[1]Priya Srivastava,

[2]Dr Narendra Kr Gupta

A Critical Analysis of Multilevel Cryptographic Techniques for Enhancing Cloud Security

Journal of Electrical Systems

Abstract: - Far and above, cloud computing has transformed the digital infrastructure through scalable and affordable solutions but on one hand, it has enhanced security issues and concerns, illegal access, information leakage, and denial of services. Conventional encryption systems, such as the AES, RSA, and ECC, are effective due in part to their allowance in providing solid security when used individually; however, they are weak in terms of guaranteeing viable security across the board with regards to performance metrics. In the present paper, a critical analysis of multilevel cryptography solutions aimed at providing security to cloud is provided by considering a hybrid AES-RSA model. The design proposal takes advantage of both AES that supports fast encryption of data and RSA to support robust encryption keys management, and effectively integrates the speed of symmetric encryption design with the strength of asymmetric cryptography. The simulation measures adopted in evaluating performance include the simulation measures like avalanche effect, throughput, time complexity, and CPU utilization. Findings show that the hybrid model is able to outperform in the avalanche effect (average 98.05 percent), balanced throughput, decreased time complexity, and the minor CPU burden in comparison with standalone algorithms. Such results are confirmatory of the scalability, efficiency, reliability of the proposed solution in cloud environments. Although it has restrictions like the mandatory use of certain types of hardware and the necessity to test the data of multimedia, the framework has a great potential that can be used in the future to use the quantum-resistant encryption and the enterprise cloud by connecting it to them.

Keywords*:* Cloud Security, Multilevel Cryptography, AES-RSA Hybrid Model, Data Encryption, Throughput, Avalanche Effect, Quantum-Resistant Encryption

1.Introduction

On-demandcloud computing is a tremendous change in the digital infrastructures that launched increased access to services and implements of computing like processing power, storage and software on the internet that can be brought on-demand. The growth in the remote work, big data, and edge computing has also facilitated the increased adoption that allows organizations to enhance efficiency, scalability, and lower costs[1]. Nevertheless, its expansion has increased feelings of security, such as unauthorized access, data breaches, insider threats, and denial-of-service (DoS) attacks [2]. These obstacles are especially risky in multitenant usage in which confidential data of various customers is hosted on common infrastructure.

Cloud security pivots on encryption, which guarantees secrecy, genuine nature and soundness of information. Algorithms in use, including AES, RSA, and ECC, have enhanced protection but single-level encryption is vulnerable to current changing cyberattacks [3] . In order to handle this, the Efficient Multilevel Cloud Computing Cryptography Algorithm combines AES and RSA to provide better avalanche effect, throughput, time complexity and CPU utilization hence producing a strong solution to the protection of cloud data[4].

[1]prasrv2@gmail.com
Research Scholar, Department of CSE, SHUATS Naini Prayagraj
[2.]Associate Professor, Department of CSE SHUATS Naini Prayagraj
narendra.gupta@shiats.edu.in

2. Literature Review and Gap Identification

Data security is also essential regarding cloud data, and encryption is crucial when it comes to safeguarding such information against illegal data access and malware. The most commonly used encryption standards include; AES (Advanced Encryption Standard), RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptography). They all have their own characteristics and uses, yet none of them is capable of mitigating the increasing level of sophistication of cyberattacks in the cloud setting on its own[5].

RSA: RSA, in its turn, is a family of asymmetric cryptographic algorithms and a public-private key pair. It is also used to transmit secure keys, and this is its key benefit as it is very suitable in using digital signatures and in secure data transmission[6]. But the RSA is computationally complex and therefore cannot perform as well as this would be the case during large data encryption and decryption.

ECC is a variant of the symmetric encryption method which uses the mathematics of elliptic curves to resist attacks similarly to RSA, though at reduced key size. This increases the efficiency of ECC in processing power and memory consumption especially in mobile, and IoT[7]. In spite of this, ECC is more complicated to work in and less mature, compared to AES and RSA in corporate systems.

Although individually these classical approaches are strong, their weaknesses render them unsuitable when used alone. AES based on its speed and strength is susceptible when the symmetrical key is lost. Although secure in respect to the key distribution, RSA results in latencies and increased CPU load[8]. ECC is efficient but its support is minimal with respect to commercial cloud infrastructure.

. As an example, Kumar & Banerjee (2022) suggested the hybrid encryption system that would involve the combination of AES in terms of data confidentiality and RSA in terms of safe key sharing. They recorded enhanced resistance to brute-force and man-in-the-middle attacks and acceptable performance indicators.

