International Journal of Modern Developments in Engineering and Science
Volume 2, Issue 9, September 2023
https://www.ijmdes.com | ISSN (Online): 2583-3138

Secure Cloud Communication – A Comparative Study of Cryptographic Protocols

P. Pranav Teja[1*], P. N. S. Praveen[2], A. Bhavya[3], J. Aishwarya[4], Surya Kanth V. Gangashetty[5]
[1,2,3,4]*Student, Department of Computer Science and Engineering, KL University, Vijayawada, India*
[5]*Professor, Department of Computer Science and Engineering, KL University, Vijayawada, India*

***Abstract*: The need for secure communication is more important nowadays in today's digital world, as many essential processes rely largely on services provided by the cloud. In securing clouds communication, this work explores a thorough comparative examination of cryptographic protocols, namely the Diffie-Hellman algorithm, RSA, and ECC. Using an experimental and observational approach, the investigation carefully investigates several performance indicators, including latency, throughput, resource utilization, and scalability. By means of meticulous examination of data, the study seeks to reveal subtleties regarding the effectiveness of every cryptography protocol, clarifying their unique advantages and disadvantages. The main objective is to provide knowledgeable viewpoints to practitioners and decision-makers so they may choose protocols for cryptography wisely that meet the various and changing needs of cloud settings. The study's findings and suggestions provide a useful manual for optimizing safe communication tactics while negotiating the complex choices among security and performance present in the ever-changing cloud computing environment. This paper is a useful resource for strengthening the security postures of cloud-based communication networks and makes a significant contribution to the current discussion on cryptographic protocols. The results reported here provide parties looking to strengthen the cybersecurity of their cloud-based services with useful information by crossing the divide among theory and real-world application.**

***Keywords*: Cryptography (ECC), Encryption process, Security.**

1. Introduction

Secure cloud communication is essential in the digital age of today, as services that are cloud-based are widely adopted and are now a must for both individuals and businesses. Cloud technologies' natural efficiency and ease of use, which enable smooth storage of information, interactions, and cooperation, have accelerated their absorption into many facets of human daily life [1]. Nonetheless, this ease of use comes with the heavy burden of guaranteeing the privacy, accuracy, and accessibility of sensitive data. Strong safety precautions are essential as more and more transactions, both personal and company, move to the cloud. Because there is a significant danger of unauthorized access, breaches of information, and other cyber-attacks, implementing safe transmission protocols is essential to maintaining the reliability of systems that are cloud-based. The technological foundation of contemporary civilization is reinforced by secured cloud interactions, which not only defend against possible cyber-attacks but also respect the values of privacy, reliability, and accessibility in this ever-changing context [2].

Understanding the complex issues and the constantly changing character of cyber threats is crucial when tackling the necessity of security communication via the cloud [3]. The need for a thorough and flexible security strategy is highlighted by the ever-growing attack area and the advanced tactics used by malevolent actors. A crucial element in attaining this level of security is the prudent choice and application of cryptographic technologies. The foundation of secure cloud communication is made up of protocols known as cryptography, which offer ways for handling keys that are encrypted, authenticate both individuals and systems, and encrypt data while it's in transit. Comprehending the various protocols for cryptography in detail is essential to customizing safety precautions to the unique requirements of cloud-based applications [4]. The field of security is full of possibilities, ranging from more sophisticated methods like homomorphic cryptography, which allows calculations on encrypted data, to more established standards like TLS/SSL, which safeguard data during transport. It is crucial to strike the correct balance between security and achievement, particularly in the setting of computing in the cloud, because flexibility and effectiveness are equally important factors [5].

In addition, the world of secure cloud communication includes adhering to specific to industries standards, information retention demands, and regulatory structures. A comprehensive strategy that incorporates regulatory frameworks, technology solutions, and ongoing surveillance and adjustment is needed to navigate these challenges [6]. The pursuit of secure cloud communication is becoming more than just a technical task as the digital environment develops; it is now a strategic necessity for both individuals and enterprises. Guarantee the robustness and dependability of systems running on the cloud in a constantly evolving digital environment, it necessitates constant creativity, cooperation, and a dedication to keeping in front of emerging dangers. Figure 1 shows the Securing Cloud Communications Framework.

