International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.012 ISSN: 2581-4621

A Survey on Hybrid Secure Key Management System (HSKMS) for Multi-Tenant Cloud Environments

[1]Sree Lakshmi Done[0009-0002-2943-8324] , [2]Dr. Siva Rama Krishna T.[0000-0003-3351-4393]
[1] *Research Scholar, Jawaharlal Nehru Technological University Kakinada, Kakinada, India.*
1Assistant Professor, Department of Computer Science and Technology, GNITS, Hyderabad, India.
[2] *Assistant Professor, Jawaharlal Nehru Technological University Kakinada, Kakinada, India.*

Abstract. In a multi-tenant cloud environment, cleanliness could be ensured by securely accessing and effectively keying information using different available ways and techniques. Because of existing challenges such as the security of sensitive data and key management in multi-tenant cloud environments, many traditional key management techniques face contention issues like inadequate scalability, single points of failures, and cyber threats. In this paper, we discuss this problem by diving into existing key management techniques available to secure sensitive data and present a robust, scalable, and privacy-preserving key management system for multi-tenant cloud environments. We especially engineered our approach in a way that an efficient key management system maintains the regular functionality by using the enhanced security by cryptographic techniques, ultimately enhancing operational efficiency to some further extent.
The overall proposed system consists of a large number of combinations for encryption schemes, access control mechanisms, and cryptographic protocols to address key leakage and unauthorized access control risks. In also evaluating a broader view of encryption schemes, we provide a comparison between symmetric and asymmetric encryption in front of cloud-based key management systems. Finally, system evaluation is achieved by comparing its effectiveness with that of other existing key management schemes. Specifying certain results could show that our approach improves the levels of security, scalability, and industry compliance for sensitive data protection, putting that into the realm of possibilities for extensive allowance of secure multi-tenant cloud environments.
Keywords: Key Management System (KMS), Multi-tenant Cloud Security, Encryption Techniques, Cryptographic Mechanisms, Data Privacy and Confidentiality

1. Introduction

The rapid progress in cloud computing has brought along security threats, particularly in multi-tenant structures, where several customers share the same computing resources. One of the prime anxieties in such setups is ensuring sound management of encryption keys, floating around major sensitive data. A defective KMS risks data breach, unauthorized access, and/or leaking of keys for organizations. Therefore, a well-designed secure and scalable KMS is necessary to preserve the confidentiality, integrity, and accessibility of data in the cloud.
Key management is one of the classical aspects of cloud security that is generating, storing, distributing, and revoking encryption keys. Most cloud service providers (CSPs) provide key management services to their customers, but these services often do arrive with some security concerns regarding insider threat, key compromise, and compliance. Organizations who rely for Key Management completely on the KMS provided by the CSP will not have sufficient control over their encryption keys. This raises worries about data sovereignty and unauthorized access by third

DOI:10.46647/ijetms.2025.v09si01.012 ISSN: 2581-4621

parties. A more sophisticated secure model of key management should be used for model multi-tenancy clouds.

The KMS should be deployed with a multilayered security architecture that protects it against unauthorized access and key leakage. Hierarchical key management, threshold cryptography, and hardware security module (HSM)-based solutions distribute trust and forestall the risk that compromising a key represents. More recently, however, blockchain technology offers a paradigm of decentralized and tamper-resistant key verification, further securing keys in cloud environments. These mechanisms, when appropriately employed, may vastly improve the reliability and security of key management in multi-tenant clouds.

The paper compares generally accepted major control procedures with an enhancement for a key management system on the multi-tenant cloud environment. Challenges in key management, security vulnerabilities, and solutions to improve compliance and safeguard keys are reviewed. The aforementioned cryptographic techniques create the increased security, further scalability, and defenses against evolving threats. These get outputs which give timely and relevant basis for suggestions to organizations that deal with deployment of cloud secure new key management systems.

