Cloud Computing Security Issues, Vulnerabilities and Recommendations

Bibhu Dash, Pawankumar Sharma, Sameeh Ullah

***Abstract*—Enterprises around the world implementing their cloud first strategy, but it often raises questions about cloud computing and its security commitments. Cloud computing is the newest web-based computing network that offers the users with convenient and flexible resources to access or function with different cloud applications. Cloud computing is the availability of the computer network services, mainly storing data and computational power, without explicit user active control. The data in cloud computing is stored and accessed on a distant server by using cloud service provider' applications. Providing protection is a main issue because information is transferred to the remote server through a medium. It is important to tackle the security issues of cloud computing before implementing it in an organization. In this paper, we call attention to the data related security issues and solution to be addressed in the cloud computing network. To protect our data and information, this paper discusses the advantages of cloud and its security concerns.**

Index Terms—**Cloud computing, Security, Data protection, Encryption, AI, Blockchain.**

.

I. Introduction

Cloud computing is a technology model that enables individuals and businesses to access and use computing resources such as servers, storage, databases, networking, software, and other resources via the internet [1]. Users can use cloud services offered by a third-party supplier instead of owning and managing physical hardware and software infrastructure. These services are hosted in data centers all around the world, and users can access them whenever they choose, paying only for the resources they use. The key aspects are:

a) On-Demand access: Users can use cloud resources on-demand through web-based interface per their usability. The flexibility allows auto scaling or manual scaling the resources up or down based on demand for cost effectiveness.
b) Elasticity: Cloud services are built to be extremely scalable. Users can quickly increase or decrease resources to meet fluctuating demand.
c) Self-Service: Without significant human aid from the cloud provider, users can provision and manage resources.
d) Resource Pooling: Cloud service providers combine processing power to serve several clients, which improves cost effectiveness and resource utilization.
e) Measured Service: Cloud has the provision to 'pay-as-you-go' model. It helps users to billed for the resources they use.

Cloud computing mainly categorized into three main service models. These are Infrastructure as a Service (IaaS), Platform as a Service(PaaS) and Software as a Service(SaaS). Cost savings, scalability, flexibility, and the ability to outsource infrastructure management responsibilities are just a few advantages of cloud computing [2]. Businesses of all sizes use it as a core component of contemporary IT to support a wide range of services and applications. Though cloud computing is a catalyst in the technological landscape, it also raises many security concerns that organizations and individuals worry about. This paper discusses what kind of concerns are arises with cloud usage and the prevention measures.

II. Cloud Security Concerns

There are many security concerns related to the cloud data and privacy protection. Organizations and individuals depending on cloud should be aware of these challenges. Some of the primary security concerns are discussed in below.

A. Data Breach

Whether due to insider threats, cyberattacks, or incorrect security configurations, data stored in the cloud may be subject to breaches. Both the cloud provider and the cloud user are frequently responsible for maintaining data security, and a user error may result in data exposure.

B. Identity and Security Management

Weak or hacked user credentials may allow unwanted access to cloud services, according to Identity and Access Management (IAM). To guarantee that only authorized users and services may access data and applications, proper IAM practices are essential.

C. Shared Resources

Resources are shared across numerous users in a multi-tenant cloud system. Although providers use tight isolation, flaws in the underlying infrastructure could allow another user to compromise the data of one user.

D. Compliance and Legal Issues

When storing data in the cloud, organizations may need to comply with certain industry rules as well as legal and

Manuscript received September 29, 2021.

Bibhu Dash, School of Computer and Information Sciences, University of the Cumberlands, Williamsburg, Kentucky, USA.

Pawankumar Sharma, School of Computer and Information Sciences, University of the Cumberlands, Williamsburg, Kentucky, USA.

Dr. Sameeh Ullah, School of Information Technology, Illinois State University, Normal, Illinois, USA

compliance issues, such as data sovereignty and privacy laws like the GDPR [3].

E. Data Loss

Despite the redundancy and backup systems used by cloud providers, data loss is still possible because of unforeseen circumstances, provider failures, or unintentional data deletion. It's essential that consumers have personal backup and recovery plans.

F. Lack of Due Diligence

Hasty cloud adoption without carefully evaluating a provider's security procedures and promises can result in flaws. Businesses should carefully investigate and vet cloud suppliers.