*Corresponding author: pranavteja6437@gmail.com

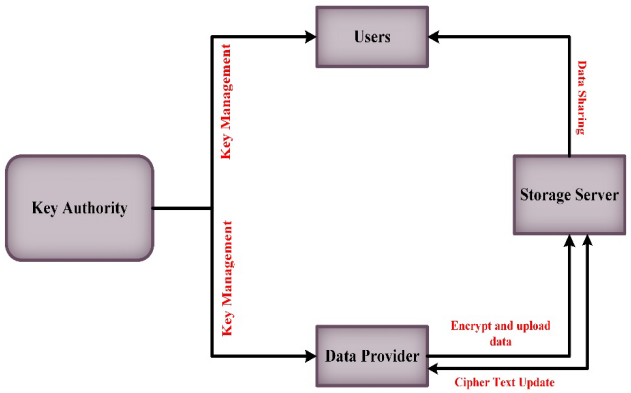

Fig. 1. Securing cloud communication framework

2. Literature Review

Zeadally et al. [7] explains that physically and virtualized networked items that gather and share information through the open Internet make up the Internet of Things (IoT). In an Internet of Things setting, numerous security threats are possible because this exchange frequently occurs over open networks. They start by quickly going over the security concerns with the Internet of Things. To guarantee safe connections, we then concentrate on current cryptography protocol norms that are either in use or are being suggested for IoT devices. Additionally, they emphasize the benefits and drawbacks of the different standards for protocols for a range of Internet of Things applications, such as consumer goods and gadgets, health, linked cars, and smart homes. In conclusion, they go over a few issues with cryptography protocol norms that remain to be resolved for Internet of Things apps in the years to come. The thorough comparison analysis might encounter difficulties taking into consideration the quickly changing state of cryptography and new threats, which could affect the research's long-term applicability.

A hyperconnected civilization is taking shape where objects and objects, or individuals and things, talk to one another via the Internet of Things. Due to the limits of the current IoT ecosystem, including power consumption, quantity, and efficiency, incorporating cloud computing capabilities is being proposed as an entirely novel model. Nonetheless, challenges remain in the new converging paradigms to address so as to reduce dangers related to information privacy and information management. Jin et al. [3] designs a homomorphic security protocol for communications for cloud computing-based Internet of Things convergence that uses RLWE for identifying users and messaging handling. To guarantee security and safety, they performed performance evaluations on both the suggested connection protocol and the transmission protocols used in the current IoT environment. Through performance examination of the suggested communication method and the present IoT environment communications procedure, the research confirmed its safety and security. To verify that the suggested communication technique offers strong safety and a comparable degree of effectiveness, the researchers performed a comparison regarding time complexities and spatial complexity in line with encrypting and decoding, respectively. The research also sought to create a secure communication infrastructure for users, from authenticating users to transmitting information through the design of a protocol for communication. The suggested encryption communications protocol's technical characteristics are not specifically stated in the announcement, which makes it difficult to evaluate its effectiveness and possible drawbacks.

Massive clustering of managed and serviced assets is employed in the cloud for computing purposes, and by utilizing the cost-per-use approach, these resources may be virtually and constantly altered to provide optimal resource utilization. Nonetheless, security apprehensions have hindered the widespread use of the cloud computers paradigm. In this way, the widespread use of the internet around the globe has hastened cryptography breakthroughs, which have emerged as an essential field in tackling most of these safety concerns.[8], A combination of a cryptographic method that uses the Paillier and Blowfish encryption protocols is being described, and its efficacy was assessed in comparison to the current mixed methods of Rivest Shamir Adleman (RSA) and the Advanced Encryption Standards (AES). Two stages of safe storage of information protocol techniques have been introduced. The suggested hybrid protocols aim to reduce computational time and the ciphertext size, hence increasing the efficiency of cloud storage. Mist server running on an Ubuntu 16.04, which platform and Virtual Box from Oracle have both been utilized for experiments. This combination of homomorphic and asymmetrical processes has proven to improve security. The use of compressing has aided in reducing computing time as well as storage capacity. Performance evaluation is being done for several block cipher methods with respect to computational complexity as well as quality of service characteristics such as weights of variables regardless of assaults, throughput, and stream duration. Utilizing Lynis 2.7.1, security evaluation is being performed by employing the Hardness indices as an auditing variable. Similarly, security for firewalls had been created in the selected mixed algorithms for stopping the previously stated methods and controlling traffic. Lastly, it has been shown that the Paillier and Blowfish combination performs better with and without compressing than other systems that use RSA and AES processes. The particular encryption systems, applications, or programs mentioned in the declaration are not made clear, which makes it difficult to evaluate the viability and potential downsides of the suggested research initiatives.

