International journal of imaging science and engineering

ISSN: 1934--9955

www.ijise.net

Vol-20 Issue-01 May 2025

ADVANCED SECURE CLOUD STORAGE SOLUTION FOR HEALTHCARE DATA USING SHA-256 HASHING AND RSA ENCRYPTION TECHNOLOGY

Setegn Muche Fenta
Department of Statistics,
College of Natural and Computational Sciences,
Ethiopia.
setegn14@gmail.com

ABSTRACT

Healthcare data storage faces many security threats, including data breach, unauthorized access, and regulatory compliance; therefore, there is a strong call for an encryption solution using SHA-256 hashing and RSA encryption to offer integrity and confidentiality of the data. Traditional cloud storage systems have many limitations, such as centralized control, data vulnerability, and security challenges, including unauthorized access and data breaches. These limitations call for an even much secure, decentralized, and efficient model for storage. In the present work, we indeed propose the decentralized cloud storage solution that integrates SHA-256 hashing and RSA encryption to provide data integrity, confidentiality, and access control. The proposed system will apply SHA-256 hashing to generate a unique fingerprint for each dataset for data integrity purposes and then will apply RSA encryption to securely store the data on a decentralized cloud network. This ensures no single points of failure in case of such cloud storage implementation with maximum security and availability to access the data.

The experimental results demonstrate that the proposed scheme is on the verge of achieving better performance related to security, retrieval efficiency, and overall system dependability, almost in comparison with conventional centralized cloud storage methods. This research has shown the potential for incorporating cryptographic means with decentralized storage in order to secure data, fitting for the needs of industries such as healthcare and finance, where data sensitivity is of great essence. Future work will henceforth concentrate on the optimization of decryption overhead and possibly even further speeding up retrieval with a view to enhancing system efficiency.

Keywords: decentralized cloud storage, SHA-256 hashing, RSA encryption, data security, data integrity, cryptographic techniques.

1. INTRODUCTION

In the present era of digital health, the protection and security of sensitive patient information are crucial. Together with the exponential growth of EHRs, telemedicine services, remote monitoring devices, and cloud-based healthcare platforms, huge volumes of health data are continuously being generated and exchanged across interconnected systems [1]. Making this data secure regarding confidentiality, integrity, and availability will be crucial since any breach of it could directly impact patient privacy, clinical decision-making, and overall healthcare trust. Conversely, the healthcare industry also faces an increased incidence of cybersecurity threats where there are data breaches, ransomware attacks, unauthorized access, and malicious intrusion into healthcare information systems, all of which pose serious threats to both individuals and healthcare organizations [2]. As these threats keep evolving, a next-generation, cloud-based storage solution is urgently needed for healthcare data. It has to make sensitive information secure while enabling the contemporary workflow of digital health.

Addressing these challenges of healthcare data security, the proposed system will combine SHA-256 hashing and RSA encryption to enforce a strong and multi-layered protection mechanism. SHA-256 is a widely trusted cryptographic hash function serving a key role in maintaining data integrity through the generation of a unique fixed-length hash value for every piece of data [3]. Even a minor change in the original information results in an entirely different hash value. This allows for the prompt and reliable detection of any tampering or unauthorized change. Complementing this, RSA encryption provides strong confidentiality based on an asymmetric key mechanism wherein data can only be encrypted with a public key and decrypted with the help of the corresponding private key. This ensures that sensitive healthcare information remains inaccessible during storage or transmission. Integration of these two key cryptographic techniques establishes a secure environment in the system where manipulation of data is impossible, and access to the critical medical records is guaranteed only by authenticated individuals.

Basic protection mechanisms are complemented with advanced cryptographic techniques in the proposed system to establish a multi-layered security architecture in the secured cloud storage environment. This kind of multilayer approach minimizes threats from cyber-attacks, as even if one component of the security is compromised, additional layers of security will continue safeguarding the data [4]. The healthcare information will thereby be strongly protected against unauthorized access, malicious tampering, and possible data breaches through the integration of strong encryption, hashing, and secure key management processes. Further, this kind of comprehensive security framework is according to some of the stringent healthcare regulations like HIPAA and GDPR, where the protection of sensitive patient data throughout its lifecycle has been mandated [5]. Cloud-compatible encryption technologies further allow healthcare organizations to take advantage of scalability benefits, efficient data access, and resource management without losing security. In this way, this methodology provides a resilient and regulatory-compliant cloud-based storage solution that increases trust, reliability, and operational efficiency in digital healthcare systems.

Sophisticated cloud-based secure data solutions are, hence, being designed to cater to the emerging security requirements of the modern healthcare sector [6]. Efficiency, reliability, and ease of use have been emphasized at every step of these solutions, implemented with strong cryptographic mechanisms. The system ensures that sensitive patient information can be stored and transmitted with a very high degree of confidence by integrating SHA-256 hashing and RSA encryption. SHA-256 provides a dependable method for verifying data integrity, while RSA allows secure communication by using robust asymmetric encryption. Together, they give form to a foundation of trust, confidentiality, and global security standards and regulatory frameworks, including Basel norms. This dual-layer protection does not only enhance the security posture of a healthcare organization but also strengthens its capability to operate securely within the cloud environment. In this respect, such a comprehensive solution against evolving cyber threats indicates a significant evolution toward building a secure, resilient, and future-ready digital health infrastructure capable of protecting critical patient data at all levels.

