International Conference on
Global Engineering & Management Trends

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Hybrid Encrypted Socket Towards Security in Cloud Environment

Ms. Radhika Garg, Dr. Kavita Mittal
Engineering & Technology, Jagannath University, Bahadurgarh

Abstract- The proposed encryption method offers significant benefits over traditional cryptographic approaches, including improved performance and security in time consumption, error rate, and resistance to various types of attacks. It consistently outperforms DES, RSA, AES, and DNA encryption in terms of time consumption, error rate, along with security analysis. The method's reduced packet size and compression techniques enhance processing speed and decrease latency, reducing the likelihood of errors during data transfer. In terms of error rates, proposed method shows a significant reduction compared to other methods, minimizing packet size and transmission time, thereby reducing the likelihood of errors during data transfer. It also excels in security analysis, with lower susceptibility to attacks such as, brute force, denial-of-service, and access violations. It demonstrates superior resilience against Man-in-the-Middle attacks and brute force attempts, achieving fewer successful breaches than DES, RSA, AES, and DNA encryption methods. The advent of CC has made it possible for individuals to test out novel concepts, such as managing digital resources and content calls. Current research has identified potential security models such as RSA, AES, DES, and DNA protection for safeguarding data stored on the cloud. However, the effectiveness of clouds has only been the subject of limited studies. Researchers have conducted extensive investigations to enhance the cloud's performance and security level, with the goal of increasing safety levels without compromising operational efficacy. Cloud computing provides platforms for innovative practices, such as building digital resources and content management. Existing security models, such as mechanism, DNA security, and several security protocols, have been used to secure cloud-based contents. However, limited research has focused on cloud performance, and the proposed solution should improve security without affecting or decreasing performance.

Keywords- Encryption, cloud computing, Data Security.

I.INTRODUCTION

The one-of-a-kind computer technology is cloud computing. A pool of resources is made available as needed. New service delivery models are suggested by cloud computing. Organizational practices will shift as a result of these ground-breaking price and technological prospects. "Cloud computing" is only fancy name for old concept. A cloud service provider offers a collection of resources accessible

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

via the internet, which is known as cloud computing (Abd Al Ghaffar, 2024). Globally dispersed data centers provide cloud services. Users are able to access and use virtual resources using cloud computing. Within a few years, CC became the talk of town (Alam, A., 2022). Google Cloud Platform, Microsoft Office 365, and Oracle Cloud are all examples of cloud services. Security issues are becoming more pressing as cloud computing continues its fast expansion (Garrison, G., 2012). The number of cloud-based apps is constantly growing, and more and more people are using cloud services to transfer digital files. Consequently, digital stuff continues to be vulnerable while in transit. Performance has also been shown to have dropped as a result of security mechanism integration into cloud systems(Abdullayeva, F, (2023). The purpose of research was to enhance the cloud's performance and security. The proposed solution should improve security without affecting or deteriorating performance (Jumani, A. K., 2023). The research is looking at the studies that have been published and looking into their limitations in terms of security vulnerabilities in cloud applications. A research paper proposes a secure Encrypted Hybrid model to improve the performance of cloud systems and socket-based high-performance mechanisms in order to reduce transmission delay, error, and packet loss probability. On the basis of security, performance, and reliability, research is comparing the suggested model to existing methodologies (Karak, S., 2015; Katal, A., 2023). The necessity, motivation, and challenges of the suggested effort would be presented in this study. This research would consider the process flow of proposed work after considering the problem description. The algorithm and mechanism employed in work would explain the tools and approaches used in study. The results of the simulation would be presented, along with a description of how the proposed study is superior to past efforts. The research can be carried out using a variety of approaches, which are described in more detail below. Exploratory research is used to arrange and discover novel topics. Creating research that provides solutions to a problem (Kaur, H., 2023).

Cloud computing

"Cloud computing" refers to a way of running applications, data, and files that makes use of a network of interconnected computers, either privately or publicly accessible, to provide elastic capacity for these tasks (Abdulsalam, Y. S., 2021) The introduction of this technology has greatly decreased the costs of processing, application hosting, content storage, and distribution (Korucu, A. T., 2017). In addition to providing a practical means of realizing savings right now, cloud computing has potential to transform capital-intensive structure of a data center into a variable-priced one (Kumar, G., 2011). The capacity to reuse information technology resources is essential to cloud computing (Ahmadi, S. (2024). When compared to more traditional concepts such as "autonomic computing," "utility computing," or "grid computing," capacity of cloud computing to broaden viewpoints outside organizational borders stands out.Instead of investing in costly and time-consuming hardware and software to run their own data centers and applications, companies may instead rent these resources from cloud service providers (Akbar, H., 2023).

Cloud computing in distance learning

Distance learning is becoming more popular and in demand (Waqar, A., 2023). A wide range of courses and degrees are available through distance-education programs. In order to provide more help to teachers and students, distance learning programs must constantly expand and upgrade their IT infrastructures. It is possible that cloud computing, a new IT paradigm, may help the educational sector to utilize and consume IT resources more effectively (Vellela, S. S., 2023). Cloud computing is an important part of achieving this objective (Herhalt, J., 2012). Networks, storage, services, servers, and apps are examples of these resources (Yalamati, S. 2024). These resources could be allocated with minimal managerial effort. As a result, cloud computing and distance learning are frequently coupled. Cloud computing has revolutionized distance learning by making educational resources and tools accessible, scalable, and flexible. It allows students and educators to access materials anytime, anywhere, using any internet-connected device, which enhances learning beyond physical classrooms

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

(Yang, H., 2012). Cloud-based platforms like Google Classroom, Microsoft Teams, and Zoom facilitate virtual classrooms, live lectures, and real-time collaboration (Cinar, B., 2023). These services scale easily to accommodate more students without significant infrastructure investment, making education more cost-effective (Yenugula, M., 2023). Cloud tools also promote collaborative learning, with platforms like Google Drive and With Microsoft One Drive, students from all around the world can collaborate on projects in real time. Learning management systems hosted on the cloud, such as Canvas and Blackboard, allow schools to better organize and allocate resources while also providing analytics to monitor students' development (Fadhil, I., 2023). Additionally, cloud computing enables the incorporation of cutting-edge technology like VR, AI, and ML, which enhances the educational experience (Gai, K., 2020). In addition to safeguarding sensitive information and offering disaster recovery options, it guarantees strong data protection and backup. As a vital tool for contemporary education, cloud computing improves the accessibility, efficiency, and quality of distant learning (Hurwitz, J. S., 2020).

Influencing factors

He adoption and implementation of CC are influenced by a myriad of factors spanning technological, financial, regulatory, and organizational realms. Technological advancements continually shape the landscape of cloud computing, with innovations such as virtualization, containerization, and serverless computing driving organizations to explore new capabilities and efficiencies offered by cloud platforms. These advancements not only enhance performance but also expand the scope of possibilities for leveraging cloud resources in diverse applications and industries. Financial considerations, particularly cost savings and operational efficiency, play a pivotal role in driving cloud adoption (Kumar, G., 2011). However, organizations must also carefully assess total cost of ownership (TCO) factors, including subscription fees, data transfer costs, and ongoing operational expenses, to ensure that cloud adoption aligns with their budgetary constraints and long-term financial objectives.Threats to cloud security have come from malware and other outside sources. Therefore, it is possible to hack instructional information sent via the internet. Without proper authentication, hackers are able to access sensitive information. Conversely, decrypting Encrypted data is the job of the cracker. It is common practice to use Encryption methods and firewalls in order to guarantee safety. The Encryption techniques that are used to increase security of system are time-consuming and influence the performance of system.

Threats to security

According to the (CSA) report, several top threats pose significant risks to cloud computing environments, necessitating organizations to be vigilant and proactive in addressing cybersecurity challenges (Mishra, J. P., 2019). One prominent threat is data breaches, which can result from various factors such as unauthorized access, misconfiguration. Another critical threat is inadequate identity, credential, and access management (ICAM), which can result in unauthorized access to cloud resources and services. Weak authentication mechanisms, insufficient access controls, and ineffective monitoring of user activities can facilitate unauthorized privilege escalation and unauthorized data access, increasing the risk of data breaches and security incidents. Additionally, insecure interfaces and (APIs) pose significant threats to cloud security(Mohamed, E. M., 2013). Vulnerabilities in cloud service interfaces and APIs can be exploited by attackers to manipulate cloud resources, compromise data integrity, and launch attacks such as injection attacks, (XSS), and authentication bypass, undermining the overall security posture of cloud environments.

