Vanshika Jain, 2024, 12:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

A Survey on Cloud Infrastructure, Attacks and Security Techniques

Vanshika Jain, Ms. Monika Raghuwanshi
CSE Department,
Technocrats institute of technology

Abstract- With the emergence of artificial intelligence and Big Data initiatives, the imperative for transitioning from traditional analog methods to contemporary solutions like cloud computing becomes increasingly inevitable. Despite the widespread acknowledgment of this necessity in current discourse. This paper has detailed about the requirement of cloud computing and its different services to solve various issues. Further paper has summarized different research work done for the file transfer and its security related models. Paper has list different attacks of cloud with security algorithm for the data transfer.

Keywords- Cloud Computing, Multi-tenant, Trust Computing, Resource Management.

I. INTRODUCTION

Cloud computing has been widely embraced as a revolutionary computing paradigm due to its inherent features of resource sharing and reduced maintenance requirements. One of the primary services provided by Cloud Service Providers (CSPs) is data storage, facilitating the sharing of data among multiple users with minimal maintenance overhead [1]. However, this shared data ownership model can introduce complexities, particularly regarding ownership issues and data usage rights when data is broadcasted to multiple users. In scenarios with a single owner, the group manager typically holds the authority to manage and modify data, while each user retains the capability to access and read data from the entire data file [2].

The complexity of data sharing, especially in a multi-owner scenario, arises from the need to protect data and maintain identity privacy, particularly in untrusted cloud environments where membership alterations are frequent [3]. Despite the advantages of cloud storage, several issues may arise if not properly addressed, potentially hindering its growth [4]. Moreover, achieving secure cloud data sharing among authenticated users at a granular level, especially within dynamic user groups, poses a significant challenge.

Cloud computing, leveraging its inherent features of data sharing and reduced preservation requirements, offers enhanced resource utilization. CSPs typically offer the concept of unlimited storage in cloud mode, although privacy concerns necessitate techniques such as data encryption before outsourcing encrypted data to clients. Developing safe and effective methods for managing dynamic user groups remains a complex task, yet the cloud's low maintenance and management costs make it an efficient and economical solution for data sharing among group members, despite inherent trust issues [5].

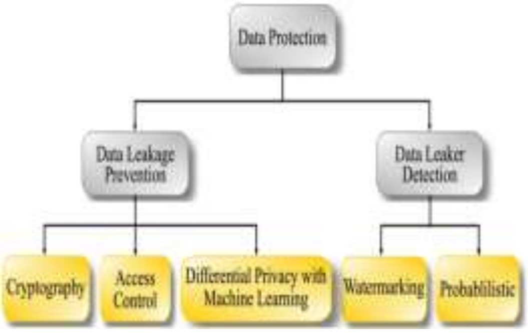

Fig. 1 Data protection schemes in cloud

Fig. 1 illustrates various data protection schemes in the cloud, highlighting the importance of preventing data leakage and detecting malicious entities responsible for breaches. Numerous models for data protection in cloud environments have been explored, focusing on leakage prevention and leaker detection. This article specifically concentrates on achieving efficient protection through these methods, as depicted in Fig. 2.

The paper is organized as follows: Section 2 provides an overview of cloud services, while Section 3 presents a literature review of cloud computing, discussing general concepts, delivery models, and deployment models. Different types of attacks are listed in Section 4, and finally, Section 5 concludes the paper by summarizing contributions and suggesting directions for future research.

II. CLOUD COMPUTING SERVICES

Infrastructure as a service (IaaS) occupies the foundational layer of the cloud computing model, dealing primarily with the provisioning of computer hardware resources such as network storage, virtual servers/machines, data centers, processors, and memory as a service [7]. By offering the elasticity of allocating physical or virtual resources, IaaS facilitates the abstraction of infrastructure, enabling scalability and provisioning without necessitating significant financial or temporal investments. Additionally, IaaS platforms prioritize security measures, including firewall implementation, intrusion detection and prevention systems (IDS/IPS), and virtual machine monitoring.

Platform as a service (PaaS): resides in the middleware of the cloud service model, providing customers with development tools, frameworks, architectures, programs, and Integrated Development Environments (IDEs). Unlike IaaS, PaaS allows customers to control applications without managing the underlying infrastructure directly. This can be advantageous in collaborative scenarios where multiple developers, situated in diverse physical locations, need to collaborate. Notable PaaS providers include Google App Engine, offering a Software Development Kit (SDK) supporting Python, Java, and Go programming languages. Despite its readiness for customer use, PaaS presents security challenges during runtime application execution and customer application deployment, including concerns related to third-party relationships, lifecycle development, and underlying infrastructure security [8].