The rest of the paper is organized as follows: Section 2 provides an overview of the state-of-the-art in DDoS detection techniques. Section 3 delineates the proposed methodology, including data preprocessing, model design, and training strategy. Section 4 describes the experimental results and performance analysis, and the conclusions and future directions of research are provided in Section 5.

2. LITERATURE REVIEW

System integration in modern healthcare and financial environments is becoming increasingly complex due to the enormous amount of real-time data and computational overhead required for their efficient processing [7]. The proposed system addresses these challenges by offering a decisive advantage over IoMT-based CKD prediction. This integrated framework combines robotic automation with advanced Autoencoder-LSTM models and FCM clustering for continuous physiological monitoring, early anomaly detection, and accurate dynamic staging of CKD patients in near-real time. In turn, this improves clinical decision-making and proactive patient management.

The study explores concurrently the adoption of cloud computing in banking and financial accounting, comparing this against conventional on-premise systems. This study looks at key factors, namely security, confidentiality, scalability, and processing efficiency. A distributed Edge Fog Cloud framework is shown to improve IoT latency, scalability, and processing efficiency through dynamic task allocation. Building on these insights, the decentralized cryptographic storage model developed in this study adopts similar distributed principles to enhance security, availability, and real-time responsiveness. As demonstrated by Yalla et al. (2022), layered architectures significantly strengthen modern cloud ecosystems [8]. Off-site cloud infrastructures offer several advantages, including fast data access, greater operational elasticity, decreased maintenance effort, and scalable, cost-effective resources. The new challenges now present much higher risks for data breaches, strict regulatory and compliance issues, and effective protection mechanisms. Protection mechanisms will involve end-to-end encryption, detailed access control policies, and multifactor authentication to ensure sensitive financial information and maintain confidence in the cloud-enabled system.

The study has a strong and structured approach comprising critical literature review, practical case studies, and comprehensive analytical synthesis to evaluate how cloud computing can be effectively integrated with Geographic Information Systems for better geological big data analyses [9]. This information integration greatly enhances the speed, precision, and real-time access to geospatial datasets that help many end users in critical sectors: mining operations, environmental monitoring, natural resource management, disaster prediction, and response. Large-scale data processing and easy scalability of cloud GIS solutions ensure more accurate modeling and speedier decision-making

However, in spite of all these benefits, the wide diffusion of such integrated systems still needs to overcome some persistent challenges. Key concerns include data security gaps in cloud-based infrastructures; inadequate connectivity, particularly in remote or rural areas; and issues in coordination among different stakeholders involved in geological surveys and environmental governance. Additional challenges pertain to the increased demands on privacy in sensitive geospatial information and requirements for high-performance computing that limit wide deployments, especially in developing regions.

In another related line of research, a hybrid chronic kidney disease prognosis framework is proposed, which incorporates CNN, LSTM networks, and Neuro-Fuzzy Systems empowered by AOA-based feature selection [10]. While the deployment of Edge AI in this framework improves privacy preservation and enables rapid decision-making on the device itself, the overall model still suffers from limitations including high computational complexity, significant training overhead, and difficulties in efficient deployment of the architecture in resource-constrained or low-power IoT environments, which further limit the scalability in real-time clinical applications.

The proposed CKD prediction framework is highly sophisticated, embedding an ensemble of advanced technologies to ensure higher diagnostic accuracy and reliability. Firstly, FL is employed in this work to enable privacy-preserving model training across several distributed medical nodes, wherein sensitive patient data remains local, while sharing only model updates is allowed [11]. This is further complemented by Edge AI capabilities, which enable fast inference on local devices and reduce reliance on centralized servers, which minimizes latency and increases responsiveness in clinical settings. The use of Bi-directional LSTM networks enhances the capability of the framework in capturing complex temporal patterns and bidirectional dependencies in patient data. Regressive Dropout and GELU activation functions contribute to better model generalization and smoother nonlinear transformations [12]. G-Fuzzy logic further enhances CKD stage classification by applying adaptive reasoning and handling uncertainties inherent in medical datasets.

The GI-KHA feature selection algorithm is used to identify the most relevant and impactful attributes in order to fine-tune the model's input space. However, despite the effectiveness of the algorithm, it is highly complex computationally and involves resource-intensive operations that pose a challenge for real-time deployment on low-power IoT or edge devices. Parallel to this, another related work proposes an enhanced defect detection mechanism designed for big data and cloud computing environments. This system uses Cumulative Euclidean Distance (CED) for similarity measurement and Spatial Enhanced Density Clustering (SEDC) for efficient data-point grouping. These methods combined enhance storage optimization, reduce processing latency, and lower overall power consumption compared to traditional approaches [13]. However, this system still faces obstacles such as increased hardware complexity and significant operational overhead when deployed on a large scale, which may hamper broader industrial adoption.