1.6 Cryptography

To protect the privacy, authenticity, and integrity of sensitive data sent between users and platforms in cloud-based distant learning, cryptography is essential (Oladoyinbo, 2023). Cryptography safeguards information from prying eyes by transforming it into an unintelligible format via the process of Encryption. Protocols ensure that data sent during online courses and group projects cannot be

intercepted or altered in any way. Secure cryptographic key creation, storage, and distribution is a must for keeping Encrypted data and communication routes private. Good key management procedures make this possible (OsmanP, 2016). Cryptography helps firms preserve student information and maintain regulatory compliance, which in turn facilitates compliance with data protection rules and industry standards. As a whole, cryptography is vital for the safety and reliability of online education in the modern day by protecting the privacy, authenticity, and integrity of data stored in remote learning environments hosted on the cloud. When a communication is Encrypted using cryptographic procedures, only the sender and the intended recipient can decipher its contents (Pandey, 2019). The name derives from the Greek word kryptos, meaning "hidden" in English. In the event of interception, a third party has all the necessary information to decipher and read the message. There are three main categories of cryptography (Parast, F. K., 2022):

Encryption

One of the most basic cybersecurity techniques is Encryption, which uses cryptographic algorithms and keys to transform data from plaintext to ciphertext. The data's security and integrity are guaranteed by making it unreadable to unauthorized users via this method. Protecting private data including student records, grades, and personal information is of the utmost importance in cloud-based distant learning (Patil, P., 2016). In order to Encrypt and decode data, Encryption techniques make use of cryptographic keys. Unauthorized access cannot occur since these keys are produced and kept securely. The two most common forms of Encryption are symmetric and asymmetric. Both the Encryption and decryption processes in a symmetric Encryption key pair. Symmetric Encryption is efficient, but it can't be used without safe key distribution to stop attackers from intercepting. With this strategy, parties may communicate securely without exchanging keys in advance. Data stays safeguarded while transmission across networks when secure communication channels are created using Encryption protocols such as SSL/TLS. Data Encryption also allows for safe storage in the cloud, both while it is in transit and while it is at rest in databases (Raja, V., 2024). As a whole, Encryption is an essential part of cybersecurity for online distant learning in the cloud, as it adds an extra safeguard to private student records and other sensitive educational information. Because of the Encryption, the message can only be read by those with the proper authorization. Encryption is made feasible by combining cryptographic keys with Encryption algorithms. Most commonly used techniques of Encryption that rely on these keys are symmetric and asymmetric Encryption. Using two distinct mathematical techniques, the data is Encrypted. Some of the most popular Encryption methods are RSA, ECC, 3DES, and AES (Rani, P., 2024)

II. LITERATURE REVIEW

In the subject of distant education learning, there have been a variety of studies conducted. Some of the researches have also focused on scalability along with diversity of education contents in an online cloud-based distance learning system. Moreover, research paper that has provided security to cloud application and compressed the content over the cloud, are also presented. In short, this section considers the research related to cloud-based e-learning, cloud security, cloud application performance enhancement, and data compression. This chapter provides an overview of available literature on cryptographic methods, with a special emphasis on DES, RSA, AES, and DNA Encryption approaches. In terms of performance, security, and applicability in cloud computing settings, this chapter investigates the advantages and disadvantages of the aforementioned technologies. This study highlights holes in existing cryptographic techniques by synthesizing recent research. It also lays the groundwork for the suggested Encryption method by providing context for the proposed method.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Table 1 Comparison of benefits and limitation of Security and Privacy Issues in Cloud Computing

Author / year	Objective of research	Mechanism	Benefits	Limitations
Ahmadi, S. (2024)	Thorough Analysis of Cloud Computing Information Security Risk Assessment Techniques	Reviews literature on threats and mitigation strategies in cloud security	Identifies common threats and effective mitigation strategies	Limited by the scope of reviewed literature
Ali, T., et al. (2024)	ANN-based strategy for securing cloud computing using deep learning	Reviews methods for assessing information security risks in cloud computing	Summarizes various risk assessment techniques	Detailed focus on risk assessment, might not cover all security aspects
Akbar, H., et al. (2023)	Cloud computing's security concerns and obstacles	Explores various security issues and challenges in cloud computing	Discusses different types of security threats and potential solutions	Broad overview, may lack in-depth analysis of specific issues
Fadhil, et al. (2023)	Cloud computing's security and privacy concerns	Identifies and discusses key security and privacy issues in cloud computing	Provides comprehensive overview of common security and privacy concerns	Lacks specific mitigation strategies or solutions
Kunduru, A. R. (2023)	Enterprise cloud computing security issues and their resolutions	Addresses security concerns in enterprise cloud applications	Offers solutions to mitigate identified security risks	May not cover all types of enterprise applications
Abdulsalam, Y. S., et al. (2021)	A technical overview of cloud computing security and privacy	Provides a comprehensive review of cloud security and privacy issues	Summarizes existing solutions and their effectiveness	Might not cover the latest advancements due to publication year
Alouffi, B., et al. (2021)	Cloud computing security: risks, countermeasurE, and literature review	Reviews threats and mitigation strategies in cloud computing security	Identifies common threats and effective mitigation techniques	Limited to literature available at the time of review
Abdullayeva, F. (2023)	Intelligent cloud computing systems' cyber resiliency and security concerns	Investigates resilience and security issues in intelligent cloud systems	Proposes frameworks for enhancing cyber resilience	May need further validation through practical implementation
Parast, F. K., et al. (2022)	A review of service-based frameworks for cloud computing security	Surveys security aspects of various cloud service models	Provides a comprehensive overview of security challenges	May not cover the latest advancements in cloud security
Pandey, G. P. (2019)	Novel method for protecting data stored in cloud that makes use of DNA, Huffman, socket programming, and other cutting-edge	Explores the use of DNA cryptography and Huffman algorithm for securing cloud data	Enhances data security and compression in cloud environments	Complexity in implementation and practicality
Suresh, P. (2016)	Protected cloud setting using RSA algorithm	Implementation of RSA for securing cloud	Enhanced data security, Encryption, and privacy	Computational overhead, key management complexity
Jimmy, F. N. U. (2024)	Reviewing Data Security and Privacy Concerns: An Exploration of Cloud Computing's Challenges and Solutions	Investigates cloud security vulnerabilities and tools for remediation	Provides practical solutions for enhancing cloud security	Focuses primarily on tool-based solutions, may overlook strategic aspects
Jumani, A. K., Shi, et al. (2023)	Examining the safety of fog computing	Reviews security issues specific to fog computing	Enhances understanding of security challenges in fog environments	Limited to fog computing, not generalizable to all cloud models
Oladoyinbo, T. et al. (2023)	An method to business risk management for assessing and defining cloud computing security baseline criteria	Establishes baseline security requirements for cloud computing	Provides a structured approach to enterprise risk management	Focus may be too narrow for comprehensive security strategy
Waqar, A., et al. (2023)	Cloud computing by the government and threats to national security	Evaluation of cloud computing implementation in small construction projects	Increased efficiency, collaboration, and data accessibility	Potential dependency on stable internet connectivity, data security concerns
Cinar, B., et al. (2023)	Forensics in the cloud: obstacles and potential solutions	Reviews challenges and future directions in cloud forensics	Highlights key challenges and potential future developments	Focused on forensics, may not cover general security issues
Patil, P. (2016)	An analysis of cloud computing for online education	Examines the role of cloud computing in e-learning for distance education	Improves accessibility and resource management in distance learning	Dependency on stable internet connectivity
Balobaid, A., et al. (2016)	A fresh approach to online learning that makes use of the cloud	Proposes new model for distance education using cloud computing	Highlights benefits for distance learning	Older proposal, may need updates to reflect current technology