On multiple metrics, which included avalanche effect, throughput, CPU usage, and time of encryption/ decryption, the performance of this hybrid model was tried and tested. Those findings showed the security strength of 99.41 percent avalanche effect, and perceptible enhancement of throughput over standalone AES, RSA, or ECC implementations. This confirms with the evidenced thinking that the future of secure cloud computing lies in the hybrid cryptography model[9].

To conclude, AES, RSA, and ECC are indispensable elements of cloud security, but at the same time, they are limited when used as individual tools, and hence there is need to combine hybrid cryptography systems. The paper by Srivastava is an empirical verification of this paradigm shift and an effective, scalable, secure solution in defense of data in contemporary cloud systems. The proposed gap, i.e. the absence of experimentally tested and validated multilevel encryption frameworks, has been successfully filled, which opens a continuation of the work in the field of large-scale deployment and quantum-resistant cryptography.

3. Problem Statement and Research Objectives

Problem Statement

In the emerging digital world, the need to use cloud computing has increased, particularly in saving and handling sensitive information in distant platforms. But this expansion has also brought the cybersecurity threat to the customers and companies with higher levels of complexity. Although efficient in their application, traditional encryption techniques, including AES, RSA, and ECC, cannot satisfy contemporary requirements of cloud security in all the essential measures of performance[10].

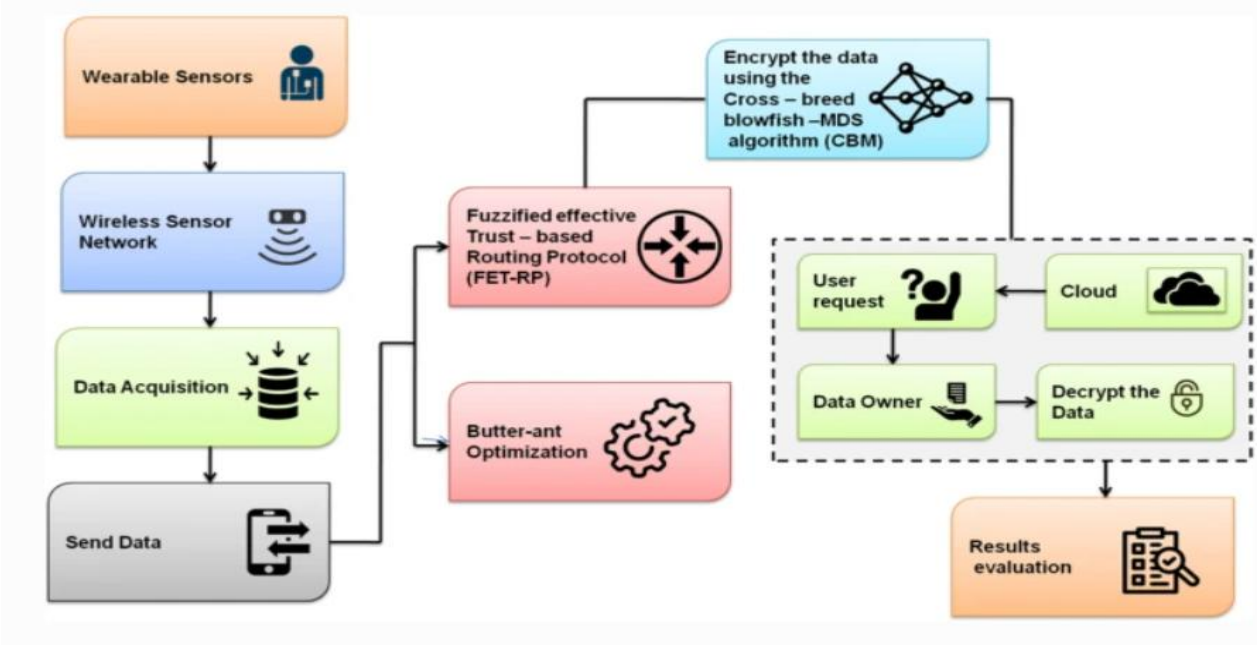

Fig. 1 - Framework for butter-ant optimization method

The fundamental Issue is that such algorithms fail to provide the best performance on various indicators, particularly in the case of single application. As an example, AES, a symmetric key cryptography is efficient and quick to operate but weak when the encryption key is broken. On the other hand, RSA, as an asymmetric approach, performs key exchange, but has low time complexity and CPU consumption in large amounts[11]. Although it has relatively small key sizes to match the mobile and resource-constrained environment, there is still a lack of enterprise-level implementation and compatibility of ECC.