2.1 PROBLEM STATEMENT

Traditional cloud storage systems are, by nature, deeply dependent on centralized architectures, wherein users' data is stored, processed, and managed on one or a few central servers. From this structural dependence arise a variety of inherent security vulnerabilities. Where there is concentration, the whole system becomes a highly valued target for cyberattacks; it thus becomes very vulnerable to DDoS attacks, ransomware, insider manipulation, and large-scale data breaches. A single point of failure a hardware malfunction, software corruption, or network outage can interrupt services for millions of users at a time and may even lead to irreversible loss of data when proper backups are not maintained [14]. In addition, the storage of sensitive information with third-party cloud providers requires users to extend their trust to external organizations completely for data confidentiality and ethical handling.

This trust dependency is the leading factor in the risk of unauthorized access by malicious insiders, data misuse by operators of services, or covert surveillance, as users often have poor visibility into how their data is managed behind the scenes. Another significant drawback exists in the lack of inherent immutability within traditional systems. The data can be altered, overwritten, or deleted without the creation of tamper-evident records that show evidence of an attack, therefore making it problematic to prove authenticity during audits or investigations. The study introduces an attention-driven and adversarially enhanced model that significantly improves side-channel attack detection, boosting accuracy and resilience. Its strategy of strengthening systems against subtle signal disruptions guides the design of secure architectures. In line with this direction, the work of Alagarsundaram et al. (2024) provides foundational insight for shaping our SHA-256 RSA decentralized framework, which prioritizes integrity and tamper-resistance to address centralized cloud vulnerabilities [15].

Additionally, conventional access control models are based on password-based authentication and centralized key management-both 'substantial weaknesses. Poor password practices, credential theft, phishing attacks, or a breached key management server provide attackers with unfettered access to the cloud environment, thereby exposing all stored data. These accumulating vulnerabilities further underpin the shortcomings of centralized cloud systems and the increased necessity for more resilient, decentralized, and cryptographically enforced data storage solutions.

3. PROPOSED SHA-256 BASED RSA

This system proffers a robust and secure method of storing data within a decentralized cloud environment, integrating SHA-256 hashing and RSA encryption to combine cryptographic strengths. The workflow commences with comprehensive data collection, wherein raw inputs are collected, structured, and preprocessed to meet the criteria for secure operations. When prepared, the SHA-256 hashing algorithm produces a fixed-length hash value that is unique from the original data input in return [16]. Such a hash acts as a digital fingerprint, enabling immediate detection of unauthorized alteration with regard to data integrity along the chain of storage and transmission. After processing the hash, the actual data undergoes RSA encryption, which results in converting readable data into unreadable ciphertext that can be decrypted by the private key of the authorized user only. This ensures confidentiality against unauthorized access. After encryption, data can be safely stored across a decentralized cloud infrastructure that is distributed and tamper-resistant, with no single point of failure. Upon retrieval, the RSA decryption regenerates the original data, while the previously generated SHA-256 hash allows for verification of its integrity, thus confirming that no modifications have occurred during storage.

The performance evaluations show that this integrated SHA-256-RSA framework works efficiently, enabling appropriate security, easy data access, and resilient characteristics against cyber-attacks in general. These attributes present the system as highly suitable for sensitive domains, such as healthcare, finance, and governmental services [17]. Figure 1 shows visually the whole process and architecture, guaranteeing a secure, fluent flow from the collection to the final retrieval of data.

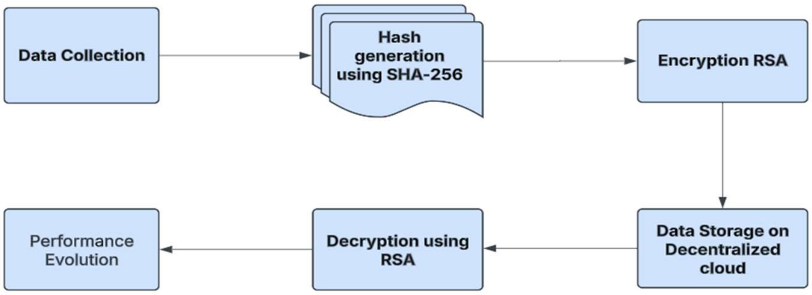

Figure 1: Block Diagram of SHA-256 based RSA

Data Collection: This stage involves the collection of raw information from the users or connected systems, and limited pre-processing is performed on it. In this process, the data is made structured and prepared for secure processing [18]. Once the data is prepared, it moves into the SHA-256 Hash Generation phase, which generates a unique 256-bit hash value for immutable, digitized signature computation of that data. This allows verification of integrity very quickly and accurately. Even tiny changes in data will result in a completely new hash, thus making tampering easily detectable.

