Impact Factor (SJIF): 6.092 E-ISSN: 2583-1615

International Journal of Research in Academic World

Received: 17/December/2024 IJRAW: 2025; 4(1):177-188 Accepted: 22/January/2025

End-to-End Security for Sensitive Healthcare Data with Twofish Encryption and Wireguard

[*1]Thinagaran Perumal

[*1]Associate Professor, Department of Computer Science, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, UPM Serdang, Selangor, Malaysia.

Abstract

The security of sensitive healthcare data is of paramount importance as modern healthcare systems increasingly depend on digital platforms for data collection, processing, and storage. Although existing solutions have made commendable progress in protecting healthcare information, persistent challenges remain—such as slow data transmission, lack of consistent end-to-end encryption, and varying system performance. To overcome these limitations, this paper presents a novel system that ensures comprehensive protection for healthcare data through robust encryption and secure cloud storage. The proposed system captures sensitive patient information from diverse sources, including EHRs and medical databases. This data is encrypted using the Two fish algorithm—a fast and highly secure symmetric key cryptographic technique known for its strong resistance to brute-force attacks. Once encrypted, the data is transmitted via Wire Guard VPN tunnels, which establish a high-speed, low-latency, and secure communication channel, thereby mitigating risks associated with data interception during transmission. Ultimately, the encrypted data is securely stored in a cloud environment that adheres to major data protection frameworks such as HIPAA and GDPR, ensuring compliance with global privacy regulations. Experimental results reveal the system's effectiveness in enhancing data security. Encryption strength fluctuated between 22% and 97% across different time intervals, with prominent peaks observed at 83% during interval 2 and 97% in interval 5. These fluctuations suggest a trend of improving security performance over time. Additionally, the system exhibits a linear relationship between encryption time and multiplication depth, with processing time increasing from 0.10 seconds at depth 0 to 0.35 seconds at depth 7. These findings highlight the system's scalability and robustness, demonstrating its capability to address critical healthcare data security issues while maintaining regulatory compliance and efficient data management.

Keywords: Healthcare data, two fish encryption, wire guard, secure transmission, cloud storage, data privacy, regulatory compliance.

1. Introduction

The healthcare industry is facing tremendous challenges in the arrival of digital health technologies that has made securing sensitive patient information an increasing challenge [1]. The enormous amounts of data from IoT devices, EHRs and medical sensors have improved the making of decisions and better patient outcomes [2]. However, their increasing volume and complexity contribute to significant privacy and security risks. Healthcare data are sensitive, making them vulnerable to unauthorized access, which could result in financial losses, reputational damage and legal outcomes; hence, adherence to many statutory procedures like HIPAA and GDPR is important for ensuring privacy and security of patients' data [3]. Therefore, there is a need for safe handling of health data in order to maintain trust and uphold the rights to privacy [4]. The rapid digital transformation of systems has necessitated modern mechanisms in safeguarding patient information [5]. This guarantees a combination of strong encryption, proven secure transmission and reliable storage methods.

There are several emerging trends that enhance the importance of healthcare data security: First, IoT-enabled devices are being used in the clinical setting such as wearables and diagnostic tools that link into patient health continuously to improve health outcomes. Enhanced connectivity has however increased risks because connectivity means more devices and therefore more points of entry for an unauthorized party. The trend appears to be fostered through increased partnerships among healthcare providers, insurance companies, biomedical firms and research organizations, which would all need access to sensitive data. Recently, more parties are collating data into their databases and with this, the risk of exposure increases. Added to this is growing criminal sophistication among cybercriminals, as well as widespread data breaches that threaten patient privacy. More health information is being directly targeted due to the rising competition for unhealthy personal health data, making such healthcare data an important asset to protect. Thus, with current horizontal sharing and analysis of healthcare data across applications, it becomes even more difficult to maintain consistent integrity and secrecy Pulakhandam *et al.* (2023) [6] support the proposed method by demonstrating how their hybrid blockchain strategy ensures secure, decentralized,

***Corresponding Author:** Thinagaran Perumal

and efficient healthcare data sharing through advanced cryptographic algorithms, reinforcing data privacy and integrity throughout the lifecycle.

Traditional approaches for safeguarding healthcare data do not meet the requirement of security threats depending on their modernity. Indeed, many healthcare systems use outdated encryption protocols like RC4 and 3DES vulnerable to contemporary cryptographic attacks. Such protection is inadequate for sensitive healthcare data. Moreover, centralized data storage systems represent a single point of failure and being breached or encountering system failure are weaknesses in cybersecurity additionally, traditional access control environments that allow unauthorized access appear to be weak and include password-based security mechanisms and lack of multi-factor authentication. Another example is physical storage with access managed manually, which raises the possibility of human errors leading to data breaches. The evolution of cyber threats evidently renders any traditional approach to security ineffectual. Healthcare organizations must therefore adjust and use more advanced and secure technologies, including modern encryption algorithms such as and secure transmission protocols like to secure sensitive patient data [7].

The old methods of securing healthcare data become insufficient in coping with the expanding complexity and sophistication of contemporary cybersecurity threats. Ray said that the legacy encryption protocols like RC4 and 3DES that are still in use in numerous healthcare systems have been demonstrated to be susceptible to modern cryptographic attacks. These old algorithms do not have this resilience, which is needed to defend very sensitive patient information in fast-changing digital landscapes. Moreover, centralized systems of storage of data contain major loopholes, becoming single points of failure. A failure or malfunction of architecture of this kind can leak enormous amounts of confidential information in a single failure. Worse still, many of the traditional access control mechanisms continue to depend on weak password-based authentication, and tend not to include sophisticated defences such as multi-factor authentication, leaving them open for attacks by unauthorized access [8].

Conventional procedures for ensuring privacy of healthcare data are becoming less effective over the increasingly complex and changing contemporary cyberthreat environment. As Ray notes, legacy encryption protocols such as RC4 and 3DES, which are well-represented in healthcare systems, have been shown to be very susceptible to modern cryptography attacks. These old algorithms also do not have the strength and flexibility required to secure patient sensitive information in high-speed digital first environments. What with healthcare data being produced and disseminated in record levels–especially through electronic health records, IoT devices and remote monitoring systems–there is urgent need for robust, resilient encryption. Unfortunately, these are the legacy systems that come short and many times fail to measure up to the responsiveness of and high-stakes data protection. Garikipati and Kumar (2020) [9] powerful GRU-based system revolutionizes threat detection and cloud security by delivering unparalleled anomaly identification and adaptive defense mechanisms, significantly empowering the proposed method to achieve unmatched healthcare data protection and fortress-level cloud management.

Additional to the problem is the use of centralized data storage systems which by nature means single point of failure. A breach, system error or malfunction in such an infrastructure may culminate in leaking of large quantities of confidential patient data in one exposure event. Also, traditional access control mechanisms often heavily rely on the basic authentication of the password type without incorporating more sophisticated security means such as MFA or biometrical verification. This makes systems vulnerable to unauthorized entry attacks, phishing attacks, and credential stealing. With cyber threats getting sophisticated and more relentless by the day, it is apparent that static security mechanisms that are out of date cannot effectively protect healthcare data anymore. There is an immediate call for migration to the modern and adaptive security infrastructures that adopt strong encryption, decentralized architectures and smart access control mechanisms as to provide complete safeguards to the privacy of patients and the system.

Besides, manual processing of physical data storage opens the door for the error of humans, which means that the possibility of data breaches is raised, and data protection regulations such as HIPAA and GDPR are not met. With cyber threats constantly changing dynamics and side, static and centralized security frameworks cannot cope. Healthcare organizations, therefore, have to move forward to the advanced and dynamic security infrastructures. This involves the use of strong encryption such as two fish, which is known to be fast and has high security key lengths, and the use of Wire Guard, a lightweight VPN protocol that offers secure low-latency data transmission for data transfer. These technologies not only improve confidentiality and integrity but also allows scalability and performance to secure the patient data at the entire lifecycle – from acquisition and transmission to storing it up in the cloud and access control.

The structure of this paper is divided into several sections: Section 2 presents a Literature Survey discussing existing methodologies and their limitations. Section 3 deals with the proposed methodologies in detail. Section 4 describes results presenting performance metrics of the system. Finally, Section 5 concludes and summarizes the findings.

