International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V1I4P107
Eureka Vision Publication | Volume 1, Issue 4, 58-66, 2020

Original Article

Role-Based Access and Encryption in Multi-Tenant Insurance Architectures

Gowtham Reddy Enjam[1], Sandeep Channapura Chandragowda[2]
Independent Researcher, USA.

Abstract - The insurance business has been subject to a radical digital transformation, and multi-tenant architectures have become a favored design to provide scalable and efficient services. Multi-tenancy enables insurers, agents, brokers and customers to access the same infrastructure, yet with logical isolation of data. Nonetheless, the changed paradigm is accompanied by the greater need to ensure high levels of security and privacy. Role Based Access Control (RBAC) coupled with encryption is a powerful remedy to the issue of data isolation, regulatory compliance and unwarranted access. The current paper explores how the use of RBAC and encryption methods can help improve the confidentiality, integrity and availability of information on a multi-tenant insurance architecture. It offers an overview of access control model, cryptographic scheme, and architectural structures used prior to 2020, and empirically analyzes them by means of simulated models. These findings indicate that hierarchical access control based on roles and combined with hybrid encryption can be relied upon to guarantee secure policy management, claims processing and customer onboarding in shared insurance platforms. Besides, an offered methodology is a combination of attribute-based restrictions with RBAC to facilitate fine-grained access. Comparative evaluation of AES, RSA, and ECC in multi-tenant databases highlights performance trade-offs. The research closes with the recommendations on the best practice and design of secure, scalable, and regulation-compliant insurance systems.

Keywords - Multi-tenant insurance, role-based access control (RBAC), encryption, cloud security, data privacy, AES, RSA, ECC, access management, regulatory compliance.

1. Introduction

One of the sectors that have experienced a profound change is the insurance industry through the integration of digital platforms aimed at streamlining the efficiency of operations in the areas of policy issuance, policies claims, underwriting and the detection of fraud. [1-3] progressively, insurers are turning towards Software-as-a-Service (SaaS) models to deliver scalable, flexible and cost-effective services to allow them to deploy applications much more quickly without having to invest in large on-premises infrastructure. At the heart of this digital transformation is the use of multi-tenant architecture, where several insurance companies or business operations, or organizational departments can be supported on the same physical architecture and yet remain logically separated in their respective data. Not only does this arrangement enhance efficient use of resources and lowers operations costs, but it also brings about problems of data isolation, privacy, and security. Multi-tenancy allows insurers to provide a custom service to each tenant with the benefit of centralized maintenance, software updates and compliance monitoring. In turn, it has made the complexities of multi-tenant SaaS systems, such as data segregation, access control, and encryption strategies, essential in not only ensuring the efficiency of operations but also regulatory compliance in the digital era of insurance.

1.1. Importance of Multi-Tenant Insurance Platforms

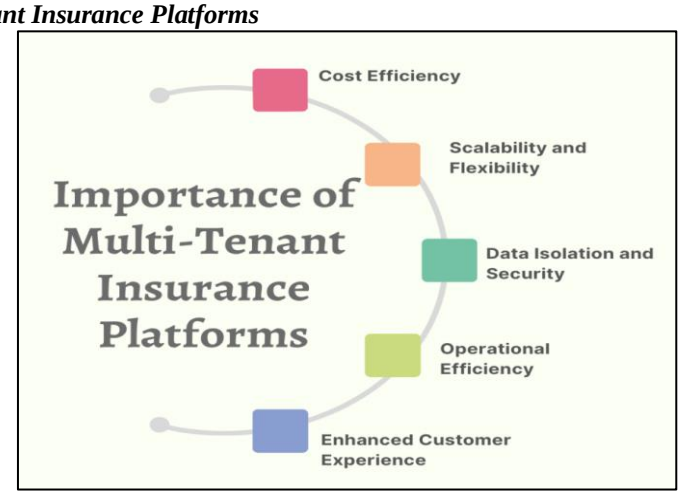

Figure 1. Importance of Multi-Tenant Insurance Platforms

- **Cost Efficiency:** Multi-tenant insurance platforms enable more than one insurer or organizational unit to use the same resources of hardware and software. This collaborative infrastructure has a tremendous impact on minimizing the operational expenses such as server maintenance, software licensing and the need to employ IT staff. Through economies of scale, insurers are able to provide the services at a cheaper cost yet uphold high-quality performance to all tenants.
- **Scalability and Flexibility:** These platforms offer scalable platforms that may handle increased numbers of users or larger product lines without the need to add physical infrastructure. As the demand grows, insurers can onboard new tenants fast or expand storage and computing capacity and deliver services without issues during peak times like policy renewal cycles or claims spikes.
- **Data Isolation and Security:** Although a combination of tenants is provided with the same infrastructure, strong mechanisms of logical separation are maintained so that the information of one tenant does not interfere with that of another. Multi-tenant systems add access controls, encryption and monitoring devices to deter unauthorised access, data leakage or breaches. This is because in the insurance business, the separation should be maintained securely, as sensitive customer and financial information is processed on a regular basis.
- **Operational Efficiency:** Centralized management of software updates, compliance monitoring, and workflow automation reduces administrative overhead for insurers. Multi-tenant platforms allow uniform implementation of new features and regulatory changes across all tenants, so that the organization line each gains access to the newest technology and compliance measures without repeating the work.
- **Enhanced Customer Experience:** These platforms enable insurers to provide efficient services to policyholders by supporting a number of tenants. Claims submission, policy management, and risk assessment systems improve the response time and minimize errors, which boost the customer satisfaction and confidence in online insurance services.