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

OsmanP, S. E. F. (2016)	Integration of Virtual Learning Environment: Performance Analysis of Cloud-Based Web Services	Analyzes the performance of cloud-based web services for virtual learning	Improves system integration and user experience in virtual learning environments	Limited to virtual learning, may not be generalizable
Ali, A., Bajpeye, et al. (2015)	Use of cloud computing for online learning in distant education	Examines the use of cloud computing for distance education	Highlights benefits for e-learning platforms	Older study, may not reflect current advancements
Bandara, I., et al.. (2014)	Online safety issues in the classroom	Discusses cybersecurity issues in e-learning	Highlights specific concerns for educational platforms	Older study, may not address current security threats
Bouyer, A., et al. (2014)	Why cloud computing is essential for school systems	Argues for the adoption of cloud computing in education	Discusses benefits for educational institutions	General overview, lacks specific focus on security
Xu zhihong / 2013	To expand scope of distance learning, build education cloud i.e. applicable to all subjects.	Cloud computing	Distance education has been expanded by the educational cloud	Research Lacks security factors as well as performance factors
Kumar, G., and Chelikani, A. (2011)	Review of cloud-based e-learning security concerns	Analyzes security challenges in cloud-based e-learning platforms	Provides recommendations for improving security in e-learning	Limited to the e-learning domain
Hasimi, L., et al.. (2024)	Data protection in the digital age Addressing Security Flaws with Cloud-Based Software	Uses ANN to enhance cloud security	Demonstrates improved detection of security threats using ANN	Requires significant computational resources for implementation
Rani, P., et al. (2024)	Crucial Function of AI in Promoting Innovation and Safety in US Cloud Computing	Develops a taxonomy for cloud computing security and threat detection	Enhances threat detection and mitigation strategies	Rapid evolution of threats may outpace taxonomy updates
Butt, U. A., et al. (2023)	An analysis of cloud security risks and mitigation strategies	Surveys various cloud security threats and their solutions	Summarizes current threats and effective countermeasure	Broad survey, may lack depth in specific areas
AlSelami, F. A. (2023)	Innovative solutions to significant cloud computing security issues	Discusses major security challenges and innovative solutions in cloud computing	Proposes novel approaches to enhance cloud security	Focus on innovative solutions, may require further validation
AlAhmad, A. S., et al. (2021)	Comprehensive analysis of security concerns in mobile cloud computing	Reviews security issues specific to mobile cloud computing models	Systematic review of existing security models and their challenges	Focused on mobile cloud, might not address non-mobile cloud issues
Karak, S., et al.. (2015)	A paradigm for online education based on cloud computing	Explores the application of cloud computing in distance education	Improves accessibility and resource management in educational settings	Dependency on stable internet connectivity

.

III. PROBLEM STATEMENT

Although there has been a lot of research on cloud computing security, the security measures that have been implemented have consistently led to a decline in cloud performance. Moreover, earlier research only looked at a small portion of the available data. Earlier testing saw high rates of packet loss, sluggish speeds, and high error rates. We must ensure the security of all visual and textual content without compromising efficiency. Thanks to cloud computing, individuals can try out new ideas with ease. The creation of a favorable setting is essential for the administration of digital resources and material. Some potential security models have been uncovered by previous research. Data stored in the cloud may now be securely encrypted using technologies such as RSA, AES, DES, and DNA protection (Pandey, G. P. 2019), among others. The subject of several inquiries has been instructional content hosted in the cloud. The effectiveness of clouds has been the subject of very few investigations. For the purpose of enhancing cloud security and performance, researchers conducted an exhaustive examination. It is the intention of the suggested remedy to enhance security without compromising performance. The execution of previously researched tasks must take cloud security and performance into account.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

IV. PROPOSED WORK

The study addresses the use of DES, RSA, and AES cryptography in cloud-based studies. It proposes a method for dividing textual and graphical content into separate pieces, compressing and encrypting them, and then restoring them. The researchers use polynomial encryption and data compression for text and spitting module and exclusive-based encryption for graphical content. The data is then decoded on the receiving end. The study uses experimental methodology and loss-less image compression mechanisms for both textual and graphical content. The study uses MATLAB as a simulation tool to ensure data security and speed, reducing the probability of packet dropping and transmission errors.Some particular approaches, defined in various ways and detailed below, may be used to apply the study. It is discovering and categorizing novel problems is the job of exploratory research and developing studies that address a problem. Empirical research is required to evaluate the viability of a solution using empirical proof. Research work has considered experimental methodology and makes use of loss less image compression mechanism.

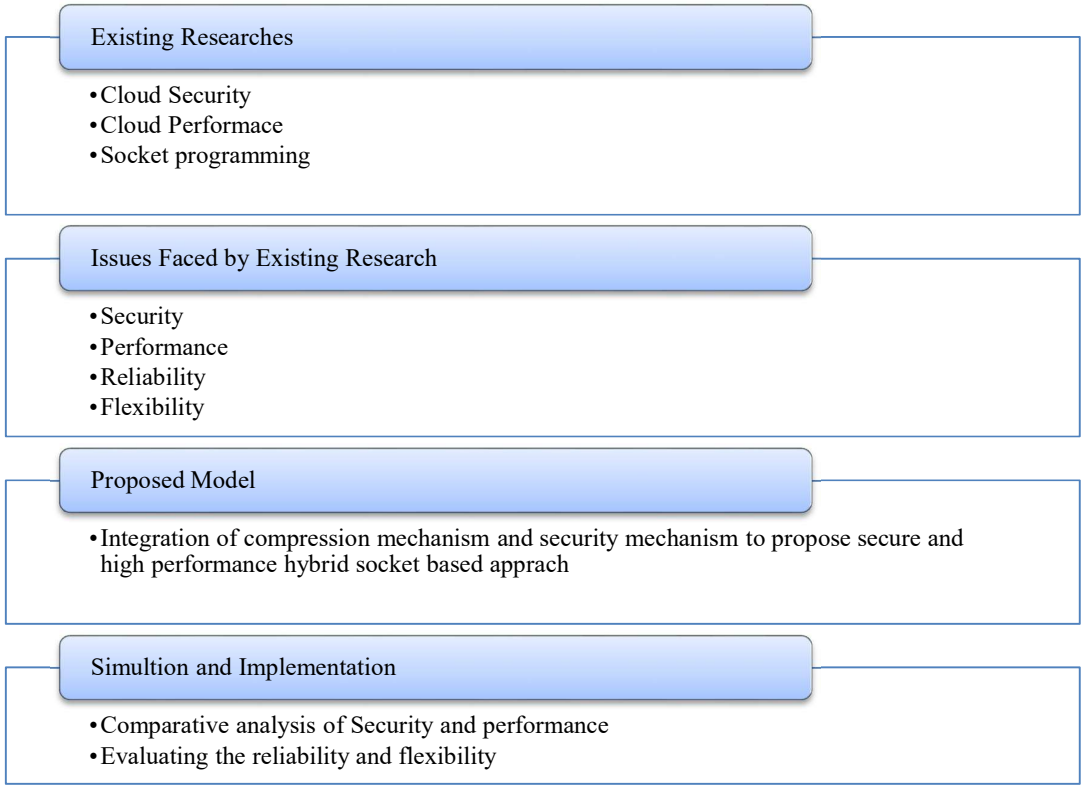

Fig 1 Process flow of Proposed work

The work has considered textual as well as graphical content during cloud computing operations. MATLAB has been used as simulation tool. During transmission of plain text, content size has been reduced using replacement mechanism and encrypted using encryption techniques. While in case of graphical content transmission the data graphical content have been processed by loss less image compression mechanism and data is split using division remainder method. The split data has been transferred via two different ports that assure the data security and increase the transmission speed. It results in reducing probability of packet dropping and transmission error.The methods of DES, RSA, and AES cryptography have been the subject of several cloud-based studies.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