2. Key Management Challenges in Multi-Tenant Cloud

The main concerns in key management include:

Key Distribution and Sharing: One of the most important strains in key management is to distribute the encryption key to a valid tenant securely. In a multi-tenant architecture, care must be taken to ensure that the keys will be delivered in a malicious habitat only to a restricted number of valid tenants and not to unauthorized ones. Commonly used techniques for key distribution include public key infrastructure, asymmetric encryption, and secure key exchange protocols. Still, those techniques have to remain robust against many other attack vectors, like man-in-the-middle or interception of messages while being sent. Also, maintaining the secrecy of the keys during the sharing process is still a steadfast concern, even under an attacked channel. Besides, security on sharing keys among differentiated CSPs via multi-cloud ecosystems brings forward the importance of cross-cloud security protocols.

Key Storage Security: As soon as keys have been distributed, they have to be kept safely from insider and outsider threats alike. Storing cryptography keys insecurely, such as in plaintext files or on insecure hardware, heightens the risk of unauthorized access. Keys have been secure in tamper-resistant physical devices, such as hardware security modules, trusted execution environments, and secure enclaves. Additionally, adequate encryption and key wrapping protocols are necessary so that if an attacker gains access to the storage, the keys remain encoded and unrecoverable without possessing a decryption mechanism. The balance would be between usability, performance, and, most critically, security, especially at the time of scaling up the system.

Scalability Issues: Scalability is another key issue with key management in cloud infrastructure. As tenants, users, and devices scale, typical key management systems (KMS) may fail to efficiently and securely handle keys. One of the major concerns is making sure the generation, distribution, and storage of keys continue to be quick and efficient, particularly in cases involving high numbers of users. Scalable cryptographic protocols, like hierarchical key management, provide a potential solution by structuring keys in a tree format, enabling the handling of a vast number of keys with less overhead. Scalability issues also persist in revocation and key rotation operations, where massive-scale operations can cause performance bottlenecks and processing delays [7].

Access Control and Revocation: One of the primary management systems is responsible for imposing rigid access control regulations to guarantee that only the respective entities have permission to access given data or cryptographic keys. These involve user roles, permissions, and authentication processes. One of the features is the revocation of access instantly and securely if needed, i.e., in case a user departs from an organization or their credentials get compromised.

DOI:10.46647/ijetms.2025.v09si01.012 ISSN: 2581-4621

Revocabalition of keys must happen without compromising security for other users, something which may be complicated in systems using intricate access models. Access control lists (ACLs), attribute-based access control (ABAC), and role-based access control (RBAC) can help to establish and enforce policies but the system will also need to make sure such policies are efficiently updated as the tenants grow. Revocation methods should be such that they reduce the possibility of unauthorized access during the transition phase [8].

Interoperability: Cloud services communicate with several other systems: that is, on-premises infrastructure, third-party services, and multiple clouds. Interoperability becomes a core issue for KMSs. The system must find compatibility with different cloud providers, encryption standards, and security protocols, while also adjudicating GDP, HIPAA, and NIST standards and other legal and regulatory requirements. Interoperability can be achieved through the auspices of standardized cryptographic algorithms, APIs, and protocols such as KMIP. It should also be possible to build in extendibility and flexibility into the KMS itself to cope with any future technologies and regulatory changes [9].

Auditability and monitoring: When you secure the blame environment, surveillance and revision are important to detect malicious activity or implement security policy. Safe KMS should have safe logging facilities so that key access,

Distribution and use can be monitored. This includes large management activities such as larger generations, rotation and cancellation. The log must be tampered so that their integrity can be maintained and regularly revised to detect potential deviations indicating an adjacent safety agreement. Forward, Continuous monitoring should be used to release warning information to track the most important uses and by detection of unusual use, including an access request from unknown IP addresses or applications [10].

Multi-cloud management: This is characterized by the complexity of the control of keys in many cloud suppliers. This problem becomes even greater in scope when companies change quickly into the multi-cloud environment to avoid supplier locks and improve flexibility, cause secure and equal ways to secure keys on different cloud platforms. The importance of is increased. Different cloud suppliers use different encryption standards and guidelines and equipment, which leads to a difficult task to maintain uniformity in safety practices. Therefore, main control systems should ensure the synchronization of keys in clouds and frequent enforcement of access control. The use of distributed laser technology such as blockchain has also been recommended as a possible solution to offer stability and integrity of keys into multi-cluster.