G. Lack of visibility and control

Cloud customers may not have full access to the underlying infrastructure, which makes it difficult to adequately monitor and secure resources [4].

H. Services from Third Parties

Many cloud apps rely on plugins or third-party services, which might increase the security concerns if those services are not properly secured.

I. Data Encryption

To prevent unauthorized access, data should be encrypted both in transit and at rest. Companies must make sure that appropriate encryption procedures are followed and that encryption keys are securely stored.

J. Vendor Lock-In

Moving data and apps across cloud providers can be difficult and may result in vendor lock-in. Long-term, this might influence flexibility and cost-effectiveness.

III. Security Strategy and Measures

Understanding each party's responsibilities is vital for properly minimizing security threats in cloud because cloud security is a shared responsibility between the cloud provider and the cloud user. Cloud security is a complex multi-factored measure (see Figure 1) and the robust security measures are outlined below.

A. Make a thorough risk assessment.

It is important to understand the business , its process and conduct a thorough risk assessment of data in cloud to understand its limitations, vulnerabilities and the risk types like both external and internal risk environments.

B. Establish effective identity and access management procedures.

Cloud is a shared service and used by vendors, customers, and multi-functional teams [5]. As different team has different requirements, establishing an effective identity and security management system is very essential.

***C.** Encrypt both data at rest and in transit.*

The crucial phase in our cloud journey is data. Therefore, data encryption and masking must be used to secure business and customer data, whether the data is at rest or in motion.

D. Audit and keep an eye on cloud resources often.

With data security and storage, cloud billing is very dynamic as it operates on pay-as-you-go mode [6]. Hence usage effectiveness and billing efficiencies are very important and for the same regular audit is often advisable.

E. Observe recommended configuration and security setting procedures.

Managing security is responsibility of both parties: the provider and the user. Hence, users need to maintain regular upgrades and maintain regular security audits with recommended configurations to keep their resources safe [7].

F. Create plans for backup and recovery.

Cloud backup and recovery must be included in an organization's enterprise risk management (ERM) strategy. Cloud backup and recovery is a crucial approach to keep corporate operations since modern business is cloud-based.

G. Update knowledge about security issues and vulnerabilities

The cloud is still in its infancy and is undergoing resource upgrades. Teams must always be informed and prepared to manage new security threats and vulnerabilities because it is an ongoing process.

H. Observe applicable laws and professional norms.

Following both internal and external governance norms and procedures is necessary when managing consumer data. In order to protect customer data, firms must adhere to both internal and external regulatory standards.

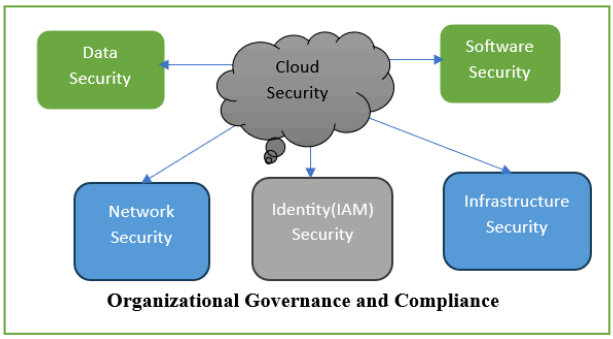

Figure 1. Cloud Security and Components [8]

IV. Components of Organizational Cloud Security Strategy

Organizational cloud strategy is very important. But it is an enterprise strategy that needs to have these components.

A. Cloud Security Policy and Governance

- *Policy Development*: Develop clear policies outlining security expectations, roles, and responsibilities.
- *Governance Framework*: Implement a governance framework to oversee cloud security efforts and ensure compliance with regulations and standards.

B. Risk Assessment and Compliance

- *Risk Assessment*: Conduct regular risk assessments to identify vulnerabilities and threats specific to your organization.
- *Compliance*: Ensure compliance with relevant industry standards and regulations (e.g., GDPR, HIPAA etc.) [2].

C. Identity and Access Management (IAM)

- *Identity Management*: Implement a robust IAM system to control and monitor user access to cloud resources.
- *Multi-Factor Authentication (MFA):* Enforce MFA to enhance identity verification.
- *Role-Based Access Control (RBAC):* Assign permissions based on roles and responsibilities.

D. Data Protection

- *Data Encryption*: Encrypt data in transit and at rest.
- *Data Loss Prevention (DLP):* Implement DLP tools to prevent unauthorized data exposure.
- *Key/Vault Management*: Properly manage encryption keys.

