of cloud computing

against the risk of losing sensitive data, and make sure the service provider they select has a solid reputation [29]. The rising availability of cloud services directly contributes to the higher danger of unauthorized people accessing sensitive data. As a result, there is a far higher chance that user data will be altered by hackers or that personal data will be misused. Confidentiality and consistency are violated by the previously mentioned behavior. Given the possibility of many issues, data security in cloud computing is a major worry. One well-known method for ensuring information security is cryptography. The information will be made illegible in order to safeguard it. Cryptographic algorithms fall into two main categories. Key algorithms fall into two main categories: symmetric and asymmetric. The public key and the private key are the two keys used in asymmetric key cryptography methods. Symmetric key techniques, on the other hand, employ a single key—referred to as the private key—for both data encryption and decryption [30]. In this case, the user's data is encrypted with the public key and decrypted with the private key. Because asymmetric key cryptography uses two different keys, it is thought to provide more security than symmetric key encryption. Even in the event that one of the keys is compromised, the encryption guarantees the confidentiality and integrity of the data. [31-34] Presented an innovative hybrid data security methodology that combines the cryptographic methods SHA256 (Secure Hash Algorithm 256-bit), ECDSA (Elliptic Curve Digital Signature Algorithm), and AES (Advanced Encryption Standard) in order to improve the security of data stored in the cloud. Several techniques are used in cloud computing to guarantee safe data or information transfer and reception, have put forth a brand-new hybrid cryptography system that improves security by utilizing the RSA (Rivest, Shamir, Adleman), Blowfish, and SHA-2 (Secure Hash Algorithm 2-bit) algorithms [35-37]. Combining symmetric and asymmetric algorithms increases the efficacy of the suggested system. Furthermore, the data integrity and secrecy are guaranteed during transfer via the SHA-2 algorithm. A new method for improving information security by combining RSA and ECC (Elliptic curve cryptography) into a unique identity-based hybrid encryption system is presented [38]. The sender encrypts the data using the identity-based hybrid encryption technique. Strong security for user data in cloud contexts is achieved hybrid two-tier agent-based system [39-41], which combines symmetric and asymmetric key methods. The user has suggested a brand-new parallel cryptography method that reduces the drawbacks of hash function algorithms and symmetric block cryptography, hence improving security. This approach makes use of the Blowfish and MD5 (Message-Digest algorithm 5) encryption techniques [42]. Table 1 shows the survey table.

Table 1 Survey Table

Method	**Key Issue Targeted**	**Advantages**	**Disadvantages**	**Research Gap**
Hypergraph-binary fruit fly optimization	Identification of trustworthy CSPs	Considers hypergraph complexities	Relies heavily on optimization algorithms	Need for simpler, more scalable solutions
Cloud model theory and AHP	Trust, cost, time in cloud service selection	Comprehensive assessment	Complexity in application	Simplification and faster assessment methods needed

Compliance monitoring mechanism	Trustworthiness of CSPs	Direct monitoring of compliance	QoS data often incomplete or unreliable	Improved data acquisition and reliability
Big data processing with MapReduce	Evaluating trustworthiness of cloud services	Efficient processing of large data sets	May overlook non-quantifiable trust factors	Integration of qualitative assessments
Integrated trust evaluation	Cloud service selection	Combines objective and subjective assessments	May exclude trustworthy feedback inadvertently	More accurate user feedback analysis needed
QoS predictions and customer satisfaction	Cloud service trust evaluations	Improves accuracy of QoS predictions	Does not consider time factor and unfair ratings	Time-aware and fairness-adjusted models required
Service QoSs and feedback ratings	Quality measurement of cloud services	Leverages multiple data sources	Neglects dynamic features of QoS	Dynamic, real-time assessment models
Two-layer classifier fusion strategy	Network intrusion detection	High accuracy in classification	Specific to certain datasets	Generalization to other contexts and datasets
CNN with multiple hidden layers	Traffic data classification	Good performance in varied datasets	Complexity and computational demands	Optimization and simplification of neural architectures
Deep transfer learning (DTL)	Reuse of knowledge for intrusion detection	High performance in intrusion detection	Dependency on pre-trained models	Development of standalone robust models
Transfer learning models	Intrusion detection efficiency	Efficient in both labeled and unlabeled data	Requires extensive pre-training of models	More autonomous learning systems

Vulnerabilities or flaws in the security protocols of cloud computing systems are referred to as cloud security vulnerabilities. Attackers may be able to use the system's weaknesses to obtain unauthorized access to private information or interfere with the regular operation of cloud services. Cloud services like Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are often used by businesses. To suit their unique requirements, businesses may also choose public, private, or hybrid cloud solutions.

