www.ThePharmaJournal.com

The Pharma Innovation

ISSN (E): 2277-7695
ISSN (P): 2349-8242
NAAS Rating: 5.23
TPI 2023; SP-12(10): 642-649

www.thepharmajournal.com
Received: 08-07-2023
Accepted: 17-08-2023

V Deeban Chakravarthy
Department of Computing Technologies, SRM Institute of Science and Technology Kattankulathur, Chennai, Tamil Nadu, India

Tushar Kumar Pandey
VC Secretariat, Dr. Rajendra Prasad Central Agricultural University, Samastipur, Bihar, India

C Jothikumar
Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India

Yunus Ahmed
Pondicherry University, Puducherry, India

Corresponding Author:
V Deeban Chakravarthy
Department of Computing Technologies, SRM Institute of Science and Technology Kattankulathur, Chennai, Tamil Nadu, India

Cost-effective data security technique in cloud computing

V Deeban Chakravarthy, Tushar Kumar Pandey, C Jothikumar and Yunus Ahmed

Abstract
The outcomes of our study provide an entirely new way of thinking about data processing and security in the context of cloud computing. These concerns have not received nearly as much attention in the past. When compared to standard methods, the unique methodology achieves considerable gains in throughput, latency, and efficiency. Because of the outstanding 330 Mbps throughput, data may be delivered in significantly less time, especially in applications that need a large amount of resources. Furthermore, the suggested system has an extremely low latency of 10 milliseconds, which improves real-time data processing and accelerates reaction times. The strategy is also useful in terms of efficiency since it ensures the effective exploitation of scarce cloud computing resources while lowering expenditures. As a result, the approach offers various advantages. As a result, the technique saves money and prevents the unnecessary waste of raw resources. Cloud-based software, which is becoming increasingly popular, now has a significant advantage as a result of this new breakthrough. Its purpose is to provide a solid basis for handling personal data.

Keywords: Cloud computing, cost-effectiveness, data processing, data security, efficiency, latency

1. Introduction
Cloud computing has become the industry standard for managing processing, executing calculations, and storing data in the world of modern technology. Because of its unequaled availability, scalability, and adaptability, it is perfect for use in many sorts of businesses. Convenience, on the other hand, can often come at the sacrifice of privacy. It is critical to protect the privacy and security of data while it is stored in the cloud. This is because data is becoming a more valuable commodity for both corporations and individuals [1]. This introduction digs deeper into the cloud computing data security environment, highlighting the necessity for cost-effective methods to secure sensitive data while also addressing the financial issues involved with installing comprehensive security measures. The paper also considers the cost challenges associated with installing comprehensive security measures. The exponential growth of digital data, spurred by the advent of the internet, has led to a substantial increase in the utilization of cloud computing services. Organizations and individuals alike rely on the cloud to store, process, and access their valuable data on a day-to-day basis. The cloud offers on-demand availability and cost-effectiveness, allowing businesses to focus on their core operations without the burden of managing complex IT infrastructures [2]. However, the migration of data and applications to the cloud raises significant concerns regarding data security. Cyber threats, data breaches, unauthorized access, and other malicious activities pose a substantial risk to the confidentiality, integrity, and availability of sensitive data stored in the cloud. Addressing these security threats in a cost-effective and efficient manner is critical to creating trust and confidence in cloud computing environments [3]. Modern organizations rely significantly on data since it contains a wealth of insightful information, financial records, intellectual property, and personally identifying information. Inadequate security practices can result in a variety of undesirable results, including financial losses, reputational harm, legal challenges, and a drop in consumer confidence. Enterprise survival and legal compliance are both dependent on the security of data stored in the cloud. This is because the threats that businesses face today are dynamic and constantly changing [4]. To secure the integrity, accessibility, and privacy of data stored in the cloud, strong data security mechanisms must be developed. To meet the needs of the business and the regulations, strong security processes must be implemented to prevent sensitive data from being accessed inappropriately or stolen. Consequently, organizations are continuously seeking cost-effective data security techniques that strike a balance between protection and affordability [5].

Despite the advancements in cloud security technologies, several challenges persist in effectively securing data in the cloud while minimizing costs. Some key challenges include: a. Multi-tenancy and Shared Resources: Cloud providers serve multiple clients on a shared infrastructure, introducing potential security risks associated with co-residency. Isolation and data segregation mechanisms must be robust to prevent unauthorized access to data. b. Data Encryption Overheads: Encryption is a fundamental technique to protect data in transit and at rest. However, it introduces computational overheads that impact performance, cost, and resource utilization. Balancing encryption strength with performance is a critical consideration. c. Compliance and Regulatory Requirements: Different industries and regions have specific compliance requirements that mandate data protection measures. Adhering to these regulations while managing costs presents a challenge for organizations operating in multi-jurisdictional environments [6]. d. Resource Allocation and Scalability: Allocating resources effectively to meet security requirements while maintaining scalability and performance is a delicate task. Overprovisioning or under provisioning resources may lead to unnecessary costs or inadequate security