2. Literature Survey

Chinnasamy and Deepalakshmi [10] has developed the invention of an IoMT and blockchain-based heart disease monitoring system for enhancing heart health assessment. The research considered limitations of some existing studies in including arrhythmia implications together with ECG and PCG data for better disease prediction. The classification was done using BS-THA and OA-CNN models, blockchain was integrated for secure data storage and MAC was used for authentication. The feature extraction methods included spectrum analysis, signal decomposition, scalogram conversion and DPCA-based selection for improving classification accuracy. However, the limitation involved computational complexity and integration issues, in addition to the probable latency in real-life implementations.

Masood *et al.* [11] dealt with federated learning and cloud-edge collaborative computing systems to tackle security problems in collaborative computing. The research created a framework for multi-national validation for evaluation of the performance of the system under attack and no attack scenarios. Implementation of the End-to-End Privacy-Preserving Deep Learning model was carried out on classifying attacks while protecting the data privacy. The effectiveness of the model was evaluated using estimates Time, Node Count, Routing Count and Data Delivery Ratio. However, some are high computational overhead, scalability issues and vulnerabilities due to evolving cyber threats.

Amanat *et al*. [12] presented the security issues the software vendors face while handling a large volume of data in cloud environments. The research employed the Analytic Hierarchy Process for systematically identifying, ranking and evaluating a category of security concerns which were about data integrity, unauthorized access and privacy of data. The results indicated that advanced encryption, AI-enabled threat detection and multi-factor authentication are the most powerful security techniques. It also provided structured recommendations to upgrade the cloud data security via real-time threat detection systems. Nonetheless, the limitations included integration complexities, computational overheads and evolving nature of cyber threats.

Molo *et al*. [13] made an overall evaluation of software vendors' security problems with huge amounts of data used over cloud platforms. It applied the AHP to derive the presented list of security priorities, with the most critical categories of security concerns, such as data integrity, transit security, and data privacy. This classic approach helped define the key security threats to cloud infrastructures, shedding light on where the priorities need to be. The findings revealed that the most effective practices for reducing threats in the cloud data environments include using advanced encryption techniques, AI-powered threat detection, and the MFA. These measures were proven to provide substantial protection in case of data breaches, unauthorized intrusions, and other malevolent actions aimed at compromising confidential data.

Abouelmehdi, Beni-Hessane, and Khaloufi [14] identifying best practices, the research also provided actionable recommendations for enhancing cloud data security, emphasizing the implementation of capable of adaptive responses to dynamic threat landscapes. However, despite these advancements, several limitations were acknowledged. Integration complexities often arise when deploying advanced security tools across heterogeneous cloud infrastructures. The study also noted considerable computational overheads, particularly when combining encryption and AI-driven monitoring at scale. Most critically, the rapidly evolving nature of cyber threats poses a continual challenge, requiring organizations to remain proactive and adaptive in their security strategies. These insights underscore the importance of investing in scalable, intelligent security frameworks that can dynamically respond to emerging threats while maintaining the performance demands of large-scale cloud operations. AI and IoT for decision-making, emphasized by Gudivaka *et al*. (2023) [15], reinforces the proposed system approach to securely managing healthcare data using proposed method to address security challenges.

Javaid *et al*. [16] has studied making security to the IoTs in terms of critical node identification, vulnerability assessment, proposing measures for security and overall performance impact analysis on the system. One of the quantitative methodologies is developed to identify the important components of IoT systems, after which a sufficient and thorough vulnerability assessment is conducted. The intrusion detection system and the various encryption techniques, including access control measures and continuous security audits, are proposed and evaluated based on the effectiveness concerning securing IoT.

Hanen, Kechaou, and Ayed [17] suggested an innovative technique called P2DS which primarily gathers financial data in mobile cloud environment study with a view of building up provisions against the growing security threats in financial institutions through an amalgamation of Attribute Based Semantic Access Control, Proactive Determinative Access scheme and Attribute Based Encryption. The framework must be capable of carrying out its action so as to encrypt quickly, classify with accuracy and promptly respond to threats. Consequently, P2DS endeavours to be a trustworthy solution for protection of sensitive financial data in dynamically changing digital area. The practical limitations emerging from the finding of this work being computational overhead, scalability and emerging cyber threats putting into account vulnerability.

Besides the findings of best practices, the research also offered practical recommendations on the strengthening of cloud data security; namely, the implementation of detection systems with adaptive responses to ever-changing environments of threats. However, with the advances, there were several limitations that were accepted. Complexities in integration are not uncommon when implementing capable security tools into diverse cloud environments. The research also indicated significant computational overheads especially when the encryption and AI-governed monitoring was used at scale. Most importantly, the quick change of cyber-threats become a constant challenge for the organizations that need to be ready to manage security measures proactively and flexibly. Such insights emphasize the need for investing in scalable, intelligent security frameworks that can adapt flexibly and, in a time,-sensitive manner to evolving threats yet still live up to the performance of large-scale cloud operations.

In the analysis laid out by D. Kumar and S [18], AI-machine learning detection of frauds occurring in the domain of finance has specifically been considered with regard to IoT. The paper elaborates on employing newer algorithms relevant to anomaly and cluster-based methods which analyze large streams of IoT data in an attempt to find fraudulent activities. The training of both supervised and unsupervised learning models, using historical transaction data, improved the fraud detection accuracy, whose credibility was then enhanced by adaptive learning methods through retraining and automatic responses to frauds. Challenges included poor data quality, computational complexity and enormous changes in dynamism of the fraud environment that dramatically impacted the fraud detection capability.

A hybrid IoT platform combining cloudlet computing and Edge-AI, for intelligent healthcare data processing, was designed by Morolong, Shava, and Gamundani [19]. The objectives of the study included data-sharing security, low latency and increased quality of decision-making processes. Advanced AI models, including Random Forest classifiers, Transformer Networks and Temporal Convolutional Networks, were utilized in this framework. Distributed processing across the system was realized by cloud computing, cloudlet and edge layers. Stream analytics processing was done through Apache Flink and blockchain was employed for secure data exchange. However, high computation costs, integration challenges and being a bottleneck for large-scale data processing were also recognized as limitations in this work. Musam *et al*. (2023) [20] significantly drives the proposed method by showcasing the effectiveness of hybrid machine learning models for improved predictions, which parallels the integration of advanced encryption techniques for secure healthcare data management

Morolong, Shava, and Gamundani [19] elevate the intelligent healthcare data processing capacity, a combination IoT platform merging cloudlet computation and Edge-AI was

fabricated to provide visionary-level solutions capable of addressing ever-growing demands made on contemporary medicine. The paper was constructed on critical goals involving safe data exchanging, low-delay messaging, as well as greater precision in making decisions. Utilizing high-capability AI models including Random Forest classifiers, Transformer Networks, and TCNs, the system made possible analysis of conditions and prediction of patient status for increased responsiveness in addition to improved clinical outcome. Layering in the infrastructure maximized the best aspects of cloud computing, cloudlets, and edge nodes so as to stabilize workloads of computing in the most efficient ways, reducing latency associated with central processing. The system further applied Apache Flink for real-time stream analysis, whereby constant observation and rapid processing of data were facilitated, pivotal in critical care environments

Darwish *et al*. [21] designed a service-oriented architecture for the system, which runs on a Hadoop-managed server cluster for processing power and data storage. This allowed for efficient management of educational resources for remote learning in enormous datasets with high concurrency. Stress testing proved that the platform could sustain many users concurrently and many data transactions reliably during times of heavy loads.

2.1. Problem Statement

Several drawbacks yet to be addressed, particularly slow data transmission is a considerable hindrance when transferring a substantial amount of sensitive health-related data, causing delays to the extent that timely patient care becomes expectedly impossible. A lack of end-to-end encryption also poses security threats inasmuch as there may not be adequate protection of healthcare data during transmission or storage. The proposed work attempts to ameliorate such situations via making transmission faster and safer, securing strong encryption to protect sensitive health care information in all aspects of its lifecycles [22].

