STM JOURNALS

Journal of
Semiconductor Devices and Circuits

ISSN: 2455-3379
Volume 12, Issue 2, 2025
May–August
DOI (Journal): 10.37591/JoSDC

https://journals.stmjournals.com/josdc

Research JoSDC

Securing Multi Cloud Environment

Sangeetha S.[1,*], Rahul Prasanth P.[2], Harshavarthan K.[2],
Aravind Kumaran A.[2], Mohammed Asraf S.[2]

Abstract

Offer improved scalability and resilience; they attempt to fulfill certain business requirements such as high availability, fault tolerance, and seamless performance under varying workloads. In recent years greater flexibility, enhanced performance, and attempts to avoid being tied to a single vendor have resulted in many organizations adopting multi-cloud environments. This, however, comes with its challenges, one of the most pressing being the security of data in the multi-platform clouds. This report outlines the risks and their management including the best practices for cybersecurity, privacy, ensuring compliance, IAM, incident response, and network driving. Addressing these very issues leads to managed services providers who provide comprehensive cloud offerings, including multi-cloud environments and architecture. The report also covers multi-cloud management security and risk governance and management, including a case study of companies that have practically perfected security aspects and successfully managed risks associated with multi-cloud environments. Considering the intricacy of multi-cloud structures, protecting such systems is a complex task. They need to be secured simultaneously from organizational processes, technical instruments, and security monitoring.

Keywords: Multi-cloud environments, security, triple DES (3DES), encryption, secure socket layer (SSL)

INTRODUCTION

Multi-cloud structures have been widely adopted by organizations, which have completely changed how businesses handle their IT infrastructure. They are now able to flexibly and quickly meet challenges and demands with the help of various cloud service providers such as Amazon Web Services, Microsoft Azure, and Google Cloud. This allows them to avoid being chained to a single provider while also enhancing performance [1]. Even though these benefits are making the demand for a multi-cloud architecture higher, new complex security concerns are arising that must be properly planned and catered to securing a multi-cloud environment which is difficult due to the variety of cloud platforms available, distinct security paradigms, and expansive attack surfaces. This allows for greater scope of risk as data and workloads are now spread out across clouds. Organizations are at risk of their data being compromised, configurations getting mismanaged, unauthorized entry, or API vulnerabilities existing. To tackle these problems, a proper risk management framework has to be devised that caters to governance, compliance, and operational management of all the clouds [2].

***Author for Correspondence**
Sangeetha S.
E-mail: sangeetha@kce.ac.in

[1]Professor, Department of Computer Science and Engineering, Karpagam College of Engineering Coimbatore, Tamil Nadu, India
[2]UG Scholar, Department of Computer Science and Engineering, Karpagam College of Engineering Coimbatore, Tamil Nadu, India

Received Date: March 27, 2025
Accepted Date: April 27, 2025
Published Date: June 26, 2025

Citation: Sangeetha S., Rahul Prasanth P., Harshavarthan K., Aravind Kumaran A., Mohammed Asraf S. Securing Multi Cloud Environment. Journal of Semiconductor Devices and Circuits. 2025; 12(2): 1–8p.

This report explores general cloud security concepts such as encryption, identity and access management (IAM), protection of computer networks, and production of secure applications (DevSecOps). Also, the focus is aimed towards the best practices for strengthening a multi-cloud security framework. Finally, the report turns its attention to the focus on the future of cloud security, for example, the application of AI and machine

learning in threat identification, the adoption of Zero Trust security models, and quantum computers changing data encryption and security sets.

LITERATURE SURVEY

Securing multi-cloud environments is a complex task due to the distributed nature of these architectures. Key security challenges include data privacy and confidentiality, identity and access management, network security, application security, incident response and disaster recovery. To mitigate these risks, organizations should implement a comprehensive security strategy.

Benefits of Multi-cloud Computing

A thorough way to deal with asset the board in a multi-cloud setting is portrayed in this work. By using multi-cloud innovation and industrially available solutions to scale assets and further enhance framework strength while remaining as cloud rationalist as could really be expected, this programming interface aims to meet the steadily expanding asset necessities [3]. Considering this, the work introduced here will include a structural examination of the asset, the executives programming interface, a significant level outline of the execution, and a trial intended to exhibit the reasonability and importance of the frameworks talked about.