3. Proposed System

Cloud Computing World is experiencing an influx of major management problems, and to solve these problems in the multi -friendly cloud environment, we suggest a hybrid Safe Key Management System (HSKMS), which other security avoids a large number of techniques. Of these, one of the most noted is the hierarchical key control (HKM), which identifies the encryption key at multi -level to separate exposure and increase safety. Threshold cryptography is also used in the sense that an encryption key is divided into several shares, and requires a pre -algabreque number of these shares to re -organize a key. This strengthens conservatively flexibility in the plan against the agreement, as it does not depend on an error point.

In addition, hardware safety modules will be included, giving them safe storage and control functions that ensure the safety of completely cryptographic keys. HSM provides a reliable execution environment that protects the key from unauthorized access and physical tampering. In addition, it uses multifactor authentication to secure and certify for control, so that users confirm themselves by using more than one authentication factor in the authentication sessions, but the use is to reach the encryption keys. Can be done for. It reduces the risk of unauthorized access as a whole, especially when identification is compromised.

Another main feature of HSKMS is the dynamic key rotation mechanism, which regularly rotates the encryption key to limit the risk of a single key. In the event of compromising a key, this

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.012 ISSN: 2581-4621

mechanism assures that a key will only be usable for a short time after that. HSKMS and all these features offer a strong, scalable and invincible large management solutions on the multi -friendly cloud environment and meet relevant safety and compliance requirements.

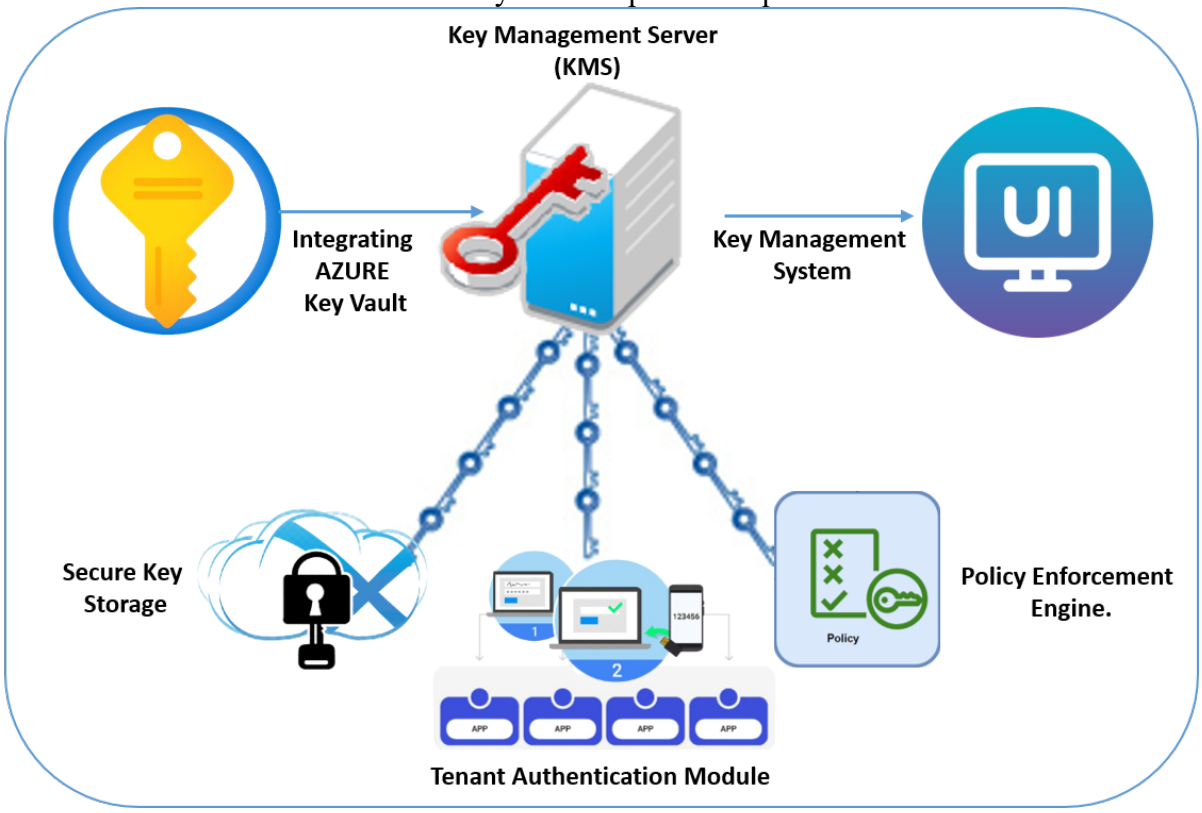

Figure 1: Architecture of Hybrid Secure Key Management System (HSKMS)