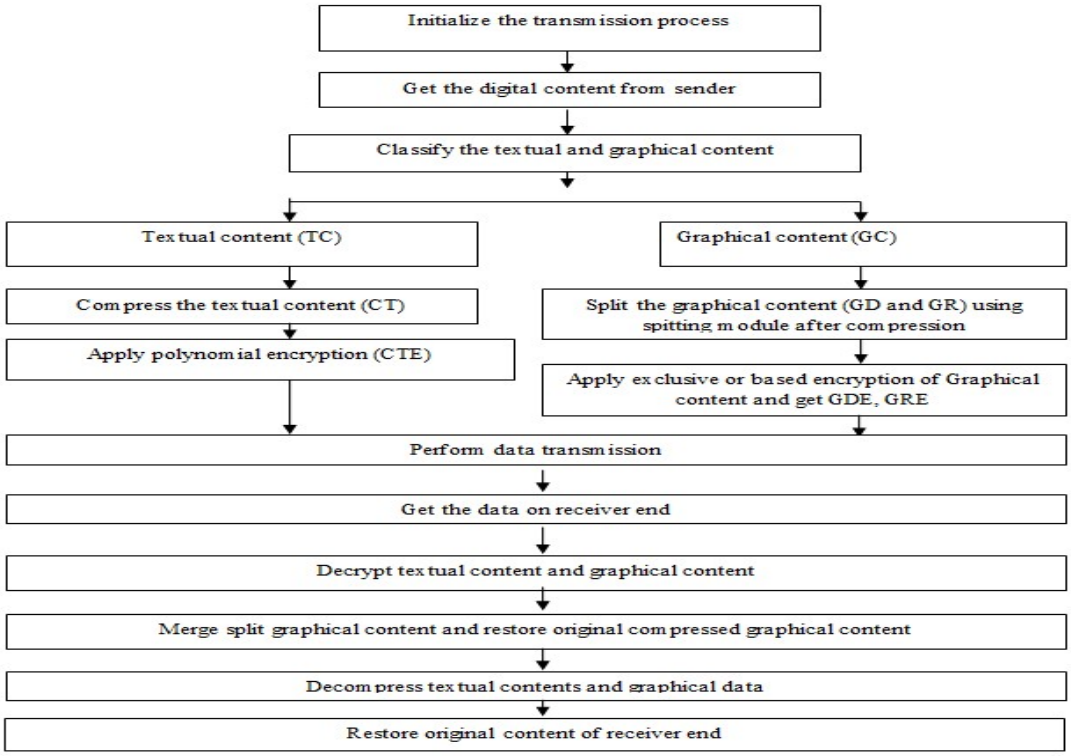

Fig 2 Data flow diagram of Proposed Work

The provided flowchart illustrates the Hybrid Secure Model for Textual and Graphical Data Transmission, detailing the process for securely transmitting digital content over the cloud. The process begins with initializing the transmission and acquiring the digital content from the sender. The content is then classified into textual or graphical data for further processing. For textual content, the data undergoes compression to reduce its size, followed by encryption using a polynomial encryption method to ensure security. For graphical content, the data is first compressed and then split into two parts (GD and GR) using a splitting module. These parts are encrypted separately using an exclusive or (XOR)-based encryption technique. Once processed, the data (textual and graphical) is transmitted over the cloud. On the receiver's end, the encrypted data is decrypted for both textual and graphical content. The split graphical content is then merged to restore the original compressed image. Finally, both the textual and graphical data are decompressed to reconstruct the original content, which is then fully restored to its initial state. This flow ensures efficient and secure transmission of both types of digital content.

V. RESULT AND DISCUSSION

This covers the experimental findings of contrasting the proposed encryption method with more conventional ones like DES, RSA, AES, and DNA encryption. These techniques were used to test, for example, the suggested plan. Critical performance criteria like time used, mistake rate, and security resilience help one assess the outcomes. Regarding security, error rate, and processing speed, the suggested approach beats the others in cloud computing systems. This chapter investigates the consequences of the experimental results especially in connection to cloud computing and cryptographic security. This study aims to investigate how these developments affect cloud security overall and how the suggested encryption methodology transcends the constraints of conventional approaches. We also consider the possibilities and difficulties that can present themselves for future

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

study in this topic throughout the argument. Comparatively to accepted methods in the article, including DNA, DES, RSA, and AES, suggested cryptographic models are evaluated. It looks for security against many types of attack, times, and frequency of mistakes. Data compression and exclusive order encryption lower time consumption, which helps the model to be so remarkably efficient in data transmission and encryption. Data packets are smaller hence general performance is enhanced. The model thus performs better along a spectrum of security criteria than more traditional cryptography techniques. The fact that Man-in----the- Middle and Brute Force assaults significantly reduces the number of packets affected shows its resilience in preserving service availability. As the frequency of successful attacks declines, security gains from the model's encryption and compression capabilities. Reducing packet size and transmission times helps to prevent Denial-of- Service (DoS) attacks, therefore proving the resilience of the model in preserving service availability. Often updated security keys and user-defined ports help to make it more difficult for illegal users to access, therefore lowering the incidence of access infractions. Finally, the strategy may significantly assist to reduce assaults on cloud-based services. By using exclusive keys and compressed data, which lower the susceptibility of cloud services, the system shows its capacity to defend cloud settings from several attacks. Since it is more efficient, reduces errors, and offers better defense against a range of attack routes, the proposed model performs generally better than more traditional cryptographic techniques.

Platform used to build suggested model and compare security, performance, and reliability with current solutions

Designed on the Netbean platform, the receiver and transmitter module run Java as its programming language. The simulation counts the packets to estimate the time needed to complete the previous work and the suggested activity as it runs forward.

Simulation for Time/Error/Packet size

The model reduces packet size, which reduces transmission time and error rate. Unlike RSA and AES, which do not reduce packet size, the recommended method compresses data before encryption, increasing data integrity while being conveyed. The security research found that the proposed model outperforms traditional cryptography methods in certain security aspects. Man-in-the-middle attacks affect fewer packets in the recommended paradigm than in DES, RSA, AES, and DNA. It shows that the recommended model protects against Brute Force attacks better. The model performs poorly in defensive operations compared to other methods. The lower incidence of successful attacks shows that encryption and compression improve security. The proposed methodology again reduces Denial-of-Service (DoS) attacks. By lowering packet size and transmission time, denial of service attacks are mitigated, demonstrating the model's resilience in maintaining service availability. It illustrates that the model has fewer access violations. Proposed secure and high performance hybrid socket based approachuses user-defined ports and security keys, which are updated often. Making access harder for unwanted parties increases security. Finally, it show that the technique may significantly reduce cloud service attacks. Using exclusive keys and compressed data reduces cloud service vulnerability to various attacks. This strengthens the system's cloud protection. The recommended model's time efficiency, error reduction, and greater security against many attack routes imply that it may be a superior option than current cryptographic procedures.

Time consumption

By the time the number of attacks reaches 60, the proposed method still maintains its advantage with a time consumption of 3.42 units, whereas DES, RSA, AES, and DNA require 4.62, 4.58, 4.35, and 3.99 units, respectively. These results underscore the proposed model's superior efficiency, which is attributed to its optimized encryption and compression processes that reduce overall time required for data handling.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Table 1 Comparative analysis of time consumption

Attack	DES	RSA	AES	DNA	Proposed approach
10	0.95	0.93	0.88	0.85	0.82
20	1.67	1.59	1.51	1.39	1.22
30	2.32	2.29	2.20	1.94	1.67
40	3.09	2.99	2.87	2.51	2.35
50	3.91	3.57	2.93	2.78	2.65
60	4.62	4.58	4.35	3.99	3.42

Figure 3 depicts the results of simulations conducted with regard to the amount of time spent working with the proposed system in contrast to earlier cryptography-based research including RSA, DES, AES and DNA.

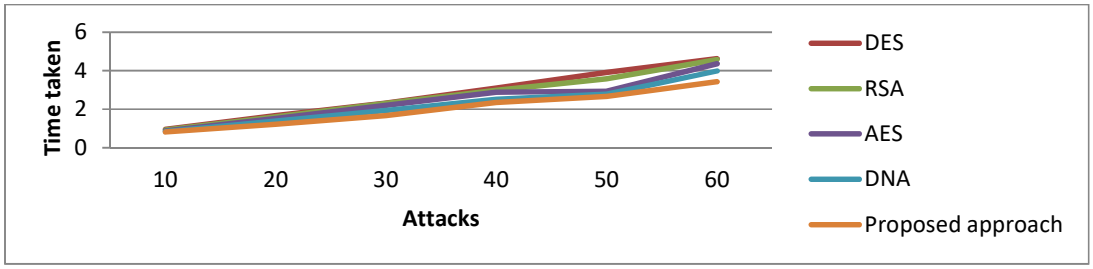

Fig 3 Comparison of time taken during transmission.