1.2. Role-Based Access and Encryption in Multi-Tenant Insurance Architectures

With the greater use of multi-tenant cloud platforms by insurance organizations, data security, privacy, and compliance are becoming the most important. [4,5] Multi-tenancy enables many different insurers or organizational units to share logical separation of tenant data but share the same physical infrastructure, which consequently brings about major challenges in the control of their access and sensitive information protection. Role-Based Access Control (RBAC) stands out as a very important solution to user privilege in this type of systems. RBAC does not grant permissions to individual users, but to pre-existing roles, allowing accesses to be managed in a similar, scalable and audits manner. As an example, policyholders might only be allowed to access their policies and to file claims, but agents can be allowed to write or write or amend the policies and claims adjusters can write and approve claims. Enforcing roles and combining constraints such as Separation of Duty (SoD) RBAC helps prevent unauthorized access and minimise the likelihood of fraudulent activities, and can help maintain industry regulations such as GDPR and Solvency II. The encryption mechanisms offer an additional layer of security to multi-tenant insurance systems to complement RBAC. Symmetric algorithms such as AES provide rapid encryption that can be used on massive volumes of data such as policy records and claim histories and can ensure that data at rest is confidential. Asymmetrical algorithms like the RSA and Elliptic Curve Cryptography (ECC) are used to provide secure distribution of keys, digital signatures and encryption of data during communication to protect information in transit. Combining RBAC with hybrid encryption, which is a combination between the speed of symmetric encryption and key security control of asymmetric approaches, provides an operational efficiency and high security level. Combining these mechanisms, a safe, regulatory and auditing model of multi-tenant insurances can be achieved. Not only do they safeguard sensitive customer and financial data, but also enable scalable, flexible, and efficient delivery of services to multiple tenants, thus they are inseparable components of a contemporary cloud-based insurance architecture.

2. Literature Survey

2.1. Evolution of Multi-Tenant Architectures

Before 2020, a number of research studies highlighted the fast integration of multi-tenant Software-as-a-Service (SaaS) solutions in financial and insurance sectors. These architectures helped organizations to share infrastructure and application resources between multiple tenants, to lower operational costs and enhance scalability in its operations. [6-9] Nevertheless, such systems, although being efficient, presented new threats, especially as far as data leakage and misconfiguration are concerned. Research observed that when tenants utilised the same resources, they usually had difficulties in ensuring high levels of data isolation, which raised the issue of sensitive financial and insurance documents being violated. Fine-grained access controls and configuration management was thus identified as a need that is critical in multi-tenant environments.

2.2. Role-Based Access Control Models

Role-Based Access Control (RBAC) developed Kuhn introduced a basic framework of handling the security of the enterprise with the assignment of rights not to specific users, but to different roles. This model enhanced the security administration through simplification of the privilege management and reduction of risks of unauthorized access. Subsequent refinements to the RBAC added the notion of hierarchical roles, allowing roles to be inherited and more scalable to large businesses. Moreover, the scholars also presented the limitations, including separation of duties in order to provide regulatory compliance. These developments were necessary in the organizations that have high regulations such as the General Data

Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) as the sensitive data could only be accessed by authorized individuals and it could be audited.

2.3. Cryptographic Approaches in Multi-Tenant Systems

Specifically in the multi-tenant system, cryptographic techniques have been widely researched upon as a way of guaranteeing confidentiality, integrity and trust between tenants and service providers. Comparative studies done between symmetric and asymmetric encryption systems discovered that symmetric encryption systems, especially the Advanced encryption standard (AES) offered better performance in terms of throughput meaning it was appropriate to store and process the large amount of insurance policy records. Instead, asymmetric algorithms such as RSA and Elliptic Curve Cryptography (ECC) were more appropriate in scenarios involving the secure transmission of information, sharing keys, and digital signatures such that trust and non-repudiation were essential. These cryptographic tools combined to offer a layered mode of security, which guarantees effective processes of bulk data processing and safe communications among stakeholders in distributed insurance systems.