E. Network Security

- *Firewalls*: Set up firewalls to control traffic to and from the cloud.
- *Intrusion Detection and Prevention (IDS/IPS) Policies:* Implement IDS/IPS to detect and block malicious activities. AI enabled IDS/IPS frameworks are very popular in the digital organizations.

F. Cloud Service Security

- *Secure Configuration*: Configure cloud services securely.
- *Patch Management*: Keep cloud resources up to date with the latest security patches.
- *Cloud-Based Security Services*: Utilize cloud-based security services for added protection.

G. Incident Response and Monitoring

- *Incident Response Plan*: Develop an incident response plan to address security breaches.
- *Security Information and Event Management (SIEM):* Use SIEM tools to monitor cloud environments for unusual activities.
- *Logging and Auditing*: Maintain detailed logs and audit cloud activities.

H. Backup and Recovery

- *Regular Backups*: Create and regularly update backups of critical data and applications.
- *Disaster Recovery Plan*: Develop a disaster recovery plan to ensure business continuity.

I. Employee Training and Awareness

- It's a very effective and important step towards cloud security. Provide employees with security training to educate them on best practices and potential threats.

J. Vendor Assessment

- Regularly assess your cloud service providers for their security practices and certifications.

K. Security Testing

- Conduct regular penetration testing and vulnerability assessments to identify and address security weaknesses.

L. Continuous Improvement

- Periodically review and update your cloud security strategy to adapt to evolving threats and technologies.

V. Solutions to Data Security Challenges

There are various techniques both AI based, and non-AI based, that contributes to cloud security and those details are highlighted below in Figure 2.

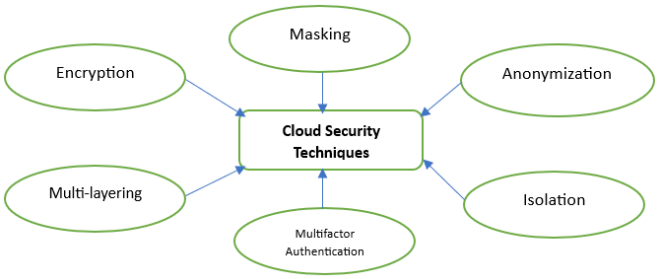

Figure 2. Techniques Enabling Cloud Security

In order for some members of the community to have easy access to information, the data owner should grant them permission, its general traditional data store practice. Heterogeneous data-centric authentication should be utilized to include data access control. A plan for data protection must be created that addresses authentication, data encryption and integrity, data recovery, user protection, and enhancing cloud data security [7, 9]. To protect users' privacy and the confidentiality of their data, data encryption should be employed. Apply encryption to data to render it completely unusable and to prevent other users from accessing it. Accessibility issues may arise with common encryption or isolation techniques.

Another approach to ensure that the data is not altered before being transferred to cloud servers is to compute the hash/anonymization of the file or data. This hash calculation can be used to ensure the accuracy of records, but maintaining it is quite challenging. Cloud computing employs access control at the user or device level. Stronger regulations apply when unauthorized users are identified via passwords or attribution [10]. The consumer might be informed that access to that portion of the data is possible via permission as a service. The owner can transfer the majority of computer-intensive tasks to the cloud with the aid of a fine-grained access management system without disclosing the servers' location or data content [11]. Data-driven architecture is most popular now a days to protect data loss and intrusion prevention.

VI. Advanced Cloud Security using AI Measures

Advanced Artificial Intelligence (AI) techniques that offer real-time threat detection, quick incident response, and proactive risk management can dramatically improve cloud security. Here are some cutting-edge AI safeguards against risks to cloud security:

A. Intrusion Detection and Prevention Using AI

Detect unusual or harmful patterns or behaviors in network traffic by using AI-driven intrusion detection systems (IDS) and intrusion prevention systems (IPS). A greater level of security is offered by AI algorithms' ability to find previously unidentified risks and adapt to changing attack methodologies.

B. Enhanced User and Entity Behavioral Analytics (UEBA)

Utilize behavioral analysis powered by AI to create a baseline of typical system and user behavior. Alerts can be set off by departures from the norm, which makes it easier to spot insider threats and zero-day assaults. In order to spot sophisticated attack patterns, UEBA can also correlate actions across several accounts and gadgets [12].