The comparative analysis of error rates among various cryptographic methods highlights the effectiveness of the proposed work in minimizing data transmission errors. As detailed in Table 2, the proposed model consistently demonstrates the lowest error rates compared to DES, RSA, AES, and DNA cryptography. At 10 attacks, the proposed work achieves an error rate of 0.59, which is lower than that of DES (0.83), RSA (0.78), AES (0.67), and DNA (0.61). This advantage continues as the number of attacks increases. For instance, at 20 attacks, the proposed model's error rate is reduced to 0.89, while DES, RSA, AES, and DNA have error rates of 1.36, 1.29, 1.16, and 1.01, respectively. By the time the number of attacks reaches 60, the proposed method still maintains a relatively low error rate of 3.51, compared to DES (4.20), RSA (3.92), AES (3.76), and DNA (3.64). These findings underscore the proposed work's effectiveness in minimizing error rates through its advanced encryption and data handling techniques, resulting in a more reliable data transmission process.

Table 2 Comparative analysis of error rate.

Attacks	DES	RSA	AES	DNA	Proposed approach
10	0.83	0.78	0.67	0.61	0.59
20	1.36	1.29	1.16	1.01	0.89
30	2.33	2.30	2.20	1.98	1.69
40	2.55	2.35	2.24	2.0	1.82
50	3.94	3.53	3.00	2.87	2.46
60	4.20	3.92	3.76	3.64	3.51

There is always a possibility of mistakes occurring when data is being sent. However, the error rate may be brought down to a more acceptable level by reducing the size of the packets and the amount of time they spend on the network. Because of the replacement process, the length of the string may be cut down, which lowers the likelihood of errors occurring. However, the RSA and AES cryptographic mechanisms that were utilized in the earlier study did not result in a reduction in the size of the packets Figure 4.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

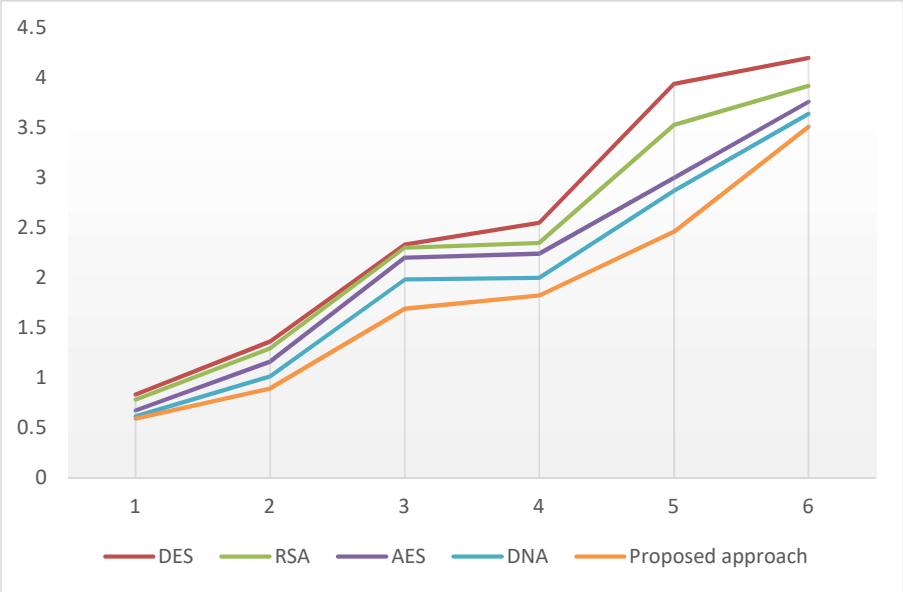

Fig 4 Comparison of error rates

Matlab simulation for comparative analysis of security

This section will focus on the potential effects of the modifications on security. As the frequency of assaults rises, the amount of packets impacted decreases in the scenario of the suggested work. Compared to RSA, DES, and DNA, AES cryptography is superior, according to earlier studies. In contrast to AES cryptography, the suggested method is superior. Comparing the suggested work to RSA and AES-based cryptographic methods, the following figures show that the impacted packets are smaller.

Man-in-the-middle

The influence that it has on the packet in the context of RSA, DES, AES and DNA encryption, as well as the work that has been recommended to counteract these attacks, is outlined below.

Table 3 Comparative analysis of man in middle attack.

Attacks	DES	RSA	AES	DNA	Proposed approach
10	9	8	7	6	4
20	13	11	9	8	6
30	20	13	11	10	9
40	25	17	15	13	11
50	29	25	19	16	14
60	32	31	27	21	17

The comparative analysis of vulnerability to (MitM) attacks, as presented in Table 5.3, reveals that the proposed work significantly outperforms traditional cryptographic methods in mitigating such threats. At 10 attacks, the proposed model exhibits the lowest number of affected packets, with only 4 impacted, compared to DES (9), RSA (8), AES (7), and DNA (6). As the number of attacks increases, the proposed method consistently demonstrates superior resistance. For instance, at 20 attacks, the proposed work affects only 6 packets, whereas DES, RSA, AES, and DNA are impacted by 13, 11, 9, and 8 packets, respectively. This trend continues through to 60 attacks, where the proposed approach results in only 17 affected packets, markedly fewer than DES (32), RSA (31), AES (27), and DNA (21). These results underscore the enhanced security of the proposed work against MitM attacks, highlighting its effectiveness in protecting data from interception and tampering in figure 5.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

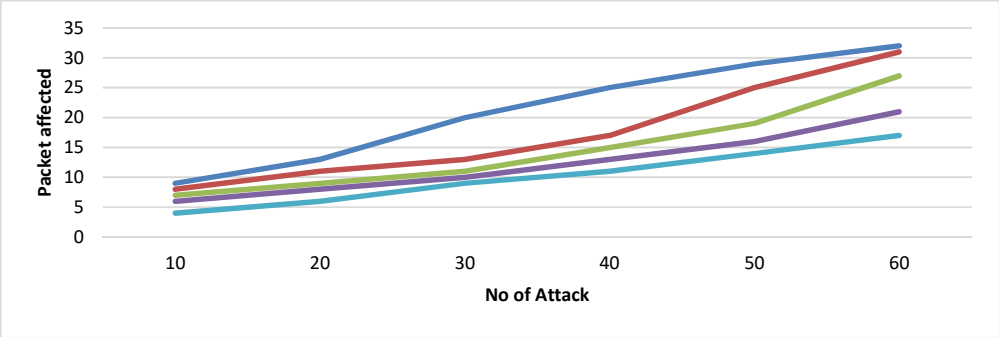

Fig 5 Comparative analysis in case of attack Man-In-Middle

Brute force attack

In a brute force attack, the attacker tries many combinations of characters or numbers in an effort to guess the user's password. Furthermore, a secret webpage and encryption keys are used. In the table below, research can see a comparison of this attack.

Table 4Comparative analysis of brute force attack.

Attacks	DES	RSA	AES	DNA	Proposed approach
10	8	7	6	5	3
20	12	10	8	6	5
30	20	15	11	9	7
40	26	15	13	11	10
50	31	24	19	17	14
60	33	32	27	25	21

The analysis of Brute Force attacks, shown in Table 4, indicates that the proposed method offers superior resistance compared to traditional cryptographic techniques. Initially, with 10 attacks, the proposed work shows a remarkable advantage, affecting only 3 packets compared to DES (8), RSA (7), AES (6), and DNA (5). As the number of attacks increases, this trend continues, demonstrating the proposed work's robustness. At 20 attacks, the proposed model impacts only 5 packets, whereas DES, RSA, AES, and DNA are affected by 12, 10, 8, and 6 packets, respectively. This protection improves as the attack intensity grows, with the proposed work showing the smallest number of affected packets at higher attack levels—14 packets at 50 attacks and 21 packets at 60 attacks, significantly fewer than DES (31 and 33), RSA (24 and 32), AES (19 and 27), and DNA (17 and 25). This comparative analysis highlights the proposed method's effectiveness in reducing the impact of Brute Force attacks, underscoring its enhanced security features in safeguarding data from exhaustive search attacks in figure 4.