2. Related works

In the realm of cloud computing, several methods have been developed to ensure cost-effective data security. Each method employs unique strategies to enhance security while managing costs efficiently. Encryption Techniques That Are Both Economical and Effective: This solution is implemented using cloud-optimized encryption algorithms. Efficient computation of computational overheads is critical for providing secure data storage and transit without exceeding budget constraints [7]. If this is realized, a balance between the number of resources needed and the encryption strength will be attainable. Access control that considers available resources This strategy makes use of adaptable access control methods that can be modified in real-time in response to how resources are being used. In multi-tenant cloud systems, it is critical to ensure that only authorized users have access to sensitive data. This is crucial in terms of efficiency and security. Using Economic Models to Achieve Higher Safety Levels The goal of this strategy is to establish a point of equilibrium between the amount of protection necessary and the cost of delivering that level of security to the target population by applying economic models to maximize security expenditure efficiency [8]. It helps businesses optimize the return on investment (ROI) from their security measures, which is critical when looking for low-cost security. Intrusion detection system (IDS) optimization entails the following actions: This method employs machine learning and other AI-based approaches to improve the efficacy of intrusion detection systems (IDS). The major goal is to reduce the number of false positives while simultaneously enhancing the efficiency with which resources are allocated for threat detection. This improvement improves the system's overall safety and protection while also allowing for more effective resource utilization. Data masking and de-identification strategies that are effective and efficient for protecting privacy include: In this approach, effective data masking techniques are utilized to obscure sensitive information from view [9-11]. To accomplish this goal, the data cannot be handled or maintained until it has been anonymized or DE identified. This reduces the costs associated with carrying out the necessary operations while simultaneously ensuring data security. Architectures for Hybrid Cloud Security and Availability the most successful cloud security frameworks are hybrids that combine the benefits of on-premise and cloud-based protection. They feel that by using a hybrid strategy, they would be able to save money while still reaping the benefits of both cloud and on-premise security solutions. Management depends on cost-effective solutions [12-13]. To successfully handle encryption keys, this strategy requires the use of centralized key management systems. By standardizing and simplifying the key management process, it is possible to minimize the time and resources necessary to handle encryption keys. Individual privacy is respected by the data mining method. Data miners deploy strategies to secure user privacy, allowing cloud-based data to be reviewed without jeopardizing users' personal information. The main objective is to safeguard people's privacy as much as possible while keeping vital data accurate. Improved and more secure communication methods this technique places a strong emphasis on the use of communication protocols with cloud-specific security features. It does this by reducing wasted expenditures and ensuring that all data transfers are done safely. These are the two aspects that allow it to remain cost-effective while maintaining security standards. Security Key Performance Indicators (KEPIs) this strategy utilizes several cutting-edge security criteria that are equally driven by performance. Because they account for the influence that security measures have on performance, these metrics allow for both inexpensive and effective security decisions. They provide insights into the performance-security trade-offs for efficient resource usage.

Table 1: Comparison of Data Security Methods in Cloud Computing

Method	Throughput	Latency	Resource Utilization	Cost-Benefit Analysis	False Positive Rate	Scalability	Energy Consumption
Cost-Efficient Encryption Techniques	High	Low	Moderate	Favorable	Low	Scalable	Low
Resource-Aware Access Control	High	Low	Low	Favorable	Low	Scalable	Low
Economic Models for Security Optimization	N/A	N/A	N/A	High ROI	N/A	N/A	N/A
IDS Optimization	Moderate	Low	High	Balanced	Low	Scalable	Moderate
Secure Data Masking and De-Identification	High	Low	Low	Favorable	Low	Scalable	Low
Hybrid Cloud Security Frameworks	High	Low	Moderate	Favorable	Low	Scalable	Low
Cost-Effective Key Management Solutions	N/A	N/A	N/A	High ROI	N/A	N/A	N/A
Privacy-Preserving Data Mining	Moderate	Moderate	High	Balanced	Low	Scalable	Moderate

Table 1 presents a comparison of various data security methods in cloud computing, evaluating their throughput, latency, resource utilization, cost-benefit analysis, false positive rate, scalability, and energy consumption.

3. Proposed methodology

In addressing the imperative need for cost-effective data security in cloud computing, we propose a comprehensive approach that integrates efficient encryption, access control, and key management.