There are a set of important hindrances that prevent the stable operation of the sensitive healthcare data management process, with slow data transmission being one of the key factors. In settings where instantaneous decisions are required–like in intensive care units, emergency response systems, and remote-patient monitoring–there could be serious consequences if there is a delay to the transmittal of critical data. This failure to quickly exchange large amounts of information that is health-related from networks to network not only affects clinical responsiveness but also affects the quality-of-care delivery. Such delays might cause diagnostic oversights, treatment delays, or, worse still, adverse outcomes to the patients, especially if healthcare workers use up-to-the-minute data for timely interventions. The existing data infrastructure in the health system of many countries is not optimized to support high-bandwidth transfers, particularly where network interruptions are more severe—rural or under-equipped settings [23].

Apart from the transmission bottlenecks, the lack of end-to-end encryption is also a grave threat to data privacy and security. Lacking strong encryption mechanisms, healthcare data is left exposed to interception, tampering, and unauthorized access throughout its movement or staying idle in a cloud. Considering the nature of highly sensitive medical records that many times contain personal identifiers, diagnostic results, medications histories, and insurance information, any leakage may lead to significant privacy breaches and legal ramifications as well as loss by the digital healthcare systems of the public trust. Besides, data breaches could pave ways for financial fraud, identity theft, or misuse of medical information. Sadly, current systems still persist with old security routine or partial data encryption, thus missing out on opportunities to protect healthcare data at various stages of their life cycle.

The suggested system aims at rectifying these weaknesses by adopting a holistic system that guarantees speed as well as security of data handling. Combining the Twofish encryption–a powerful symmetric key cryptography system, the system ensures maximum data protection at its collection to its final storage. At the same time, the implementation of WireGuard VPN tunnels allows low-latency, secure transfer of encrypted data across networks, thus, removing vulnerabilities along the way. Such dual-layered approach not only increases the level of confidentiality and integrity but also helps comply with the data protection regulation, including HIPAA and GDPR. The ultimate aim is to establish a robust digital infrastructure through which sensitive healthcare data can easily be moved across in security, thereby allowing informed decision-making timeously and improved patient outcome. With this amalgamation of the latest encryption and secure transmission techniques, the proposed system becomes a step further to ensure reliable end to end protection of data in the healthcare sphere.

Proposed system is addressing current weaknesses in healthcare data management, providing an all-inclusive, two-layered security framework. At the centre of this technique lays the incorporation of Twofish encryption that is a very secure symmetric key algorithm, known for its speed and immunity to cryptographic attacks. Twofish can be utilized at each step of the data life cycle – from collection to storage – in order to safeguard sensitive health information in its encrypted state from unwanted access. Such a level of security is especially important in the sphere of healthcare, where concerns of patient data discreetness are extremely critical.

Implementation of sophisticated AI models such as Random Forest classifiers, Transformer Networks, and TCNs, the system enabled real-time condition analysis and patient status prediction, enhancing responsiveness as well as clinical outcome. This layering of infrastructure leveraged the capabilities of cloud computing, cloudlets, and edge nodes to balance workloads of computing in an efficient manner, minimizing latency due to centralized processing. The system also employed Apache Flink for real-time stream processing, through which constant monitoring and speedy processing of data were allowed, vital within critical care settings

3. Proposed Methodologies

The proposed system for securing sensitive health data is showed in Figure 1. The process begins with Data Collection, in which patient data is collected from various sources. Once collected, it is then encrypted using Twofish encryption to keep it secure during transmission. Once encrypted, it is then transmitted to the cloud storage using WireGuard, which uses a high-performance VPN protocol for securely transporting the data. Finally, the last part would be the cloud storage itself, which keeps the data confidential and integral while authorizing its access. This is an effective process specifying a strong security solution over the life course of healthcare data.

The sensitive healthcare data security is an overall multi-layered concept intending to keep the confidentiality, integrity, and security of patient information within the whole

lifecycle of the data. The process starts with Data Collection in which data is sourced from multiple trusted sources, including the (EMRs), IoT-enabled healthcare devices, medical databases, and clinical monitoring systems. This step is highly important because it entails management of high volumes of very sensitive and personal information on patient history, diagnosis, treatment, and live health values. Rather at the time when any transmission occurs, this data is filtered and pre-processed to eliminate redundancies and unnecessary info by the system itself to maximise efficiency as well as accuracy. When refined, the data is encrypted using the two fish encryption which is a fast and symmetric key cryptographic technique that is reputable for its high key lengths, vulnerability to brute attacks and narrow processing costs. This encryption process makes sure that the healthcare data gets encrypted and remains unreadable and inaccessible to unauthorized users even in case of interception of such data during transit. Radhakrishnan *et al.* (2022) [24] notably reinforce the proposed method by integrating scalable cloud security through Salsa20 encryption and TLS, synergistically enhancing VPN-based protection for resilient, efficient, and comprehensive healthcare data safeguarding.

After encryption, the data is sent to cloud storage via WireGuard, a new, lightweight VPN protocol known for high-speed traffic and strong cryptographic security. WireGuard provides a secure VPN tunnel between the data origin and the cloud server, with encrypted data moving safely without vulnerability to external attacks while in transit. This tunnel is authenticated using public-private key exchanges, which validate the endpoints' identities that are communicating and protect against man-in-the-middle attacks. Data is subsequently stored in a secure environment within the cloud with access controls, audit trails, and data integrity checks to allow only authorized healthcare providers or systems to view or change the data [25].

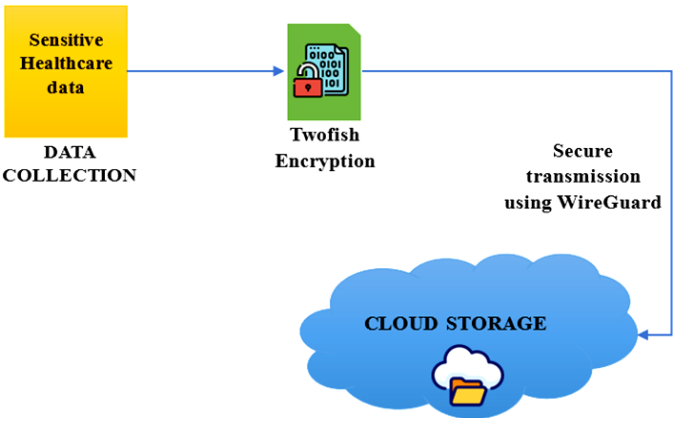

Fig 1: Architecture for securing sensitive health data

3.1. Data Collection

Sensitive healthcare data collected from multiple sources, including electronic medical records and medical databases [26]. That includes health parameters along with their medical history, diagnoses, treatments and other critical health-related information. Afterward, this data goes into the processing phase, where (removes) irrelevant and unnecessary information so that relevant data is retained. This preliminary step is crucial in the maintenance of accuracy and efficiency about the data while ensuring that things remain private regarding patients. The prepared data then go through a secured encryption process where it would be transported to the cloud for storing and further management, thereby assuring the protection of sensitive healthcare information all through the process. Sensitive healthcare data gathered from various sources such as electronic medical record and medical database. That is health parameters and their medical history, diagnoses, treatments, and so on which are critical pieces of health-related information. Then this data enters in the processing phase where (removes) useless and unwanted information, such that only relevant data is kept. The integration of Decision Trees and K-Nearest Neighbours of Budda, 2021[27] substantially strengthens IoT security by reducing false positives to 3% and achieving 95% accuracy, enhancing Ping Flood attack detection in IoT networks This initial step is very necessary in ensuring that the maintenance of accuracy and efficiency is kept on the data as well as maintaining things private as far as the patients are concerned. Subsequently, the prepared data undergoes a secured encryption process, whereby it would be transported to the cloud for storing and further managing the same without necessarily posing a threat on the sensitive healthcare related information throughout this whole process.

