ISSN: 2581-3404 (Online) IF: 5.68 (SJIF)
IJIRTM, Volume-8, Issue-1, January-2024.

A Review on Cloud Computing, Security Issues and Techniques

Dinesh Kumar Malviya[1], Pooja Meena[2], Chetan Agrawal[3]
Dept. of CSE, Radharaman Institute of Technology & Science, Bhopal, India[1, 2, 3]
dineshrgibpl@gmail.com[1], meena.pooja1@gmail.com[2], chetan.agrawal12@gmail.com[3]

Abstract: *Cloud computing is a network-built invention that allows users to access information whenever they need it. Existing cloud computing systems have stringent safeguards in place to preserve user data confidentiality. Cloud computing is made up of a number of technologies and regulations to protect infrastructure, services, and data. Since the infrastructure is not owned by the customer, the conventional security architecture is quite difficult to implement. The paper presented the review associated with cloud computing as well as strategies for users to mitigate these risks and problems. The paper also covers the current challenges for cloud computing to protect their infrastructure from threats and hackers.*

Keywords:- Cloud Computing, Security Issues, Techniques Used, Encryption.

Introduction

Cloud computing represents a shift in how computing resources are utilized and managed, involving a network of systems, either in private or public networks, to offer scalable infrastructure for applications, data, and file storage. This model allows for significant cost savings and transforms data centers from capital-intensive setups to variable-priced environments. It is characterized by on-demand service usage, shared resource consumption, scalability, and payment for only what is used, accessed over a network. This shift in IT service delivery offers businesses and IT numerous benefits, such as reduced costs, enhanced scalability, flexibility, improved capacity utilization, higher efficiencies, and mobility [1]. However, the security and reliability of cloud computing services, often promoted by providers, have been questioned due to various incidents. As mobile device usage grows, securing expanding network boundaries becomes a challenge, shifting the security focus from data centers to protecting ad hoc endpoints [2].

II. Cloud Computing Security

Cloud Computing (CC) technology has become widely popular for offering extensive resources accessible over the internet, facilitating global access anytime. This has led many IT companies to transition their operations to the cloud, benefiting from a rich set of features like access to shared resources at lower costs. These resources can be quickly allocated and released with minimal management effort. CC enables the sharing, management, and storage of data on remote servers, avoiding reliance on internal resources or personal devices.

Users can access various cloud services and programs without needing to purchase or install software on their computers. CC employs various technologies like web services, virtualization, applications, and operating systems to provide virtualized resources. The primary advantages of CC include cost reduction, increased productivity, stability, scalability, easy management, and high availability.

III. Importance of security in cloud environments

Cl Cloud computing provides companies with advanced capabilities, including enhanced customer service through improved data collection and storage, increased flexibility through remote working and rapid scalability, and greater convenience via interconnected systems that enable fast file and data sharing.
However, the potential risks of misconfiguration and the constant threat from cybercriminals necessitate robust security measures in any cloud environment. Cloud security is crucial in this context. It helps to significantly bolster the protection of digital assets and minimize the risks associated with human error. Implementing effective cloud security measures can greatly reduce the chances of an organization suffering from a significant loss due to a preventable breach.

IV. Techniques to provide Cloud Security

Symmetric Encryption: Symmetric encryption is a method where a single key is used for both encrypting and decrypting data. This approach is also known as "secret key" encryption. The key must be kept confidential and is often shared through secure, out-of-band methods like face-to-face discussions. The strength of symmetric encryption lies in its speed and cryptographic robustness per bit of key.
Asymmetric Encryption: Asymmetric key encryption, also known as public key encryption, involves the use of key pairs—public and private keys—for cryptography. The public key is distributed openly, while the private key is kept confidential and used for decryption. This method is widely used to secure communication over the internet. The RSA algorithm is a common choice for asymmetric key encryption, offering secure transactions online. Asymmetric encryption is generally slower than symmetric encryption due to the more complex computations involved.
Hash Functions: A hash function is a mathematical algorithm that converts digital data of any length into a fixed-length output, commonly known as a hash, hash value, or message digest. This process, called hashing, is irreversible, meaning the original data cannot be easily retrieved from the hash. Formally, a hash function is expressed as H: D → R, where D represents the domain of all possible input values (binary strings of any length) and R represents the range of fixed-length output values. The function maps any input value m to a condensed numerical output h of a predetermined length. In the field of cryptography, a hash function that meets certain criteria is called a cryptographic hash function.
Digital Signatures: Digital signatures are a crucial component of digital security, created based on the content of the document to be signed and private information exclusive to the sender. In practice, rather than using the entire message, a hash function is applied to produce a fixed-size message digest. This ensures efficiency and security, as hash functions like MD-5 (Message Digest 5) and SHA (Secure Hash Algorithm) are designed to make it extremely unlikely for two different messages to yield the same hash value.
Attribute-Based Encryption: Attribute-Based Encryption (ABE) plays a pivotal role in enhancing data security in cloud computing environments by providing a flexible and fine-grained access control mechanism. ABE is a cryptographic technique that allows data owners to define access policies based on