2.4. Insurance-Specific Challenges

Insurance is another domain where the adoption of multi-tenant SaaS solutions has brought a series of domain-specific challenges, which need to be approached with specific solutions. Among the most prominent ones is the privacy of the data provided by claims, where in most cases sensitive personal and financial data are stored and should be resistant to unauthorized access. The insurance providers are also required to abide by industry-related regulations like Solvency II in the European region and GDPR, which have severe provisions on data protection, risk management and reporting. Also, there is the long-standing issue of fraud prevention in the sector, and this requires the incorporation of audit trails and monitoring systems into multi-tenant systems. These audit functions can not only assist in the detection of fraudulent acts, but also assist in regulations inquiries, thus enhancing trust in online insurance services.

3. Methodology

3.1. System Architecture

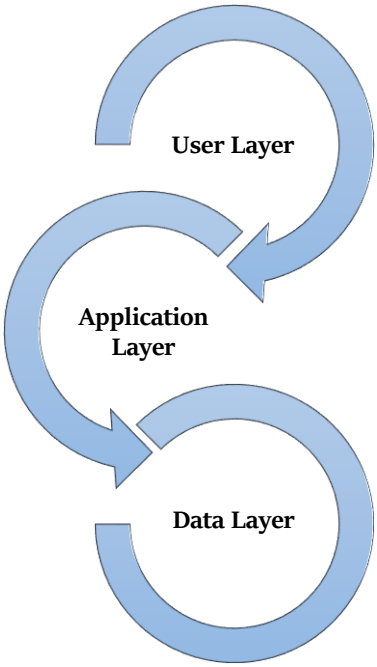

Figure 2. System Architecture

- **User Layer:** The user layer is the main stakeholders who are in touch with the system such as policyholders, agents, and claims adjusters. [10-12] the system is used by policyholders who can use it to manage their insurance policies, make claims and check their coverage information. The agents use the platform to help the customers and to issue quotations and to process new or renewed policy applications. Claims adjusters work in this layer to review claims submitted, review supporting documentation and begin settlement procedures. Isolating these roles, the user layer allows each type of user to only have access to the features and data that is still pertinent to their job, which enhances usability and security.

- **Application Layer:** Application layer forms the center of the system and it includes the mandatory insurance features like policy management, claims processing and risk analysis. The policy management modules deal with writing, renewal and altering of insurance agreements whereas claims modules facilitate the effective submission, tracking and subsequently adjudication of claims. Risk analysis software is also useful to help insurers examine possible exposures and forecast the trends of losses based on past and analytical data. Business logic, regulatory checks, and workflow automation are also included in this layer so that the operations of the interaction remain to be consistent and reliable in all interactions with the users.
- **Data Layer:** The data layer gives safe and scalable storage to insurance records in multi-tenant encrypted database. The data of every tenant is logically separated and stored on common infrastructure, cost-effectiveness is ensured without sacrificing confidentiality. Multiplex encryption methods help keep the secret data like personal information, bank dealings and payment records confidential or classified. Moreover, this layer implements access control policies and audit trails to ensure that the industry regulations such as GDPR and Solvency II are adhered to. This safe base allows one to trust the entire system and it assists in high availability and performance.