3.2. Encryption

After all the data has been collected, it goes through the process of encryption through a confidentiality and integrity step meant for sensitive healthcare data. Then, the collected data is encrypted using twofish encryption algorithm. This is a symmetric-key cipher that is very strong and has advantages of fast processing. In the Twofish encryption algorithm, the data are encrypted before transmission into cloud storage to ensure that unauthorized persons cannot read the data [28]. The algorithm accepts up to a 256-bits long key, which guarantees very high security. Thus, the data will be rendered secure and unreadable by, in case it gets intercepted during transmission or accessed by users without any permission has been utilized by the system in securing sensitive healthcare information-from the time of collection to transmission and storage-of patient records and health metrics [29]. Avalanche Effect also plays an important role in securing the encryption process; a minor change in the input (a single bit) causes a dramatic avalanche effect and unpredictable effect on the ciphertext. Thus, from the viewpoint of an attacker, it becomes impossible to decipher the encrypted data based on any identifiable pattern, thereby making it less susceptible to cryptanalysis and improving the overall security

Collected sensitive healthcare data goes through an intense encryption process to achieve confidentiality and data integrity. This is a key security effort to ensure that patient records and health metrics are not accessed or messed up by unauthorized personnel. It uses Twofish encryption algorithm, a strong symmetric-key encryption known for its efficiency and strength. Twofish makes data confidential prior to being sent to cloud storage, where confidential information will remain unreadable for unauthorized users who happen to get hold of it. This encryption type will provide Lenovo Secure Thoughts Application key lengths of up to 256 bits that, in turn, provides a tough barrier against probable security threats. At the point of data collection to the transmission and storage, Twofish encryption is incorporated in the system, to ensure that sensitive healthcare information is most protected. The research work by Bhavya Kadiyala *et al.* (2023) [30] validates using hybrid encryption-communication models, extensively supporting this proposed secure healthcare framework through proven improvements in data protection, scalability, and efficiency..

For Twofish encryption, the general process can be expressed as follows,

Let, $\mathbb{P}$ as Plaintext (128-bit block), K as Key (up to 256 bits) and $\mathbb{C}$ as Ciphertext (128-bit block).
The encryption process is summarized as equation (1),

$$C = F(P, K) \quad (1)$$

Where, $\mathbf{F(P,K)}$ is the Twofish encryption function that transforms the plaintext $\mathbb{P}$ using the key K, F includes multiple rounds of operations such as substitution using S-boxes, key mixing and permutation.
Mathematically, $\mathbf{F(P,K)}$ can be written as a composition of multiple rounds $\mathbb{R}$ (16 rounds in Twofish), where each round applies a function using the subkey derived from the original key and it's represented as equation (2),

$$C = F_R\left(F_{R-1}(\dots(F_1(P,K)))\right) \quad (2)$$

In each round of Twofish encryption, the input is XORed with a round key derived from the main key (key mixing). Then, substitution is performed using S-boxes for non-linear transformations. Finally, permutation shuffles the bits to ensure diffusion, spreading the influence of each bit across the output.
The final result after 16 rounds is the ciphertext C.

3.3 Secure Transmission in Cloud

After the data is encrypted, it gets safely transmitted under Wire Guard. All data transmits securely under lately called a modern high-performance VPN protocol. Secure transmission through Wire Guard begins by establishing a secured VPN tunnel between two endpoints that are authenticated to each other reciprocally through a public-private key pair exchange. After the building of the tunnel, confidentiality and data integrity due to encryption by a certain type of algorithm will govern the data being transmitted. The encrypted data, therefore, transits securely via the established VPN tunnel to the destination, where it is safe from view or modification by any unauthorized third party. The encrypted data is decrypted using the recipient's private key with integrity checking once they are in the designated destination. Wire Guard is especially known for low latency and small overhead, ensuring the effective yet secure transmission of data. minimizes latency and overhead at all times, hence minimizing resource use for a much-enhanced experience for real-time applications within the healthcare system. By using WireGuard, encrypted healthcare data packets are directly sent without being written on with any unauthorized access or interference during transit, ensuring their privacy and compliance with data protection standards.
Once the sensitive healthcare data has been encrypted with Twofish algorithm, it is transmitted in secure manner through WireGuard (VPN) that is modern and high performance protocol [31]. WireGuard is a lightweight program, secure as well as efficient, so it is particularly suitable for real-time and resource-critical applications like in healthcare. The process starts by setting up a secure communicating terminal or a VPN tunnel between the sender and receiver [32]. This tunnel involves a public-private key pair exchange, whereby each end-point validates each other to ensure the availing of data between the trusted sources. The authentication process itself guarantees that any third party who would try to intercept or even access the data without receiving the appropriate authorization is automatically cut off from the communication loop. The tunnel, after created, can be used as a secure conduit through which all the health care data encrypted is transferred through.
In this tunnel, details of data remain protected and kept against tampering. The encrypted packets are not subjected to intermediate networks or systems through which intermediate vulnerabilities are eliminated drastically, thereby reducing the risk of leakage of information or unauthorized access to the data. Wire Guard implementation of contemporary cryptographic primitives, namely ChaCha20 for encryption and Poly1305 for message authentication makes sure that, in case data packets are intercepted, they would be in form of unreadable and unverifiable data without the corresponding keys. At the receiving end, the data is decrypted using the private key of the recipient with inbuilt integrity checks to assure that the data is not tampered or altered in the course of the data transfer. This ensures the data comes in a natural form, not tampered with, preserving confidentiality, accuracy, and integrity that is highly needed in processing sensitive patient data. The ease and efficiency with which Wire Guard has been designed also decreases its possible failure points and makes the implementation's auditing easier, which contributes to a more secure system. The approach by Swapna Narla *et al* (2019) [33]. Inspired this method by demonstrating high-accuracy cloud-based health analytics, driving the need for secure transmission and storage protocol integration.
The Wire Guard will be of specific importance in healthcare settings, considering its low latency, minimal computational overhead, as well as the high throughput, which are key aspects of efficient processing of high-rate or time-critical medical data. For such examples as remote patient monitoring or telemedicine, or IoT based diagnostic tools such benefits mean faster and more secure transfer of data utilizing the minimum number of resources. Compared to the traditional VPN protocols that may create significant delays or complicated settings, the Wire Guard provides streamlined VPN-performance, allowing instantaneous data transfer, even though limited networks. In addition, its tiny codebase makes it easy to uphold and verify while minimizing the attack surface to the DSL casing in comparison to bloated VPN alternatives. With the implementation of Wire Guard, the proposed system guarantees smooth and safe delivery of encrypted data on healthcare without a risk of interception or manipulation that complies with privacy regulations like HIPAA and GDPR. This implementation is an essential part of the development of end-to-end data security that will establish the trust and reliability needed for the contemporary digital healthcare infrastructures.

Common Threats to Cloud Data Transmission

Cloud data transmission is prone to a number of threats that are capable of undermining the confidentiality, integrity, and availability of confidential data. Perhaps the most popular threat is the MitM attack where an attacker intercepts communication between a user and a cloud service with the prospect of changing or stealing data. Likewise, through eavesdropping and packet sniffing, attackers will be able to follow unencrypted data transmissions of which sensitive information such as login credentials or personal data can be intercepted. Data tampering is another big issue where data is deliberately altered as it is being transmitted, creating misinformation or system failure. Session-hijacking also raises the threat, since the attackers make use of session-tokens to gain unfavoured access to user accounts or services.

Other major threats are replay attacks, where captured data is resent to trick the system to unintended operations, and DNS spoofing, which misleads users to false cloud services where they are used to steal credentials or transmit malwares. These attacks are also exacerbated by insider threats, where individuals that have rightful access to information misuse their position to intercept or leak data. In order to address these risks, strong security measures like end-to-end encryption, secure authentication protocol, digital signatures, and round-the-clock monitoring systems need to be put in place. It is not only the protection of privacy of users but also their trust and reliability in cloud services.

DNS Spoofing and Redirection

DNS spoofing and redirection is an attack where an attacker corrupts the DNS responses to refer a user to a malicious or fraudulent website as opposed to a legitimate website. DNS is like the phone book of the internet which allows converting human-readable names into the internet machines known representation. In the DNS spoofing, an attacker alters DNS records, whether taking over DNS servers, or spoofing DNS traffic to make the fake IP address to be returned. This has the effect of actively redirecting users to malicious sites, extremely similar to legitimate sites, commonly used for phishing, credential theft, or malware spreading [34].

This attack is particularly dangerous because it is rather difficult to distinguish by an average user. It doesn't mean that even if a user enters the proper website address, the browser may be hijacked because of the tampered DNS reply [35]. It is a method that attackers can use to steal login credentials, install spyware, or to conduct man-in-the-middle attacks. To defend against DNS spoofing and redirection, the companies can take such security measures as DNSSEC cryptographically verifying responses from the DNS, using encrypted DNS protocols such as DNS over HTTPS (DoH) or DNS over TLS (DoT). In addition, it is possible to make DNS servers more secure and monitor the traffic for anomalies that can decrease the probability of such attacks.