Khan et al. [9] explains the electronic and physical realms are linked by a new and developing technology called the Internet of Things (IoT). Uses for Internet of Things (IoT) technology can be found in many different domains, including homes, medical care, public transportation, sanitation and water supply, and monitoring the environment. Yet since IoT devices that are smart have limited computational, interactions, storage spaces, and power capacities, there are numerous security risks associated with the Internet of Things, despite its limitless potential. There are numerous cryptographic methods that are computationally light and suitable for these limited-in-resource IoT gadgets. However, because networks at those ends are

capable of processing security protocols that require more computing power and because they function in surroundings that are comparatively more hostile, lightweight approaches leave the rich in resources endpoints of the Internet of Things (such as edge, fog, or clouds modes) exposed. IoT systems have asymmetric computing its very nature, therefore security mechanisms need to be flexible enough to adjust to the availability of resources at the node on which they run. The framework of the Internet of Things, the computing power of end devices, edge, fog, and cloud computing platforms, and the current state of lightweight cryptography protocols are all covered in this overview. An examination of the benefits, limitations, and weaknesses of the current lightweight cryptographic solutions emphasizes the necessity for elastic secure protocols that can adjust to the asymmetrical abilities of various Internet of things nodes.

3. Problem Statement

A thorough examination of cryptographic techniques and how they are utilized in communication over clouds is provided by the literature study. The basic concepts and implementations of encryption protocols, which include TLS, IPsec, and Signal Protocol, which are frequently utilized in cloud communication applications like storing files and messaging apps, are examined. The research reveals a wide range of difficulties related to the execution of encryption protocols in cloud systems, from complex managing key processes to scalability constraints. New developments in cryptography after quantum computers and the incorporation of homomorphic encryption are emphasized, offering perspectives on the changing environment [10]. Through a comprehensive evaluation of the body of existing literary works, the study points out deficiencies in research, including underutilized applications, a dearth of studies on particular cloud communication solutions, and real-world implementation issues. Prominent results from earlier research add to a body of knowledge by providing insightful information about the security posture, weaknesses, and comparisons of cryptographic systems. This comprehensive investigation goes beyond the boundaries of cryptography, taking into account interdisciplinary perspectives that link cryptographic techniques to confidentiality of information, network safety, and compliance with regulations. The previous study, which provides an in-depth knowledge of the present state of encryption protocols in the setting of secure cloud interactions, essentially acts as a fundamental step that informs additional study efforts.

4. Methodology

A. Data Gathering

The selection of cloud communication services for analysis is a strategic process aimed at ensuring a well-rounded evaluation of cryptographic protocols. In acknowledging the diverse nature of cloud-based communication, a comprehensive range of services has been chosen for examination. File storage services have been included to assess cryptographic protocols in the secure storage and sharing of data, particularly relevant for organizations managing sensitive information. Messaging platforms form a key component, allowing the study to scrutinize cryptographic protocols' influence on real-time interactions, file attachments, and overall communication security. Collaboration tools are integral for evaluating secure collaboration scenarios, including document versioning and simultaneous editing. Video conferencing services are essential in the contemporary landscape of remote work, offering insights into how cryptographic protocols contribute to secure virtual meetings and data transmission. Email services, with their pervasive use, are included to explore cryptographic protocols in ensuring the confidentiality of email content and attachments. Social collaboration platforms, VoIP services, and document sharing and editing platforms further enrich the analysis, addressing unique challenges in secure information sharing, voice communication, and collaborative document management. This diverse selection ensures that the study captures the nuanced security requirements of various cloud communication scenarios, providing a holistic understanding of how cryptographic protocols contribute to the safeguarding of sensitive information in the digital age.