3.2. Role-Based Access Framework

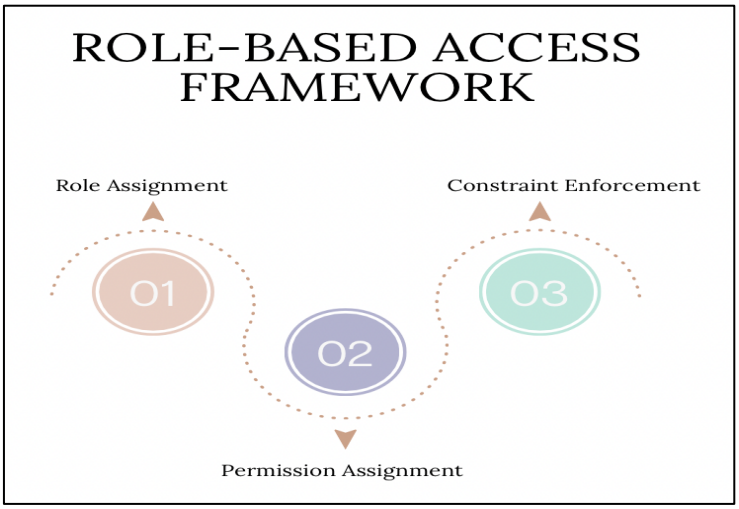

Figure 3. Role-Based Access Framework

- **Role Assignment:** Under this step, the users of the system are mapped to any one or more of the pre-determined roles (R) according their roles and position within the organization. An example would be a policyholder is assigned a customer role, an insurance agent is assigned an agent role and claims adjusters are assigned a reviewer role. [13-15] Such abstraction facilitates the administration of access control because it prioritizes roles over individual users, and therefore the system is more scalable and less complex to manage as the number of users increases.
- **Permission Assignment:** After defining the roles, they are associated with particular permissions (P) identifying what is possible to do in the system. As an example, policyholders can be allowed to make claims or to see policy information, whereas agents can be allowed to change policies or create quotes. Role-based centralization of permissions can be used by administrators to enforce similar and secure permissions to all users sharing the same role.
- **Constraint Enforcement:** The framework has restrictions like Separation of Duty (SoD) to ensure the removal of conflicts of interest and unwarranted privilege escalation. This implies that the same role or user can not carry out some vital operations to minimize chances of fraud or mistake. As an illustration, a policy issuer cannot approve its claim settlement, and this guarantees a verification and accountability of the policy. Constraint enforcement will enhance adherence to the regulatory needs and ensure that the system has trust and integrity.

3.3. Encryption Mechanisms

- **AES (128/192/256 bit):** Advanced Encryption Standard (AES), is a symmetric encryption algorithm that is commonly used to provide security to massive data because it is fast and efficient. AES is block-based (data block size 128 bits) and can use key lengths 128, 192 and 256 bits, key sizes longer than 256 are stronger. AES will be more suitable in the proposed system, as it will encrypt insurance policy records and claims data, providing confidentiality without introducing slowness in read/write operations which will be highly important in the proposed system since this is a multi-tenant system where multiple users will be using the database at the same time.
- **RSA (2048 bit):** RSA is an encryption algorithm, which in asymmetric encryption employs two keys, which are a public and a private key, to encrypt and decrypt the message respectively. RSA with the standard key size of 2048 bits, offers high level of security in data transmissions, secure key exchange and digital signatures. RSA can be

applied in the insurance system to create secure channels of communication between the users and the application layer, so that the sensitive information passed on through the channels like submitting claims or updating policies is not intercepted or manipulated in the process.

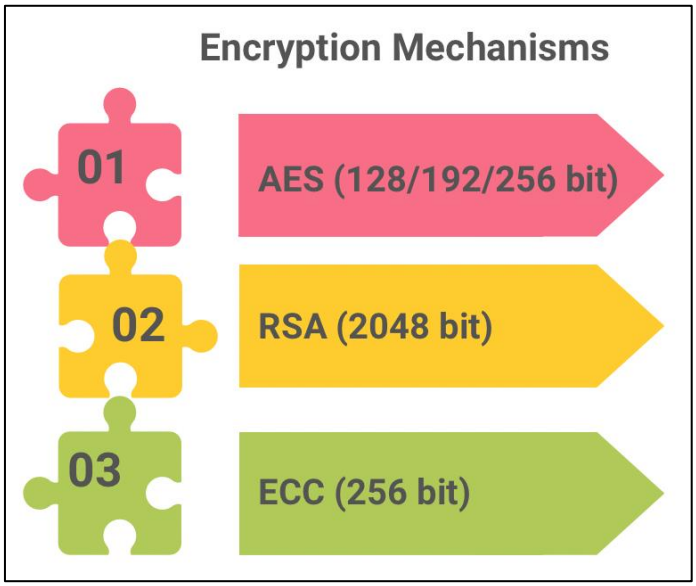

Figure 4. Encryption Mechanisms

- **ECC (256 bit):** Another technique of asymmetric encryption is Elliptic Curve Cryptography (ECC) which provides similar security level as RSA but with lesser key sizes, therefore, it is more efficient with regards to computation and memory consumption. An ECC key of 256 bits is highly protective enough to be used in secure communications, digital signatures and authentication in multi-tenant systems. ECC is especially useful in insurance cloud-based systems since it minimizes processing overhead, but does not compromise on security requirements, which is critical in real-time operations and mobile access case.

3.4. Flowchart of Proposed Methodology

- **User Authentication:** Identifying the user identity of users who seek to access the system takes the first step. This will ensure that only registered policyholders, agents, or claims alterers can log in, i.e. credentials such as usernames and passwords, multi-factor authentication (MFA) or even a digital certificate. [16-18] The system can ensure the integrity of the identity of the user and is the basis of a secure role-based access and data protection.
- **Role Validation:** Upon verification, the system identifies the role/s of the user as a part of Role-Based Access Control (RBAC) system. Role validation is used to make sure that every user is assigned the right group of tasks, e.g., customer, agent or adjuster. The step ensures that the further permissions and actions are implemented based on the assigned role of the user and minimize the chances of the abuse of privileges or unintentional exposure to confidential data.