4. Results

The results segment evaluates crucial performance metrics of the proposed system. The analysis entails cloud storage speed, encryption time and Avalanche Effect across encryption trials. These metrics showcase the performance, efficiency and security of the system under different conditions so that one can look into its strengths and weaknesses further. Yalla's (2023) [36] model enhances the proposed method by combining encryption with efficient scheduling, achieving high accuracy and encryption strength, thereby ensuring secure, reliable, and optimized healthcare data management.

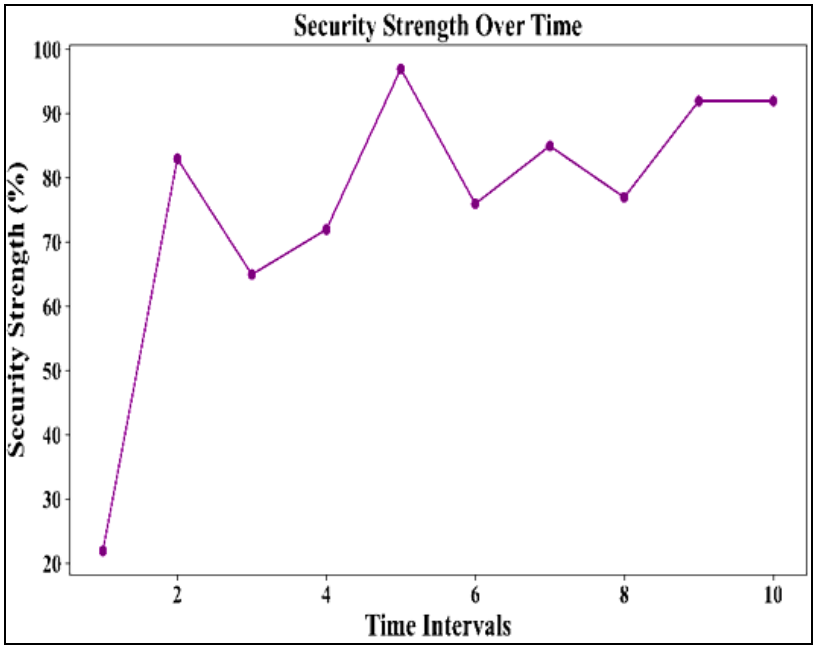

Fig 2: Security Strength

Figure 2 shows the trends of security strength with respect to the intervals of time. As the chart shows, the measurement of security strength varies between 22%-97% for particular time windows with high peaks at specific intervals such as 2 (83%), 5 (97%) and 9 (92%) of the timeline. It started low at the first-time interval (22%), rose sharply above that and then stabilized at high levels, showing that the mechanism of security becomes stronger over time. Trends would indicate that security performance of the system improves gradually, with the intermittent fluctuations showing resilience and effectiveness of the security measures applied [37].

The graph called "Security Strength over Time" illustrates the way in which the security strength (in percentage) changes for various stretches of time. Sequential time intervals are represented by the x-axis and while the security strength, represented on the y-axis, is used in the form of a percentage.

At first, the security strength is rather low at approximately 22% but it quickly increases to more than 80% at the second interval. The graph shows fluctuations after such a spike with peaks and troughs over the next intervals. The maximum possible level of security strength gets to within 98% of the value by the middle of the fifth period of time.

Such fluctuations indicate that the evaluated security measures or protocols are dynamic and open to change-possibly because of updates or adaptions, or due to an external influence on system resilience. In spite of the variations, the general trend points towards a trend towards enhanced security strength getting stabilized over time, particularly in the later intervals where the strength lies above 90%. This might mean that the system is having increased resistance causing it to adapt to threats better and thus being kept in more secure manner.

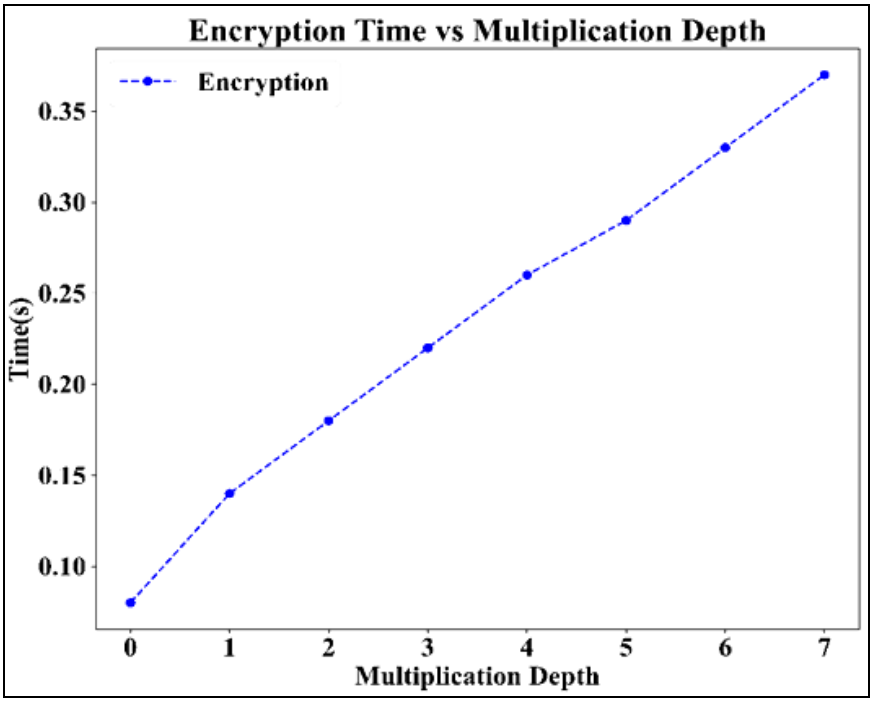

Fig 3: Encryption Time vs Multiplication Depth

Figure 3 shows how encryption time varies with the increase in multiplication depth. The association states that as the multiplication depth varies from 0 to 7, the encryption time also changes, with values ranging from about 0.10 seconds at depth 0 to around 0.35 seconds at depth 7. The blue dashed line indicates a linear growth in encryption time as the multiplication depth increases. This results in higher multiplication depths being more complex in computations and therefore longer encryption times are taken as well [38].

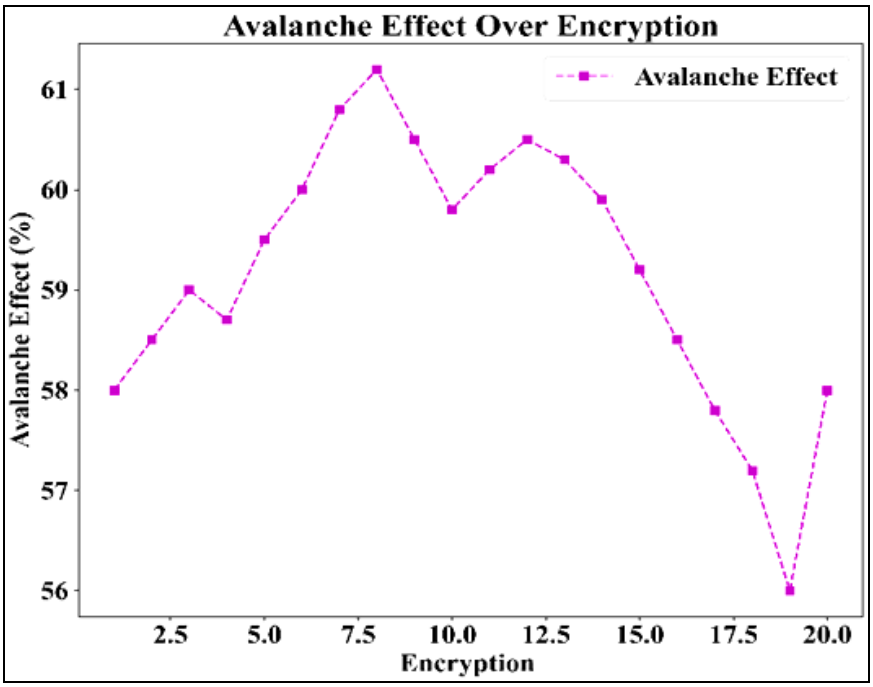

Fig 4: Avalanche Effect over Encryption

Figure 4 presents the Avalanche Effect through a number of encryption attempts. The plot shows how the Avalanche Effect varies from 56% to 61%. Starting from 58% in encryption attempt 1, it rises to a peak value of 61.2% at attempt 8 and then gradually returns to 58% at attempt 20. The dashed line indicates possible increase then final stabilization of the Avalanche Effect that describes how minute changes in the input affect the ciphertext; this is critical for the determination of the security of the encryption algorithm. The integration of federated models by Sareddy and Hemnath (2019) [39] strengthens this proposed encryption-transmission framework by showcasing decentralized, secure, and low-latency architectures ideal for protecting sensitive healthcare data.