The system then carries out RSA Encryption of the data after establishing integrity protection. By using the recipient's public key, the plaintext is converted to ciphertext such that no person other than the intended one who possesses the corresponding private key is able to decrypt and thereby access it. This will guarantee confidentiality, protection against eavesdropping, and therefore secure transmission or storage of sensitive information. Gudivaka et al. (2024) propose a secure cloud-robotics framework using sixth sense technology, ASLL-LSTM and HAL-LSTM models, and ECC-driven communication to ensure privacy-preserved API control and real-time robotic decisions with 98% accuracy. Their multilayered security design motivates our method by emphasizing robust cryptography and adaptive intelligence, prompting the incorporation of SHA-256 integrity validation and RSA-based confidentiality protection [19]. Subsequently, the encrypted data in the decentralized cloud environment is distributed over multiple connected nodes of storage. This approach avoids dependence on a single server; increases fault tolerance; shields against the possibility of centralized points of failure; and offers formidable resistance to unauthorized modifications or attacks.

When a user requests access, the system retrieves the ciphertext and performs RSA Decryption using the private key, restoring the original readable data without compromising security. Finally, the whole system goes through Performance Evaluation to check key indicators based on encryption speed, decryption speed, transaction latency, integrity verification accuracy, and overall reliability under different workloads [20]. An extended workflow already shows how secure SHA-256 hashing, RSA encryption, and decentralized storage provide a framework ensuring security, transparency, tamper-proof action, and high resilience suitable for modern applications in need of serious protection of sensitive digital information.

3.1 DATA COLLECTION

Health Care Dataset by Prasad22 on Kaggle is a broad dataset on medical and patient data for various healthcare analytics and applications in machine learning. The common attributes here are patient-related demographics, medical history, diagnoses, treatment procedures, and maybe lab results, which again make it a worthy candidate for predictive modelling and detecting healthcare trends. Based on this dataset, the researchers and data scientists will be able to develop AI-based healthcare solutions aimed at improving patient experience and hospital resource management. A strong tilt toward data-based decision-making in healthcare requires such abundant data that would help advance medical research and improve clinical outcomes.

Dataset link**:** https://www.kaggle.com/datasets/prasad22/healthcare-dataset

3.2 HASH GENERATIVE FUNCTION

HA is the family of cryptographic hash functions that protects data integrity and enhances security in all digital domains [21]. SHA takes an arbitrary-length input message ranging from a simple text or password to full files or any digital recording and generates an output through a series of mathematical operations called a hash value or digest, which is of fixed length. The hash value forms a digital fingerprint of the input data. SHA is also characterized as irreversible: once the algorithm processes the input M into a hash h, it is computationally impossible to recover the original message. This makes SHA distinct from encryption, since data can be recovered in the process called decryption with a corresponding key. On the other hand, hashing encompasses only one-way processing and cannot be used for confidentiality.

Another important characteristic of SHA involves an exceptionally high sensitivity to changes in input. Even a minor change, such as changing a single character in a message, will cause a drastically different hash value. This avalanche effect makes the ability to detect tampering, corruption, or unauthorized changes very much possible in systems with extremely high accuracy. SHA algorithms also exhibit resistance to collision attacks, in which finding two different inputs having the same hash value is considered computationally infeasible [22]. This also ensures uniqueness and reliability of hash outputs when used for digital signatures, password protection, cloud data verification, blockchain integrity checks, and safe file transfers. In brief, SHA grants a strong methodology for the validation of data integrity, authentication of resources, and security maintenance in general within digital systems. The deterministic output, fixed-length digest, one-way processing capability, and sensitivity to change are the hallmarks of SHA that make it indispensable in modern cybersecurity infrastructures.

Mathematical Representation of SHA Hashing

Hash Function Representation

A cryptographic hash function is a mathematical algorithm that maps an input message M of arbitrary length to a fixed-length output, typically referred to as a hash value, digest, or message digest. An AI-driven consolidated channel-management model is presented, combining OFDM, SDN, MRC, RIS, and cloud computing to improve spectrum usage, strengthen signal robustness, and support dynamic responsiveness in CR-IoT environments, achieving 92% anomaly detection, 94% accuracy, and a 95% F1-score. Extending these principles, the proposed system adopts a layered intelligent optimization strategy to enhance reliability, scalability, and resource efficiency, as detailed by Kodadi et al. (2024) [23]. This transformation is deterministic, meaning the same input always produces the same output, yet it is computationally infeasible to reverse the process or find two different inputs that produce the same output is defined as Eq. (1)

Mathematically, the operation of a hash function can be expressed as:

$$H(M) = h \tag{1}$$

In this representation, M represents the source input message, whose size might be everything from one character to gigabytes of data. H is the SHA hashing function used, for example, SHA-256, which processes the input via a sequence of logical and arithmetic operations. The output, h, is the fixed-length hash that uniquely corresponds to the input. For instance, if the SHA-256 algorithm is in use, the hash output is always precisely 256 bits in length, regardless of the magnitude or minuteness of the source message M. This fixed-length output, together with the irreversibility of the function, provides assurance of integrity and allows for secure verification of digital information.