C. Machine Learning for Anomaly Detection

Identify probable security breaches by using machine learning algorithms to find anomalies in system logs, network traffic, and user behavior [11, 13]. Traditional rule-based systems may miss patterns that machine learning can find.

D. AI-Enabled Predictive Analytics

To foresee possible security threats and vulnerabilities, use predictive analysis. In order to proactively identify potential hazards and weaknesses, AI may evaluate historical data and present trends.

E. Implement Cloud Provider Specific AI Tools

Many cloud service providers offer security capabilities powered by AI that are specially designed for their platforms. As an example: AWS provides Amazon GuardDuty, which employs AI to identify threats inside AWS settings [11].

F. AI models for Access and Vulnerability Management

Utilize AI to scan cloud environments for vulnerabilities, then rank remediation activities according to their likelihood to be exploited and their potential impact [14]. Reduce the attack surface by using AI to enforce fine-grained access controls based on user behavior, location, and device.

G. AI-Driven User Awareness and Training

Utilize AI to create individualized and flexible security awareness training for staff members so they are more prepared to identify and respond to security risks.

H. Security Recommendations Based on AI

In order to help enterprises improve their security posture, several cloud security solutions provide AI-generated recommendations for enhancing security setups and policies[15].

It is important to note that, while AI can vividly improve cloud security, it should be considered as only one part of a larger security plan organizations should have, that also involves best practices, policy enforcement, and user monitoring [14, 16]. To keep up with changing dangers in the cloud environment, regular monitoring, assessment, and adaptation are obligatory.

VII. Blockchain for Improved Cloud Security

Due to its tamper-proof encryption/masking, blockchain technology is well-known in the business. The confidentiality, integrity, and accessibility of data and services in the digital era depend on two distinct but related fields of technology: blockchain and cloud. If both technologies can implement together (Hybrid cloud security solutions), it will enhance safety measures in all kinds of cloud systems (i.e., private, public and hybrid clouds) [12]. Some of the solution aspects are discussed in detail below.

1. *Decentralized Identity and Access Management:* A secure, decentralized identity management system can be provided by blockchain. Blockchains can be used to hold user digital identities, and smart contracts can be used to regulate user access to cloud resources. This can enhance access control and lower the danger of identity theft [13].
2. *Immutable Audit Trails:* Blockchains provide an unchangeable record of all transactions and modifications. Cloud providers may ensure that logs and records cannot be altered by adopting a blockchain for recording and auditing reasons, offering a trustworthy source of truth for security incidents and compliance [13, 17].
3. *Tamper-Resistant Timestamping:* Critical documents and events can be securely timestamped in a cloud environment using blockchain timestamps. This can help to guarantee the validity and integrity of papers and logs.
4. *Immutable Records for Incident Response:* A blockchain can be used to securely record all activities taken during the incident response process in the event of a security incident or data breach [17]. This makes sure that no logs or records—which can be crucial for post-incident analysis and legal compliance—can be removed or altered.
5. *Smart Contracts for Security Policies:* It is worth noting that organizations need to add smart contracts security policies in their enterprise security management (ESM) process [18]. It is possible to automate and enforce security regulations using smart contracts. For instance, a smart contract can initiate security responses in the event of a security breach or automatically enforce access control restrictions.
6. *Distributed Storage and Data Provenance:* In distributed storage solutions, where data is broken up, encrypted, and spread across several nodes, blockchain technology can be used. Data integrity is ensured by maintaining the data's provenance,

which makes it impossible for an attacker to compromise the data.

7. *Tokenized Vault Management and Data Encryption:* Using a blockchain to store encryption keys and administer tokenized vaults can increase security. The immutability of the blockchain makes sure that keys aren't altered and that they may be quickly accessed for data encryption and decryption (see Figure 3).

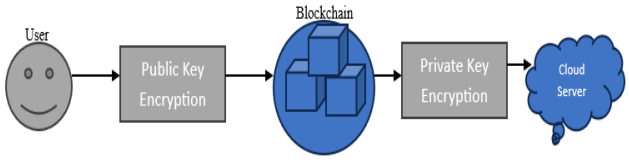

Figure 3. Blockchain Enabled Advanced Encryption for Cloud Server

It's vital to keep in mind that while blockchain can improve cloud security, it is not a universally applicable fix. Before integrating blockchain technology into their cloud security strategy, enterprises should carefully consider implementation and evaluate their unique security demands and risk considerations.