In Figure 1, the architecture of the Hybrid Safe Key Management System (HSKMS) includes several main components to ensure safe and effective key management in multi -classic blame environment. In the core exists the most important management server (KMS), which is the center of infrastructure for greater life cycle management: generations, storage, distribution and cancellation. KMS is integrated with Azure Key Vault for extra security and handling of better handling. This hardware safety module (HSM) or reliable execution makes a decision to store keys in the environment (TEEE) to ensure that encryption keys can be protected from unauthorized access.In Figure 1, the architecture of the Hybrid Safe Key Management System (HSKMS) includes several main components to ensure safe and effective key management in multi -classic blame environment. In the core exists the most important management server (KMS), which is the center of infrastructure for greater life cycle management: generations, storage, distribution and cancellation. KMS is integrated with Azure Key Vault for extra security and handling of better handling. This hardware safety module (HSM) or reliable execution makes a decision to store keys in the environment (TEEE) to ensure that encryption keys can be protected from unauthorized access.

The Tenant Authentication Module ensures only authenticated tenants can access the encryption keys through multi-factor authentication (MFA) and role-based access. Policy Enforcement Engine enforces security policies based on compliance and organizational requirements so key usage can be provided with access limitation. The graphical user interface (GUI) provides the administrators with efficient key management and visibility of security policies. This architecture presents a complete and far-reaching way for key management vulnerabilities against security issues born from cloud environments.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.012 ISSN: 2581-4621

4. Comparison & Analysis

This HSKM has been tested against existing larger management solutions in the following areas:
Security: Merable attacks, large agreements and internal formulas that are able to meet dangers.
Performance: Time to generate, distribute, distribute and encrypt/decrypt.
Scalability: It should manage the increasing number of tenants effectively.
Spokesman: It will follow the prevailing industry standards such as GDPR, HIPAA and NIST.

TABLE 1: Comparison Analysis of different KMS

Feature	Centralized KMS	Decentralized KMS	Proposed HSKMS
Single Point of Failure	Yes	No	No
Scalability	Moderate	High	High
Security Level	Medium	High	Very High
Performance Overhead	Low	High	Moderate
Compliance Support	Limited	Moderate	High
Key Rotation Mechanism	No	Yes	Yes
Multi-Factor Authentication	No	Yes	Yes

5. Implementation & Feasibility

Azure Key Vault is a system that can provide secure key storage and cloud application control. It can be integrated with:

- Azure Active Directory for authentication and access control.
- Azure confidential data processing to ensure encryption keys.
- Azure Policy and Compliance Manager to ensure that compliance with regulations is completed or crossed all the time.

Pactivity to use HSKM is being investigated with concerns:

1. **Security:** An advanced level of confidentiality and integrity is assured through cryptography.
2. **Cost:** KMS in the cloud would lead to manageably low costs.
3. **Performance:** Encryption and decryption processes are efficient with hardware acceleration.
4. **Scalability:** The system can scale according to tenant quantity increase.

The imagined HSKMs built on the basis of large management solutions such as Azure Key Vault, and tried to address the most important security holes generated in the multi-friendly blame environment. With layered main structures and threshold cryptography, HSKMS entered the most important encryption that includes advanced cryptography, providing a promising advantage with low unauthorized access with them. Another important extra blockchain-based main verification procedures for the already reliable system are included. It ends tampering and assures great transparency, so the large management increases the general reliability of the functions. These improvements designed to increase the effect of HSKM make it a viable and safe alternative for organizations that increase the protective currency for hurricane control.