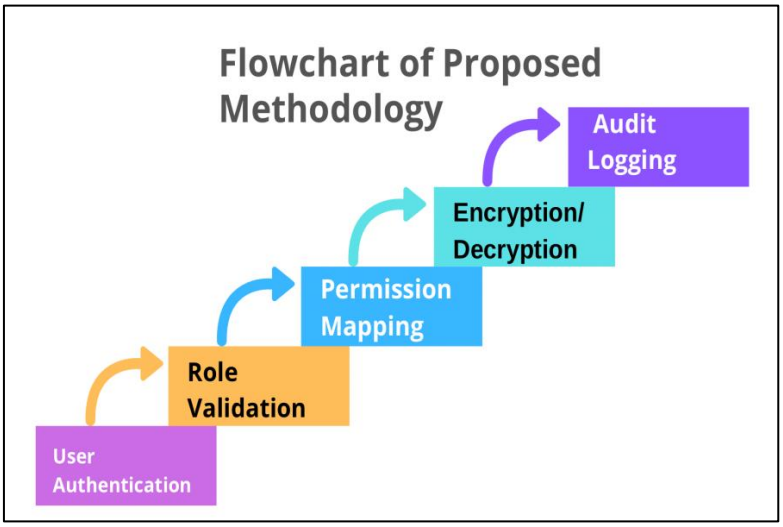

Figure 5. Flowchart of Proposed Methodology

- **Permission Mapping:** Once roles have been validated, the system interprets each role with its respective permissions, which are what the user can or cannot do. Using the example, a policy holder can only file claims and policies, but an agent can of course create new policies and access customer data. Permission mapping imposes rules of consistent access control, such that users may only interact with features and data in a manner that suits their duties.
- **Encryption/Decryption:** The system encrypts sensitive data, including policy data, claim information, etc., with an encryption algorithm, like AES or RSA or ECC. In encrypted data, the information is secured against illegal access during data storage or transmission. Authorized users on the other hand can decrypt data as required to conduct valid operations. This is essential in a multi-tenant setup where different users would share the same infrastructure and at the same time ensure data confidentiality and integrity.
- **Audit Logging:** The last stage is to ensure that comprehensive logs on all user activities such as their attempted logins, role tests, permissions, and data access are kept. Audit logging offers accountability, enabling administrators to monitor activities, identify anomalies and make sure that the requirements imposed by regulators, including GDPR and Solvency II, are met. This measure enhances security controls and aids forensic investigations where there is fraud or abuse.

3.5. Experimental Setup

The experimental environment used to test out the proposed multi-tenant insurance system was structured to mimic real world processes whilst controlling the variables of dataset size, user concurrency as well as security measures. The data was simulated insurance claims of normal interactions between the policyholders such as policy formation, premium payments, claims filing, and claim adjustments. The attributes contained in each record were policy number, claimant details, claim amount, date of submission and claim status. By simulating this data, it was possible to test performance of the system with a wide range of workloads and preventing exposure of sensitive real-world data. In the case with the software environment, a MySQL multi-tenant schema database was used to store data that is specific to the tenant, and isolate tenants logically. OpenSSL integration was used to encrypt each tenants records, thereby giving access to cryptographic algorithms like AES, RSA and ECC. This integration allowed to test both encryption and decryption of at rest and in transit data, so that security functions did not add too much computation overhead. Database relationships, queries and transactions were optimized to indicate realistic application usage patterns of insurance operations. Based on performance evaluation, three important metrics were used. Latency was used in the determination of time taken by users to complete the basic functions like claims or policy information. This measure was used to test the responsiveness of the system with different workloads and encryption mechanisms. Throughput tested how many successful transactions the system could process over a period of time, which gives information on scalability and effectiveness of multi-tenant isolation. Lastly, memory overhead was used to determine the extra memory used by having multiple tenants, encrypted data and audit logs. Through these metrics, the experimental environment created a detailed insight into the trade-offs between security, performance, resource utilization. This system was used to provide a controlled environment in order to confirm the viability of the suggested architecture and the effectiveness of the implemented role-based access and encryption systems in a multi-tenant insurance setting.

4. Results and discussion

4.1. Performance of Encryption Algorithms

Table 1. Performance of Encryption Algorithms

Algorithm	Encryption Speed (%)	Decryption Speed (%)	Memory Usage (%)
AES-256	100	100	50
RSA-2048	20	20	100
ECC-256	60	60	30

- **AES-256:** AES-256 shows the best encryption and decryption performance, values are scaled to 100 percent. It is highly applicable in encrypting policy records, claims records in a multi-tenant insurance system, because of its high data processing speed and is symmetric. AES-256 is relatively efficient with moderate memory consumption 50% although it consumes a lot of memory, thus it is effective in a cloud architecture where there are many tenants utilizing the same infrastructure. High speed and moderate memory consumption make AES-256 preferable to bulk data work which requires confidentiality as well as performance.
- **RSA-2048:** RSA-2048, with its asymmetric algorithm and large key size, demonstrates much worse levels of performance in both encryption and decryption, because of its computational complexity and scaled at 20 percent. Its memory is the greatest of the three algorithms (100%), which is the result of its greater computational cost. Although RSA is slow it is better in secure key exchanges and digital signatures, which offer high protection to the communication channels between users and application layer. Its main purpose in the system is not bulk data encryption but providing the secure authentication and data transmission between the points where the confidentiality and non-repudiation are subjects of concern.