attributes rather than traditional user roles. The use of attributes, such as user characteristics or system properties, enables more dynamic and context-aware access control, addressing some of the limitations of traditional access control models. One of the key advantages of ABE is its ability to enforce access policies based on various attributes, allowing for highly granular control over who can access specific data. This is particularly valuable in cloud environments where data is often shared among multiple users or across organizations with diverse access requirements. ABE empowers data owners to define access policies that consider attributes like user roles, organizational affiliations, or any other relevant characteristics. Moreover, ABE contributes significantly to data confidentiality. Through the use of encryption, ABE ensures that only authorized users, based on the defined attribute policies, can decrypt and access sensitive information. This aligns with the principle of the least privilege, minimizing the risk of unauthorized data exposure. ABE also facilitates secure data sharing and collaboration in the cloud. As organizations increasingly engage in joint projects or share data across departments, ABE allows for seamless and secure collaboration. Authorized users can access the data based on their attributes, fostering collaboration without compromising security. In addition to these advantages, ABE helps address the challenges associated with the dynamic nature of cloud environments. Users' attributes can be updated or modified over time, allowing access policies to adapt to changes in organizational structures or user roles without requiring a complete overhaul of the access control system. While ABE offers notable benefits, its implementation requires careful consideration of factors such as key management, scalability, and performance. Nevertheless, as cloud computing continues to evolve, the role of ABE becomes increasingly critical in providing a robust and flexible security framework that aligns with the dynamic and collaborative nature of modern cloud environments. Researchers and practitioners alike are exploring and refining ABE techniques to further strengthen its applicability and effectiveness in addressing the evolving challenges of cloud data security.

V. Literature Review

Sandoval et al. [1] focused on the security of cloud storage where users encrypt their data before outsourcing it. The key feature is allowing shared data access and enabling the service provider to search and retrieve encrypted data. The approach is proven viable through experiments using Barreto-Naehrig curves. Liu et al. [2] developed a novel method for keyword search on encrypted data, which also supports data deduplication, focusing on fine-grained authorization, keyword indistinguishability, signature unforgeability, and maintaining ciphertext confidentiality. Their method proves efficient in terms of bandwidth, storage, and computation. Khashan et al. [3] introduced OutFS, a user-side encrypted file system that provides transparent encryption for data storage and sharing. OutFS demonstrates high efficiency and throughput, offering robust security against attacks like brute-force, eavesdropping, and man-in-the-middle.

Ameri et al. [4] presented a cryptographic method known as key-policy attribute-based temporary keyword search (KP-ABTKS), which maintains keyword secrecy and guards against selectively chosen keyword attacks. This scheme, validated under the Decisional Bilinear Diffie-Hellman assumption, offers a practical solution with encryption complexity linearly related to the number of attributes involved.