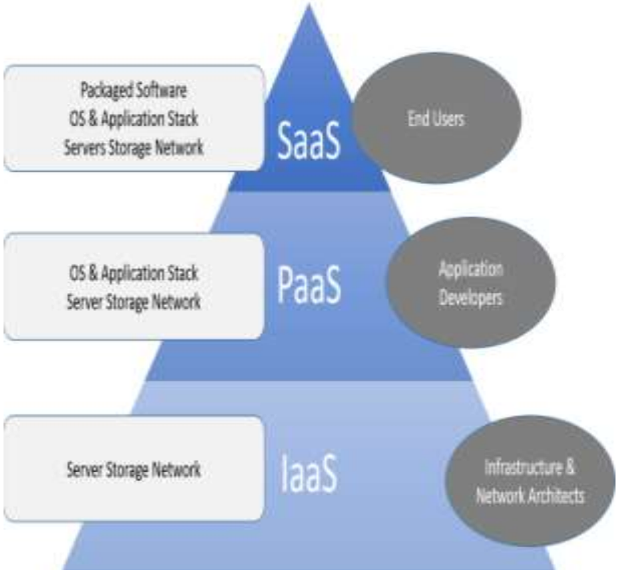

Fig. 2 Cloud computing architecture [6].

Software as a service (SaaS) represents the apex model within cloud computing delivery models, comprising a collection of remote computing services. Positioned at the top layer, SaaS enables the deployment of applications remotely by third-party vendors, granting customers access to cloud service provider (CSP) applications hosted on cloud infrastructure via the internet. SaaS holds a prominent position in the cloud market, experiencing rapid growth. Examples of SaaS providers include Google App and Salesforce. However, from a customer security perspective, vulnerabilities leading to potential breaches are continuously being identified and addressed [9].

Virtualization Virtualization is a transformative process that involves the abstraction and separation of hardware components from the operating system on a physical machine. At the heart of this process lies the notion of a Virtual Machine (VM), which serves as a virtualized representation of a physical computing environment. These VMs are orchestrated and managed on a host system by specialized software known as a virtual machine monitor or hypervisor. The hypervisor plays a pivotal role in facilitating virtualization by serving as an intermediary layer between the VMs and the physical hardware. There are two primary classifications of hypervisors: Type 1 and Type 2. Type 1 hypervisors, also known as bare-metal hypervisors, operate directly on the underlying hardware, managing hardware resources autonomously and overseeing the operation of guest operating systems. Conversely, Type 2 hypervisors, referred to as hosted hypervisors, function as software applications within a conventional operating system environment.

Elastic computing represents a paradigm shift in the provisioning and management of computing resources, offering scalable, on-demand resources delivered as a service over Internet technologies. Elastic compute clouds are characterized by automated management systems that facilitate the dynamic allocation and provisioning of VMs across cloud computing infrastructure.

A notable example of an elastic computing platform is Amazon's Elastic Compute Cloud (EC2), which enables multiple applications and servers from various clients to operate concurrently within its cloud environment. Each client's perspective of the cloud infrastructure is tailored to their specific needs and usage patterns.

One of the most significant advantages of elastic computing lies in its flexible payment and usage model. Unlike traditional IT approaches where organizations must make substantial upfront investments in hardware infrastructure to accommodate peak computing demands, elastic computing operates on a pay-as-you-go basis. Clients are billed based on their actual resource consumption, typically measured in standardized units. This consumption-based pricing model empowers organizations to optimize their IT expenditure by only paying for the resources they utilize, thereby minimizing upfront capital expenditure and maximizing operational efficiency.

III. LITERATURE SURVEY

Francis K. Mupila et al. [9] put forth a comprehensive conceptual framework designed to mitigate an array of authentication threats within cloud computing environments. Their approach revolves around the implementation of an intricate encrypted certificate and token build-up mechanism, strategically utilizing the geographic position of users to bolster security measures. By integrating these innovative strategies, the system aims to fortify defenses against potential data breaches, unauthorized access attempts by non-privileged users, and malicious cyberattacks. While the authors introduce a promising authentication methodology for enhancing cloud security, further empirical investigation is warranted to ascertain its practical feasibility and performance efficacy. Additionally, there exists a conspicuous research gap pertaining to the assessment of the reliability and scalability of the proposed authentication mechanism, particularly within the context of large-scale cloud infrastructures.