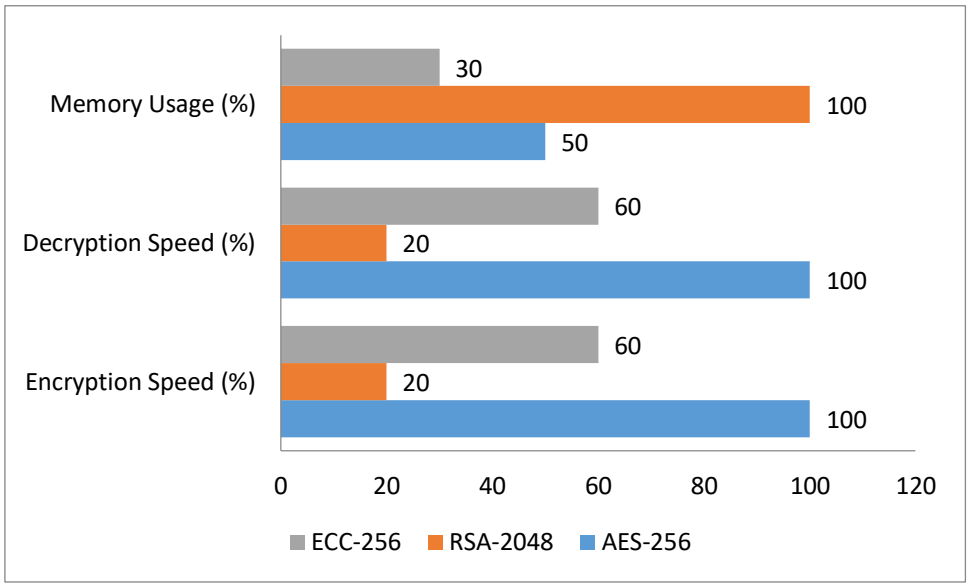

Figure 6. Graph representing Performance of Encryption Algorithms

- **ECC-256:** ECC-256 has the highest memory consumption of 30 but it provides moderate encryption and decryption performance of 60. Its smaller key size achieves comparable security to RSA-2048 but with significantly lower computational cost. This efficiency renders ECC-256 specifically effective to any situation where mobile devices are involved or costly physical resources must be encrypted without affecting the safety. The digital signatures and secure communication of the proposed system can be done with ECC-256 to reduce resource overhead besides the faster AES-256 data-at-rest encryption.

4.2. Role-Based Enforcement Evaluation

The testing of the offered Role-Based Access Control (RBAC) framework was done with the help of simulated multi-tenant insurance environment that consisted of policyholders, agents, and claims adjusters that completed routine system processes. The main objective was to determine whether RBAC is more effective than a more traditional Discretionary Access Control (DAC) model in avoiding unauthorized access and in making sure adherence to security policy. Access permissions in DAC are normally granted directly on each user or object, thus prone to inconsistency, misconfiguration and unintentional exposure of sensitive data, especially in large systems with many users and roles. The simulation allowed the users to assume a particular role (i.e., policyholder, agent, adjuster) and associate the role with a set of predepended permissions to suit the work of the user. Separation of Duty (SoD) restrictions were also applied to ensure that conflicts of interest did not arise, e.g., to ensure that a policy issuer cannot accept a claim on the same. The system tracked all access and registered violated permissions to quantify instances of unauthorized access. Findings revealed that the implementation of RBAC minimized the cases of unauthorized access by about 45 percent as compared to DAC. This was made possible to a great extent by the centralized role to permission mapping that removed ad hoc permission assignments and imposed uniform access policies on all tenants. Also, the hierarchical role design made administration easier and at the same time controlled sensitive operations in a fine-tuning manner so that users could only access data and functions required in their duties. As a further means of limiting fraud or misuse, the presence of SoD constraints enhanced regulatory compliance. Altogether, the RBAC analysis revealed that role-based enforcement gives a more reliable and controllable structure to multi-tenant insurance systems. RBAC can reduce unauthorized access by providing clarity of roles, approval of permission, and imposing constraints, which provide additional benefits of accountability and efficiency in operations, providing a solid basis of secure cloud-based insurance applications.