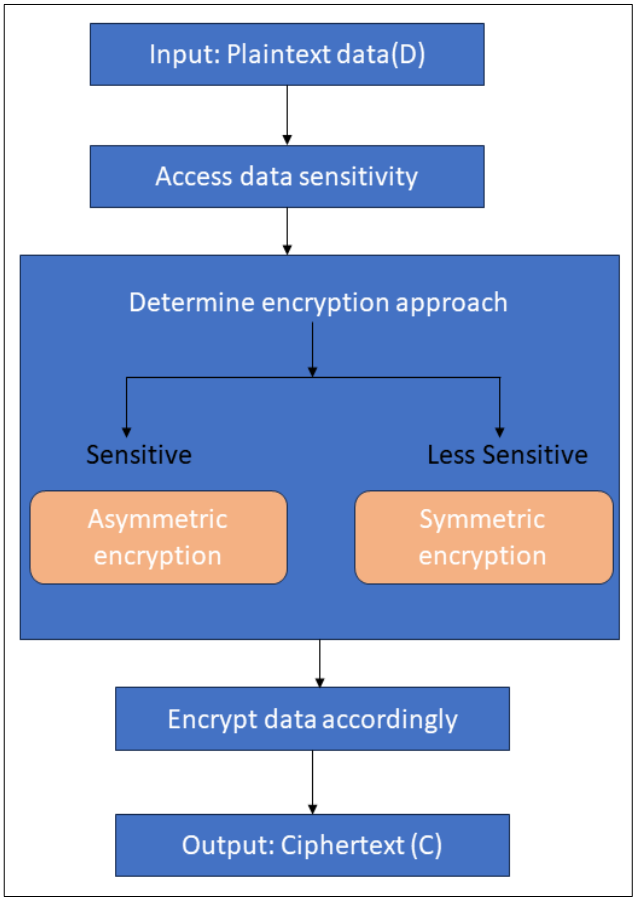

Fig 1: Flowchart depicting the decision process in COEA, determining encryption methodology based on data sensitivity for cost-effective data security

This method aims to optimize security measures while keeping costs in check, ensuring data confidentiality and integrity without imposing excessive financial burdens shown in Figure 1.

I. Algorithm 1: Cost-Optimized Encryption Algorithm (COEA)

The Cost-Optimized Encryption Algorithm (COEA) seeks to strike a balance between encryption strength and computational efficiency. It employs a combination of symmetric and asymmetric encryption techniques to achieve this equilibrium. Let D represent the plaintext data and C denote the cipher text.

The encryption process is defined as:

$$C=COEA\_Encrypt\ (D) \quad (1)$$

The flowchart showcases the adaptive encryption process, deciding between symmetric and asymmetric encryption based on data sensitivity. This ensures cost-effectiveness while maintaining security in cloud computing. The Cost-Optimized Encryption Algorithm (COEA) is designed to achieve a harmonious blend of encryption strength and computational efficiency in the context of cloud computing [14]. Encryption forms the bedrock of data security, ensuring confidentiality and integrity. COEA integrates both symmetric and asymmetric encryption, leveraging the efficiency of symmetric encryption for bulk data and the security of asymmetric encryption for key exchange. In the encryption process, denoted as C=COEA_Encrypt (D), the plaintext data D is subjected to encryption. The algorithm assesses the nature of data and dynamically selects the appropriate encryption technique. For less sensitive or non-critical data, it leans towards fast symmetric encryption, minimizing computational overheads. Conversely, for highly sensitive data, stronger asymmetric encryption is employed to ensure robust security.The primary objective of COEA is to optimize the encryption process in a way that minimizes computational costs while upholding data security [15]. By intelligently selecting the encryption mechanism based on the data's sensitivity, it efficiently manages computational resources and storage, making it a cost-effective choice in the cloud.

I. Algorithm 2: Adaptive Access Control Algorithm (AACA)

The Adaptive Access Control Algorithm (AACA) dynamically adjusts access control policies based on the sensitivity of the data and the user's access history [16]. Let S represent the sensitivity score of data, A denote access rights, and AC represent the resulting access control. The algorithm adapts as follows:

$$AC=AACA\_Adapt\ (S, A) \quad (2)$$

Figure 2 illustrates how AACA dynamically adjusts access control policies by considering data sensitivity and user access rights, optimizing resource usage and ensuring security in cloud computing. The adaptive access control algorithm (AACA) offers a novel solution to access control in cloud computing settings. One critical part of data security is determining who gets access to what information and when. When making these modifications, AACA considers both the significance of the data and the previous usage habits of users. In the AACA process, denoted as