B. Outline of the Proposed Framework

Security criteria encompass the fundamental principles that safeguard the integrity, confidentiality, and authentication of transmitted and stored data. This includes assessing the protocol's capability to maintain data confidentiality, ensure data integrity against tampering, establish robust authentication mechanisms, and effectively manage cryptographic keys. On the other hand, performance criteria focus on the efficiency and scalability of the cryptographic protocol. This involves evaluating factors such as latency, measuring the time delay in encryption and decryption processes; throughput, assessing the data transfer rate; resource utilization, examining the impact on system resources; and scalability, gauging the protocol's ability to adapt to varying workloads and data volumes. To quantify these criteria, specific metrics are defined, offering a quantifiable and standardized approach to the evaluation process. This dual-dimensional framework ensures a comprehensive assessment of cryptographic protocols, facilitating informed decision-making in the selection and implementation of protocols that strike an optimal balance between robust security measures and efficient performance in cloud communication scenarios.

The research methodology for this study adopts a comparative approach, combining elements of experimental and observational design to thoroughly assess the cryptographic protocols: Diffie-Hellman algorithm, RSA, and ECC, within the dynamic context of cloud communication. The comparative study design enables a nuanced evaluation of the security and performance attributes of each protocol, crucial for understanding their real-world applicability. In the experimental setup, the Diffie-Hellman algorithm is implemented for secure key exchange, RSA for public-key cryptography, and ECC as a symmetric key block cipher for data at rest. The evaluation involves comprehensive testing of each protocol's setup, including key generation, distribution,

encryption, and decryption processes, emulating scenarios encountered in cloud communication environments. Data collection encompasses traffic analysis to measure latency, throughput, and security metrics such as successful encryption rates. Additionally, resource monitoring provides insights into the impact of each cryptographic operation on system resources. The ensuing quantitative and qualitative data analysis will offer a comprehensive understanding of the strengths and weaknesses of each cryptographic protocol, informing practical decision-making in the selection and implementation of secure communication solutions for cloud environments.

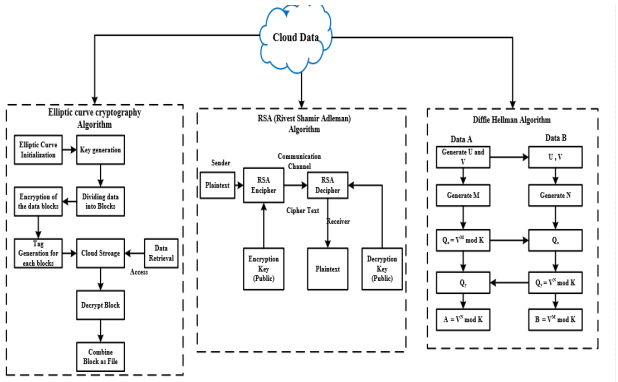

Fig. 2. Conceptual framework of the study

C. *Elliptic Curve Cryptography (ECC)*

When it comes to performance standards, ECC is a noteworthy cryptography technique that uses mathematical features of elliptical curves to facilitate safe communications. ECC is assessed in this part using efficiency and safety standards. The efficacy of elliptic curve-based encryption in protecting the privacy of information, elliptic curve signatures that are digital in guaranteeing data integrity, and the use of reliable authentication techniques like elliptic curve-based key transfers in establishing ECC security are all considered. Performance metrics, including latency, productivity, utilization of resources, and scalability, are evaluated in detail. To make an ECC evaluation procedure standardized and quantifiable, particular quantifying criteria are specified[11]. ECC is implemented for safe key transfer as well as information encryption in the experimental context, and the key generations, shipping, and decrypt operations are thoroughly tested. Latency, throughput, and safety indicators are measured by traffic evaluation, while the effects of ECC on the system's resources are shown by resource management.