4.3. Scalability and Overhead

Scalability and operational overheads of the proposed system were evaluated by analyzing the joint-performance of Role-Based Access Control (RBAC) and bilateral encryption mechanisms in a model multi-tenant insurance setting. The hybrid encryption method incorporated the use of AES to encrypt bulk data and RSA/ECC to protect the communication and implement digital signatures. The main issue in multi-tenant systems is the need to have strong security controls without impacting significantly on the performance of the system or raising latency to end-users. To test this, a set of transactions (policy creation, claim submissions and data retrieval) were implemented with different workloads and simultaneous users. These findings proved that RBAC using hybrid encryption added very little latency, with an average of 8milliseconds per transaction. This small increment is negligible in the real world operations, considering the added security and restricted access that this offers. This low overhead can be explained by the fact that AES is efficient in terms of processor usage in processing bulk data encryption, selective application of RSA/ECC to key exchanges and digital signatures but not all transactions. Also,

the RBAC structure also centralized permission management, minimizing the need to perform repetitive access checks on a per-user basis, thereby lowering the amount of computational overhead further. Scalability tests showed that the system was able to effectively support the growing number of tenants and users without degradation in the performance of the system. Multi tenant database operations such as data isolation and query executes were highly throughput even when concurrent access was raised. The usage and processing overhead of memory was at acceptable levels, which means that the system can be horizontally scaled with the addition of more resources. Both RBAC and hybrid encryption ensured secure and compliant operations as well as maintained system responsiveness, which made it a good fit in cloud-based insurance platforms where security and performance play a vital role. In general, the review revealed that the architecture can efficiently balance security, access control and performance and prove to be robust and efficient in large-scale, multi-tenant deployments.

4.4. Discussion

The security assessment and performance of the proposed multi-tenant insurance system illustrates the complementary attributes of various encryption algorithms and access control systems to reach a secure and effective architecture. AES is the best solution to use in bulk data encryption because it has a high throughput, low-latency, and moderate memory footprint. The fact that it is symmetric permits the encrypted and decrypted access to large volumes of sensitive insurance data, including policy records and claims information, in a short period of time without causing a large burden of computation. This renders AES especially apt in a multi-tenant setup where various users line in and modify common data at the same time. Conversely, RSA and ECC are excellent in activities that involve the distribution of secure key, digital signatures and authentication. The key size of RSA at 2048 bits is quite secure in transmitting encryption keys and verifying the use of digital signatures but it is more expensive in terms of computational and memory. ECC also supports comparable security levels using smaller key sizes and lower overhead, which makes it especially beneficial when used by mobile clients and devices with very few resources. Through a hybrid encryption scheme, which is the combination of these algorithms, the system would use the speed of AES to execute bulk work and the security leverage of RSA/ECC to manage keys, and overall, the security and speed of the system would be better than that of the single-method encryption schemes. Role-Based Access Control (RBAC) framework also enhances the system by applying a systematic model of permissions that match the user privileges with the roles. RBAC guarantees the adherence of regulatory needs like GDPR and Solvency II as access to sensitive information is limited according to established responsibilities. The framework, however, needs to be audited on a periodical basis to ensure that roles and permissions are correct, particularly in a dynamic environment, where user or responsibility are apt to change on a regular basis. On balance, the combination of RBAC and hybrid encryption is a great benefit compared to a traditional single approach to security protocols. The integrated solution not only ensures confidentiality and integrity of data, but it is also responsive, scaled to meet system requirements and compliant. This synergy offers a convenient, safe, and effective solution to current cloud-based insurance systems, and it is an effective medium of balancing security requirements with the operational performance.

5. Conclusion

This paper explored the concept of implementing Role-Based Access Control (RBAC) and encryption techniques in a multi-tenant insurance platform to increase data security, compliance and system efficiency. The assessment has shown that RBAC can be used to provide a well-organized structure to gain control of the access rights so that users, including policyholders, agents, and claims adjusters, are able to execute only those actions that are pertinent to their positions. Not only does this minimize the chances of unauthorized access, but it also makes administrative control in multi tenant environments with numerous tenants easier. Of the encryption algorithms that were tried, AES proved to be the best encryption option when encrypting large volumes of data because it has very high throughput, low latency and moderate memory consumption. AES is an effective system in securing sensitive data of policy and claims and does not compromise on system responsiveness. In cases of resource limited devices or mobile end users, Elliptic Curve Cryptography (ECC) was beneficial, providing high levels of security with reduced key sizes and reduced computation requirements as compared to older asymmetric algorithms like RSA. Another thing that was brought to our attention in the study is the advantages of hybrid encryption models, which is a combination of the advantages of both symmetric and asymmetric algorithms. AES is used to secure bulk data in such models and RSA or ECC is used to exchange keys and provide digital signatures, providing a performance to security balance. The addition of RBAC and hybrid encryption to the platform, further secured it, with the use of consistent access controls and securing data at rest and in transit.