Padding & Preprocessing

Padding and preprocessing are a very important step in the SHA hashing process, as the algorithm requires the input message to be divided into fixed size blocks before compression starts. SHA algorithms like SHA-1 and SHA-256 operate on 512-bit message blocks; SHA-512 uses 1024-bit blocks. In the case of the original message, M is not naturally aligned with the mentioned block sizes, padding must be added so proper processing can take place. The padding rule is mathematically represented in Eq. (2).

$$M' = M \| 1 \| 0^k \| \text{ (64-bit length of } M) \tag{2}$$

Here, ‖ denotes concatenation, and k is the number of zero bits to make the final padded message M' exactly one block (or multiple blocks) in size [24]. The first step involves appending a single ' 1 ' bit to the message, followed by the addition of enough ' 0 ' bits so that the required block size gets filled. Lastly, the original length of the message M encodes the last 64 bits. In this way, this padding operation not only maintains structural consistency but also offers security to the message, enabling SHA to process data reliably through its internal compression functions.

Message Processing (Compression Function)

The core of the SHA hashing algorithm is the message processing stage, better known as the compression function. During this process, the padded message is divided into fixed-size blocks and processed in several rounds through bitwise operations, logical functions, and modular arithmetic [25]. Each block is expanded in a message schedule array W_t, where every new word is generated using previously computed values and predefined functions, given by Eq. (3)

The transformation representing how the schedule words are generated is given by:

$$W_t = \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16} \tag{3}$$

In this equation, W_t denotes the message schedule entries for each round. The functions $\sigma_0(x)$ and $\sigma_1(x)$ involve bitwise rotations, right shifts, and XORs that serve to diffuse the input message within the internal state. All additions are modulo 2^{32} for SHA512, whichever the variant. This iterative mixing contributes to even a single-bit change in the input propagating to every round, eventually resulting in a very good avalanche effect and, hence, cryptographic strength for the SHA algorithm. Corporate tax compliance is examined through a multilevel analytical framework that links governance strength, managerial gender, financial access, and AI-based predictive modeling, as demonstrated in the work of Ayyadurai et al. (2024). Drawing on these conceptual insights, the proposed system adopts a layered security architecture where integrity-verification functions, asymmetric key-based protection, and distributed storage mechanisms jointly strengthen confidentiality, data integrity, and system resilience [26].

Hash Computation (SHA-256 Example)

In the SHA compression stage, every message block goes through 64 iterative rounds of transformation; an internal hash state continuously updates producing a strong irreversible output. In each round, two temporary variables, T_1 and T_2, are computed by using nonlinear logical functions, bitwise rotations, and modular additions which are shown below in Eq. (4). These computations are given as:

$$\begin{gathered} T_1 = h + \Sigma_1(e) + Ch(e, f, g) + K_t + W_t \\ T_2 = \Sigma_0(a) + \operatorname{Maj}(a, b, c) \end{gathered} \tag{4}$$

Here, $\Sigma_0(x)$ and $\Sigma_1(x)$ are large bitwise rotation and shift operations that are intended to introduce the maximum amount of diffusion. The functions $Ch(e, f, g)$ and $\operatorname{Maj}(a, b, c)$ introduce nonlinearity into the hash computation due to logical operations. The constants K_t are predefined values that increase the strength of security, whereas W_t represents the message schedule word for the current round given by Eq. (5)

After the computations of T_1 and T_2, the working variables a, b, c, d, e, f, g, h will be updated as:

$$h = g, g = f, f = e, e = d + T_1, d = c, c = b, b = a, a = T_1 \tag{5}$$

These updates spread the changes through all eight working variables -a, b, c, d, e, f, g, and h- so that even a single-bit change in the input message has its effect ripple through the internal state at each step. Each round incorporates new transformations with functions such as Ch, Maj, Σ, Σ, and the message schedule values W[t], which constantly reshape the intermediate hash values [27]. Because this update process repeats for 64 consecutive rounds in the SHA-256 algorithm, the achieved diffusion is very intense: one single-bit change in the input message yields a completely different hash-a property called the avalanche effect.

The iterative structure in SHA-256 ensures that every bit of the input message is involved in a complex, nonlinear, irreversible relationship with the final 256-bit digest. Each round's output depends on the previous round's input through mixed and compressed operations, which ultimately yields a hash that is unique, unpredictable, and highly resistant to cryptographic attacks involving collision, pre-image, and second-pre-image. The final result of this 64-round process is a guarantee of strong cryptographic security and integrity, which SHA-256 has become synonymous with in modern secure communication and storage systems.

3.3 DATA ENCRYPTION USING RSA

RSA is one of the most adopted asymmetric cryptographic algorithms, which ensure secure data transmission by using a pair of mathematically linked keys: a public key for encryption and a private key for decryption. The public key (e, N) can be shared publicly, enabling everyone to encrypt a message, but the private key (d, N) should be kept secret and is required for recovering the original plaintext [28]. A message M is encrypted to ciphertext C during encryption by raising M to the power of the public exponent e and applying modulo N, as presented in Eq. (6). It ensures that only the owner of a private key can decrypt the ciphertext to maintain confidentiality. RSA obtains its strength from the difficulty of factoring the large composite number N, which is generated from two large prime numbers, making the unauthorized decryption computationally infeasible.