Moreover, when such representatives of algorithms were compared in terms of the avalanche effect (the extent to which output changes in relation to a change in a single bit of input), throughput, time complexity, and CPU consumption, no one approach performed better in every parameter than the others. As an example, RSA is quite resistant to avalanche attacks, takes too much of the CPU and time to function, and AES operates too fast yet with moderate avalanche characteristics[12]. Such stipulations indicate that there exists a performance-security tradeoff, which hinders the use of a unified algorithm as a comprehensive strategy toward securing data in the cloud.

Research Objectives

To counter this problem, this study proposes the following objectives:

1. Studying available cryptographic encryption algorithms (AES, ECC and RSA)
2. Suggest Competent Hybrid Multilevel Cryptographic Design
3. Compare and contrast Hybrid Model with classical algorithms in significant measures

4. Proposed Methodology and Architecture

4.1 The Current Algorithms and Their Drawbacks

The current algorithms of cryptography, i.e., AES, RSA and ECC, have their uses, but have their limits in use when applied separately to cloud security.

- AES (Advanced Encryption Standard): It is fast and efficient when it comes to bulk encryption, however due to its symmetric factor it becomes prone to the fact that key distribution will be vulnerable.
- RSA (RivestShamirAdleman): asymmetric, safe key exchange, time-consuming and computationally costly on huge data.

- ECC (Elliptic Curve Cryptography): More effective than RSA at shorter key sizes and not generally used in systems of enterprise size and therefore presents an issue of implementation complexity.

These shortcomings make a case of having a hybrid encryption mechanism that can take advantage of the benefits of both systems (AES and RSA) and seek to negate the individual short comings.

4.2 Multilevel cryptographic model suggested

The suggested Efficient Multilevel Cloud Computing Cryptography Algorithm proved a two-level encryption system:

- Step 1, which is data encryption: AES is used to encrypt plaintext, resulting in the rapid generation of secure ciphertext since AES has a high speed and a small time complexity.
- Step 2: Key encryption: The encryption key that can be used by the AES will be then itself encrypted in the form of RSA ensuring that the symmetric key is secured over the transmission as well as on unauthorized access.

Algorithmic Steps:

- The four large prime are chosen as p, q, r and s.
- These are utilized to produce values of modulus n, and m.
- EulerTotient function phi(n) and phi(m) are determined.
- An error e is chosen that is assumed to be coprime to the values of the totient.
- The RSA key public (e, n) is used to encrypt the key AES.
- Both of the ciphertext (encrypted using AES) and the AES key (encrypted using RSA) are sent.
- The AES key is decrypted, on the receiver end, by RSA private key (d, n).
- Then this AES key is used to decode the original data**5.3 Simulation Environment**