Graph titled as “Encryption Time vs Multiplication Depth” can be used to depict the relation between encryption time (in seconds) and multiplication depth in a homomorphic encryption system. The multiplication depth is represented by the x-axis, which indicates the number of the multiplicative actions that can be made on the ciphertexts without

decryption. The right-hand y-axis represents the corresponding encryption time for each depth. One can explain from the graph that as the level of multiplications rises the time of encryptions also rises. This trend is illustrated by a dashed blue line with dots, having the linear or mildly exponential growth pattern.

It is possible to explain this increased time for encryption due to the larger depth of multiplication by the growing computational complexity and the need for more resources in deeper homomorphic calculations [40]. A multiplication depth at a deeper level enables more complicated encrypted operations but will necessitate more advanced encryption level with a larger set of parameters, hence further processing load. The above graphical representation shows a crucial trade-off in Homomorphic encryption. Where whereas deeper computation capability is achieved the delays needed in encryption will be prolonged as well which may affect the system performance and scalability [41].

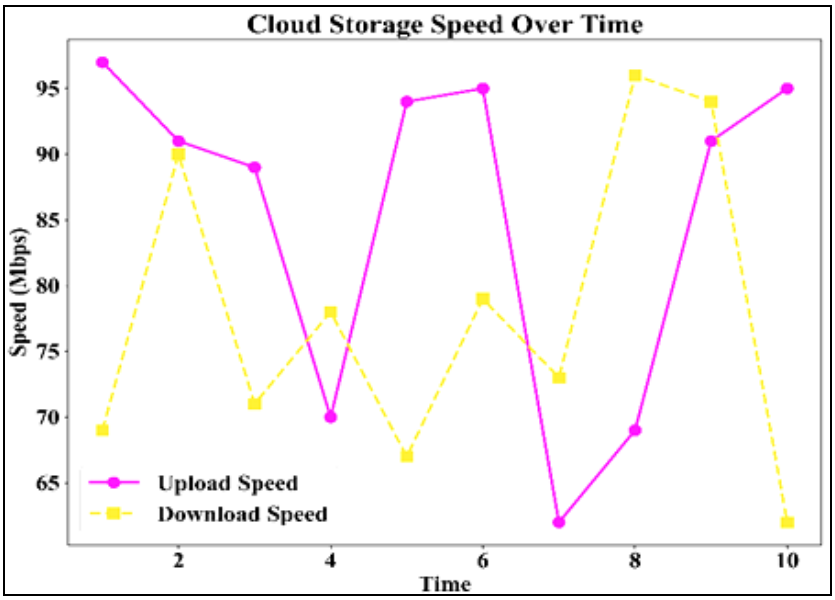

Fig 5: Cloud Storage Speed

Cloud storage upload and download speeds (in Mbps) with respect to 10 times are given in figure 5. Upload speed represented by the magenta line shows fluctuations between around 75 Mbps and 95 Mbps, with the highest peaks at 1, 3, 5 and 9 intervals of time. Opposing that, the download speed represented by the yellow dashed line ranges between 65 Mbps and 85 Mbps and also dips at 3, 6 and 8 times. This different speed shows that cloud storage services are not consistent as upload speeds are always higher than download speeds in all intervals. Ayyadurai's (2023) [42] groundbreaking Authorized Public Auditing Scheme fortifies the proposed method by guaranteeing ironclad data integrity using cutting-edge digital signatures, Proof of Retrievability, and robust TLS/SSL protocols, thwarting all tampering and unauthorized cloud breaches.

The graph of "Encryption Time vs Multiplication Depth" demonstrates the increase in time for encryption with the increase in multiplication depth in a homomorphic encrypting scheme. The x-axis names the multiplication depth that means the number of allowed consecutive multiplicative operations on encrypted data without decryption in between. The y-axis names the encryption time in second, from 0.10 seconds at the 0-depth to 0.35 seconds in the 7-depth. The plotted line continues upward steadily, expressing the linear relationship between the encryption time and the multiplication depth [43].

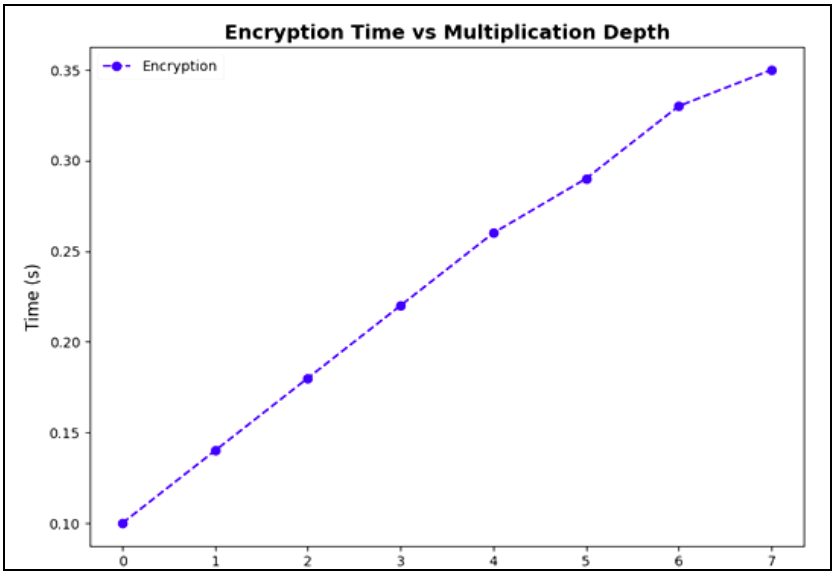

Fig 6: Encryption Vs Multiplication Depth

This linear growth is an indication of a certain rate of increase of the total processing time with respect to encryption complexity that is by allowing deeper operations. Scalability is expected to be positive because performance degradation remains underrated when stronger encryption parameters come into play. Such predictability is of high consideration in critical time-bounded applications such as healthcare data protection, wherein both high security and acceptable processing speeds must be confirmed. The very nature of homomorphic encryption facilitates secure computations over encrypted data, while the graph proves that the system can scale without any excessive delays. Sharadha Kodadi's (2022) [44] approach is useful because it shows how secure and efficient cloud-based prediction and resource optimization can be, motivating the proposed method to adopt strong encryption and fast transmission for enhanced healthcare data protection.

The "Cloud Storage Performance over Time" graph shows download and upload speed variation across 10 test periods. The horizontal axis is sequential test periods, and the vertical axis is speed measured in megabits per second (Mbps). Two lines are drawn: a blue dashed line with circles representing download speed, and a green dashed line with squares representing upload speed. From the graph, we can see that upload speeds always exceed download speeds, varying between 75 Mbps and 95 Mbps, while download speeds vary between 65 Mbps and 85 Mbps. Both values fluctuate, indicating volatility in cloud storage performance perhaps due to network conditions or server load. However, the overall speeds are quite high and consistent, reflecting the system's suitability for managing healthcare data transmissions that demand both reliability and efficiency.