Urvashi Rahul Saxena et al. [10] delve into a detailed exposition of the intricate algorithmic modules employed to govern various operational responsibilities within cloud computing ecosystems. They elucidate the integration of membership rights management, user revocation protocols, as well as encryption and decryption procedures. Through the utilization of advanced encryption techniques, data owners are empowered to securely store their data in cloud environments, leveraging role-based access control mechanisms to regulate data access permissions. Furthermore, the project facilitates seamless data sharing among authorized users. The proposed approach amalgamates Identity and Broadcast based Encryption methodologies with a Role-Based Encryption (RBE) scheme, thereby ensuring the integrity and confidentiality of data stored within public cloud repositories.

Mohammad Payam et al. [11] introduce an innovative collaborative framework aimed at enhancing the security of cloud-based file sharing through the synergistic integration of blockchain technology and attribute-based encryption (ABE) protocols. Leveraging the inherent advantages of blockchain, such as decentralized consensus mechanisms and tamper-proof transaction records, the system establishes smart contracts as a means of governing access control between data owners and users. Each data owner autonomously creates a bespoke smart contract, enabling users to request access to specific files via registered transactions. In response, the data owner furnishes the requisite credentials to authorized users, thereby facilitating the decryption of the intended files stored within cloud storage infrastructure. Notably, the proposed scheme is characterized by its decentralized architecture, fault-tolerant operation, and robust resilience against denial-of-service (DoS) attacks. The encryption of file data is achieved through the embedding of cipher-keys within access polynomials, thereby ensuring secure data access and preserving user anonymity through the judicious application of ABE schemes.

O. A. Khashan et al. [12] introduce OutFS, an innovative encrypted file system specifically tailored to cater to the unique security requirements of cloud-based data storage and sharing. Central to the architecture of OutFS is a sophisticated hybrid encryption scheme, which seamlessly integrates symmetric and asymmetric encryption methods to ensure robust data protection. Notably, the key management framework is meticulously designed to facilitate convenient and secure access to encrypted data. To further bolster data security, the system incorporates identity-based encryption (IBE) protocols, thereby enhancing the confidentiality and integrity of shared data within cloud environments.

X. Gao et al. [13] propose a novel scheme aimed at enhancing the integrity and confidentiality of data stored within cloud repositories, particularly in scenarios where Third-Party Auditors (TPAs) are tasked with verifying data integrity without compromising user privacy. Leveraging a newly devised Relation Authentication Label (RAL) mechanism, the proposed scheme enables TPAs to audit the integrity of all encrypted cloud files containing user-specified keywords. Notably, this auditing process is conducted without revealing sensitive information pertaining to the contents or quantity of encrypted files. By capitalizing on the unique attributes of the RAL, the proposed scheme ensures the authentication of file relations while safeguarding data privacy.

IV. ATTACKER TYPES AND RISKS

A multitude of security threats and challenges within cloud computing echo those encountered by organizations managing internal infrastructure or following conventional outsourcing models. The attackers targeting each delivery model in cloud computing can be broadly classified into two groups [14]:

1. Internal Attackers

These individuals are affiliated with the cloud service provider, customer, or other third-party organizations involved in supporting cloud operations.

They may wield authorized access to cloud services, customer data, or supporting infrastructure and applications, depending on their role.

Internal attackers exploit existing privileges to gain further access or collaborate with external parties to launch attacks compromising information confidentiality, integrity, and availability within the cloud service.

2. External Attackers

These assailants lack affiliation with the cloud service provider, customer, or supporting third-party organizations.

They lack authorized access to cloud services, customer data, or supporting infrastructure and applications.

External attackers exploit technical, operational, process, and social engineering vulnerabilities to infiltrate cloud service providers, customers, or third-party organizations, aiming to compromise information confidentiality, integrity, and availability within the cloud.

Cloud security risks vary across different delivery models and are influenced by factors such as the sensitivity of information assets, cloud architectures, and security controls within specific cloud environments. Below, we outline these risks in a general context, unless explicitly referring to a particular cloud delivery model [15]:

Privileged User Access
Cloud providers typically have unrestricted access to user data, necessitating robust controls to mitigate the risk of privileged user access leading to the compromise of customer data.

Data Location and Segregation
Customers may lack visibility into the geographic location of their data, raising concerns about potential commingling with other customers' information.

Data Disposal
The deletion and disposal of cloud data pose inherent risks, particularly in scenarios involving dynamic hardware provisioning.

The risk of residual data persisting in data stores, backups, and physical media during decommissioning is heightened within the cloud environment.