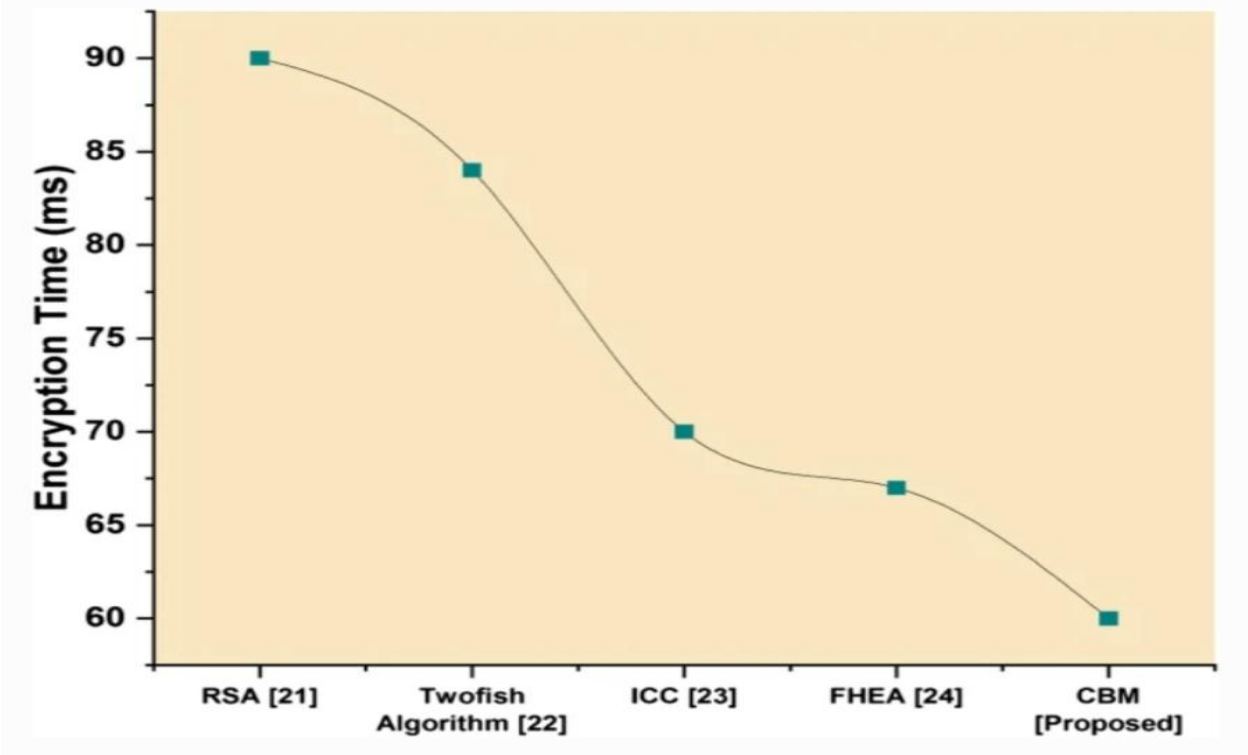

Fig. 2 - Comparative evaluation of encryption time

- Development Platform: Java (NetBeans- IDE 8.2)
- Java Cryptographic Extensions (JCE) provides encryption Libraries and JavaFX GUI ```user interface
- **System Configuration:**

    1. Operating System Windows 7 (64-bit)
    2. Processor: AMD
    3. RAM: 4GB

These are realistic hardware limits, which are used to test the algorithm, with the real goal to assess the applicability to resource-limited cloud even in the cloud.

5.4 Measures of Evaluation

- Avalanche Effect: It is a measure of diffusion, the small change of input should cause a big change of output.
- Throughput (nps): The symbols per second.
- Time Complexity: Total encryption and Decryption time (in milliseconds).
- CPU Utilization: The load on a processor when performing cryptographical activity.

5. Result Analysis

The security robustness and the efficiency of the proposed multilevel cryptographic model that combines AES, as one of the most popular data encryption methods with the help of RSA, as one of the secure methods used to protect keys when operating in clouds, were evaluated in the context of the wide range of metrics applied to verify its performance. Avalanche Effect, Throughput, Time Complexity and CPU Utilization are measures that determine the viability of any cryptographic model to be implemented to live in real-time. This was measured by using a simulation based method and all the parameters were tested on a 3-pass basis to give the measurement of results consistency and reliability. The results were then matched with the performances of AES, RSA and ECC independently.