The services and models discussed above show a number of cloud security flaws [43-44]. Every service model has its own unique set of limitations. It is the service provider's duty to protect the privacy of their customers and guarantee the security of the services they offer. They tackle the idea of security from this specific perspective. An additional component that guarantees the security of the solution being used by consumers is the perspective of the consumer. Figure 4 shows the cloud security issues.

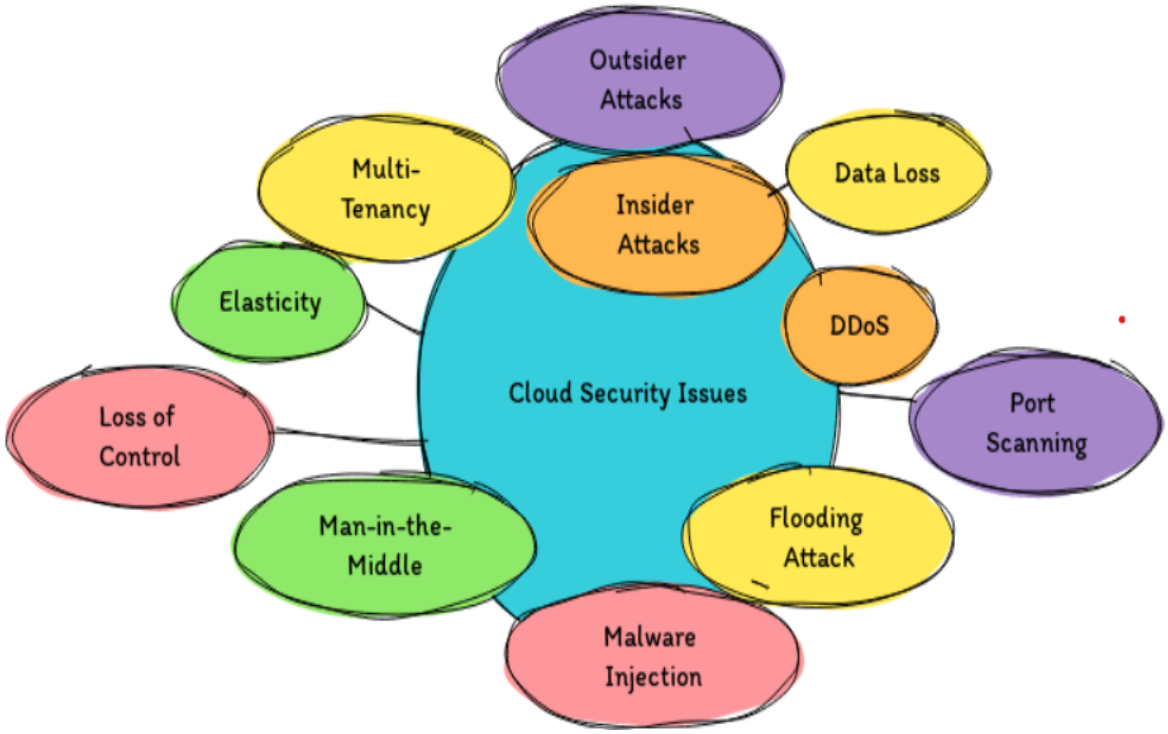

Figure 3 cloud security issues

- **Multi-tenancy** The shared computing, memory, storage, and resource sharing features of the cloud paradigm are particularly built for this [44]. Lower expenses are attained via efficient use of the resources that multi-tenancy offers. In cloud computing, several tenants who are situated at the provider's facility on the same physical or logical platform share processing power, storage, and application services. Data breaches, information leaks, compromised encryption, and heightened attack susceptibility are among the repercussions.

- **Elasticity** Resource elasticity is a term used to describe the ability of a system to automatically allocate and provide resources in response to changes in workload. It measures the extent to which a system can adapt to workload variations. The purpose of this system is to ensure that the available resources are closely aligned with the demand at any given time. The concept of elasticity is intricately linked to scalability. As stated, customers are provided with the flexibility to modify their scale according to their requirements. The scalability feature allows tenants to efficiently utilize resources that were previously allocated to another tenant. The situation presents a potential risk of compromising confidentiality.