E-Investigations and Protective Monitoring
Cloud customers' ability to conduct electronic investigations within the cloud may be constrained by the chosen delivery model and the complexity of cloud architecture. The deployment of monitoring systems is contingent upon the cloud service provider's infrastructure, limiting customers' control over investigations.

Assuring Cloud Security
Customers face challenges in ensuring the security of systems they do not directly control. Assurance mechanisms, such as Service Level Agreements (SLAs) and the right to audit security controls within contractual agreements, are essential for maintaining trust and accountability in cloud security practices.

V. BLOCK CHAIN TECHNOLOGY

Blockchain technology was unveiled by Satoshi Nakamoto in 2008 [16]. Blockchains function as decentralized digital ledgers, where transactions undergo cryptographic verification and are grouped into blocks. These blocks are securely linked together, facilitating easy detection of any tampering [17]. With each added block, it becomes increasingly challenging to alter previous blocks, ensuring the tamper-resistance of the chain. The ledger is replicated across the network, and any inconsistencies are automatically resolved following established protocols [17]. The general structure of a blockchain is depicted in Figure 3.

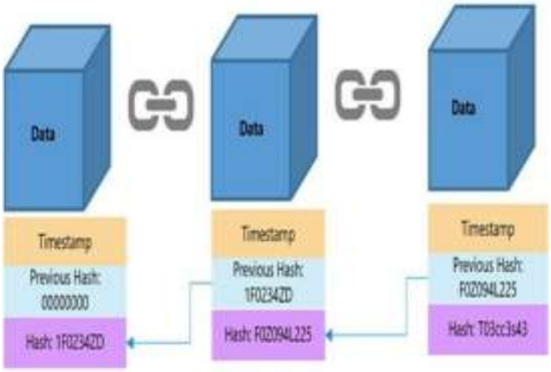

Fig. 3 Blockchain architecture.

Blockchain represents a form of distributed ledger technology introduced to the world by Satoshi Nakamoto in 2008 [18]. Its applications span various sectors, including banking, finance, business, government, and other miscellaneous fields. Compared to contemporary technologies, blockchain offers several advantages in terms of security, privacy, trust, and transparency, which will be elaborated upon in subsequent sections. In blockchain, data and information are securely communicated among users within a network using hash functions [19]. Hash functions provide a cryptographic signature, ensuring immutability.

The attributes of blockchain are summarized in Figure 6 and are elucidated as follows:

Secure. Data and information are encrypted, safeguarding them from unauthorized access. Through cryptographic algorithms, public and private keys maintain the integrity and confidentiality of shared information. Digital signatures authenticate data exchanges.

Programmable. Blockchain features programmable capabilities that extend beyond mere data recording. With self-executing codes embedded within its chain of blocks, manual code development is obviated, rendering it a programmable technology.

Anonymous. Users within the network remain anonymous, enhancing integrity. Blockchain utilizes addresses programmed via cryptographic algorithms, eschewing real identifiers and preserving user anonymity.

Distributed. Ledgers within blockchain are distributed across multiple nodes, granting simultaneous access to records for all users. Unlike traditional systems reliant on centralized servers, blockchain ensures data accessibility across every node, mitigating redundancy.

Unanimous. Changes require unanimous consensus among all network users, thwarting manipulation by specific individuals or groups. Blockchain eliminates control by singular entities prevalent in traditional systems.

Immutable. Data, once inputted, is immutable barring exceptional circumstances. Altering one block necessitates changes to all subsequent blocks, rendering modifications exceedingly difficult.

Timestamp. Each record is timestamped and stored chronologically within blocks. Once assigned, timestamps are unalterable, precluding denial of transactions in the future.

VI. DATA SECURITY ALGORITHMS

RING-SIGNATURE: A ring signature is like a digital signature that can be done by any member of a group of users, each with their own keys [20]. So, when a message is signed with a ring signature, it's like someone from a particular group of people is saying they endorse it. One important thing about a ring signature is that it's really hard for someone to figure out which member's key was used to make the signature. Ring signatures are kind of similar to group signatures, but there are two main differences: first, you can't find out who made a specific signature, and second, you can use any group of users without needing to set anything else up.

1. AES Algorithm

The Advanced Encryption Standard (AES) has three different ways of encrypting stuff: AES-128, AES-192, and AES-256. Each one works by taking chunks of data that are 128 bits long and using special codes, called keys, to scramble them up [21]. Depending on how long the key is—either 128, 192, or 256 bits—AES makes it harder for bad guys to unscramble the data. AES makes the data go through 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each round does different things to the data to make it even more scrambled.