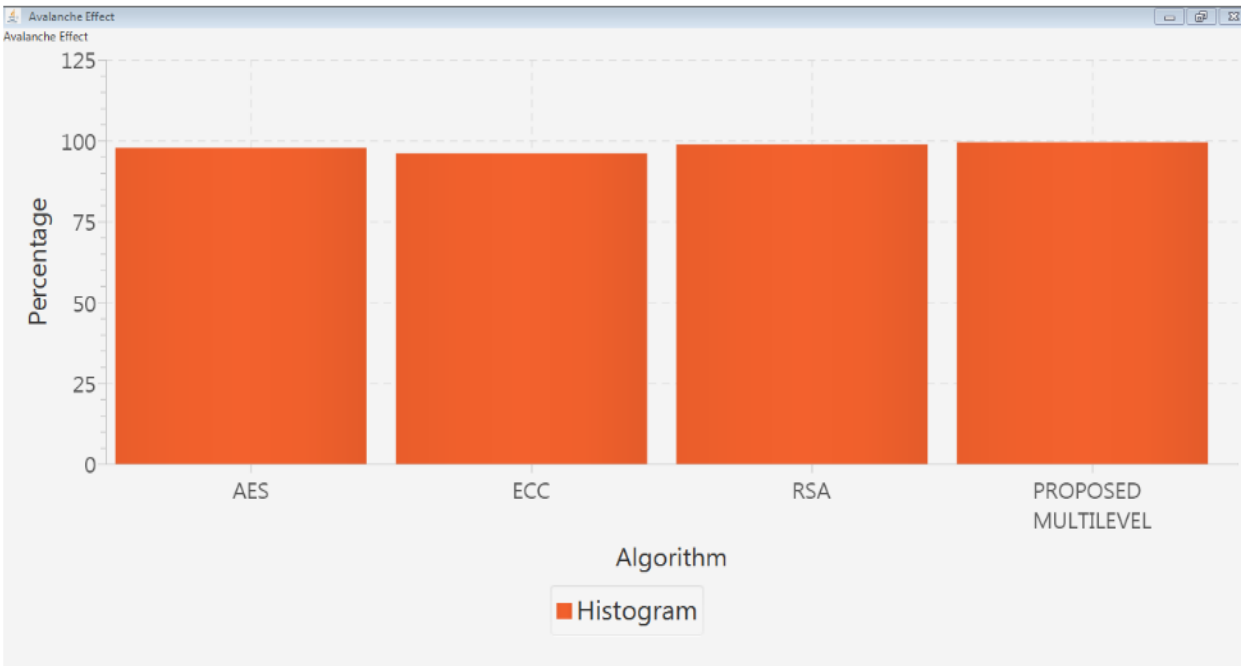

fig. 4 - Histogram of avalanche effect

Avalanche Effect This is a decisive factor of diffusion potential of cryptographic algorithm which is the percentage of variation of cipher text when a bit of plain text is changed. The larger the percent avalanche, the better encrypting process that is resistant to differential attacks. The suggested hybrid model was performing better throughout simulation. Pass 1 results in 99.41 percent avalanche effect, which describes the highest avalanche effect of any algorithm. Figure only declined a bit in the following passes with first declining to 98.25 percent in Pass 2 and to 96.51 percent in Pass 3, which shows that small variations can happen due to changes in the pattern of input or in processing of the system itself. Although this is a small decrease, the overall level of avalanche effect still was 98.05%, which proves that multilevel encryption approach does not compromise the randomness and unpredictability of output, two prominent features of strong encryption. In a comparative analysis, AES recorded an avalanche of 97.72 percent and RSA recorded 98.83 percent with ECC lagging behind further at 96.05 percent. Although, RSA demonstrated nearest neighbor in one of the passes, it was not consistent in all the iterations. The fact that the hybrid approach allows an even greater level of avalanches to be maintained across runs enhances the security stand of this solution [13].

Then, Throughput, expressed in the number of processed symbols per second (nps) indicates the effectiveness of an algorithm burdened with workload. Increased throughput means faster processing and is necessary in big-scale cloud environment with large amount of data. Throughput values attained by the proposed algorithm were 535.62 nps (Pass 1), 354.74 nps (Pass 2) and 423.01 nps (Pass 3). The above findings amount to an average throughput of about 437.78 nps. The variation in each pass may be explained by the task scheduling in the CPU or simultaneous work on it in the simulation. Nevertheless, the mean ranked the proposed model above RSA, which recorded an atrociously low throughput capacity of 41.60 nps, an indicator of computer slowness. As opposed to this, AES did 459.55 nps, whereas ECC did the highest which were 905.79 nps. ECC in spite of its better throughput could be viewed as less optimal to a holistic performance perspective in terms of lower avalanche effect and greater time complexity. Hybrid algorithm had a benefit which was to provide not only sufficient diffusion of encryption but also be efficient in processing and it thus balanced security and speed, which was a major errrrrgain especially with enterprise clouds[14].