- **Insider attacks** The cloud model is organized around several tenants and is located inside the provider's single management domain. There is an internal threat to the company. There are no hiring policies or suppliers for cloud workers [45]. As a result, it is not too difficult for a third-party vendor to obtain unauthorized access to an organization's data and use it for malicious purposes or to transmit it to another party illegally.
- **Outsider attacks** The Corporation is quite concerned about the public leaking of confidential corporate information. When it comes to interface count, cloud networks usually have more than private networks. Hackers and other attackers may be able to destroy connections by taking advantage of the API's (application programming interface) vulnerability [46-47]. When opposed to insider attacks, which may occasionally be discovered, the threat level from these attacks is lower.
- **Loss of control** Through the use of location transparency, cloud computing enables enterprises to have a limited understanding of the actual place in which their data and services are kept. The provider is able to provide cloud-based services from any location. There is a possibility that the organization will lose data in this specific case. Furthermore, it's possible that the business is unaware of the security protocols put in place by the service provider.
- **Data Loss** Since there are several tenants in a cloud environment, it is impossible to guarantee data integrity and security. Data loss may cause a business to incur financial losses as well as a drop in clientele. To update or erase data without first creating a backup copy is an excellent illustration of this.
- **Man in middle attack**: - The attacker establishes a unique connection and speaks with the cloud user over its secret network, which is entirely under their control.
- **Distributed denial of service attacks**: - A Distributed Denial of Service (DDoS) attack occurs when a large volume of network traffic overwhelms servers and networks, prohibiting users from accessing a specific Internet-based service.
- **Port scanning**: - A port is a predefined location used for the exchange of information. The port scanning process is initiated after the subscriber has successfully configured the group. During the configuration of the internet, an automated procedure known as port scanning is performed. It is crucial to recognize that participating in this activity carries the possibility of increasing security concerns [48].
- **Malware Injection**. A notable problem in cloud computing is the substantial volume of data that must be sent back and forth between the user and the cloud provider. Implementing user identification and permission systems is therefore required [49]. Malevolent code can be included to jeopardize data transit between the cloud provider and the user. The original user might thus have to wait until the job that was illegally added is finished.
- **Flooding Attack,** the issue with the cloud lies in the quantity of servers that engage in data sharing and communication. The authentication of the requested jobs occurs after the processing of the requests, resulting in significant utilization of CPU (Central Processing Unit) and memory resources. The servers in question may become overloaded over time, resulting in increased strain on other servers [50]. The system experiences an overload due to the aforementioned factors, resulting in a disruption of its normal operation.

3 CONCLUSION

In conclusion, cloud computing's transformative potential is closely tied to its ability to provide scalable, flexible, and cost-effective solutions across industries. However, these benefits also bring about significant security challenges that require comprehensive strategies to mitigate risks effectively. This survey has presented a detailed classification of prevalent attack vectors and analyzed their implications across various cloud deployment models. By evaluating existing security frameworks, countermeasures, and best practices, we have highlighted their efficacy and identified critical gaps requiring further research. Moving forward, it is essential for stakeholders to adopt a proactive, collaborative approach that integrates robust technical measures, regulatory compliance, and organizational policies to build resilient cloud security architectures. Only through these combined efforts can we ensure that cloud computing continues to be a secure and trusted platform for organizations in the digital age.

ACKNOWLEDGEMENT:

I would like to express our sincere gratitude to all those who have supported and contributed to this research project. Primarily, I extend our heartfelt thanks to our guide for his unwavering guidance, invaluable insights, and encouragement throughout the research process. No funding is raised for this research.

REFERENCES

[1] U. O. Matthew, J. S. Kazaure, A. Onyebuchi, O. O. Daniel, I. H. Muhammed and N. U. Okafor, "Artificial Intelligence Autonomous Unmanned Aerial Vehicle (UAV) System for Remote Sensing in Security Surveillance," 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), Abuja, Nigeria, 2021, pp. 1-10, doi: 10.1109/CYBERNIGERIA51635.2021.9428862.

[2] J. Meyer and S. Boll, "Smart health systems for personal health action plans," 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom), Natal, Brazil, 2014, pp. 404-410, doi: 10.1109/HealthCom.2014.7001877.