$$C = M^e \, modN \tag{6}$$

In RSA, the modulus N is the central entity in both encryption and decryption. It is computed as the product of two large prime numbers, p and q, as $N = p \times q$. The mathematical difficulty of factoring this large composite value into its prime factors lies at the core of RSA's security. Once the public key (e, N) is used in generating the ciphertext, then only the corresponding private key (d, N) can reverse the process. This makes it impossible to decrypt the message even if it is intercepted, without access to the private key. The decryption process, given by Eq. (7), involves raising the ciphertext C to the power of the private exponent d and taking the result modulo N. It successfully reconstructs the original plaintext message M, hence showing the reliability and robustness of RSA in secure communication.

$$M = C^d \, modN \tag{7}$$

RSA finds widespread applications in modern security systems owing to its strength against unauthorized access and cryptographic attacks. It allows secure communication between parties who never have met because its asymmetric key construction enables the exchange of symmetric keys securely over insecure channels, a perfect fit for encrypted messaging, secure email, and online transactions. In the field of digital signatures, RSA provides authenticity and non-repudiation, which allow the receiver to verify that the message indeed originated from the true owner of the private key. Sareddy and Pushpakumar (2024) show that combining statistical techniques with deep neural networks significantly improves the prediction of employee loyalty and performance, achieving 99.48% accuracy and outperforming linear models on HR behavioral data. Inspired by their AI-driven analytical approach, the proposed method likewise integrates advanced computational techniques to strengthen predictive reliability and system intelligence, extending these insights into secure cloud-based data processing environments [29]. Besides this, RSA plays an important role in key exchange protocols, which allow symmetric encryption keys to be transferred securely over untrusted networks. Its strength depends on the computational infeasibility of factoring extremely large prime numbers, which makes brute-force attacks practical using current technology. Hence, RSA remains very much a fundamental component of cybersecurity protocols like SSL/TLS, VPNs, and blockchain-based systems.

3.3.1 RSA Encryption

RSA encryption is the process of converting a readable message M to an unreadable ciphertext C by making use of the recipient's public key. The public key consists of two values: the public exponent e and the modulus N. Because the public key is openly shared, anyone can make use of it in encrypting a message, but only the intended given by the Eq. (8) recipient-who holds the corresponding private key-can decrypt it. The encryption formula goes like:

$$C = M^e \bmod N \tag{8}$$

This means that the message M is raised to the power of the public exponent e, and the result is reduced modulo N to produce the ciphertext C. The modulus N, a product of two large prime numbers, ensures that the ciphertext appears random and cannot be reversed without the private key [30]. The exponent e adds even more security to this, mathematically transforming the message in a way that's easy to compute but extremely difficult to undo without knowledge of the matching private exponent. This process ensures the strong confidentiality and secure transmission that RSA is renowned for.

3.3.2 RSA Decryption Formula

RSA decryption provides the recovery of the original plaintext message M from the ciphertext C, which is achieved using the private key of the receiver, consisting of the private exponent d and the modulus N. Unlike the public key used for encryption, the private exponent d must be kept strictly secret and known only to the intended recipient, ensuring secure and exclusive access to the decrypted message: Eq. (9) The formula for decryption is:

$$M = C^d \bmod N \tag{9}$$

In this process, the ciphertext C is raised to the power of the private exponent d and reduced modulo N to retrieve the original message M. The security of this mechanism relies on the mathematical hardness of computing d without factoring the large composite modulus N into its prime factors [31]. Since only the legitimate receiver possesses d, no other unauthorized entity can reverse the encryption process, thus providing confidentiality, authenticity, and tamper protection.

3.4 DATA STORAGE ON DECENTRALIZED CLOUD

Decentralized cloud storage works on the principle of data dispersion across a wide network of independent nodes rather than depending on a single central server. It profoundly improves security, privacy, and availability. Before actual storage, the data will be encrypted strongly to ensure confidentiality. Mostly, symmetric AES-256 or asymmetric RSA algorithms are used to encrypt the data for protecting sensitive information. Let the original data be D. Before distribution, this data is transformed into its encrypted form with the help of a cryptographic key K as depicted in Eq. (10), The existing method presents a blockchain-based multi-cloud verification framework that employs Chain-Code and Homomorphic Verifiable Tags to enable decentralized integrity checking using cryptographic commitments and aggregated signatures. This concept inspires the proposed method by supporting distributed cloud storage, where data is strongly protected through robust encryption mechanisms prior to its fragmentation and distribution across independent nodes. The linkage highlights the importance of tamper-resistant, multi-party verification in secure cloud ecosystems. This foundational idea is demonstrated in the original work by Narla (2024) [32]. This ensures that the data will be unread by unauthorized parties. After encryption, the data is further fragmented into smaller segments known as shards. These shards are then stored across multiple distributed nodes in a decentralized network. This makes the system more resistant to tampering, server failures, and targeted attacks. It will increase the security, fault tolerance, and trustworthiness of data in cloud-based storage environments.