Time Series Models for Predicting Security in Multi-cloud Environments

ARIMA

ARIMA (Auto Regressive Integrated Moving Average) is a popular statistical time series forecasting model. It is based on time series forecasting models on the fact that a linear function of the time series past values can be used to estimate future time series values and includes trend (AR), difference (I), and noise (MA) components [4].

Multi-Cloud Security Application

ARIMA can be employed to predict security measures such as failed login attempts or network traffic volume within multi-cloud systems.

Exponential Smoothing

Exponential smoothing comprises a technique of forecasting where an emphasis on past observations is progressively reduced and more weight is given to the latest data. As such, this technique could provide forecasts using time series as input.

Application in Multi-Cloud Security

The application of this method is useful for short-term forecasting of predictions within environments with changing security events. For instance, it can be employed to monitor and predict the daily patterns of network traffic and login attempts on a real-time basis.

Limitations

The limitation of exponential smoothing is its increased efficiency when employed in short-term predictions. This disadvantage can severely affect attempts at long-term forecasting, such as trends in multi-cloud cyber threat predictions and attempts.

IMPORTANCE OF SECURITY IN THE CLOUD

Securing data, applications, and infrastructure in a multi-cloud environment is crucial as the ecosystem comprises multiple cloud service providers. Unlike a single cloud service, multi-clouds are exposed to unauthorized access, data breaches, and disruptions of services. The multi-dimensional nature of the environment amplifies the difficulty of ensuring proper management of several security tools, configurations, and policies of different platforms and their respective attack surfaces [5]. Because of the traditional security tools, there are gaps in threat detection and incident response due to their lack of multidisciplinary coverage. Organizations need to switch to unified monitoring tools for

security information and events management (SIEM) so everything is stored in one single area. This leads to better detection of threats and faster resolution of problems.

SCOPES AND LIMITATIONS

The aim of this study is to amplify the strength of the multi-cloud environment's security fundamentals through the adoption of different sets of security controls. This involves the objective of implementing selection of the appropriate cloud service providers, enhancing the network infrastructure, instituting strong identity and access management, protecting sensitive data, ensuring application security, and formulating plans for incident response and disaster recovery planning and execution [6]. In pursuing better security, it is worth noting that this project has limitations. Security measures include making allowances for certain risks and impacts that must be accepted. Even though this project significantly improves security, it is worth repeating that a 100% safe is unattainable. The multi-faceted nature of the landscape places a requirement for constant monitoring, assessment, and adjustment of security measures together with the organizational infrastructure.

SECURITY CHALLENGES

Data Privacy and Protection

- *Agriculture is Sensitive:* The system requires and captures sensitive information such as images of crops and weeds, farm structures, and environmental conditions, which the system processes. With this information, one can gain access to/edit confidential information concerning proprietary farming practices, resources, and productivity usage.
- *Data Leak:* Unauthorized individuals may use this data for espionage or competitive theft, which might result in financial loss, or gaining intelligence in surveillance.

Network and Cloud Security

- *Cloud-based Data Storage:* Numerous developed agricultural systems depend on cloud-based platforms to safely keep and analyze data. These platforms are vulnerable to several safety issues, including unauthorized proactive security controls, data copying or deletion, and denial of service attacks [7].
- *Man-in-the-Middle Attacks:* Attackers can potentially control the communication flow between IoT devices and sensors to the cloud servers. They can inject, erase, or modify the data, which can be used against weed detection systems, leading to false action.

ENCRYPTION MEASURES FOR PROTECTING DATA

Symmetric Encryption Algorithms

This technique uses a single key for both the encryption and decryption processes to maintain the confidentiality and integrity of the information.

- *Algorithms:* These include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES).
- *Strengths:* Fast working speed, which makes it ideal for large-scale encryption of data; as well as designed for areas with limited resources.
- *Limitations:* There are complex issues regarding key management, such as if the keys are compromised, there may be vulnerabilities, and there are problems with the keys being securely distributed.

Asymmetric Encryption Algorithms

Asymmetric encryption, which is referred to as public-key cryptography, makes use of two keys: one for encryption and the other for decryption. This method ensures an increased security level and the ability to open secure communication channels.

- *Algorithms:* RSA (Rivest-Shamir- Adleman), Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange are the most common.