[3] Sha Yang. 2022. Application of Cloud Computing Technology in Smart Home Modeling Design. In 2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM2021). Association for Computing Machinery, New York, NY, USA, 989–992. https://doi.org/10.1145/3495018.3495318.

[4] Y. Yuan, H. He, H. Amirpour, L. Qu, C. Timmerer and F. Chen, "IoT Privacy Protection: JPEG-TPE With Lower File Size Expansion and Lossless Decryption," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2024.3385268.

[5] N. Yang, C. Tang, Z. Xiong and D. He, "RCME: A Reputation Incentive Committee Consensus-Based for Matchmaking Encryption in IoT Healthcare," in IEEE Transactions on Services Computing, doi: 10.1109/TSC.2024.3387691.

[6] J. Hu, Y. Zhao, B. H. M. Tan, K. M. M. Aung and H. Wang, "Enabling Threshold Functionality for Private Set Intersection Protocols in Cloud Computing," in IEEE Transactions on Information Forensics and Security, doi: 10.1109/TIFS.2024.3402355.

[7] L. Xu, X. Cheng, W. Tian, H. Wang and Y. Zhang, "Cloud-assisted Privacy-Preserving Spectral Clustering Algorithm within a Multi-User Setting," in IEEE Access, doi: 10.1109/ACCESS.2024.3404265.

[8] R. Elhabob et al., "Equality Test Public Key Encryption With Cryptographic Reverse Firewalls for Cloud-Based E-Commerce," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2024.3405496.

[9] S. Das and S. Namasudra, ‘‘Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure,’’ IEEE Trans. Ind. Informat., vol. 19, no. 1, pp. 821–829, Jan. 2023.

[10] Y. Wan, X. Lin, K. Xu, F. Wang, and G. Xue, ‘‘Extracting spatial information of IoT device events for smart home safety monitoring,’’ in Proc. IEEE INFOCOM Conf. Comput. Commun., May 2023, pp. 1–10.

[11] Y. Miao, F. Li, X. Li, J. Ning, H. Li, K. R. Choo, and R. H. Deng, ‘‘Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system,’’ IEEE Trans. Dependable Secure Comput., early access, Jul. 4, 2023, doi: 10.1109/TDSC.2023.3292129.

[12] D. Ghopur, J. Ma, X. Ma, Y. Miao, J. Hao, and T. Jiang, ‘‘Puncturable ciphertext-policy attribute-based encryption scheme for efficient and flexible user revocation,’’ Sci. China Inf. Sci., vol. 66, no. 7, Jul. 2023, Art. no. 172104.

[13] X. Feng, J. Ma, S. Liu, Y. Miao, X. Liu, and K. R. Choo, ‘‘Transparent ciphertext retrieval system supporting integration of encrypted heteroge- neous database in cloud-assisted IoT,’’ IEEE Internet Things J., vol. 9, no. 5, pp. 3784–3798, Mar. 2022.

[14] T. Liu, Y. Miao, K. R. Choo, H. Li, X. Liu, X. Meng, and R. H. Deng, ‘‘Time-controlled hierarchical multikeyword search over encrypted data in cloud-assisted IoT,’’ IEEE Internet Things J., vol. 9, no. 13, pp. 11017–11029, Jul. 2022.

[15] D. X. Song, D. Wagner, and A. Perrig, ‘‘Practical techniques for searches on encrypted data,’’ in Proc. IEEE Symp. Secur. Privacy., May 2000, pp. 44–55.

[16] F. Li, J. Ma, Y. Miao, X. Liu, J. Ning, and R. H. Deng, ‘‘A survey on searchable symmetric encryption,’’ ACM Comput. Surv., vol. 56, no. 5, pp. 1–42, May 2024.

[17] Z. Li, J. Ma, Y. Miao, X. Liu, and K.-K.-R. Choo, ‘‘Forward and backward secure keyword search with flexible keyword shielding,’’ Inf. Sci., vol. 576, pp. 507–521, Oct. 2021.

[18] Y. Miao, R. H. Deng, K. R. Choo, X. Liu, J. Ning, and H. Li, ‘‘Optimized verifiable fine-grained keyword search in dynamic multi-owner settings,’’ IEEE Trans. Dependable Secure Comput., vol. 18, no. 4, pp. 1804–1820, Jul. 2021.