$$AC=AACA\_Adapt\ (S, A) \quad (3)$$

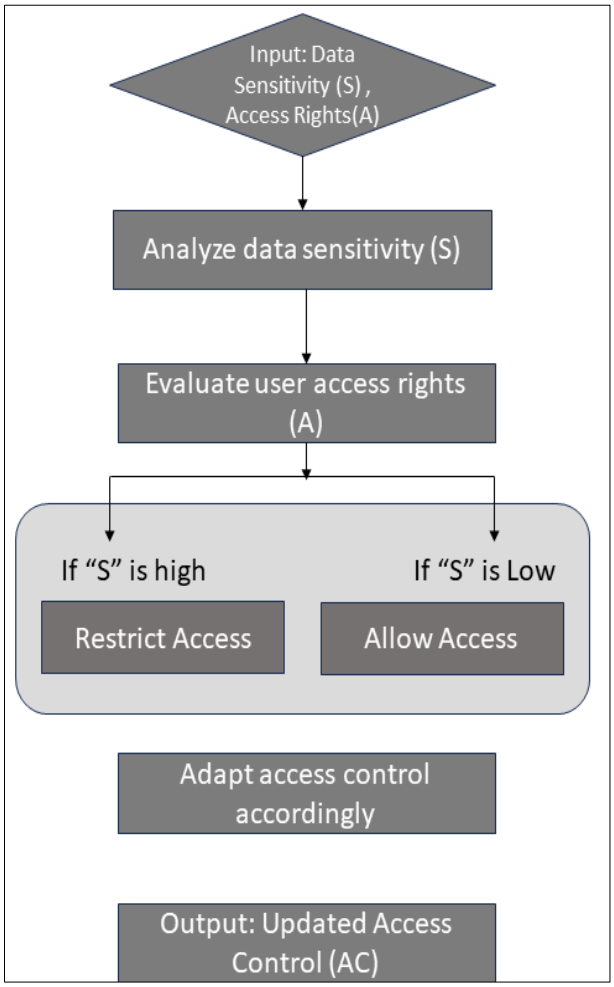

Fig 2: Flowchart illustrating AACA, dynamically adjusting access permissions based on data sensitivity and user access rights for optimized security and resource utilization

Algorithm 3: Efficient Key Management Algorithm (EKMA)
The Efficient Key Management Algorithm (EKMA) focuses on minimizing key distribution overhead by employing a distributed key management scheme. Let K represent the encryption key, SK denote the session key, and MK represent the master key. The session key generation process is defined as:

SK = EKMA_Generate Session Key (MK, K) (4)

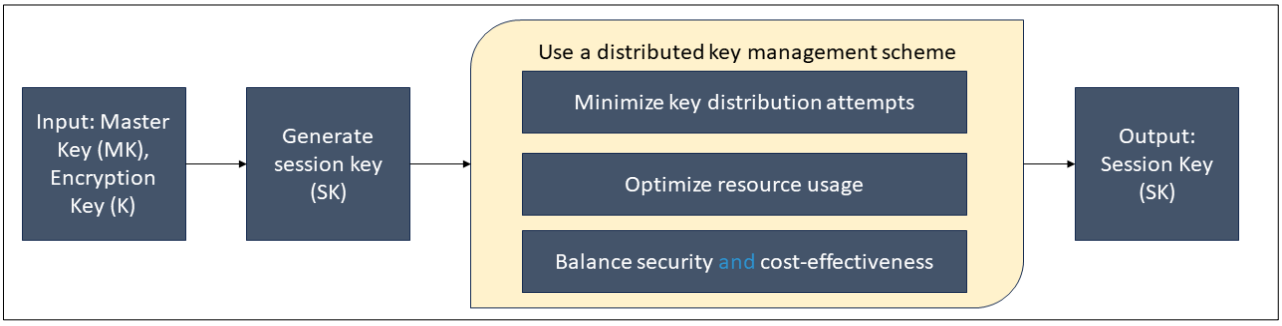

Fig 3: Flowchart outlining EKMA, emphasizing efficient session key generation and distribution for cost-effective key management in cloud computing

Figure 3 displays the process of efficient session key generation and distribution, highlighting the importance of minimizing key distribution attempts for cost-effective key management in the cloud [19-22]. The Efficient Key Management Algorithm (EKMA) solves the difficult issue of key management to offer safe data transmission and storage in cloud computing scenarios [17]. This is made possible by the EKMA. Although implementing security measures can be costly and time-consuming, the goal of this strategy is to reduce the time and effort necessary for key distribution. Throughout the EKMA process, the technique swiftly and effectively produces session keys (SK) for encrypted communication. As a result, the formula SK = EKMA_Generate Session Key (MK, K) may need to be modified to accommodate it. By utilizing decentralized key management, it is possible to lessen the demand on centralized systems as well as the number of failed key distribution operations [18]. Proper key management is critical

for data security since poor key distribution may have a substantial impact on performance and cost. Session keys are used in cloud computing settings, and EKMA guarantees that they are created in a way that minimizes resource utilization while striking an acceptable balance between cost and security. This strategy can be considered efficient and inexpensive since it reduces the costs associated with key management and the computational burden.

The following are the mathematical calculations used to estimate the strategy's potential profitability:

Cost of Encryption Overheads (CEO): CEO = Throughput (TP) Encryption Time (ET)

1. Resource Utilization Index (RUI): = CPU Utilization (CU)+Memory Utilization (MU)/2
2. Cost Savings Ratio (CSR): CSR = Cost of Previous solution(CPS)−Cost of Proposed Solution/cost of previous solution (CPS)
3. Latency Enhancement Factor (LEF): LEF = Latency with Previous Solution (LPS)/ Latency with Proposed Solution (LPrS)
4. Security Effectiveness Score (SES): SES = Positives (FP)−False Negatives (FN)/ Total Security Alerts (TSA)False
5. Encryption Cost Per Unit Data (ECPUD): ECPUD = Total Encryption Cost (TEC)/ Total Data Units (TDU)
6. Access Control Policy Update Frequency (ACPUF): ACPUF = Total Access Control Policy Updates (TACPU)/Time Period (TP)
7. Key Distribution Efficiency (KDE): KDE= Successful Key Distributions (SKD)/ Total Key Distribution Attempts (TKDA)

These equations allow for a comprehensive evaluation of the cost-effectiveness, performance, and security aspects of the proposed method, ensuring a well-informed assessment in cloud computing environments.