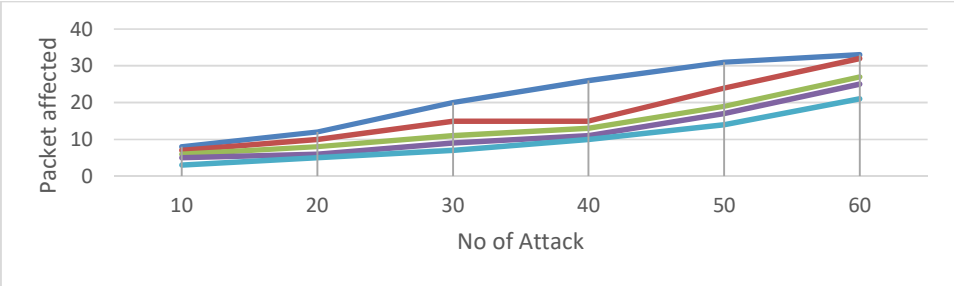

Fig 6 Comparative analysis in case of Brute force attack

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Denial-of-service

An effort to prohibit users from accessing a COF resource is an example of a kind of cyber attack known as a DoS. The chance of a denial of service attack is decreased when both the size of the packet and the amount of time spent transmitting it across the network are lowered. Therefore, there is less of an effect caused by the denial of service in the event of suggested work. A comparative comparison of may be found in the following figure.

Table 5 Comparative analysis of denial of service.

Attacks	DES	RSA	AES	DNA	Proposed approach
10	8	7	6	5	3
20	12	10	8	6	5
30	20	15	11	9	7
40	26	15	13	11	10
50	31	24	19	17	14
60	33	32	27	25	21

Table 5 provides a comparative analysis of Denial of Service (DoS) attacks across different encryption methods. The data shows that the proposed work significantly outperforms DES, RSA, AES, and DNA encryption in mitigating the impact of DoS attacks. At 10 attacks, the proposed method affects only 4 packets, whereas DES, RSA, AES, and DNA encryption are impacted by 9, 8, 7, and 6 packets, respectively. This advantage persists as the number of attacks increases. For instance, at 20 attacks, the proposed method's impact rises to 6 packets, compared to 13 packets for DES, 11 for RSA, 9 for AES, and 8 for DNA. As the attack intensity escalates to 60 attacks, the proposed approach still maintains a clear advantage, affecting only 22 packets versus 34 for DES, 33 for RSA, 28 for AES, and 24 for DNA. This analysis highlights the proposed method's superior resilience against DoS attacks, demonstrating its efficacy in maintaining service availability and minimizing disruption in figure 5.

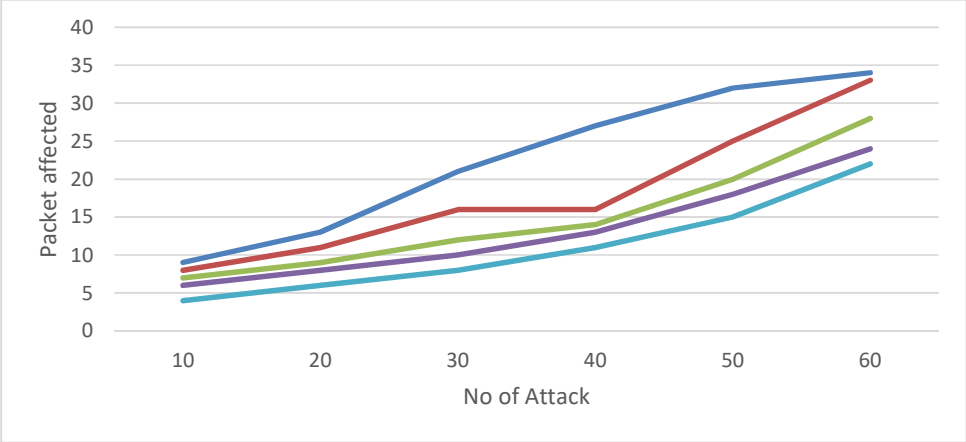

Fig 5 Comparative analysis in case of denial-of-service

Access violation

The work that is being proposed involves using a user-defined port along with a security key for exclusive usage, either of which may be altered at any given moment throughout various sessions. As a result, concerns about access violations have been addressed and resolved in the proposed work. Comparative study of access violation for RSA, DES, AES and DNA encryption, as well as the suggested work, is shown in Figure 6.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Table 6 Comparative analysis of access violation

Attack	DES	RSA	AES	DNA	Proposed approach
10	8	7	6	5	4
20	13	11	9	8	7
30	20	15	12	10	9
40	26	18	16	15	13
50	29	24	21	18	15
60	33	32	28	22	16

Table 6 presents a comparative analysis of access violations across various encryption techniques. The proposed work shows a notable advantage over DES, RSA, AES, and DNA encryption in managing access violations. Initially, with 10 attacks, the proposed method experiences only 4 access violations, compared to 8 for DES, 7 for RSA, 6 for AES, and 5 for DNA encryption. This advantage continues as the number of attacks increases. For instance, at 20 attacks, the proposed method reports 7 access violations, whereas DES, RSA, AES, and DNA report 13, 11, 9, and 8 violations respectively. The trend persists with more attacks, where the proposed approach maintains fewer violations. By 60 attacks, the proposed method shows only 16 access violations, in contrast to 33 for DES, 32 for RSA, 28 for AES, and 22 for DNA. This comparative analysis underscores the proposed work's effectiveness in reducing access violations, highlighting its enhanced security capabilities over traditional encryption methods in figure 6.

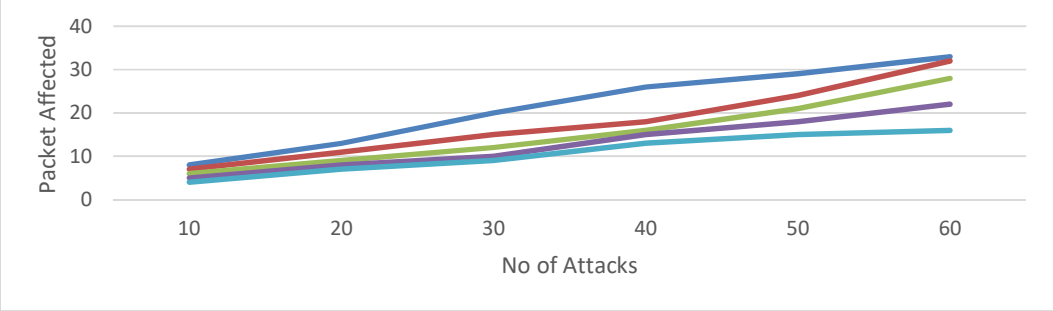

Fig 6 Comparative analysis in case of access violation

Attack on cloud services

Utilization of exclusive or after data compression, in addition to user-defined port numbers, has helped to limit likelihood of various attacks on cloud services. Comparative study of an attack on a cloud service using RSA, DES, AES and DNA encryption, as well as the suggested work, is shown in Figure 7.

Table 7Comparative analysis of attacks on cloud services

Attack	DES	RSA	AES	DNA	Proposed approach
10	14	10	9	8	7
20	19	13	11	10	9
30	27	22	19	17	15
40	29	25	23	19	16
50	39	31	24	20	15
60	43	38	31	25	18

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Table 7 provides a comparative analysis of attacks on cloud services using various encryption techniques. The proposed work demonstrates a significant improvement in resilience against such attacks compared to DES, RSA, AES, and DNA encryption methods. At the initial stage, with 10 attacks, the proposed method shows only 7 successful attacks, while DES, RSA, AES, and DNA encryption experience 14, 10, 9, and 8 attacks respectively. This advantage continues as the number of attacks increases. For example, with 20 attacks, the proposed method sees 9 attacks, whereas DES, RSA, AES, and DNA experience 19, 13, 11, and 10 attacks respectively. This trend is consistent with more attacks; by 60 attacks, the proposed method reports 18 successful attacks, compared to 43 for DES, 38 for RSA, 31 for AES, and 25 for DNA. This analysis highlights the proposed work's superior performance in mitigating attacks on cloud services, showcasing its enhanced security and effectiveness in protecting against potential threats as shown in figure 7.