2. Elliptical Curve Cryptography (ECC) Algorithm

Elliptical Curve Cryptography (ECC) is a way to keep things secret when sending them over the internet [22]. It uses a kind of math called elliptic curves to make special secret codes that are smaller and faster than other methods. ECC can make codes that are as strong as other methods, but with smaller numbers. Instead of using big numbers, ECC uses math with these curves to make secret codes. This helps make things more secure without needing as much computer power. ECC is getting more popular, especially for mobile phones, because it's good at keeping things safe without using up too much battery or processing power.

VII. CONCLUSION

This survey paper provides a comprehensive examination of trust management, delving into key aspects such as the semantics of data sharing and different types of attacks. Additionally, the paper identifies various models aimed at enhancing the security of cloud data. Notably, the research highlights the effectiveness of policies alongside encryption in bolstering data security. Furthermore, it sheds light on the contributions of researchers who have focused on enhancing node trust, thereby improving overall work performance independently of other resources. Looking ahead, future research endeavors may explore integrating trust, policy, and encryption models to further enhance the security of cloud data.

REFERENCES

1. GuoC. et al. Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage Future Gener. Comput. Syst.2018
2. WangY. et al. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain IEEE Access (2019)
3. XuS. et al. Secure fine-grained access control and data sharing for dynamic groups in the cloud IEEE Trans. Inf. Forensics Secur. 2018.
4. PadmajaK. et al.A real-time secure medical device authentication for personal E-Healthcare services on cloud computing Int. J. Syst. Assur. Eng. Manag. 2021.
5. SudhakaranP. et al. Secured authentication and key sharing using encrypted negative password in IoT devices ECS Trans. 2022.
6. Josiah Dykstra et al. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques Digit. Investig. (2012).
7. Rajkumar Buyya et al. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility Future Gener. Comput. Syst. (2009).
8. Haolong Fan et al. An integrated personalization framework for SaaS-based cloud services Future Gener. Comput. Syst. (2015).
9. Francis K. Mupila, Himanshu Gupta. “An innovative authentication model for the enhancement of cloud security”. Innovations in Computer Science and Engineering, Springer, Singapore (2021), pp. 447-455.
10. Urvashi Rahul Saxena, Taj Alam Role based access control using identity and broadcast based encryption for securing cloud data J. Comp. Virol. Hack. Tech., 18 (3) (2022), pp. 171-182.
11. Mohammadpayam Almasian , Alireza Shafieinejad. "Secure cloud file sharing scheme using blockchain and attribute-based encryption". Computer Standards and interface, sciencedirect, 2024.
12. O. A. Khashan, "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System," in IEEE Access, vol. 8, pp. 210855-210867, 2020.
13. X. Gao, J. Yu, Y. Chang, H. Wang and J. Fan, "Checking Only When It Is Necessary: Enabling Integrity Auditing Based on the Keyword With Sensitive Information Privacy for Encrypted Cloud Data," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 6, pp.
14. Security and Security andPrivacy Privacy Privacy Issues in Cloud Computing Computing Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.
15. J. Li, N. Li, and W. H. Winsborough, “Automated trust negotiation using cryptographic credentials,” in Proc. ACM Conf. Computer and Communications Security (CCS), Alexandria, VA, 2005
16. Moulahi, T.; Jabbar, R.; Alabdulatif, A.; Abbas, S.; El Khediri, S.; Zidi, S.; Rizwan, M. Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. Expert Syst. 2023, 40, e13103.
17. Prajapati, P.; Shah, P. A review on secure data deduplication: Cloud storage security issue. J. King Saud-Univ.-Comput. Inf. Sci. 2022, 34, 3996–4007.
18. B. Marr, “A very brief history of blockchain technology everyone should read,” 2018.
19. Kamal Kumar, Vinod Kumar, Seema, Mukesh Kumar Sharma, Akber Ali Khan, M. Javed Idrisi, "A Systematic Review of Blockchain Technology Assisted with Artificial Intelligence Technology for Networks and Communication Systems", Journal of Computer Networks and Communications, vol. 2024.

20. Aishwarya Shetty, Archana, Bhavya Y.P, Varun Rao, Vidya Rao. "Secure Data Sharing Among Multiple users in Cloud Computing". ICACT, VOLUME 4 - ISSUE 22, 2016.
21. S. J. Gabriel and P. Sengottuvelan, "An Enhanced Blockchain Technology with AES Encryption Security System for Healthcare System," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021, pp. 400-405
22. B. Ranganatha Rao, B. Sujatha. "A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security", Measurement: Sensors, Volume 29, 2023.