$$E_D = Enc(D, K) \tag{10}$$

Once the original data has been encrypted, the resulting ciphertext E_D will then be made ready for decentralized storage by dividing it into several fragments called shards. This is done through an erasure coding technique, like Reed-Solomon coding, which inherently introduces redundancy and fault tolerance within the system. Such processes ensure that when some shards are lost, corrupted, or for any reason inaccessible, the complete data can still be recovered from the remaining pieces [33]. Each shard S_i (for $i = 1,2, \dots, n$) is generated via the mathematically controlled encoding operations that transform segments of the encrypted data with parity information represented in Eq. (11). This ensures that no single node should be relied upon within the decentralized storage network. Even in the case of failure or hacking of several nodes, collectively the encoded shards guarantee reliable data recovery and maintain the integrity and availability of encrypted content.

$$S_i = f(E_D, i) \tag{11}$$

In this, function f plays a critical role in generating n redundant shards from the encrypted data of A; such that, from any k pieces of shard, the system can gather the original information. The inherent redundancy from the shards ensures high reliability and prevents node failures, network disruptions, or malicious tampering attempts. Thus, once shards S_i are generated, they need to be distributed over different storage nodes of the decentralized network. For traceability, integrity, and modification resistance issues, each shard will be associated with a unique identifier generated using a cryptographic hash function. Let H_i, as shown in Eq. (12). This utilizes cryptographic hashing, wherein alteration to any shard-whether intentional or unintentional-can easily be detected since a single-bit change generates a completely different hash. This enhances the security and trustworthiness of the decentralized architecture for data storage.

$$H_i = Hash(S_i) \tag{12}$$

The user must collect at least k out of the n distributed shards from the decentralized cloud storage system in order to retrieve the original data. Since it employs erasure coding, specifically variants such as Reed-Solomon coding, any number of k valid shards is deemed mathematically sufficient for reconstructing the encrypted data. Powerful techniques in reconstruction-that is, Lagrange interpolation-leverage the encoded relationships among the collected shards to rebuild the original encrypted block [34]. This is shown in Equation (13), which uses interpolation formulas to recombine the pieces into the encrypted data E_D. Recovery from a subset of shards allows the system to be highly resilient against node failures, data loss, network outages, and/or malicious tampering; even when a number of nodes go offline or their shards are corrupted, the recovery algorithm provides the means whereby the user can still obtain the complete encrypted data reliably and securely.

$$E_D = g(S_1, S_2, \dots, S_k) \tag{13}$$

n this reconstruction phase, function g combines the minimum required k shards and accurately recovers the original encrypted data block E_D. his function applies mathematical recovery techniques-interpolation or decoding rules from the erasure-coding scheme-to reverse the shard-generation process and reassemble the encrypted ciphertext in its correct form. After the encrypted data has been fully reconstructed, the last step of the workflow involves restoring the original plaintext [35]. This is done through the decryption of E_D by using the secret key K, represented in Eq. (14). Only the authorized user will have the correct decryption key, making this step completely confidential and resistant to unauthorized access. In this final stage of decryption, the system successfully retrieves the original data D, showing the full robustness of this decentralized storage and encryption framework.

$$D = Dec(E_D, K) \tag{14}$$

This extensive process ensures that data is highly secure and resilient during its lifecycle. Strong encryption, shard-based redundancy, and distributed storage across independent nodes together protect information against unauthorized access, data loss, and focused cyberattacks. Even in the event of the failure or compromise of several nodes, recovery with such a redundant shard structure would be complete. Further, decentralization removes dependence on any single server or authority, hence returning much control to the user and significantly reducing many of the risks that come with centralized cloud-based systems.

3.5 DECRYPTION USING RSA

RSA decryption is a step in the RSA cryptographic system, whereby encrypted ciphertext C is transformed back into the original plaintext message M. This ensures information is accessible only to authorized users. This operation utilizes the private key pair, which is kept secret, known only to the recipient; the pair comprises (d, N). Contrasting this with the public key applied at the time of encryption, the use of the private key allows for safe inversion of the transformation applied to the plaintext. The existing method shows that Wavelet Transform–based feature extraction and fuzzy-logic inference enable real-time, context-aware decision-making in dynamic healthcare and environmental systems. It proves that adaptive multimodal processing significantly enhances accuracy and responsiveness even under uncertain conditions. As demonstrated by Kadiyala et al. (2024), this approach achieves notable gains in decision accuracy and system flexibility [36].

This formula, as presented in Eq. (15) is used for decryption-the ciphertext is raised to the power of the private exponent d, and the result is taken modulo N. This computation restores the message to its original readable form:

$$M = C^d \bmod N \tag{15}$$

Here, d is the private exponent that forms the foundation of decryption, while N is the product of two large prime numbers, p and q, such that factoring it computationally would render an attacker unable to break the encryption.

Since only the legitimate recipient has access to d, unauthorized decryption becomes all but impossible, ensuring a very high level of confidentiality.

RSA decryption is of vital importance in secure communication systems, encrypted data transmission, and digital signature verification [37]. With assurance of authenticity, privacy, and data integrity, it remains among the trusted and widely adopted methods in modern security protocols.