Ali et al. [5] proposed a lightweight revocable hierarchical Attribute-Based Encryption (LW-RHABE) scheme. This scheme is efficient in computational overhead, with most operations performed by the cloud server. It features flexible and scalable key delegation and user revocation mechanisms, with these functions managed by multiple key authorities. The scheme's security is established in the standard model and based

on the hardness of the Decisional Bilinear Diffie-Hellman (DBDH) problem. Miao et al. [6] proposed two improved schemes (ABKS-HD-I and ABKS-HD-II) to support multi-keyword search and user revocation. These schemes differ from existing attribute-based keyword search (ABKS) schemes as their computation overhead scales with the number of user attributes rather than system attributes. They are secure against both chosen-plaintext attacks (CPA) and chosen-keyword attacks (CKA) in the random oracle model. Empirical studies with real-world datasets demonstrate feasibility and efficiency in practical applications. Zhang et al. [7] proposed an attribute-based ranked searchable encryption scheme with revocation capabilities. This scheme ranks ciphertext documents using the TF×IDF principle and returns only the top-k relevant files. It introduces separate encryption and decryption servers, outsourcing many computations to these servers to reduce the client's computational overhead. The scheme also features real-time attribute revocation and offloads most update tasks to the cloud, further reducing user-side computation. Performance evaluations indicate that this scheme is feasible and more efficient than existing ones.

Zhang et al. [8] aimed to improve leakage rates in prime order group encryption schemes. They use an extension of lattice-based trapdoors to achieve a maximum leakage rate of $1-o(1)$, and ensure anonymity to protect receiver privacy. The scheme is reducible to the standard Decision Linear (DLIN) assumption in the selective security model and is resistant to Chosen Plaintext Attacks (CPA security). Zhang et al. [9] addresses key abuse and key escrow issues in attribute-based encryption (ABE) within cloud computing. Their scheme, based on prime order bilinear groups, is shown to be selectively secure in the standard model.

Yu et al. [10] proposed a new construction of searchable encryption with fine-grained access control, utilizing key-policy attribute-based cryptography. This method supports logical operators like AND, OR, and threshold gates for generating trapdoors. The data owner encrypts index keywords according to a specified access policy. Comprehensive security analysis and implementation results demonstrate that the scheme is provably secure and practical for real-world applications. Liao et al. [11] proposed a secure approach to reduce the overall overhead of the cloud server in scenarios where multiple users require outsourced decryption for the same ciphertext. This approach decreases the decryption computation cost for users and ensures that the cloud server's overhead is independent of the number of users requesting the service. The paper also extends this approach to a RCCA-secure ABE-OD scheme. Wang et al. [12] introduced an anonymous distributed fine-grained access control protocol with verifiable outsourced decryption in public clouds (VOD-ADAC). This novel concept uses pseudonym techniques to achieve high user anonymity, allowing users to frequently change independent pseudonyms in social spots. Security and performance analyses confirm that the VOD-ADAC protocol is secure and efficient.

Zhang et al. [13] proposed a privacy-preserving Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme that features efficient authority verification with constant size secret keys, achieving selective security under specific cryptographic assumptions. This scheme shows computational benefits.

Ahuja et al. [14] introduced a scalable attribute-based access control scheme for cloud storage, extending CP-ABE for flexible access privilege delegation and shared access. It employs a hierarchical user structure to enhance scalability and fine-grained control. Zaghloul et al. [15] developed the Privilege-based Multilevel Organizational Data-sharing scheme (P-MOD), aimed at simplifying hierarchy management in growing user bases, particularly for healthcare record management on mobile devices. It demonstrates greater efficiency in computational complexity and storage space. Wang et al. [16] proposed a fast CP-ABE scheme optimized for mobile devices with limited resources. This scheme includes a mechanism for

verifying decryption correctness and focuses on securing healthcare data while reducing local computational load, showing promising results in efficiency. De et al. [17] introduced a decentralized attribute-based encryption (ABE) scheme featuring fast encryption, outsourced decryption, and user revocation. Compared to other ABE schemes, this approach significantly reduces computation times for both data owners and users, making it highly suitable for mobile devices.