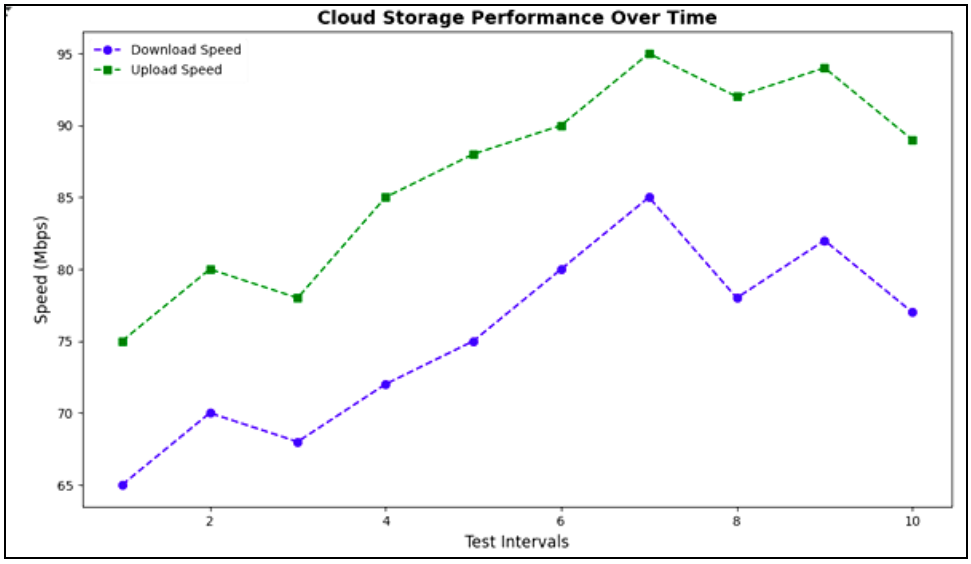

Fig 7: Cloud Storage Performance Over time

5. Conclusions and Future Enhancements

This paper presents a robust system that ensures the protection of sensitive healthcare data through the use of the Twofish encryption algorithm, WireGuard for secure transmission and cloud storage for data management. The proposed system guarantees the confidentiality, integrity and secure transmission of healthcare data throughout its entire lifecycle. The encryption strength fluctuates between 22% and 97% across different time intervals, with notable peaks at 83% in interval 2 and 97% in interval 5, highlighting improvements in security performance over time. Testing results showed that cloud storage download speeds fluctuate between 65-85 Mbps, while upload speeds range from 75-95 Mbps, indicating some variability in cloud storage performance. The Avalanche Effect fluctuates between 56% and 61%, ensuring that small changes in the input result in substantial, unpredictable changes in the ciphertext, enhancing the system's resistance to cryptanalysis. Encryption time increases linearly with multiplication depth, ranging from 0.10 seconds at depth 0 to 0.35 seconds at depth 7, demonstrating the system's ability to scale encryption strength while maintaining predictable processing times. Addressing challenges like slow data transmission and lack of end-to-end encryption in existing systems, future work can focus on integrating automated threat intelligence to dynamically monitor and respond to emerging security threats, further strengthening the system's resilience and security over time. Additional to the problem is the use of centralized data storage systems which by nature means single point of failure. A breach, system error or malfunction in such an infrastructure may culminate in leaking of large quantities of confidential patient data in one exposure event. Also, traditional access control mechanisms often heavily rely on the basic authentication of the password type without incorporating more sophisticated security means such as MFA or biometrical verification. This makes systems vulnerable to unauthorized entry attacks, phishing attacks, and credential stealing. With cyber threats getting sophisticated and more relentless by the day, it is apparent that static security mechanisms that are out of date cannot effectively protect healthcare data anymore. There is an immediate call for migration to the modern and adaptive security infrastructures that adopt strong encryption, decentralized architectures and smart access control mechanisms as to provide complete safeguards to the privacy of patients and the system [45].

This paper is the presentation of a complete and robust security system that aims to safeguard sensitive healthcare data with the help of multi-layered-security-architecture framework. The incorporation of the Twofish encryption algorithm, WireGuard for secure data transmission, and cloud storage for convenient management of data ensure end-to-end protection of healthcare data during its entire lifecycle by the proposed system [46]. The effectiveness of the system is illustrated from its performance metrics: encryption strength

ranges between 22% and 97% for different time intervals, with strong peaks of 83% and 97% observed at intervals 2 and 5, respectively-which shows progressive strengthening of security. Cloud storage performance is moderately varied, with download speeds of 65–85 Mbps and upload rates between 75–95 Mbps, a realistic light load pattern in changing network set-ups. Besides, the system yields some Avalanche Effect between 56% and 61%, indicating its capability in creating significant changes in ciphertext despite the slightest changes in plaintext, thus enhancing its strength against cryptanalysis. The encryption time scales linearly with the multiplication depth: from 0.10s at depth 0 to 0.35s at depth 7, providing a consistent scaling without undesired performance drops. The research work of Poovendran Alagarsundaram (2020) [47] on cloud-based DDoS detection inspired this proposed work focus on, low-latency, and cloud-adaptive security, guiding the integration for safeguarding sensitive healthcare data effectively.

The proposed system addresses the major issues with existing infrastructures for securing healthcare data, beyond technical performance matters. Traditionally, centralized data storage systems put all the eggs in one basket, creating a hugely risky scenario, wherein a breach or error could result in a massive exposure of sensitive patient data. Also, a rudimentary authentication scheme, such as choosing a password, is what basically keeps it open to being flagged by some phishing attack or credential theft. With cyber threats growing advanced and relentless, the old static security paradigm simply cannot work anymore. This paper firmly advocates that the building blocks of the current security framework must be cast aside in Favor of an adaptive, next-generation framework featuring strong encryption, decentralized data storage, and intelligent access control such as multi-factor authentication and biometric verification. Such measures would ensure higher privacy guarantees and uphold integrity while supporting a resilient defense posture against modern cyber threats with future-proof capabilities.

References

1. Chenthara S, Ahmed K, Wang H and Whittaker F. “Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing,” IEEE Access. 2019; 7:74361–74382. doi: 10.1109/ACCESS.2019.2919982.
2. Griebel L *et al*., “A scoping review of cloud computing in healthcare,” BMC Med. Inform. Decis. Mak. 2016; 15(1):17. doi: 10.1186/s12911-015-0145-7.
3. Deshmukh P. “Design of cloud security in the EHR for Indian healthcare services,” J. King Saud Univ.-Comput. Inf. Sci. 2017; 29(3):281–287. doi: 10.1016/j.jksuci.2016.01.002.
4. Bhatia S and Malhotra J. “Morton Filter-Based Security Mechanism for Healthcare System in Cloud Computing,” Healthcare. 2021; 9(11):1551. doi: 10.3390/healthcare9111551.
5. Almalawi A, Khan AI, Alsolami F, Abushark YB and Alfakeeh AS. “Managing Security of Healthcare Data for a Modern Healthcare System,” Sensors. 2023; 23(7):3612. doi: 10.3390/s23073612.
6. Pulakhandam W. “Towards a trustless marketplace: public-private blockchain integration using network-wide agreement and collaborative endorsement,” *Int. J. Appl. Sci. Eng. Manag*, 2023, 17(2).
7. Liao WH and Qiu WL. “Applying analytic hierarchy process to assess healthcare-oriented cloud computing service systems,” SpringerPlus. 2016; 5(1):1030. doi: 10.1186/s40064-016-2686-3.
8. Dang LM, Md. Piran J, Han D, Min K. and Moon H. “A Survey on Internet of Things and Cloud Computing for Healthcare,” Electronics. 2019; 8(7):768. doi: 10.3390/electronics8070768.
9. Garikipati V. “Optimizing Traffic Management and Cloud Security in Software Networks Using Advanced Deep Learning Models for Application and Attack Classification,” *Int. J. HRM Organ. Behav*, 2020, 8(3).
10. Chinnasamy P and Deepalakshmi P. “HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud,” *J. Ambient Intell. Humaniz. Comput*. 2022; 13(2):1001–1019. doi: 10.1007/s12652-021-02942-2.
11. Masood I, Wang Y, Daud A, Aljohani NR and Dawood H. “Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure,” Wirel. Commun. Mob. Comput. 2018; 1:2143897, Jan. 2018, doi: 10.1155/2018/2143897.
12. Amanat A, Rizwan M, Maple C, Zikria YB, Almadhor AS and Kim SW. “Blockchain and cloud computing-based secure electronic healthcare records storage and sharing,” Front. Public Health. 2022; 10:938707, doi: 10.3389/fpubh.2022.938707.
13. Molo MJ *et al*., “A Review of Evolutionary Trends in Cloud Computing and Applications to the Healthcare Ecosystem,” Appl. Comput. Intell. Soft Comput, 2021, 1–16. doi: 10.1155/2021/1843671.
14. Abouelmehdi K, Beni-Hessane A and Khaloufi H. “Big healthcare data: preserving security and privacy,” J. Big Data. 2018; 5(1):1. doi: 10.1186/s40537-017-0110-7.
15. Gudivaka BR, Gudivaka RL, Gudivaka RK and Basani DKR. “AI-Powered Digital Twins Integrated with IoT for Advanced Pandemic Analytics: Transforming Urban Healthcare Infrastructure and Enabling Resilient, Data-Driven Response Mechanisms,” *Int. J. Inf. Technol. Comput. Eng.,* 2023, 11(2).
16. Javaid M, Haleem A, Singh RP, Rab S, Suman R and Khan IH. “Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers,” Int. J. Cogn. Comput. Eng. 2022; 3:124–135. doi: 10.1016/j.ijcce.2022.06.001.
17. Hanen J, Kechaou Z and Ayed MB. “An enhanced healthcare system in mobile cloud computing environment,” *Vietnam J Comput. Sci*. 2016; 3(4):267–277. doi: 10.1007/s40595-016-0076-y.
18. Kumar D and Dr. SS. “Enhancing Security Mechanisms for Healthcare Informatics Using Ubiquitous Cloud,” J. Ubiquitous Comput. Commun. Technol. 2020; 2(1):19–28. doi: 10.36548/jucct.2020.1.003.
19. Morolong MP, Shava FB and Gamundani AM. “Cloud computing security in health cyber physical systems,” J. Discrete Math. Sci. Cryptogr. 2023; 26(5):1553–1568. doi: 10.47974/JDMSC-1821.
20. Musam VS, Ganesan S, Musham NK and Kurunthachalam A. “Hybrid Machine Learning Models For Improving Pediatric Readmission Prediction Using Cloud-Based EMR Analytics,” *Int. J. Manag. Res. Rev*, 13, 3.
21. Darwish A, Hassanien AE, Elhoseny M, Sangaiah AK and Muhammad K. “The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems,”