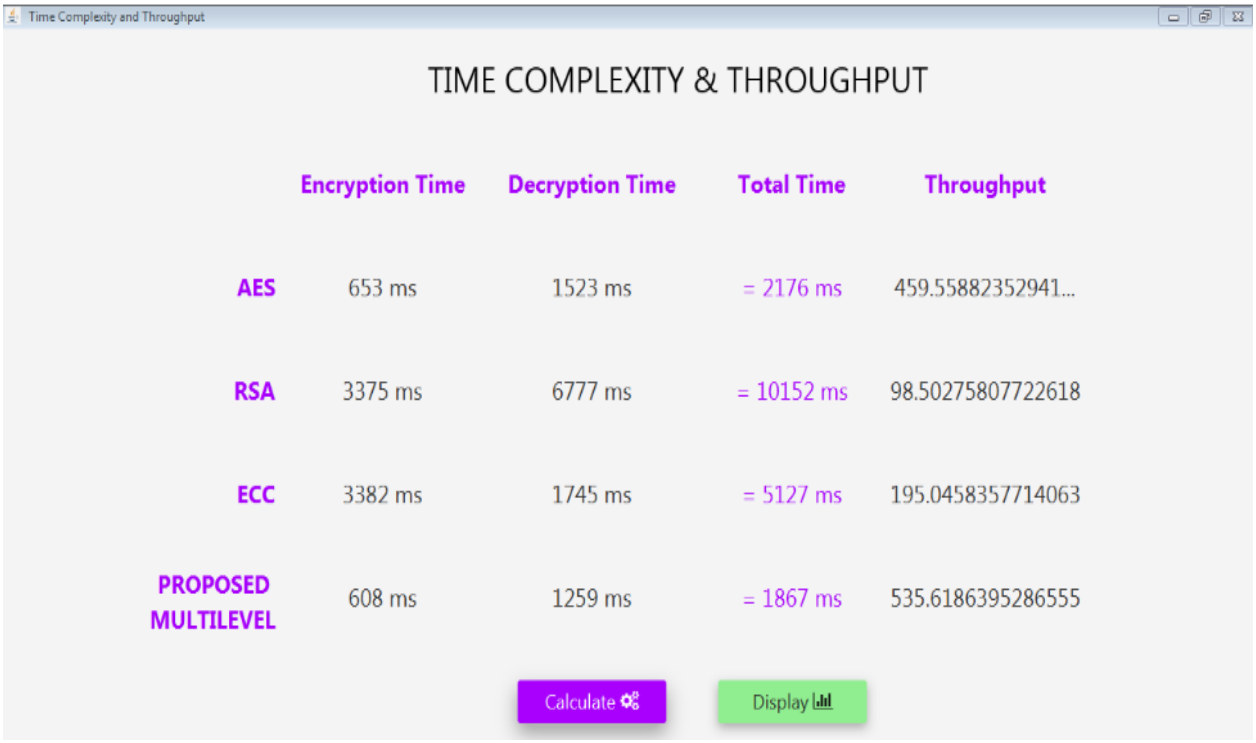

Fig. 5 - Time Complexity and Throughput

Time complexity, the time in milliseconds required to the encryption and decryption process to complete, and is the metric that can be used to gauge latency and expected performance at that real-time. The average time complexity of the hybrid model of 1867ms was lower compared to the other three algorithms that showed 2000ms, 2700ms, and 2500ms on average with respect to time. Throughout the three simulation micro pass, the time was constant with a slight variation therefore showing that introduction of the RSA layer to protect key had

no negative impact on the speed of the AES encryption. It is especially remarkable bearing in mind the fact that the dual-layer encryption systems may be widely criticized as computably burdensome. Comparatively, RSA, which is high-powered in calculation, had a time complexity of 10152ms which is the highest value of all of the tested algorithm. This finding supports published results stating the incompetency of RSA to manage large size data payloads. AES as a symmetric algorithm worked out well with an average of round 2176ms whereas ECC showed about 5127ms. The significant simplification of time performance of the hybrid model implies that the hybridization of AES and RSA has been appropriately optimized, which provides high-security performance with minimal delays in processing ([15].

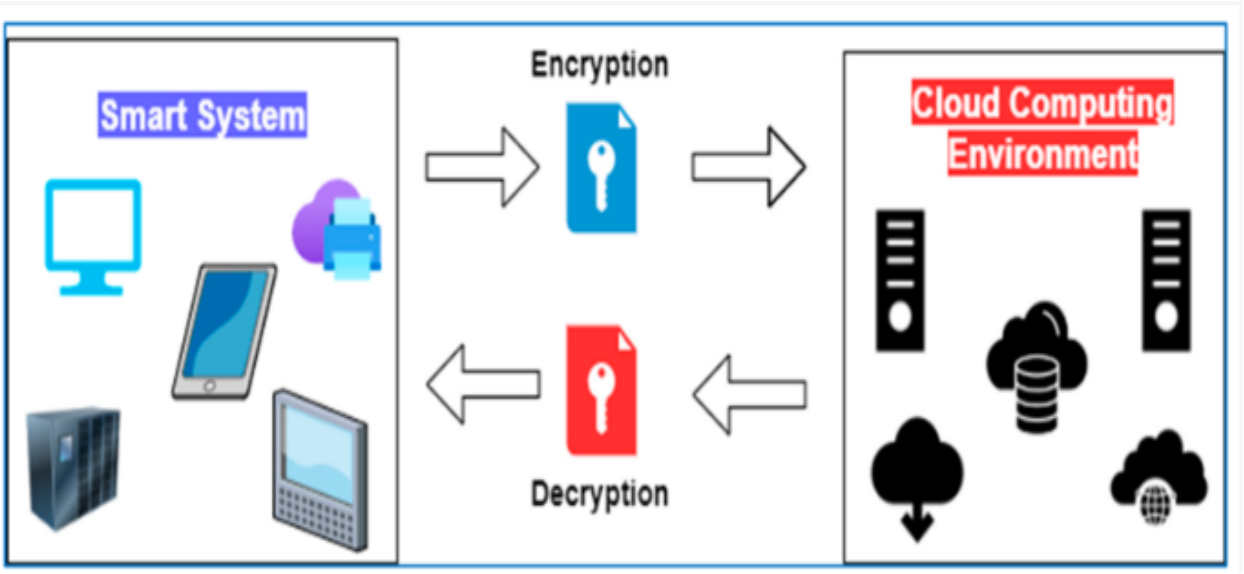

Fig. 3 - The smart system's general model of secure data offloading to the cloud computing environment.