- *Strengths:* The most impressive feature is the added protection that comes from separate public and private keys, making it difficult to obtain. This allows for enhanced protection during key exchanges and for digital signatures.
- *Limitations:* It is slower when compared to symmetric encryption, which requires higher processing speeds, makes the device work harder than it normally has to, and is more likely to be targeted by quantum computing attacks [8].

ACCESS CONTROL MECHANISMS IN MULTI-CLOUD

Role Based Access Control (RBAC)

With RBAC, certain users are given access to the system based on their previously defined roles within the organization which in turn allocates permissions that are suited for that user-role.

- *Components*: Different types of roles assigned permissions, as well as role assignments are the main components of an RBAC system [9].
- *Advantages:* It makes access easier to manage, cutting down on administrative work, all the while increasing security through the principle of least privilege.
- *Implementation:* Common actions taken in the implementation of RBAC include role creation, role assignment, and role revocation.
- *Attribute-Based Access Control (ABAC):* ABAC considers user data, conditions of the environment as well as any resources and uses them to grant appropriate access for the user.
- *Attributes:* Attributes are defined as user-centric (role or department) as well as resource-centric (sensitivity). Also, some environmental factors such as time of access can be included too.
- *Advantages:* These attributes enable trustworthy granular access control, context-aware authorization, as well as high scalability for complex access control policy.
- *Policy Evaluation:* Policies are generated from attribute-value pairs. Access requests are always filtered and evaluated against these policies before any access is granted.

Policy-Based Access Control

Policy-based access control makes use of a pre-specified group of rules or policies that let users gain access depending the on the set criteria and conditions for that access.

- *Policies:* These set of rules are made using attributes, roles, contextual factors and resource properties.
- *Enforcement:* Policies are evaluated, and access control policies are set by evaluating these rules to the organizational security and policy guidelines [10].
- *Flexibility:* On the other hand, policy based access control is flexible in that the user is able to change the access control policies as need arises in the business activities and policies.

Multi-Factor Authentication (MFA)

Security is enhanced using MFA using different factors for different levels of authentication to verify identity prior to providing access.

- *Factors:* These factors may include a password which the user knows, a smart card or a token, or any form of biometric authentication.
- *Security Enhancement:* It improves security by preventing unauthorized individuals from gaining access since multiple forms of authentication are needed as opposed to just a password.
- *Implementation:* MFA can be configured through a myriad of methods for authenticating such as SMS messages, biometrics, one-time passwords, and hardware tokens.

SECURITY MEASURES

Secure Socket Layer (SSL)

SSL is a cryptographic protocol from the 90's, akin to TLS, aimed at creating secure network connections and maintaining data confidentiality and integrity.

- *Transition to TLS:* Due to some weaknesses in the earlier versions of SSL, the protocol has been replaced with TLS in newer systems.

- *Encryption and Authentication:* SSL makes use of algorithms as well as digital certificates for data encryption and provides mutual authentication.
- *Legacy Considerations:* Although SSL is not as widespread as it was before, legacy, older applications, and devices sometimes still depend on it for secure communications.

Transport Layer Security (TLS)

TLS is a cryptographic protocol that provides confidentiality as well as integrity to information sent through client-server applications, browsers, and email servers.

- *Encryption:* Using both asymmetric and symmetric encryption algorithms, TLS ensures the protected transmission of information in codes, thus securing the data's confidentiality.
- *Authentication:* By enabling mutual authentication of clients and server identities, TLS helps to prevent man-in-the- middle attacks.
- *Certificate Authorities (CAs):* TLS makes use of digital certificates sold by trusted CAs to confirm server identities and link to them securely.

Virtual Private Network (VPN)

A VPN is an encrypted virtual tunnel placed above a public network, such as the internet, which allows remote users to access private network resources safely.

- *Tunneling Protocols:* IPsec (Internet Protocol Security) and SSL/TLS VPN are examples of tunneling protocols. VPNs can be used to wrap data packets and encrypt them for safe transmission [11].
- *Authentication and Authorization:* To have control over the resources which users can access on the network, VPNs use approaches such as usernames, password, digital certificates, and multi-factor authentication.
- *Use Cases:* VPNs are mostly used for the purpose of remote access to corporate networks and secure communication for distributed sites, as well as for anonymous internet surfing.