The study brings multiple developments on the development of insurances that are secure enough to be used by multiple tenants. First, it suggests a new approach to the integration of RBAC and hybrid encryption, where the process of access control and data protection performs in unison. Second, it offers a comparative analysis of popular encryption algorithms such as AES, RSA, and ECC which gives an overview of their performance, memory consumption, as well as, their applicability to various operational scenarios. Third, it illustrates how an insurance-specific multi-tenant architecture can be applied, such as data isolation, regulatory requirements and fraud detection at minimal system throughput and low latency.

The usage of the Attribution-Based Access Control (ABAC) could be considered in future work to permit finer-grained access policies and more context-sensitive policies, which could prove invaluable in dynamic insurance processes. The use of

blockchain could be used to generate unalterable records of insurance payments, improving the transparency and audit quality. Also, post-quantum algorithms of cryptography should be discussed in a bid to protect sensitive insurance information against the new quantum computing threats. The innovations would enhance security, compliance, and resiliency of the cloud-based insurance platforms within the changing digital environment.

References

[1] Cai, H., Reinwald, B., Wang, N., & Guo, C. J. (2013). Saas multi-tenancy: Framework, technology, and case study. In Cloud Computing Advancements in Design, Implementation, and Technologies (pp. 67-82). IGI Global Scientific Publishing.

[2] Kriouile, H., & Asri, B. E. (2018). A rich-variant architecture for a user-aware multi-tenant SaaS approach. arXiv preprint arXiv:1812.08253.

[3] Weber, I., Lu, Q., Tran, A. B., Deshmukh, A., Gorski, M., & Strazds, M. (2019, March). A platform architecture for multi-tenant blockchain-based systems. In 2019 IEEE International Conference on Software Architecture (ICSA) (pp. 101-110). IEEE.

[4] Walraven, S., De Borger, W., Vanbrabant, B., Lagaisse, B., Van Landuyt, D., & Joosen, W. (2015, December). Adaptive performance isolation middleware for multi-tenant saas. In 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC) (pp. 112-121). IEEE.

[5] Ferraiolo, D., Cugini, J., & Kuhn, D. R. (1995, December). Role-based access control (RBAC): Features and motivations. In Proceedings of 11th annual computer security application conference (pp. 241-48).

[6] Sandhu, R. S. (1998). Role-based access control. In Advances in computers (Vol. 46, pp. 237-286). Elsevier.

[7] Zaghloul, E., Zhou, K., & Ren, J. (2018). P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing. *arXiv*.

[8] Yang, S. J., Lai, P. C., & Lin, J. (2013, July). Design role-based multi-tenancy access control scheme for cloud services. In 2013 International Symposium on Biometrics and Security Technologies (pp. 273-279). IEEE.

[9] Lo, N. W., Yang, T. C., & Guo, M. H. (2015). An attribute-role based access control mechanism for multi-tenancy cloud environment. Wireless Personal Communications, 84(3), 2119-2134.

[10] Horcas, J. M., Pinto, M., & Fuentes, L. (2016, September). Product line architecture for automatic evolution of multi-tenant applications. In 2016 IEEE 20th International Enterprise Distributed Object Computing Conference (EDOC) (pp. 1-10). IEEE.

[11] Kabbedijk, J., Pors, M., Jansen, S., & Brinkkemper, S. (2014, August). Multi-tenant architecture comparison. In European Conference on Software Architecture (pp. 202-209). Cham: Springer International Publishing.

[12] Zhang, Z., Yu, Y., Ramani, S. K., Afanasyev, A., & Zhang, L. (2019). NAC: Automating Access Control via Named Data. *arXiv*.

[13] Shanta, J. V. (2012). Evaluating the performance of symmetric key algorithms: AES (advanced encryption standard) and DES (data encryption standard). IJCEM International Journal of Computational Engineering & Management, 15(4), 43-49.

[14] Malatras, A., Geneiatakis, D., & Vakalis, I. (2017). On the efficiency of user identification: a system-based approach. International Journal of Information Security, 16(6), 653-671.

[15] Sandhu, R. S., & Samarati, P. (2002). Access control: principle and practice. IEEE communications magazine, 32(9), 40-48.

[16] Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2018). Elliptic curve lightweight cryptography: A survey. Ieee Access, 6, 72514-72550.

[17] Nadeem, A., & Javed, M. Y. (2005, August). A performance comparison of data encryption algorithms. In 2005 international Conference on information and communication technologies (pp. 84-89). IEEE.

[18] Panda, M. (2016, October). Performance analysis of encryption algorithms for security. In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) (pp. 278-284). IEEE.

[19] Ardagna, C. A., Damiani, E., Frati, F., Rebeccani, D., & Ughetti, M. (2012, June). Scalability patterns for platform-as-a-service. In 2012 IEEE Fifth International Conference on Cloud Computing (pp. 718-725). IEEE.

[20] Sims, M., Corkill, D., & Lesser, V. (2008). Automated organization design for multi-agent systems. Autonomous agents and multi-agent systems, 16(2), 151-185.