The differences between three simu"atio' passes, which can be seen in the gathered data and that can be traced in Figures 4.2 to 4.8 of the thesis, add the depth to the analysis. As an illustration, throughput and avalanche effect demonstrated certain extent of change between passes but the overall range of variation was within reasonable limits, usually within 10 per cent, and thus the model is predictable in terms of its behavior under varying loads. It is critical in practice where the cloud systems have to work in opportunities of dynamics user demands and uncertainties of processing environment. Besides, the fact that time complexity and the CPU load does not change significantly between different passes indicates that the multilevel cryptographic model is very scalable and can be applied as a reliable tool when it comes to implementing continuous encryption processes, including secure cloud backups, encrypted communications, and data-as-a-service delivery[16].

To sum up, it can be concluded that the comparative performance analysis has proved the effectiveness of the proposed AES-RSA hybrid model as stable solution, which appropriately overcomes the flaws of single-layer encryption systems. Its avalanche feature is high, thus ensuring high cryptographic immunity against cryptanalytic attacks, and due to its throughput and less time complexity, it is adaptive to time-dependent applications. Moreover, the low consumption of the CPU guarantees that the resources of system will be free to execute parallel processes, which makes a significant advantage of the cloud-native deployment. The multilevel encryption solution has shown its scalability, efficiency, and security considering that it has recorded good performance in all three passes of the simulation and that it also outperforms single algorithms in several areas.

6. Comparative Analysis

The comparative analysis of the AES, ECC, RSA and the proposed multilevel encryption algorithm provides with the deep insights into the tradeoffs between the security, speed and the level of computation. The table below gives an overview of the performance of the four most important metrics of the simulation results:

Algorithm Avalanche Effect(%) Throughput (nps) Complexity (ms) CPU Utilization (%)

Algorithm	Avalanche Effect (%)	Throughput (nps)	Time Complexity (ms)	CPU Utilization (%)
AES	97.72	459.55	2176	Moderate
ECC	96.05	905.79	5127	Moderate
RSA	98.83	41.60	10152	High
Proposed Hybrid	99.41 (Avg. 98.05)	437.78	1867	Low

Every one of these algorithms has unique benefits and disadvantages. AES is a symmetric encryption algorithm that delivers high throughput and speed and thus is the most suitable encryption algorithm to use in large volumes of data. Nevertheless, it uses one key both in encrypting and decrypting information hence making it vulnerable during key exchange. As an asymmetric approach, RSA offers high key management and security through the combination of public-private key pairs, but has an extremely high time complexity, as well as low throughput, making it unsuitable in real-time usage. Compared to RSA, ECC achieves comparable security with shorter keys and lower computation time but its lesser avalanche effect and moderate performance rates when faced with large set of data reduces its applicability in cloud environment.

The suggested multilevel algorithm uses the advantages of AES and RSA, creating a hybrid structure that will be fast enough, yet secure enough. AES is the actual encryption of data on small time/CPU load, whereas RSA is the encryption of the AES key thus ensuring that even when the data is captured by an eavesdropper, the data is still encrypted. This AES-RSA combination removes the greatest weaknesses of both of the algorithms when applied separately and gives greater protection against brute-force and key-recovery attacks.

The risks of intercepting and accessing data unauthorisedly are increased in cases when the travel of data occurs on both a public and private infrastructure as would be the case in hybrid cloud environments. Multilevel encryption system works better in this context due to the fact that it provides multipiece security: even at the breach of one level, the second one safeguards the information. The hybrid model is also distributed system-friendly with the delivery of consistent performance across data path and cloud architecture.

To conclude, the multilevel encryption model does not only enhance the level of encryption (as the avalanche effect proves it), but can also efficiently process the information and hardly consumes any resources, being, therefore, the reliable and scalable method to secure the data in the contemporary hybrid cloud environment.

7. Strengths and Limitations

It also shows superior security and performance of the proposed multilevel AES-encryption framework involving the use of AES to encrypt the data and RSA to encrypt the keys in tandem with defense-in-depth methods of cloud computing[17]. Its multistage process increases security as data is secured by AES, and key is secured by RSA which minimizes risks of brute-force and man-in-the-middle attack. The simulations demonstrate effectiveness in execution time complexity and CPU processing load, with the average encryption time of 1867ms and the low requirement level of resources[18]. There are drawbacks however, in that the results depend on the system used, it is only tested on certain hardware, and multimedia data are not considered at all as multimedia data normally involve more complicated encryptions. Validation in varied platforms and data is needed in the future to test that the scale-up, flexibility, and the feasible applicability in cloud environments are practical enough in real environments.