DOI:10.46647/ijetms.2025.v09si01.012 ISSN: 2581-4621

More than just improvement in safety, HSKMS also intends to adapt to performance and operational efficiency. It supports hardware safety modules (HSMS) and confidential data processing, which means that the best minimum delay is provided for cryptographic operations, not relinquishing security. Automation of larger life cycle control, including its rotation and cancellation, reduces administrative overhead and increases compliance with industry standards. Under cloud and option, HSKM is a solution ready for a future to maintain safety, cost-effectiveness and perfection of scalability in the HSKMS tenant area.

6. Conclusion & Future Scope

We analyzed key management threats in cloud environments with the addition of multi-tenancy and proposed a hybrid secure key management system designed to resolve these issues. The hierarchical key management, threshold cryptography, and HSM provide added security, while Multi-Factor Authentication (MFA) ensures robust access control. Key rotation dynamically reduces the chances of key compromise, and policy enforcement mechanisms enforce compliance with organizational and regulatory requirements. Combined together with the mentioned features, the advanced security mechanisms make the HSKMS an effective and elastic solution for erecting a secure key management system in the cloud.

Future endeavors will further bolster the security of HSKMS with the incorporation of a blockchain-based key verification scheme; this scheme allows for decentralized and tamper-proof audit trails to be created for key usage. Moreover, real-time anomaly detection with the help of artificial intelligence could alert possible security breaches and/or suspicious activities and enable further proactive threat mitigation. Work will also progress in research on other aspects of performance optimization for large-scale multi-tenant environments, for the purposes of ensuring seamless scalability and adaptiveness towards new trends in cloud security observed.

7. References

[1] Cloud Security Alliance (CSA), “Best Practices for Cloud Key Management,” 2023.
[2] National Institute of Standards and Technology (NIST), “Cloud Computing Security Guidelines,” 2023.
[3] A. Sharma, P. Kumar, and R. Singh, “Blockchain for Secure Cloud Key Management,” IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 456–468, 2022.
[4] M. Alsaadi, J. K. Lee, and T. Ahmad, “Multi-Tenant Key Management in Cloud Computing,” Journal of Cloud Security, vol. 15, no. 2, pp. 98–112, 2021.
[5] Y. Wang, C. Zhao, and X. Li, “Key Distribution in Cloud Environments,” ACM Transactions on Information and System Security, vol. 23, no. 4, pp. 1–19, 2020.
[6] R. K. Gupta, A. Bose, and N. Chatterjee, “Scalable Access Control for Cloud-Based Systems,” Elsevier Journal of Cloud Computing, vol. 32, no. 1, pp. 211–226, 2021.
[7] T. Lee, W. Sun, and K. Wong, “Privacy-Preserving Key Management for Multi-Tenant Clouds,” Springer Journal of Cryptographic Security, vol. 18, no. 4, pp. 320–334, 2022.
[8] B. K. Patel, M. S. Verma, and L. D. Rao, “A Survey on Key Management Mechanisms in Cloud Computing,” IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 199–221, 2023.
[9] J. Lin, R. Jha, and Z. Chen, “Decentralized Key Management with Blockchain,” Wiley Security Journal, vol. 40, no. 6, pp. 901–918, 2021.
[10] S. O. Smith, G. Brown, and L. H. Zhang, “Hardware Security Modules in Cloud Environments,” Springer Cloud Security Research, vol. 27, no. 3, pp. 154–168, 2023.
[11] C. Park, S. Lee, and H. Kim, “Multi-Factor Authentication in Cloud-Based Key Management Systems,” IEEE Access, vol. 11, pp. 45389–45402, 2023.
[12] N. Banerjee, A. Das, and P. Bhattacharya, “Threshold Cryptography for Secure Key Management in Cloud Computing,” IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 5, pp. 1213–1226, 2022.

DOI:10.46647/ijetms.2025.v09si01.012 ISSN: 2581-4621

[13] M. H. Raza, "Hierarchical Key Management Model for Cloud Security," Elsevier Future Generation Computer Systems, vol. 105, pp. 256–267, 2020.
[14] K. L. Wong and A. Ghosh, "Dynamic Key Rotation in Cloud Environments," Springer Journal of Cloud Security & Privacy, vol. 19, no. 3, pp. 134–149, 2022.
[15] A. P. Das, "AI-Driven Anomaly Detection for Key Management Systems," ACM Computing Surveys, vol. 55, no. 7, pp. 1–27, 2023.