PRIVACY MEASURES AND COMPLIANCE

General Data Protection Regulation (GDPR)

GDPR is one of the most important data protection regulation within the EU, which aims to protect the privacy and data of people against any unauthorized use.

Key Requirements

Oftentimes, GDPR has been portrayed as a heavy and loose set of guidelines. However, its main and single most important rule is that the law applies to all companies doing business with any person whether done online or offline. In broad strokes, GDPR mandates explicit informed consent for data processing, transparency in data handling practices, the establishment of data subject rights, obligation to notify data subjects of data breaches, and to have properly appointed Data Protection Officers (DPOs) [4].

Compliance Framework

Following the requirements of GDPR, a set of guidelines, regulations and laws internally applicable must be created. This includes the creation of policies governing the means and ways data processing activities should be carried out. Resources must also be allocated to ensure regular reviews and audits of reports and progress made towards fulfilling these set policies.

Health Insurance Portability and Accountability Act (HIPAA)

This Act, alongside its regulations, has been referred to as the foundation of healthcare IT because it sets minimum necessary standards that must be in place whenever sensitive patient health information (PHI) is being used [6].

Privacy Rule

The HIPAA Privacy Rule requires each Covered Entity and Business Associate to have appropriate safeguards that will ensure the confidentiality, integrity, and security of Protected Health Information while being used and transmitted. These standards seek to protect individual medical records and personal health information such as data use, disclosure, and security.

Security Rule

The HIPAA Security Rule during the implementation of the Act required Covered Entities to put in place adequate encrypted firewalls to limit, control, and prevent access to any electronic protected health information (ePHI) to unauthorized people [9].

ISO/IEC 27001 Certification

ISO/IEC 27001 is an international standard's document that specifies requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organization.

Certification Process

To get ISO/IEC 27001 certification, an accredited certifying body evaluates an organization's information security management system in accordance with the standards set by the certificate.

Benefits

After attaining ISO/IEC 27001 certification, an organization gains customer trust at the same time as demonstrating commitment towards mitigating the risks associated with data breaches and other cyber threats.

ADDRESSING THREATS AND VULNERABILITIES

- *Denial of Service (DoS) Attacks:* The purpose of DoS attacks is to obstruct the cloud services by incapacitating the target system or network through excessive resource consumption or traffic.
- *Prevention Measures:* Employing network firewalls, intrusion detection and prevention systems, and implementing rate limiting, can effectively defend against DoS attacks. Additionally, mitigation of this type of DoS attack is commonly referred to as DDoS and is widely utilized [3].
- *Incident Response:* To mitigate the impacts of DoS attacks, it is important to develop incident response plans, constantly watch for anomalies in network traffic, and coordinate with ISPs and CSPs.

Insider Threats and Data Leakage

Insider threats are intentional security risks that insiders contrive such as employees, contractors, or even partners use their sensitive access to confidential information to harm the company.

- *Mitigation Strategies:* Engaging with security tools to monitor confidentiality and privacy standards that contain least privilege access, while also proactively engaging with customers by training them on security best practices and putting in place DLP strategies can greatly assist in alleviating inside threats and information loss.
- *Detection Techniques:* Inside threats may be dealt with effectively by employing and integrating DLP systems with SIEM software for responsive and proactive detection of actions that may indicate malicious intent.

Malware and Ransomware Attacks

In Malware and Ransomware assaults, the malware is placed in a target system, while data under malware control is encrypted with ransom to be demanded later, and both pose a great menace to data availability and integrity [11].

- *Prevention Measures:* Infections via malware or ransomware can be avoided through strict endpoint protection, improving network security, and filtering emails. Regular security maintenance can also drastically reduce chances of such infections.

- *Guidelines for Responding:* Prior planning strategies call for creation of incident response plans, law enforcement communication channels, and offline backups for crucial data which can aid response to malware or ransomware attacks.

CSP Compromise

CSP compromise is best described as a scenario where an external attacker or a malicious insider is able to gain entry and utilize cloud services, infrastructure, or data, hence resulting in severe implications on the confidentiality and integrity of such data [2–4].

- *Security Assurance:* It becomes of utmost importance to assess the security posture of the cloud service provider and the ability to defend against compromise by scrutinizing their security controls, certifications, and adherence to industry standards, for example SOC 2 or ISO/IEC 27001.
- *Shared Responsibility Model:* With the advent of multi-cloud environments, it is worthwhile to note that it is important to understand the shared responsibility model in order to allocate security roles and tasks between the customer and the CSP.