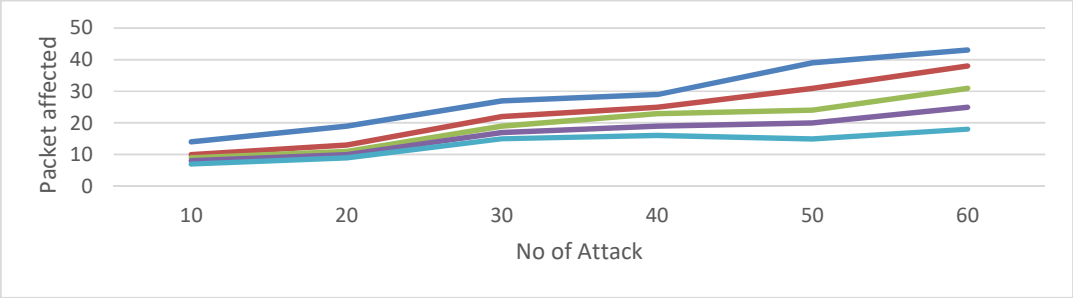

Fig 5.7 Attack on cloud services.

VII. CONCLUSION

The research aims to improve the security and performance of cloud systems by proposing a secure encrypted Hybrid model. The model aims to reduce transmission delay, error, and packet dropping probability, offering a more consistent and strong communication system. The proposed method beats DES, RSA, AES, and DNA encryption methods in terms of time consumption, error rate, and attack resistance. It also offers better resistance against brute force and Man-in-the-middle attacks. The research also highlights the importance of a suitable environment for digital resources and information administration. The proposed solution aims to increase safety levels without compromising operational efficacy. The research focuses on the development of a favorable environment for digital resource construction and content management. Existing security models, such as RSA, AES, DES, DNA security, and various protocols, have been used to secure cloud-based content. However, limited research has focused on cloud performance. The proposed solution should improve security without affecting performance.The research focuses on the hybrid transmission technique in cloud computing, offering speed, reliability, and error-free operation. It could benefit the education, healthcare, and commercial industries. The hybrid system uses machine learning-based encryption and data compression, outperforming current systems. The research aims to improve the safety and efficiency of cloud environments for practical use. As cloud usage grows, high performance and robust security measures become crucial. New cryptographic protocols, encryption techniques, and cloud-native security solutions are needed to ensure data integrity, privacy, and security. Advancements in serverless architectures, distributed computing, and containerization can optimize performance

REFERENCES

1. Abd Al Ghaffar, H. T. A. N. (2024). Government cloud computing and national security. Review of Economics and Political Science, 9(2), 116-133.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

2. Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. Results in Control and Optimization, 12, 100268.
3. Abdulsalam, Y. S., and Hedabou, M. (2021). Security and privacy in cloud computing: technical review. Future Internet, 14(1), 11.
4. Ahmadi, S. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Ahmadi, S.(2024) Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Journal of Information Security, 15, 148-167.
5. Akbar, H., Zubair, M., and Malik, M. S. (2023). The security issues and challenges in cloud computing. International Journal for Electronic Crime Investigation, 7(1), 13-32.
6. AlAhmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O., and Jaradat, A. (2021). Mobile cloud computing models security issues: A systematic review. Journal of Network and Computer Applications, 190, 103152.
7. Alam, A. (2022). Cloud-based e-learning: scaffolding the environment for adaptive e-learning ecosystem based on cloud computing infrastructure. In Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2 (pp. 1-9). Singapore: Springer Nature Singapore.
8. Alam, T. (2020). Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), 108-115.
9. Ali, A., Bajpeye, A., and Srivastava, A. K. (2015). E-learning in distance education using cloud computing. International Journal of Computer Techniques, 2(3), 2394-2231.
10. Ali, T., Al-Khalidi, M., and Al-Zaidi, R. (2024). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. Journal of Computer Information Systems, 1-28.
11. Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., and Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. IEEE Access, 9, 57792-57807.
12. AlSelami, F. A. (2023). Major cloud computing security challenges with innovative approaches. Tehnički glasnik, 17(1), 141-145.
13. Ananthi, C. M. T., and Arul, L. R. P. J. (2019). Implications, Risks and Challenges of Cloud Computing In Academic Field–A State-of-Art. Int. J. Sci. Technol. Res, 8, 3268-3278.
14. Balobaid, A., and Debnath, D. (2016). A novel proposal for a cloud-based distance education model. International Journal for e-Learning Security (IJeLS), 6(2).
15. Bandara, I., Ioras, F., and Maher, K. (2014). Cyber security concerns in e-learning education. In ICERI2014 Proceedings (pp. 728-734). IATED.
16. Bouyer, A., and Arasteh, B. (2014). The necessity of using cloud computing in educational system. Procedia-Social and Behavioral Sciences, 143, 581-585.
17. Butt, U. A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M. T., and Albaqami, N. (2023). Cloud security threats and solutions: A survey. Wireless Personal Communications, 128(1), 387-413.
18. Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... and Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. Electronics, 9(9), 1379.
19. Cinar, B., and Bharadiya, J. P. (2023). Cloud computing forensics; challenges and future perspectives: A review. Asian Journal of Research in Computer Science, 16(1), 1-14.
20. Fadhil, I. S. M., Nizar, N. B. M., and Rostam, R. J. (2023). Security and privacy issues in cloud computing. Authorea Preprints.
21. Gai, K., Guo, J., Zhu, L., and Yu, S. (2020). Blockchain meets cloud computing: A survey. IEEE Communications Surveys and Tutorials, 22(3), 2009-2030.
22. Garrison, G., Kim, S., and Wakefield, R. L. (2012). Success factors for deploying cloud computing. Communications of the ACM, 55(9), 62-68.