The qualitative as well as quantitative characteristics of ECC are the primary objective of the following information study, which also evaluates its advantages and disadvantages in relation to additional cryptographic methods. The final section of this part summarizes the research on ECC and provides those making decisions with useful information for choosing cryptography protocols that best match strong security with effective performance in the ever-changing world of cloud communication infrastructures. The purpose of including ECC in the suggested framework is to advance the knowledge of how it improves the safety postures of cloud-based communication networks.

D. *Rivest-Shamir-Adleman (RSA)*

Rivest-Shamir-Adleman, or RSA, is a popular public-key system of cryptography that is essential to the security of online transactions and communications. RSA, which was created in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, transformed cryptography by presenting the idea of asymmetrical key encrypting. Two keys are used by the systems: a key that is private for decryption and a public key that's used for encryption. The RSA issue, or the computational difficulties of factoring the result of two large numbers that are prime, is the foundation for the safety of RSA [12].

With RSA, the communication is encrypted by the person who sends it utilizing the public key of the receiver, and the person who receives it is able to decrypt it with their personal key. The foundation of secure communication involves this asymmetry, which permits data to remain private and secure. RSA is frequently used to encrypt sensitive data, including electronic signatures, and online transactions, as well as the creation of secure Internet routes of communication. Although RSA is resilient, its safety is dependent on the duration of the key; higher key lengths are advised to fend off potential assaults as processing power improves. The long-lasting importance of RSA in the cryptography community highlights its fundamental function in guaranteeing the privacy and safety of electronic communication across a range of uses.

E. *Diffie-Hellman Algorithm*

A fundamental cryptography protocol known as the Diffie-Hellman key exchange method was first presented by Whitfield Diffie and Martin Hellman in 1976. It allows two individuals to securely transfer key cryptography via an insecure communications channel. It serves as the foundation for creating a secret key that is shared among both parties without needing individuals to be aware of one another's private information beforehand [13]. The continuous logarithmic problem's difficulties determine the Diffie-Hellman algorithm's safety. A number of steps are involved in the key transfer procedure:

1. *Parameters choosing:* A huge prime integer (p) and the primitive roots modulus p(g) are two open variables that both sides agreed upon.
2. *Public Key Transfer:* Utilizing the predetermined variables, each side creates a secret key (a or b) and determines the public key (A or B). Next, publicly accessible keys are transferred via the unreliable channel.
3. *Shared Secrets Estimation:* The two parties separately calculate a secret key they share utilizing their personal keys and the publicly available keys they receive. The method works by overcoming the issue of discrete logarithms, which prevents an eavesdropper from readily determining the secret that was shared even when publicly accessible keys are transferred in a transparent way.

A number of safe communication procedures, such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) for safeguarding online traffic, employ the Diffie-Hellman algorithm extensively. It is significant because it contributes to the basis of contemporary encrypted communication by offering a safe way for organizations to reach an understanding of a common confidentiality agreement across a network that is not trusted.

5. Result

Performance metrics were carefully examined in this comparison of cryptographic approaches (Diffie-Hellman, RSA, and ECC) for safe communication through the cloud. The results provide detailed insights into the advantages and disadvantages of every protocol, assisting those making decisions in choosing cryptographic protocols appropriate for various cloud environments. With the ever-changing Internet computing ecosystem, the research offers a useful guide for optimizing secure communication techniques and managing the intricate trade-offs between safety and efficiency. This work greatly improves cloud-based communications network trustworthiness by crossing the theory-application gap. Here is a condensed illustration of table 1 that compares Diffie-Hellman, ECC, and RSA depending on important characteristics.

Different features of the encryption protocols RSA, ECC, and Diffie-Hellman are compared in this investigation. Despite being used extensively for cryptography and electronic signatures, RSA is vulnerable to quantum attacks due to its lengthy key needs and high computing overhead. ECC is an effective solution for resource-constrained contexts, such as mobile phones, because it uses shorter keys and can withstand quantum assaults. Diffie-Hellman, which is typically used in safe key exchange, performs moderately well. It is based on the discrete logarithm challenge and is flexible with respect to key length. This brief summary encapsulates the most important characteristics, enabling decision-making when choosing cryptographic protocols that meet a range of security requirements and application scenarios.