[19] Q. Huang, G. Yan, and Q. Wei, ‘‘Attribute-based expressive and ranked keyword search over encrypted documents in cloud computing,’’ IEEE Trans. Services Comput., vol. 16, no. 2, pp. 957–968, Mar. 2023.

[20] Y. Miao, F. Li, X. Li, Z. Liu, J. Ning, H. Li, K. R. Choo, and R. H. Deng, ‘‘Time-controllable keyword search scheme with efficient revocation in mobile e-health cloud,’’ IEEE Trans. Mobile Comput, vol. 23, no. 1, pp. 1–15, May 2023.

[21] Y. Miao, Q. Tong, K. R. Choo, X. Liu, R. H. Deng, and H. Li, ‘‘Secure online/offline data sharing framework for cloud-assisted industrial Internet of Things,’’ IEEE Internet Things J., vol. 6, no. 5, pp. 8681–8691, Oct. 2019.

[22] M. D. Green and I. Miers, ‘‘Forward secure asynchronous messaging from puncturable encryption,’’ in Proc. IEEE Symp. Secur. Privacy, May 2015, pp. 305–320.

[23] T. V. Xuan Phuong, R. Ning, C. Xin, and H. Wu, ‘‘Puncturable attribute- based encryption for secure data delivery in Internet of Things,’’ in Proc. IEEE INFOCOM Conf. Comput. Commun., Apr. 2018, pp. 1511–1519.

[24] S.-F. Sun, X. Yuan, J. K. Liu, R. Steinfeld, A. Sakzad, V. Vo, and S. Nepal, ‘‘Practical backward-secure searchable encryption from symmetric puncturable encryption,’’ in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2018, pp. 763–780.

[25] B. Waters, ‘‘Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,’’ in Proc. Int. Workshop Public Key Cryptogr. Taormina, Italy: Springer, 2011, pp. 53–70.

[26] Sahai and B. Waters, ‘‘Fuzzy identity-based encryption,’’ in Proc. Adv. Cryptol. (EUROCRYPT), Aarhus, Denmark. Alexandria, VA, USA: Springer, 2005, pp. 457–473.

[27] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ‘‘Attribute-based encryption for fine-grained access control of encrypted data,’’ in Proc. 13th ACM Conf. Comput. Commun. Secur., Alexandria, VA, USA, Oct. 2006, pp. 89–98.

[28] U. C. Yadav and S. T. Ali, ‘‘Ciphertext policy-hiding attribute-based encryption,’’ in Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI), Kochi, India, Aug. 2015, pp. 2067–2071.

[29] S. Hohenberger and B. Waters, ‘‘Online/offline attribute-based encryp- tion,’’ in Public-Key Cryptography—PKC, Buenos Aires, Argentina. Springer, 2014, pp. 293–310.

[30] S. Chen, J. Li, Y. Zhang, and J. Han, ‘‘Efficient revocable attribute-based encryption with verifiable data integrity,’’ IEEE Internet Things J., vol. 11, no. 6, pp. 10441–10451, Mar. 2024.

[31] C. K. Chaudhary, R. Sarma, and F. A. Barbhuiya, ‘‘RMA-CPABE : A multi-authority CPABE scheme with reduced ciphertext size for IoT devices,’’ Future Gener. Comput. Syst., vol. 138, pp. 226–242, Jan. 2023.

[32] J. Li, Y. Zhang, J. Ning, X. Huang, G. S. Poh, and D. Wang, ‘‘Attribute based encryption with privacy protection and accountability for CloudIoT,’’ IEEE Trans. Cloud Comput., vol. 10, no. 2, pp. 762–773, Apr. 2022.

[33] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, ‘‘Public key encryption with keyword search,’’ in Proc. Adv. Cryptol. (EUROCRYPT), Interlaken, Switzerland. Springer, 2004, pp. 506–522.

[34] A. Wu, Y. Zhang, J. Zhu, Q. Zhao and Y. Zhang, "Hierarchal Bilateral Access Control With Constant Size Ciphertexts for Mobile Cloud Computing," in IEEE Transactions on Cloud Computing, doi: 10.1109/TCC.2024.3386126.