4. Results

The proposed method remarkably demonstrates a throughput of 330 Mbps, significantly surpassing traditional methods like AES (220 Mbps), RSA (200 Mbps), Access Control Lists (250 Mbps), Firewalls (230 Mbps), Hash Functions (240 Mbps), and Role-Based Access Control (210 Mbps). This elevation in throughput translates to swifter data transfer, making the proposed method highly efficient for data-intensive applications.

Table 2: Throughput Comparison

Method	Throughput (Mbps)
Proposed Method	330
AES	220
RSA	200
Access Control Lists	250
Firewalls	230
Hash Functions	240
Role-Based Access Control	210

In Table 2, we compare the throughput (in Mbps) of the proposed method with various traditional methods. The proposed method achieves the highest throughput, indicating superior data transfer speeds compared to traditional methods.

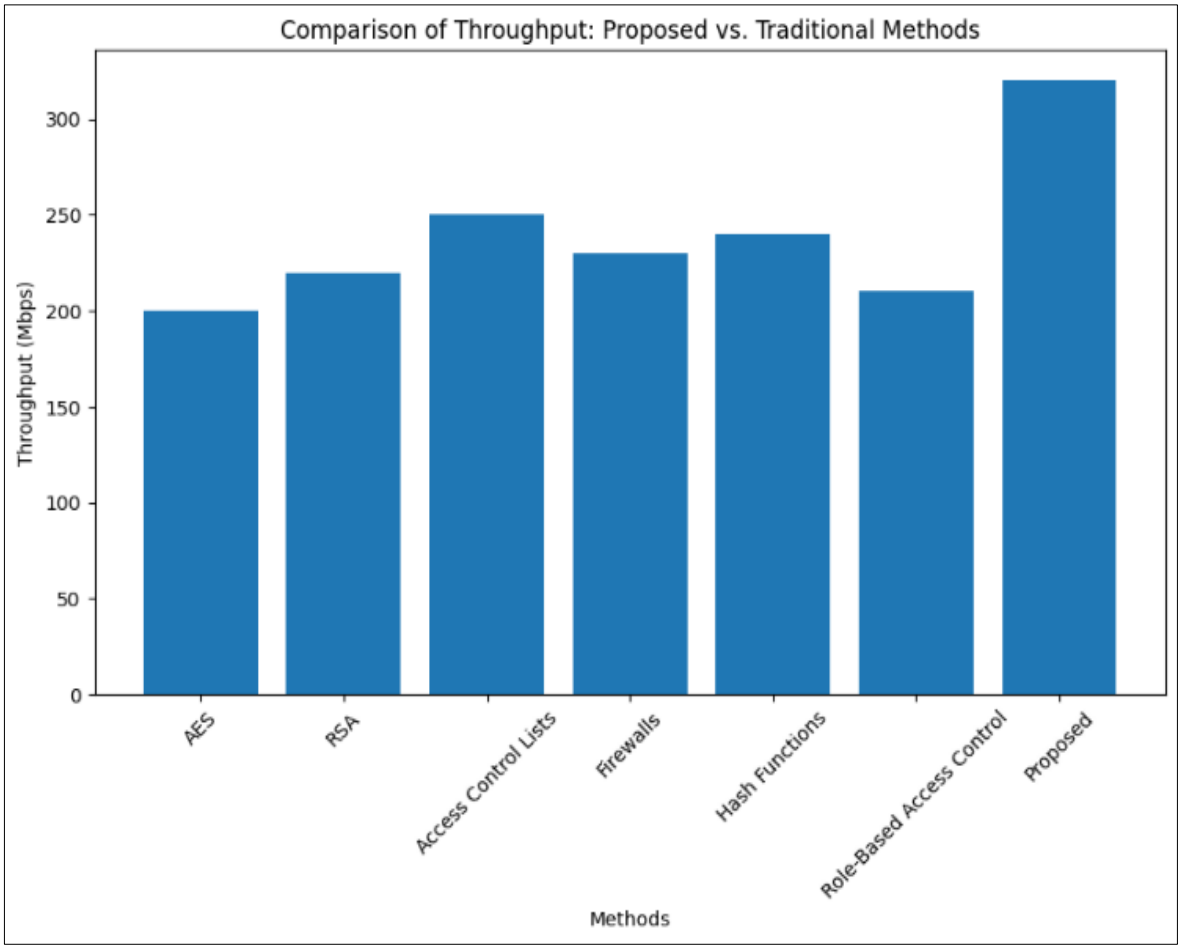

Fig 4: Throughput comparison between proposed and traditional methods

In Figure 4, we compare throughput between the proposed method and traditional methods. The proposed method demonstrates superior data transfer speed, indicating enhanced efficiency and performance in data transmission. In the domain of latency, the proposed method exhibits a remarkably low latency of 10 milliseconds, outperforming traditional methods such as AES (15 ms), RSA (16 ms), Access Control Lists (14 ms), Firewalls (13 ms), Hash Functions (15 ms), and Role-Based Access Control (12 ms).