VIII. Conclusion

Cloud Computing has its pros and cons. The portability, effectiveness, usefulness, and cost savings feature of cloud computing is particularly enticing. This newest technological innovation has many advantages for customers but also raises several security issues. We have outlined some applications of cloud computing as well as some of its difficulties in this essay. This study demonstrates that integrating this technology into an organization after addressing different security concerns can result in significant improvements. Here, we've covered some crucial cloud computing data and non-data security problems and their fixes using AI. Future research will need to assess several cloud-related issues, including security, privacy, effectiveness, property, economics, available talents in the market and other non-technical concerns. As cloud is evolving, its security measures need to be investigated further and its security issues have to be thoroughly investigated.

Acknowledgment

We appreciate Dr. Azad Ali of the University of the Cumberlands in Kentucky taking the time to review and proofread our work and provide guidance so that we could write this paper to the best of our ability.

References

[1] Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1-48.

[2] Manoharan, D. J. S. (2021). A novel user layer cloud security model based on chaotic Arnold transformation using fingerprint biometric traits. *Journal of Innovative Image Processing*, *3*(1), 36-51.

[3] Alatawi, S., Alhasani, A., Alfaidi, S., Albalawi, M., & Almutairi, S. M. (2020, September). A survey on cloud security issues and solution. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1-5). IEEE.

[4] Brumă, L. M. (2021, August). Cloud security audit–issues and challenges. In *2021 16th International Conference on Computer Science & Education (ICCSE)* (pp. 263-266). IEEE.

[5] Shyla, S. I., & Sujatha, S. S. (2019). Cloud security: LKM and optimal fuzzy system for intrusion detection in cloud environment. *Journal of Intelligent Systems*, *29*(1), 1626-1642.

[6] Popli, M. (2019, March). A survey on cloud security issues and challenges. In *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 230-235). IEEE.

[7] Maurer, T., & Hinck, G. (2020). *Cloud security: a primer for policymakers*. Carnegie Endowment for International Peace.

[8] Rao, P. M., & Saraswathi, P. (2021). Evolving cloud security technologies for social networks. In *Security in IoT Social Networks* (pp. 179-203). Academic Press.

[9] Verma, G., & Adhikari, S. (2020). Cloud computing security issues: a stakeholder's perspective. *SN Computer Science*, *1*(6), 329.

[10] Wani, A. R., Rana, Q. P., & Pandey, N. (2019). Analysis and countermeasures for security and privacy issues in cloud computing. *System performance and management analytics*, 47-54.

[11] Surya, L. (2018). Streamlining cloud application with AI technology. *International Journal of Innovations in Engineering Research and Technology [IJIERT] ISSN*, 2394-3696.

[12] Sangui, S., & Ghosh, S. K. (2021). Cloud Security Using Honeypot Network and Blockchain: A Review. *Machine Learning Techniques and Analytics for Cloud Security*, 213-237.

[13] Dash, B., & Swayamsiddha, S. (2020). Blockchain Adoption in Enterprises: Opportunities and Challenges.

[14] Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. *IEEE Access*, *9*, 20717-20735.

[15] Dash, B. (2020). Life on the Edge from Legacy to Cloud Computing: A Case Study on Insurance Industry.

[16] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. *Electronics*, *9*(9), 1379.

[17] Kanimozhi, V., & Jacob, T. P. (2019, April). Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. In 2019 international conference on communication and signal processing (ICCSP) (pp. 0033-0036). IEEE.

[18] Subramanian, E. K., & Tamilselvan, L. (2019). A focus on future cloud: machine learning-based cloud security. *Service Oriented Computing and Applications*, *13*(3), 237-249.

Bibhu Dash is a Ph.D. student in School of Computer and Information Sciences at University of the Cumberlands, KY. His research interests are in Big data, data security in cloud and AI. He has more than 14 years of IT experience in database design, data security, cloud analytics and big data management.

Pawankumar Sharma is a Ph.D. student in School of Computer and Information Sciences at University of the Cumberlands, KY. His research interests are in Cloud, Cyber security, AI and Customer analytics.

Dr. Sameeh Ullah is a visiting Professor in School of Information Technology at Illinois State University, Normal, IL. He has more than 14 years of academia and industry experience and his research interests are Deep Learning, Cyber security and Blockchain.