Miao et al. [18] presented a secure Multi-authority CP-ABKS (MABKS) system to reduce the computational and storage burden on resource-limited devices in cloud systems. The system is extended to support malicious attribute authority tracing and attribute updates. Experimental results using real-world datasets demonstrate the efficiency and practicality of the MABKS system. Huang et al. [19] proposed a secure data group sharing and conditional dissemination scheme with multi-owner capabilities in cloud computing. It allows data owners to securely share private data with a group via the cloud and enables data disseminators to distribute data to new groups if attributes satisfy access policies. Security analysis and experimental results affirm the scheme's practicality and efficiency. Zhongxiang et al. [20] introduce a new encryption scheme called MA-RUABE, which stands for revocable and traceable undeniable ciphertext policy attribute-based encryption. This scheme is notable for its quick and precise data traceability, which helps prevent the leakage of user keys by malicious actors. It also features a direct revocation mechanism that greatly improves computational efficiency. Additionally, the scheme addresses the problem of centralized power in single-attribute permission systems by incorporating a multi-permission mechanism. A security analysis of the system confirms its robustness, particularly its resilience against chosen plaintext attacks.

Table 1: Research Contribution for Cloud Security

Ref	Technique Used	Key Findings
[1]	Encryption with curves	Viable shared data access and retrieval in encrypted cloud storage
[2]	Encrypted data keyword search with deduplication	Efficient in storage, computation; supports fine-grained authorization
[3]	User-side encrypted file system	High throughput, secure against various attacks
[4]	Key-policy attribute-based temporary keyword search	Maintains keyword secrecy, secure against SCKA, practical
[5]	Lightweight revocable hierarchical ABE	Efficient computation, flexible key delegation, secure in standard model
[6]	Attribute based keyword search	Efficient multi-keyword search
[7]	Attribute-based ranked searchable encryption	Feasible, efficient, reduces client computational overhead
[8]	Prime order group encryption with lattice-based	High leakage rate reduction
[9]	ABE scheme in cloud computing using prime order bilinear groups	Addresses key theft issues
[10]	Searchable encryption with fine-grained access control	Supports complex logical operators, provably secure, practical for real-world applications

VI. Current Challenges and Future Scope

The current challenges in cloud computing security focus on enhancing encryption methods for data privacy, efficient searchability of encrypted data, and scalable access control, especially for mobile devices. Key areas include developing user-friendly encrypted file systems, keyword search mechanisms, and attribute-based encryption schemes that balance security with computational efficiency. Future developments are expected to address issues like data leakage, key misuse, and the demand for dynamic, responsive cloud services. The emphasis is on creating advanced cryptographic techniques that ensure robust security while maintaining functionality and user accessibility in a cloud environment.

VII. Conclusion

Cloud computing has emerged as a key platform for data sharing, addressing the rapidly increasing demands for data exchange. To prevent data leaks, encryption by users before sharing is essential. Access control is a critical element in this context, acting as the primary defence against unauthorized data access. In this review paper we described the brief review on cloud computing and its security issues for future to handle.

References

[1] M. Morales-Sandoval, M. H. Cabello, H. M. Marin-Castro, and J. L. G. Compean, “Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud,” IEEE Access, vol. 8, pp. 170101–170116, 2020, doi: 10.1109/ACCESS.2020.3023893.

[2] X. Liu, T. Lu, X. He, X. Yang, and S. Niu, “Verifiable Attribute-Based Keyword Search Over Encrypted Cloud Data Supporting Data Deduplication,” IEEE Access, vol. 8, pp. 52062–52074, 2020, doi: 10.1109/ACCESS.2020.2980627.

[3] O. A. Khashan, “Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System,” IEEE Access, vol. 8, pp. 210855–210867, 2020, doi: 10.1109/ACCESS.2020.3039163.

[4] M. H. Ameri, M. Delavar, J. Mohajeri, and M. Salmasizadeh, “A Key-Policy Attribute-Based Temporary Keyword Search scheme for Secure Cloud Storage,” IEEE Trans. Cloud Comput., vol. 8, no. 3, pp. 660–671, 2020, doi: 10.1109/TCC.2018.2825983.

[5] M. Ali, M.-R. Sadeghi, and X. Liu, “Lightweight Revocable Hierarchical Attribute-Based Encryption for Internet of Things,” IEEE Access, vol. 8, pp. 23951–23964, 2020, doi: 10.1109/ACCESS.2020.2969957.

[6] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, “Attribute-Based Keyword Search over Hierarchical Data in Cloud Computing,” IEEE Trans. Serv. Comput., vol. 13, no. 6, pp. 985–998, 2020, doi: 10.1109/TSC.2017.2757467.