AUDITING AND MONITORING

In the context of image processing and deep learning-based weed detection systems, auditing and monitoring involve security and reliability measures that are very necessary. This activity is critical in tracking the known weak spots, tracking the malicious activities, system performance, and for identification of security vulnerabilities [8]. Potential risks must be addressed and monitored through efficient auditing and business processes to ensure the system functions at peak level in an agile agricultural setting [12].

CONCLUSION

The project brought into focus how critical managed identity services are to identity management, particularly the Azure Active Directory and the AWS IAM which could be utilized to issue and enforce security policies while at the same time reducing risks to unauthorized access in cross cloud platforms. In addition, we discussed these phenomena along with the construction of Virtual Private Networks (VPNs), firewalls, and the segmentation of networks to ensure that communication channels between resources located at different clouds were secured. Data security for sensitive information and data were also reviewed such as ensuring information is encrypted during transmission, stored or in rest. Additionally, the other main conclusion during this project is that monitoring and detection must be made in real-time. Some of the tools that can help are the Azure Security Center, AWS Security Hub, and the Google cloud security command center. These tools allow the organization where they are deployed to keep track of any risks that might be present in their multi-cloud-enabled setups. Furthermore, such tools allow the organization to rapidly address any identified risks. Also, automating security threats management alongside incorporation of security in the DevOps pipelines can also help mitigate human error and increase efficiency. Users can bolster security further by using machine learning and AI-based solutions to develop and respond to threats in real time. Additionally, it is important for organizations to continuously update their multi-cloud security practices to comply with industry standards and regional legal requirements that are always changing.

REFERENCES

1. Anwarbasha H, Sasi Kumar S, Dhanasekaran D. An efficient and secure protocol for checking remote data integrity in multi-cloud environment. Sci Rep. 2021 Jul 2; 11(1): 13755.
2. Bhagavan S, Gharibi M, Rao P. Fedsmarteum: Secure federated matrix factorization using smart contracts for multi-cloud supply chain. In 2021 IEEE International Conference on Big Data (Big Data). 2021 Dec 15; 4054–4063.
3. Bucur V, Miclea LC. Multi-cloud resource management techniques for cyber-physical systems. Sensors. 2021 Dec 15; 21(24): 8364.

4. Zhu QH, Tang H, Huang JJ, Hou Y. Task scheduling for multi-cloud computing subject to security and reliability constraints. IEEE/CAA J Autom Sin. 2021 Mar 10; 8(4): 848–65.
5. Kavitha S, Bora A, Naved M, Raj KB, Singh BR. An internet of things for data security in cloud using artificial intelligence. Int J Grid Distrib Comput. 2021; 14(1): 1257–75.
6. Viswanath G, Krishna PV. Hybrid encryption framework for securing big data storage in multi-cloud environment. Evol Intell. 2021 Jun; 14(2): 691–8.
7. Lahmar F, Mezni H. Security-aware multi-cloud service composition by exploiting rough sets and fuzzy FCA. Soft Comput. 2021 Apr; 25(7): 5173–97.
8. Naidu PR, Guruprasad N, Gowda VD. A high-availability and integrity layer for cloud storage, cloud computing security: from single to multi-clouds. In J Phys: Conf Ser. IOP Publishing. 2021 May 1; 1921(1): 012072.
9. Naqvi HH, Alyas T, Tabassum N, Farooq U, Namoun A, Naqvi SA. Comparative analysis: intrusion detection in multi-cloud environment to identify way forward. Int J Adv Trends Comput Sci Eng. 2021 May; 10(3): 2533–2539.
10. Reddy AR. The role of artificial intelligence in proactive cyber threat detection in cloud environments. Neuro Quantology. 2021 Dec; 19(12): 764–73.
11. Nassif AB, Talib MA, Nasir Q, Albadani H, Dakalbab FM. Machine learning for cloud security: a systematic review. IEEE Access. 2021 Jan 25; 9: 20717–35.
12. Komperla RC. Ai-Enhanced Claims Processing: Streamlining Insurance Operations. J Res Adm. 2021; 3(2): 95–106.