[35] Premakumari Pujar, Ashutosh Kumar, Vineet Kumar, “Efficient plant leaf detection through machine learning approach based on corn leaf image classification” IAES International Journal of Artificial Intelligence (IJ-AI), Vol. 13, No. 1, March 2024, pp. 1139~1148, ISSN: 2252-8938, DOI: 10.11591/ijai.v13.i1.pp1139-1148.

[36] Sreedhara, S.H., Kumar, V., Salma, S. (2023). Efficient Big Data Clustering Using Adhoc Fuzzy C Means and Auto-Encoder CNN. In: Smys, S., Kamel, K.A., Palanisamy, R. (eds) Inventive Computation and Information Technologies. Lecture Notes in Networks and Systems, vol 563. Springer, Singapore. https://doi.org/10.1007/978-981-19-7402-1_25.

[37] Y. Cai, H. Yao, Y. Gong, F. Wang, N. Zhang and M. Guizani, "Privacy-Driven Security-Aware Task Scheduling Mechanism for Space-Air-Ground Integrated Networks," in IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2024.3392389.

[38] L. Yushi, J. Fei and Y. Hui, "Study on application modes of military Internet of Things (MIOT)," 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, 2012, pp. 630-634, doi: 10.1109/CSAE.2012.6273031.

[39] Y. Zixuan, W. Zhifang and L. Chang, "Research on marine environmental monitoring system based on the Internet of Things technology," 2016 IEEE International Conference on Electronic Information and Communication Technology (ICEICT), Harbin, China, 2016, pp. 121-125, doi: 10.1109/ICEICT.2016.7879665.

[40] M. Masoumi, H. R. D. Oskouei, M. M. Shirkolaei, and A. R. Mirtaheri, ‘‘Substrate integrated waveguide leaky wave antenna with circular polarization and improvement of the scan angle,’’ Microw. Opt. Technol. Lett., vol. 64, no. 1, pp. 137–141, Jan. 2022, https://doi.org/10.1002/mop.33047.

[41] Mohammadi Shirkolaei, M., & Ghalibafan, J. (2021). Magnetically scannable slotted waveguide antenna based on the ferrite with gain enhancement. Waves in Random and Complex Media, 1–11. https://doi.org/10.1080/17455030.2021.1983234.

[42] U. O. Matthew, J. S. Kazaure, A. Onyebuchi, O. O. Daniel, I. H. Muhammed and N. U. Okafor, "Artificial Intelligence Autonomous Unmanned Aerial Vehicle (UAV) System for Remote Sensing in Security Surveillance," 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), Abuja, Nigeria, 2021, pp. 1-10, doi: 10.1109/CYBERNIGERIA51635.2021.9428862.

[43] J. Meyer and S. Boll, "Smart health systems for personal health action plans," 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom), Natal, Brazil, 2014, pp. 404-410, doi: 10.1109/HealthCom.2014.7001877.

[44] Sha Yang. 2022. Application of Cloud Computing Technology in Smart Home Modeling Design. In 2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM2021). Association for Computing Machinery, New York, NY, USA, 989–992. https://doi.org/10.1145/3495018.3495318.

[45] S. K. Lee, M. Bae, and H. Kim, ‘‘Future of IoT networks: A survey,’’ Appl. Sci., vol. 7, no. 10, p. 1072, 2017, https://doi.org/10.3390/app7101072.

[46] W. Li et al., ‘‘System modelling and performance evaluation of a three-tier Cloud of Things,’’ Future Gener. Comput. Syst., vol. 70, pp. 104–125, May 2017, DOI:10.1016/j.future.2016.06.019.

[47] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, ‘‘Secure integration of IoT and Cloud Computing,’’ Future Gener. Comput. Syst., vol. 78, pp. 964–975, Jan. 2018, doi.org/10.1016/j.future.2016.11.031.

[48] N. Zhang et al., "Software Defined Networking Enabled Wireless Network Virtualization: Challenges and Solutions," in IEEE Network, vol. 31, no. 5, pp. 42-49, 2017, doi: 10.1109/MNET.2017.1600248.

[49] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark and X. Shen, "Partner selection and incentive mechanism for physical layer security," in IEEE Transactions on Wireless Communications, vol. 14, no. 8, pp. 4265-4276, Aug. 2015, doi: 10.1109/TWC.2015.2418316.

[50] J. Ni, K. Zhang, X. Lin and X. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," in IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 601-628, Firstquarter 2018, doi: 10.1109/COMST.2017.2762345.