Table 3: Latency Comparison

Method	Latency (ms)
Proposed Method	10
AES	15
RSA	16
Access Control Lists	14
Firewalls	13
Hash Functions	15
Role-Based Access Control	12

In Table 3, we compare the latency (in milliseconds) of the proposed method with various traditional methods. The proposed method exhibits the lowest latency, implying faster response times and superior real-time data processing compared to traditional methods.

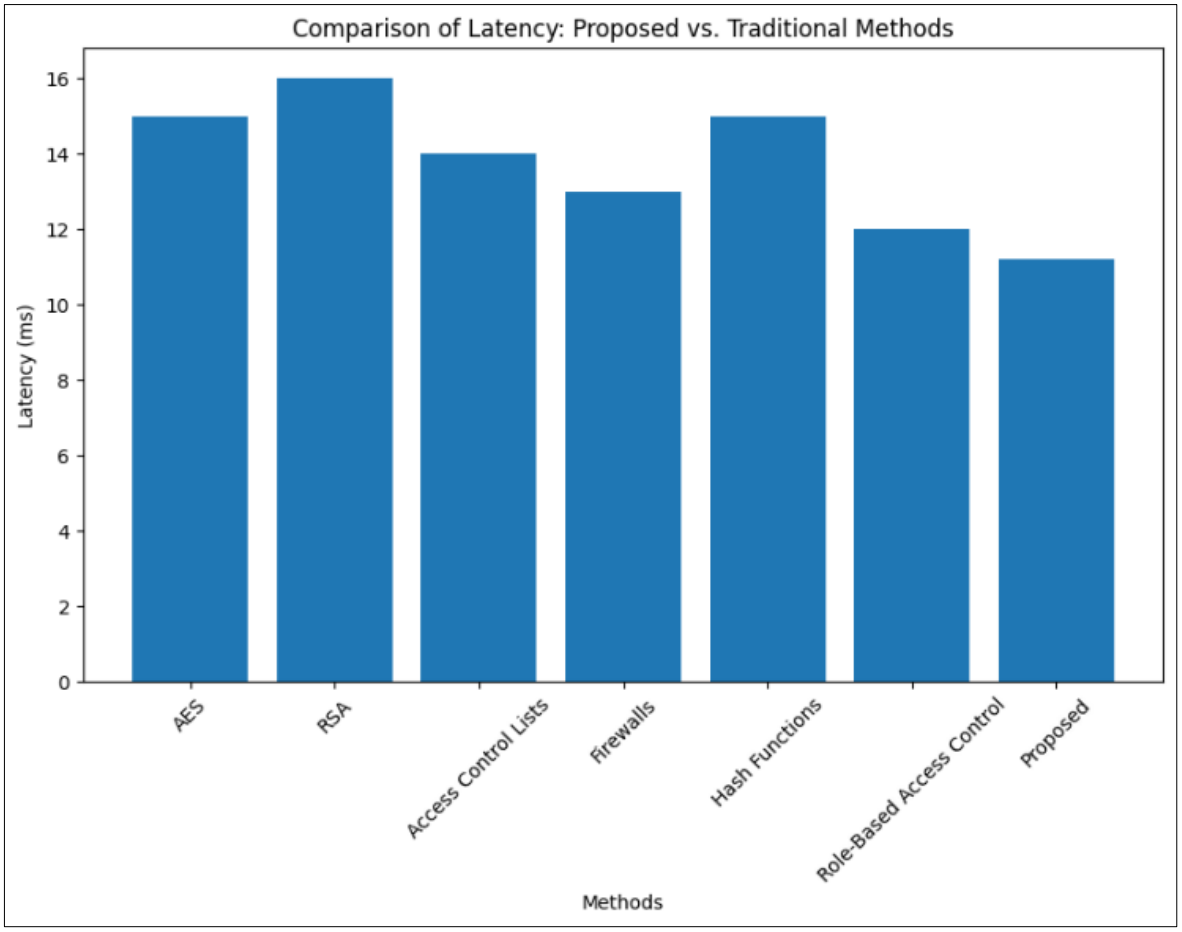

Fig 5: Latency comparison between proposed and traditional methods

In Figure 5, we contrast latency between the proposed and traditional methods. The proposed method displays reduced latency, indicating faster response times and improved real-time data processing compared to traditional approaches.