J. Ambient Intell. Humaniz. Comput. 2019; 10(10):4151–4166. doi: 10.1007/s12652-017-0659-1.
22. Yin BLB and Rana ME. "A Critical Review of Cloud Computing Adoption, Data Security Concerns, and Impact in the Healthcare Landscape," in 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Manama, Bahrain: IEEE, Jan. 2024, 1–7. doi: 10.1109/ICETSIS61505.2024.10459350.
23. Farid F, Elkhodr M, Sabrina F, Ahamed F and Gide E. "A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services," Sensors. 2021; 21(2):552. doi: 10.3390/s21020552.
24. Radhakrishnan P, Musham NK, Ganesan S, Musam VS & Karthick M. Optimizing healthcare data collection and security through cloud computing. *International Journal of Modern Electronics and Communication Engineering*, 2022, 10(1). https://ijmece.com/ijmeceadmin/upload/ijlbps_67e3db479042c.pdf."
25. Abughazalah M, Alsaggaf W, Saifuddin S and Sarhan S. "Centralized vs. Decentralized Cloud Computing in Healthcare," *Appl. Sci.* 2024; 14(17):7765. doi: 10.3390/app14177765.
26. Alharbi F, Atkins A and Stanier C. "Understanding the determinants of Cloud Computing adoption in Saudi healthcare organisations," Complex Intell. Syst. 2016; 2(3):155–171. doi: 10.1007/s40747-016-0021-9.
27. Budda R."Revolutionizing IoT Attack Detection: Decision Trees and K-Nearest Neighbors for Efficient Ping Flood Recognition," *Int. J. Appl. Sci. Eng. Manag*, 2021, 15(4).
28. Bhatia T, Verma AK and Sharma G. "Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing," Concurr. Comput. Pract. Exp. 2020; 32(5):e5520. doi: 10.1002/cpe.5520.
29. Chang SC, Lu MT, Pan TH and Chen CS. "Evaluating the E-Health Cloud Computing Systems Adoption in Taiwan's Healthcare Industry," Life. 2021; 11(4)310. doi: 10.3390/life11040310.
30. Kadiyala B. "Integrating multivariate quadratic cryptography with affinity propagation for secure document clustering in IOT data sharing," *Int. J. Inf. Technol. Comput. Eng,* 2023, 11(3).
31. Kebache R *et al*., "Reducing the Encrypted Data Size: Healthcare with IoT-Cloud Computing Applications," Comput. Syst. Sci. Eng., 2024, 1–10. doi: 10.32604/csse.2024.048738.
32. Humayun M, Alsirhani A, Alserhani F, Shaheen M and Alwakid G. "Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency," *J. Cloud Comput.* 2024; 13(1):37. doi: 10.1186/s13677-024-00602-2.
33. Narla S. "A Cloud-Integrated Smart Healthcare Framework for Risk Factor Analysis in Digital Health Using Light GBM, Multinomial Logistic Regression, and SOMs," *Int. J. Comput. Sci. Enigineering Tech*., 2019, 4(1).
34. Liu J, Tang H, Sun R, Du X and Guizani M. "Lightweight and Privacy-Preserving Medical Services Access for Healthcare Cloud," IEEE Access. 2019; 7:106951–106961. doi: 10.1109/ACCESS.2019.2931917.
35. Abbas H, Maennel O and Assar S. "Security and privacy issues in cloud computing," Ann. Telecommun. 2017; 72:(5–6):233–235. doi: 10.1007/s12243-017-0578-3.
36. Yalla RKMK. Innovative data management in cloud-based component applications: A dual approach with genetic algorithms and HEFT scheduling. *Int J Eng Sci Res*. 2023; 13(1):94-105."
37. Paul M, Maglaras L, Ferrag MA and I. Almomani, "Digitization of healthcare sector: A study on privacy and security concerns," ICT Express. 2023; 9(4):571–588. doi: 10.1016/j.icte.2023.02.007.
38. Al-Issa Y, Ottom MA and Tamrawi A. "eHealth Cloud Security Challenges: A Survey," *J. Healthc. Eng*, 2019, 1–15. doi: 10.1155/2019/7516035.
39. Sareddy MR "Optimized Federated Learning for Cybersecurity: Integrating Split Learning, Graph Neural Networks, and Hashgraph Technology," *Int. J. HRM Organ. Behav*., 2019, 7(3).
40. Singh S, Pankaj B, Nagarajan K, Singh NP and Bala V. "Blockchain with cloud for handling healthcare data: A privacy-friendly platform," Mater. Today Proc. 2022; 62:5021–5026. doi: 10.1016/j.matpr.2022.04.910.
41. Banimfreg BH. "A comprehensive review and conceptual framework for cloud computing adoption in bioinformatics," Healthc. Anal. 2023; 3:100190. doi: 10.1016/j.health.2023.100190.
42. Ayyadurai R, "An authorized public auditing scheme for dynamic big data storage in platform as a service," *Int. J. HRM Organ. Behav.,* 2023, 11(4).
43. Mbonihankuye S, Nkunzimana A and Ndagijimana A. "Healthcare Data Security Technology: HIPAA Compliance," Wirel. Commun. Mob. Comput., 2019, 1–7, doi: 10.1155/2019/1927495.
44. Kodadi S. "High-Performance Cloud Computing and Data Analysis Methods in the Development of Earthquake Emergency Command Infrastructures," *J. Curr. Sci.,* 2022, 10(3).
45. Agapito G and Cannataro M. "An Overview on the Challenges and Limitations Using Cloud Computing in Healthcare Corporations," Big Data Cogn. Comput. 2023; 7(2):68 doi: 10.3390/bdcc7020068.
46. Kumar V, Jangirala S and Ahmad M. "An Efficient Mutual Authentication Framework for Healthcare System in Cloud Computing," *J. Med. Syst.* 2018; 42(8):142. doi: 10.1007/s10916-018-0987-5.
47. Poovendran A. Analyzing the Covariance Matrix Approach for DDOS HTTP Attack Detection in Cloud Environments. *International Journal of Information Technology & Computer Engineering*, 2019, 7(1), ISSN 2347–3657.