[7] L. Zhang, J. Su, and Y. Mu, “Outsourcing Attributed-Based Ranked Searchable Encryption With Revocation for Cloud Storage,” IEEE Access, vol. 8, pp. 104344–104356, 2020, doi: 10.1109/ACCESS.2020.3000049.

[8] L. Zhang, X. Gao, F. Guo, and G. Hu, “Improving the Leakage Rate of Ciphertext-Policy Attribute-Based Encryption for Cloud Computing,” IEEE Access, vol. 8, pp. 94033–94042, 2020, doi: 10.1109/ACCESS.2020.2995480.

[9] Z. Zhang, P. Zeng, B. Pan, and K.-K. R. Choo, "Large-Universe Attribute-Based Encryption With Public Traceability for Cloud Storage," IEEE Internet Things J., vol. 7, no. 10, pp. 10314–10323, 2020, doi: 10.1109/JIOT.2020.2986303.
[10] Y. Yu, J. Shi, H. Li, Y. Li, X. Du, and M. Guizani, "Key-Policy Attribute-Based Encryption With Keyword Search in Virtualized Environments," IEEE J. Sel. Areas Commun., vol. 38, no. 6, pp. 1242–1251, 2020, doi: 10.1109/JSAC.2020.2986620.
[11] Y. Liao, G. Zhang, and H. Chen, "Cost-Efficient Outsourced Decryption of Attribute-Based Encryption Schemes for Both Users and Cloud Server in Green Cloud Computing," IEEE Access, vol. 8, pp. 20862–20869, 2020, doi: 10.1109/ACCESS.2020.2969223.
[12] H. Wang, D. He, and J. Han, "VOD-ADAC: Anonymous Distributed Fine-Grained Access Control Protocol with Verifiable Outsourced Decryption in Public Cloud," IEEE Trans. Serv. Comput., vol. 13, no. 3, pp. 572–583, 2020, doi: 10.1109/TSC.2017.2687459.
[13] L. Zhang, Y. Cui, and Y. Mu, "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing," IEEE Syst. J., vol. 14, no. 1, pp. 387–397, 2020, doi: 10.1109/JSYST.2019.2911391.
[14] R. Ahuja and S. K. Mohanty, "A Scalable Attribute-Based Access Control Scheme with Flexible Delegation cum Sharing of Access Privileges for Cloud Storage," IEEE Trans. Cloud Comput., vol. 8, no. 1, pp. 32–44, 2020, doi: 10.1109/TCC.2017.2751471.
[15] E. Zaghloul, K. Zhou, and J. Ren, "P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing," IEEE Trans. Big Data, vol. 6, no. 4, pp. 804–815, 2020, doi: 10.1109/TBDATA.2019.2907133.
[16] S. Wang et al., "A Fast CP-ABE System for Cyber-Physical Security and Privacy in Mobile Healthcare Network," IEEE Trans. Ind. Appl., vol. 56, no. 4, pp. 4467–4477, 2020, doi: 10.1109/TIA.2020.2969868.
[17] S. J. De and S. Ruj, "Efficient Decentralized Attribute Based Access Control for Mobile Clouds," IEEE Trans. Cloud Comput., vol. 8, no. 1, pp. 124–137, 2020, doi: 10.1109/TCC.2017.2754255.
[18] Y. Miao, R. H. Deng, X. Liu, K.-K. R. Choo, H. Wu, and H. Li, "Multi-Authority Attribute-Based Keyword Search over Encrypted Cloud Data," IEEE Trans. Dependable Secur. Comput., vol. 18, no. 4, pp. 1667–1680, 2021, doi: 10.1109/TDSC.2019.2935044.
[19] Q. Hang, Y. Yang, W. Yue, and Y. He, "Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing," IEEE Trans. Cloud Comput., vol. 9, no. 4, pp. 1607–1618, 2021, doi: 10.1109/TCC.2019.2908163.
[20] He, Zhongxiang, et al. "Revocable and Traceable Undeniable Attribute-Based Encryption in Cloud-Enabled E-Health Systems." Entropy 26.1 (2024): 45.