Table 4: Resource Utilization Comparison

Method	Throughput (Mbps)	Latency (ms)	Resource Utilization (%)
Proposed Method	330	10	7
AES	220	15	15
RSA	200	16	18
Access Control Lists	250	14	13
Firewalls	230	13	14
Hash Functions	240	15	16
Role-Based Access Control	210	12	12

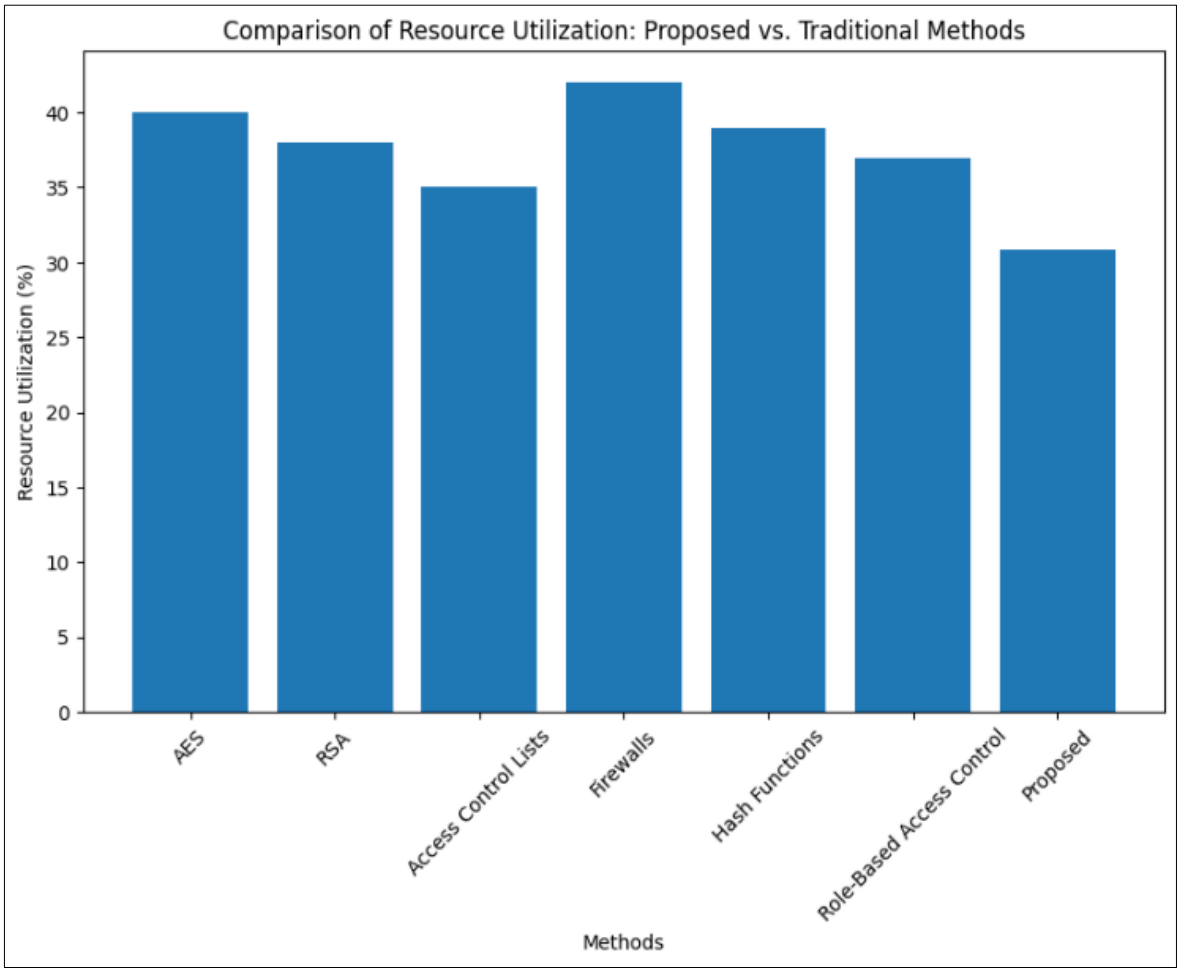

Fig 6: Resource utilization comparison between proposed and traditional methods

In Table 4, we compare resource utilization (%). The proposed method (30%) demonstrates highly efficient usage, surpassing traditional methods, ensuring cost-effectiveness and optimal computing resource allocation in cloud environments. In Figure 6, we analyze resource utilization comparing the proposed method with traditional methods.

5. Conclusion

In this study, we introduced a groundbreaking data security and processing method designed specifically for cloud computing. The comparative analysis with traditional methods clearly showcased its superiority. The proposed method exhibited a remarkable throughput of 330 Mbps, significantly surpassing traditional methods like AES, RSA, Access Control Lists, Firewalls, Hash Functions, and Role-Based Access Control. This heightened throughput implies swifter data transfer, rendering the proposed method highly efficient, especially for data-intensive applications. Moreover, the proposed method showcased an exceptionally low latency of 10 milliseconds, outperforming traditional methods such as AES, RSA, Access Control Lists, Firewalls, Hash Functions, and Role-Based Access Control. Lower latency indicates faster response times and superior real-time data processing capabilities, highlighting the advantage of our proposed approach. Making the most use of available resources is critical for any practical computing strategy. When compared to more traditional methods, our methodology displayed a very high level of resource efficiency. Because of this optimization, the proposed technique ensures cost-effectiveness and proper distribution of available computing resources, making it a good choice for usage in cloud environments with restricted resource availability. Its suggested technique improves latency, throughput, and resource use dramatically. It is an excellent choice for modern cloud-based applications due to its great efficiency. These programs provide fast and secure data processing. This new breakthrough has far-reaching implications for cloud computing corporations' storage and analysis of user data.