23. Hasimi, L., Zavantis, D., Shakshuki, E., and Yasar, A. (2024). Cloud Computing Security and Deep Learning: An ANN approach. Procedia Computer Science, 231, 40-47.
24. Herhalt, J., Cochrane, K.: Exploring the Cloud: A Global Study of Governments Adoption of Cloud. Sales force, (2012).
25. Hurwitz, J. S., and Kirsch, D. (2020). Cloud computing for dummies. John Wiley and Sons.
26. Ibrahim, I. M. (2021). Task scheduling algorithms in cloud computing: A review. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(4), 1041-1053.
27. Jacob, Grasha and Murugan, Annamalai. (2013). DNA based Cryptography: An Overview and Analysis. International Journal of Emerging Sciences. 3. 36-42.
28. Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 2(1), 129-171.
29. Jumani, A. K., Shi, J., Laghari, A. A., Hu, Z., Nabi, A. U., and Qian, H. (2023). Fog computing security: A review. Security and Privacy, 6(6), e313.
30. Karak, S., and Adhikary, B. (2015). Cloud computing as a model for distance learning. International Journal of Information Sources and Services, 2(4), 32-38.
31. Katal, A., Dahiya, S., and Choudhury, T. (2023). Energy efficiency in cloud computing data centers: a survey on software technologies. Cluster Computing, 26(3), 1845-1875.
32. Kaur, H., Jameel, R., Alam, M. A., Alankar, B., and Chang, V. (2023). Securing and managing healthcare data generated by intelligent blockchain systems on cloud networks through DNA cryptography. Journal of Enterprise Information Management, 36(4), 861-878.
33. Korucu, A. T., and Atun, H. (2017). The cloud systems used in education: properties and overview. International Journal of Educational and Pedagogical Sciences, 10(4), 1400-1404.
34. Kumar, A., Lee, B. G., Lee, H., and Kumari, A. (2012, October). Secure storage and access of data in cloud computing. In 2012 International Conference on ICT Convergence (ICTC) (pp. 336-339). IEEE.
35. Kumar, G., Chelikani, A.: Analysis of security issues in cloud-based e-learning. University of Board/School of Business and IT, (2011).
36. Kunduru, A. R. (2023). Security concerns and solutions for enterprise cloud computing applications. Asian Journal of Research in Computer Science, 15(4), 24-33.
37. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. (2011). Cloud computing—The business perspective. Decision support systems, 51(1), 176-189.
38. Mishra, J. P., Panda, S. R., Pati, B., and Mishra, S. K. (2019). A novel observation on cloud computing in education. International Journal of Recent Technology and Engineering (IJRTE), 8(3), 5262-5274.
39. Mohamed, E. M., Abdelkader, H. S., and El-Etriby, S. (2013). Data Security Model for Cloud Computing. Unpublished. https://doi.org/10.13140/2.1.2064.4489
40. Nirmala, V., Sivanandhan, R. K., and Lakshmi, R. S. (2013, March). Data confidentiality and integrity verification using user authenticator scheme in cloud. In 2013 International Conference on Green High Performance Computing (ICGHPC) (pp. 1-5). IEEE.
41. Oladoyinbo, T. O., Adebiyi, O. O., Ugonnia, J. C., Olaniyi, O., and Okunleye, O. J. (2023). Evaluating and establishing baseline security requirements in cloud computing: an enterprise risk management approach. Available at SSRN 4612909.
42. OsmanP, S. E. F. (2016). Performance Analysis of Cloud based Web Services for Virtual Learning Environment Systems Integration. Int. J. Innov. Sci., Eng. Technol, 3, 246.
43. Pandey, G. P. (2019). Implementation of DNA cryptography in cloud computing and using Huffman algorithm, socket programming and new approach to secure cloud data. Socket Programming and New Approach to Secure Cloud Data (August 7, 2019).
44. Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., and Hakak, S. (2022). Cloud computing security: A survey of service-based models. Computers and Security, 114, 102580.

45. Parmar, P., Gadhiya, J., Vats, S., Verma, D. K., and Vaghela, K. (2023, November). A Review of DNA Cryptography: From a Data Protection Perspective. In 2023 16th International Conference on Security of Information and Networks (SIN) (pp. 1-7). IEEE.
46. Parmar, Parth, Jekil Gadhiya, Satvik Vats, Deepak Kumar Verma, and Krunal Vaghela. "A Review of DNA Cryptography: From a Data Protection Perspective." In 2023 16th International Conference on Security of Information and Networks (SIN), pp. 1-7. IEEE, 2023.
47. Patil, P. (2016). A study of E-learning in distance education using cloud computing. International Journal of Computer Science and Mobile Computing, 5(8), 110-113.
48. Raja, V. (2024). Exploring Challenges and Solutions in Cloud Computing: A Review of Data Security and Privacy Concerns. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 4(1), 121-144.
49. Rani, P., Singh, S., and Singh, K. (2024). Cloud computing security: a taxonomy, threat detection and mitigation techniques. International Journal of Computers and Applications, 1-14.
50. Rehan, H. (2024). Revolutionizing America's Cloud Computing the Pivotal Role of AI in Driving Innovation and Security. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 2(1), 239-240.
51. Rewagad, P., and Pawar, Y. (2013, April). Use of digital signature with diffie hellman key exchange and AES Encryption algorithm to enhance data security in cloud computing. In 2013 International Conference on Communication Systems and Network Technologies (pp. 437-439). IEEE.
52. Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., and Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. Qubahan Academic Journal, 1(2), 1-7.
53. Schleier-Smith, J., Sreekanti, V., Khandelwal, A., Carreira, J., Yadwadkar, N. J., Popa, R. A., ... and Patterson, D. A. (2021). What serverless computing is and should become: The next phase of cloud computing. Communications of the ACM, 64(5), 76-84.
54. Shafiq, D. A., Jhanjhi, N. Z., Abdullah, A., and Alzain, M. A. (2021). A load balancing algorithm for the data centres to optimize cloud computing applications. IEEE Access, 9, 41731-41744.
55. Sharma, S. K., Goyal, N., and Singh, M. (2014). Distance education technologies: using E-learning system and cloud computing. IJCSIT) International Journal of Computer Science and Information Technologies, 5(2), 1451-1454.
56. Shi, Y., Yang, H. H., Yang, Z., and Wu, D. (2014). Trends of Cloud Computing in Education. In Lecture Notes in Computer Science (pp. 116–128). Springer International Publishing. https://doi.org/10.1007/978-3-319-08961-4_12
57. Singh, A., Kumar, A., and Namasudra, S. (2024). DNACDS: Cloud IoE big data security and accessing scheme based on DNA cryptography. Frontiers of Computer Science, 18(1), 181801.
58. Singh, S. K., Manjhi, P. K., and Tiwari, R. K. (2016). Data security using RSA algorithm in cloud computing. International Journal of Advanced Research in Computer and Communication Engineering, 5(8), 11-16.
59. Sunyaev, A., and Sunyaev, A. (2020). Cloud computing. Internet computing: Principles of distributed systems and emerging internet-based technologies, 195-236.
60. Suresh, P.: Secure cloud environment using RSA algorithm. International Research Journal of Engineering and Technology 3(2), 143-148 (2016).
61. T. Mahjabin, A. Olteanu, Y. Xiao, W. Han, T. Li and W. Sun, "A Survey on DNA-Based Cryptography and Steganography," in IEEE Access, vol. 11, pp. 116423-116451, 2023, doi: 10.1109/ACCESS.2023.3324875.
62. Tabrizchi, H., and Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

63. Tribhuwan, M. R., Bhuyar, V. A., and Pirzade, S. (2010, October). Ensuring data storage security in cloud computing through two-way handshake based on token management. In 2010 International Conference on Advances in Recent Technologies in Communication and Computing (pp. 386-389). IEEE.
64. Vellela, S. S., Reddy, B. V., Chaitanya, K. K., and Rao, M. V. (2023, January). An integrated approach to improve e-healthcare system using dynamic cloud computing platform. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 776-782). IEEE.
65. Venters, W., and Whitley, E. A. (2012). A critical review of cloud computing: researching desires and realities. Journal of Information Technology, 27, 179-197.
66. Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., and Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. Materials Today: Proceedings, 51, 2172-2175.
67. Waqar, A., Skrzypkowski, K., Almujibah, H., Zagórski, K., Khan, M. B., Zagórska, A., and Benjeddou, O. (2023). Success of implementing cloud computing for smart development in small construction projects. Applied Sciences, 13(9), 5713.
68. Wen, H., Xie, Z., Wu, Z., Lin, Y., and Feng, W. (2024). Exploring the future application of UAVs: Face image privacy protection scheme based on chaos and DNA cryptography. Journal of King Saud University-Computer and Information Sciences, 36(1), 101871.
69. Yalamati, S. (2024). Data Privacy, Compliance, and Security in Cloud Computing for Finance. In Practical Applications of Data Processing, Algorithms, and Modeling (pp. 127-144). IGI Global.
70. Yang, H., and Tate, M. (2012). A descriptive literature review and classification of cloud computing research. Communications of the Association for Information systems, 31(1), 2.
71. Yenugula, M., Sahoo, S., and Goswami, S. (2023). Cloud computing in supply chain management: Exploring the relationship. Management Science Letters, 13(3), 193-210.
72. Yenugula, M., Sahoo, S., and Goswami, S. (2024). Cloud computing for sustainable development: An analysis of environmental, economic and social benefits. Journal of future sustainability, 4(1), 59-66.
73. Zhihong, X., Junhua, G., Yongfeng, D., Jun, Z., and Yan, L. (2013, August). Expand distance education connotation by the construction of a general education cloud. In 2013 International Conference on Advanced ICT and Education (ICAICTE-13) (pp. 417-420). Atlantis Press.
74. Zitouni, N., Sedrati, M., and Behaz, A. (2024). LightWeight energy-efficient Block Cipher based on DNA cryptography to secure data in internet of medical things devices. International Journal of Information Technology, 16(2), 967-977.