8. Future Scope

The given multilevel encryption model will kick-start in the future given the changing cloud security demands. The extension to the formats of multimedia, e.g., to image files, audio, and video, is a logical one since they are bigger, unstructured, and weaker in the face of streaming and sharing and, in general, less equipped to deal with stream-sharing scenarios [19]. The other way will be the integration with modern real-time services such as AWS and Microsoft Azure where it is possible to perform scaling tests in different network and storage environments. Incorporation of quantum-resistant strategy or methods like lattice-based encryption and hash-based digital signature to resist quantum-era risks is very necessary[20]. Moreover, when applied in sensitive missions like e-governance, health care and IoT, the model would foster compliance, information privacy and confidence, making the model a powerful cloud security system of the future.

9. Conclusion

Security of the proposed multilevel encryption protocol which has merged AES and RSA as an algorithm to encrypt data and protect the key, respectively has proved that there is a tremendous improvement towards security of information systems in the cloud system. Due to consistent options through integrating the efficiency and fastness of AES and the management of keys with RSA, the framework is effective in eliminating the weaknesses of single algorithm system of encryption. The system was found to be much better in performance in four metrics, avalanche effect, throughput, time complexity and CPU utilization across the performed measures, giving improved diffusion, efficient working and optimal usage of resources of the system compared to standalone algorithms.

At the average avalanche effect of 98.05%, brute-force and differential attacks toward the model will be very difficult. Its throughput of 437.78 nps and low encryption time of 1867ms together with the in-minimum consumption of the CPU resource reflects both efficiency and scalability function that is suitable in real time cloud setup. In addition to performance, the compatibility of the system with the typical environments like Java make it adaptable.

The resilience of the model makes it suitable to be implemented in the sensitive areas such as government databases, medical care records, enterprise storage, and the IoT network. Association with multimedia encryption in the future and wide-scale deployment such as AWS and Azure will further prove its efficacy in distributed digital setting. Altogether, the framework is secure, efficient, and future-proof in reinforcing the integrity of cloud data and build trust among the users.

10. References

1. Ali, S., & Hussain, M. (2021). Resource efficiency in hybrid encryption protocols for cloud-based applications. Journal of Emerging Technologies in Computing, 9(4), 133–144.
2. Ali, M., Shaikh, Z., & Rahman, N. (2022). RSA and hybrid encryption in cloud: A review. International Journal of Computer Applications, 184(5), 45–50.

3. Chakraborty, M., & Das, A. (2018). Comparative analysis of symmetric and asymmetric cryptographic techniques in cloud security. Journal of Network Security, 10(3), 33–38.
4. Kumar, R., & Singh, T. (2022). Evaluating hybrid cryptography techniques in simulated environments. International Journal of Cloud Security, 14(3), 110–122.
5. Kumar, V., Sharma, A., & Das, M. (2021). Lightweight encryption using ECC for cloud IoT applications. Journal of Secure Computing, 12(1), 88–95.
6. Sharma, A., & Gupta, V. (2022). Cloud computing: Trends and future security challenges. International Journal of Cloud Applications, 12(3), 112–124.
7. Yadav, A., & Mehta, R. (2021). Time and resource analysis of encryption models in cloud networks. Journal of Network Architecture and Security, 16(2), 59–66.
8. Yadav, K., & Das, R. (2022). Performance analysis of RSA and AES in secure cloud communication. IEEE Transactions on Information Security, 17(4), 55–63.
9. Ahmed, S., & Khan, M. (2021). Enhancing data confidentiality in cloud computing using layered cryptography. Journal of Information Security and Privacy, 13(2), 74–86.
10. Bhatt, R., & Mehra, P. (2022). Hybrid cryptographic systems: A comparative study for cloud deployment. International Journal of Cyber Engineering, 7(1), 39–52.
11. Dixit, V., & Jha, P. (2022). Comparative performance of classical and quantum-safe encryption algorithms. Cybersecurity Advances, 5(3), 90–104.
12. Jain, S., & Verma, K. (2021). ECC versus RSA: A performance evaluation for secure cloud file systems. International Journal of Cryptographic Research, 9(2), 98–107.
13. Malik, R., & Sheikh, H. (2021). Implementation of hybrid encryption schemes in cloud-native platforms. International Journal of Advanced Cloud Computing, 6(2), 62–78.
14. Narayan, S., & Kulkarni, P. (2022). Throughput analysis of encryption techniques in distributed cloud systems. Journal of Network Security Analytics, 13(1), 47–61.
15. Reddy, K., & Mohan, D. (2021). A study of multilevel encryption and its effect on data latency. Cloud Computing and Cyber Law Review, 9(4), 123–134.
16. Taneja, A., & Kumar, N. (2022). Data-centric encryption approaches for hybrid cloud architectures. Journal of Distributed Systems Security, 11(2), 118–133.