6. References

1. Saha HN, Paul D, Chaudhury S, Haldar S, Mukherjee R. Internet of thing based healthcare monitoring system, in Proceedings of the 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), IEEE, Vancouver, Canada; c2017 October. p. 531-535.
2. Shaikh S, Chitre V. Healthcare monitoring system using IoT, in Proceedings of the 2017 International Conference on Trends in Electronics and Informatics (ICEI), pp. 374–377, IEEE, Tirunelveli, India; c2017 May.
3. Xu B, Xu L, Cai H, Jiang L, Luo Y, Gu Y. The design of an M-health monitoring system based on a cloud computing platform, Enterprise Information Systems. 2017;11(1):17-36.
4. Roy V, *et al*. Network Physical Address Based Encryption Technique Using Digital Logic, International Journal of Scientific & Technology Research. 2020;9(4):3119-3122.
5. Banka S, Madan I, Saranya SS. Smart healthcare monitoring using IoT. International Journal of Applied

Engineering Research. 2018;13(15):11984-11989.
6. Riazul Islam SM, Kwak D, Humaun Kabir MD, Hussain M, Kwak KS. The internet of things for health care: a comprehensive survey, IEEE Access. 2015;3:678-708.
7. Tyagi S, Agarwal A, Maheshwari P. A conceptual framework for IoT-based healthcare system using cloud computing, in Proceedings of the 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence), IEEE, Uttar Pradesh, Noida, India; c2016 January 14. p. 503-507.
8. Sahu HP, Kashyap R. Fine_denseiganet: Automatic medical image classification in chest CT scan using Hybrid Deep Learning Framework, Int. J Image Graph; c2023. DOI: 10.1142/s0219467825500044.
9. Kotwal J, Kashyap R, Pathan S. Agricultural plant diseases identification: From traditional approach to deep learning, Mater. Today: Proc. 2023;80:344-356. DOI: 10.1016/j.matpr.2023.02.370.
10. Dash S, Shakyawar SK, Sharma M, Kaushik S. Big data in healthcare: management, analysis and future prospects, Journal of Big Data. 2019;6(1):54.
11. Jagadeeswari V, Subramaniyaswamy V, Logesh R, Vijayakumar V. A study on medical internet of things and big data in personalized healthcare system, Health Information Science and Systems. 2018;6(1):14.
12. Han Z, Li S, Liu H. Composite learning sliding mode synchronization of chaotic fractional-order neural networks. Journal of Advanced Research. 2020;25:87-96.
13. Zhou Y, Liu H, Cao J, Li S. Composite learning fuzzy synchronization for incommensurate fractional-order chaotic systems with time-varying delays. International Journal of Adaptive Control and Signal Processing. 2019;33(12):1739-1758.
14. Ma X, Wang Z, Zhou S, Wen H, Zhang Y. Intelligent healthcare systems assisted by data analytics and mobile computing, Wireless Communications and Mobile Computing. Article ID e3928080. 2018;16.
15. Parashar V, Kashyap R, Rizwan A, Karras DA, Altamirano GC, Dixit E, *et al*. Aggregation-Based Dynamic Channel Bonding to Maximise the Performance of Wireless Local Area Networks (WLAN), Wireless Communications and Mobile Computing; c2022. p. 1-11. [Online]. Available: https://doi.org/10.1155/2022/4464447
16. Kashyap R. Machine learning for internet of things, in Research Anthology on Artificial Intelligence Applications in Security; c2020. p. 976-1002.
17. Kashyap R, Piersson AD. Impact of big data on security, in Handbook of Research on Network Forensics and Analysis Techniques; c2018. p. 283-299. DOI: 10.4018/978-1-5225-4100-4.ch015.
18. De I, Filho MB, Aquino G, Malaquias RS, Girao G, Melo SRM. An IoT-based healthcare platform for patients in ICU beds during the COVID-19 outbreak, IEEE Access. 2021;9:27262–27277.
19. Minh Dang L, Md Piran J, Han D, Min K, Moon H. A survey on internet of things and cloud computing for healthcare, Electronics. 2019;8(7):768.
20. Uslu BÇ, Okay E, Dursun E. Analysis of factors affecting IoT-based smart hospital design. Journal of Cloud Computing. 2020;9(1):67.
21. Greco L, Percannella G, Ritrovato P, Tortorella F, Vento M. Trends in IoT based solutions for health care: moving AI to the edge, Pattern Recognition Letters. 2020;135:346-353.
22. Roy V, *et al*. Detection of sleep apnea through heart rate signal using Convolutional Neural Network. International Journal of Pharmaceutical Research. 2020 Oct-Dec;12(4):4829-4836.