This study compares the key lengths of three cryptographic protocols: Diffie-Hellman, ECC, and RSA. It finds a distinct difference. When the length of the key increases, RSA grows more prominently, ECC performs remarkably well, and Diffie-Hellman grows somewhat. Interestingly, ECC needs far lower key lengths to get similar security levels. This brief summary illustrates the key length consequences for every protocol, which helps decision-makers choose cryptographic techniques that meet security needs.

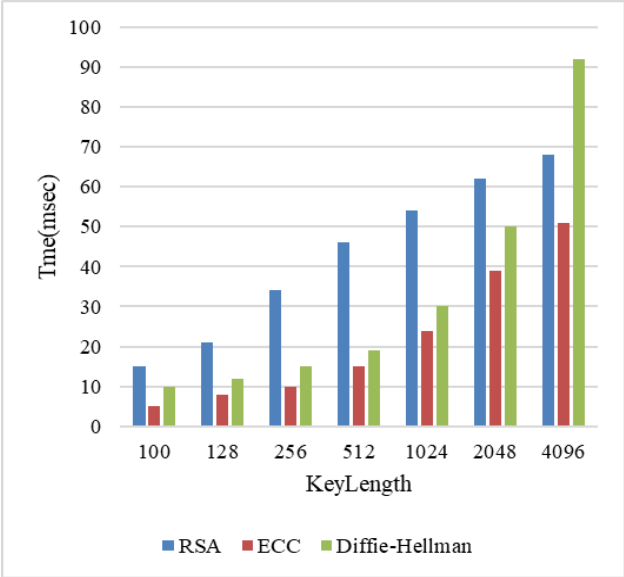

Fig. 3. Encryption time

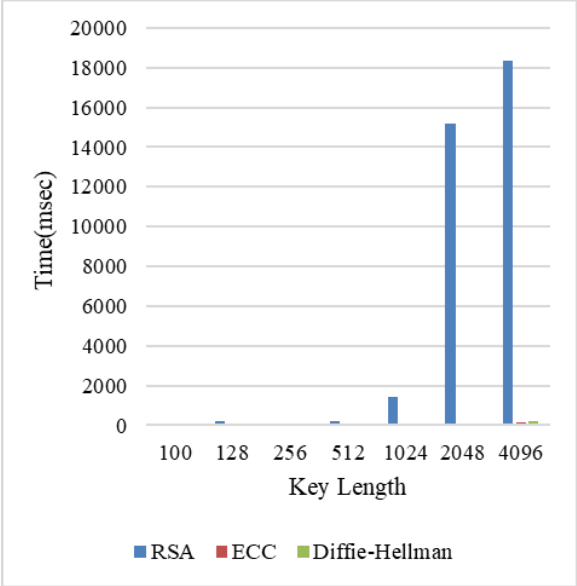

Fig. 4. Decryption time

Table 1
Comparative analysis of cryptographic Protocols: RSA, ECC, Diffie-Hellman

Criteria	RSA	ECC	Diffie-Hellman
Length of key	Longer keys are necessary.	Reduced key lengths are adequate	Key lengths vary based on safety guidelines
Complexity of Computation	Comparatively high computational burden	Effective in both encryption and generating keys.	Computational complexity in the middle
Security	Susceptible to quantum assaults	Able to withstand quantum attacks	Dependent on the discrete logarithm problem and resistant to quantum threats
Performance	Slower in terms of encryption and generating keys.	Quicker in terms of encryption and generating keys.	Moderate output, particularly in big groups
Application	Extensively utilized for encryption, key sharing, and digital signatures	Frequently utilized on mobile phones and in settings with limited resources	Mostly utilised for key exchange, particularly when creating secure connections

Table 2
Encryption time for RSA, ECC, Diffie-Hellman

Key Length	RSA	ECC	Diffie-Hellman
100	15	5	10
128	21	8	12
256	34	10	15
512	46	15	19
1024	54	24	30
2048	62	39	50
4096	68	51	92

Table 3
Decryption time for RSA, ECC, Diffie-Hellman

Key Length	RSA	ECC	Diffie-Hellman
100	88	11	16
128	188	25	31
256	62	36	47
512	218	51	63
1024	1453	63	78
2048	15203	89	109
4096	18381	159	187

This study compares the decryption times of three cryptographic protocols: Diffie-Hellman, ECC, and RSA. Based on key length, a distinct trend is observed. Longer key lengths significantly increase the RSA decryption time, which can reach much higher levels. ECC continuously exhibits effective decryption at all key lengths, highlighting its intrinsic benefit in this regard. In terms of decryption time, Diffie-Hellman is in between RSA and ECC, while being faster than RSA in general. This succinct analysis offers insightful information on how well each cryptographic protocol decrypts, assisting in the selection of suitable protocols depending on particular key length needs.

6. Summary and Conclusion

To sum up, this contrasting examination of the encryption protocols Diffie-Hellman, RSA, and ECC highlights how crucial safe communication is in today's digital world, wherein cloud-based services are integral to many daily operations. The detailed analysis of performance metrics, including throughput, latency, resource usage, and scalability, provides insight into the subtle differences in efficiency between every cryptographic protocol. The research is a useful tool for those making decisions and professionals, providing well-informed perspectives to help choose cryptographic protocols that meet the varied and changing requirements of cloud environments.

The study helps to optimize safe communication techniques by offering an in-depth comprehension of the benefits and drawbacks of every procedure, traversing the complex trade-offs between safety and efficiency that accompany the dynamic internet computing of the surroundings.

Furthermore, this research's conclusions and suggestions provide a useful guide for improving cloud-based communications networks' safety posture. Besides philosophical concerns, the work seeks to close the divide between cryptographic theories and practical implementation. Accessing the ever-changing landscape of cloud security, the findings presented here provide users with pertinent and helpful data to help them decide on actions that will improve the trustworthiness of their cloud-based systems. This work makes a significant contribution to the current discussion on cryptographic protocols at a time when the convergence of theory and practice is critical, laying the groundwork for dependable and safe cloud communication techniques.

References

[1] A. Bangar and S. Shinde, "Study and comparison of cryptographic methods for cloud security," *Int J Comput Sci Eng Inf Technol Res*, vol. 4, no. 2, pp. 205–213, 2014.

[2] S. Ambika, S. Rajakumar, and A. Anakath, "A novel RSA algorithm for secured key transmission in a centralized cloud environment," *Int. J. Commun. Syst.*, vol. 33, no. 5, p. e4280, 2020.

[3] B.-W. Jin, J.-O. Park, and H.-J. Mun, "A design of secure communication protocol using RLWE-based homomorphic encryption in IoT convergence cloud environment," *Wirel. Pers. Commun.*, vol. 105, pp. 599–618, 2019.

[4] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Comput. Sci. Rev.*, vol. 33, pp. 1–48, 2019.

[5] A. Katal, S. Dahiya, and T. Choudhury, "Energy efficiency in cloud computing data centers: a survey on software technologies," *Clust. Comput.*, vol. 26, no. 3, pp. 1845–1875, 2023.

[6] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in IoT-based cloud computing: A comprehensive survey," *Electronics*, vol. 11, no. 1, p. 16, 2021.

[7] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet Things*, vol. 14, p. 100075, 2021.

[8] B. Seth *et al.*, "Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm.," *Comput. Mater. Contin.*, vol. 67, no. 1, 2021.

[9] M. N. Khan, A. Rao, and S. Camtepe, "Lightweight cryptographic protocols for IoT-constrained devices: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4132–4156, 2020.

[10] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure," *Appl. Sci.*, vol. 11, no. 10, p. 4580, 2021.

[11] S. Shukla and S. J. Patel, "A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing," *Computing*, vol. 104, no. 5, pp. 1173–1202, 2022.

[12] P. Kalpana and S. Singaraju, "Data security in cloud computing using RSA algorithm," *Int. J. Res. Comput. Commun. Technol. IJRCCT ISSN*, pp. 2278–5841, 2012.

[13] F. Li *et al.*, "Privacy-aware secure anonymous communication protocol in CPSS cloud computing," *IEEE Access*, vol. 8, pp. 62660–62669, 2020.