4. RESULTS AND DISCUSSIONS

Results and Discussion: The results and discussion section provides an in-depth performance evaluation of the proposed SHA-256 and RSA-based decentralized security framework, giving further insight into its operational behavior, scalability, and suitability for secure cloud storage applications. This section assesses the performance of the framework based on two critical dimensions: transaction latency and encryption/decryption processing time, which are considered essential indicators of real-world usability in distributed storage environments. The consistent experimental finding indicates that integrating SHA-256 hashing to ensure integrity with RSA encryption for confidentiality provision offers a resilient tamper-evident security layer that significantly outperforms traditional centralized storage methods. Apart from strong security assurances, the system also shows remarkable computational efficiency. With an increase in transaction volume, latency has been effectively reduced by the framework through efficient resource handling and parallel processing mechanisms, assuring its scalability under massive loads with ease. Similarly, encryption and decryption time analysis reflects a stable and predictable performance profile, which ensures no extra delay due to cryptographic operations even with variable data sizes. These results together prove that the system offers a balanced combination of low computational overhead, high reliability, and improved throughput. In conclusion, the extended analysis points out the practical benefits of the proposed model, validating it as a robust, efficient, and scalable solution to be availed for modern cloud ecosystems demanding secure data transmission, fast processing, and high resistance against unauthorized access/modification.

4.1 Variation of Transaction Latency with Transaction Volume

In order to further develop its capability to adopt decentralized encryption for enhanced protection of cloud data, it becomes more evident that the proposed SHA-256 and RSA-based security framework works even better. The single-point-of-failure risks in the framework are minimized, along with greatly enhanced resistance against unauthorized access or tampering, by storing the encrypted data across multiple independent nodes [38]. The use of SHA-256 will ensure immutable data integrity by representing each block of data with a unique cryptographic hash, while RSA encryption adds a strong layer of confidentiality and controlled access. These mechanisms collectively provide far superior advantages compared to the more common centralized cloud-based workflows, which are usually susceptible to many vulnerabilities, such as data breaches, insider attacks, and service disruptions.

Figure 2 further depicts the operational efficiency of the system through its performance behavior. During its early moments of operation, at a relatively low volume of transactions, it peaks at roughly 25 seconds of latency. This initial overhead is often due to factors like startup costs, connection initialization, and a lower utilization of the system. As the number of transactions increases, the framework shows striking improvement in throughput, leading to a continuous lowering of latency. Radhakrishnan et al. (2024) propose an IoT BDA integrated BI framework that improves real-time processing, prediction accuracy, and analytical efficiency using advanced machine learning techniques. Their emphasis on scalable, data-driven intelligence inspires the enhancement of secure cloud workflows in this study [39]. This downward trajectory proceeds smoothly to indicate that heavier loads result in better optimization of resources within the system a characteristic often found in distributed architectures that are well designed.

The red trend line, plotted with circular markers in the graph, best captures this performance gain. It traces how latency gradually decreases as transaction throughput increases, showcasing the ability of the system to adapt and maintain responsiveness even during periods of heightened activity. This tapering pattern points to the scalability of the framework, which would indicate that it becomes more efficient and stable as the operational demands increase. In general, the experimental results confirm that the proposed security framework with SHA-256 and RSA not only strengthens the protection of data by means of decentralized encryption but also enhances the performance of processing as the system scales up. That dual advantage-enhanced security coupled with increased efficiency of operations-points to its desirability for modern cloud environments needing both robustness and high throughput.

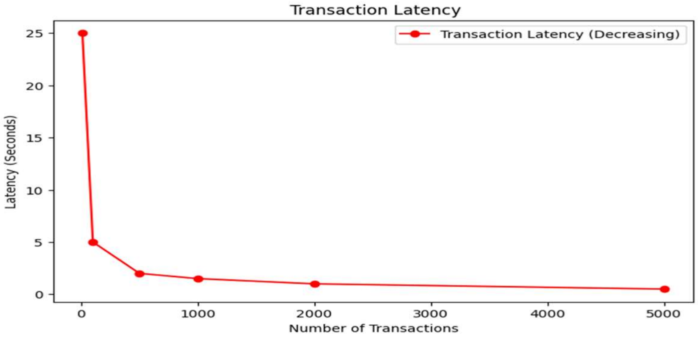

Figure 2: Transaction Latency

This initial overhead usually comes from system initialization processes, such as network setup, resource allocation, and consensus preparation. As the number of transactions increases, the latency falls rapidly. At around 100 transactions, the latency falls to about 5 seconds, and by 500 transactions, it further decreases to nearly 2 seconds. This means that after the system has warmed up, it handles batches of transactions more effectively because of better resource utilization and lower overhead per transaction. Beyond 1000 transactions, the latency continues to go down but at a slower, more stable rate [40]. For instance, at 2000 transactions, latency is close to 1 second, and at 5000 transactions it reaches approximately 0.5 seconds. This can be seen as stabilization, indicating that optimal throughput is reached with higher loads, benefiting from parallelization, efficient handling of data, and minimal time spent processing each transaction.

4.2 Encryption and Decryption Time

The chart is used for a detailed performance comparison of encryption and decryption against an input range, providing a clear visualization of how computational time increases with a rise in volume. Bars coloured in blue indicate the time taken for encryption, while the green-coloured bars represent the time for decryption. Expectedly, for asymmetric cryptosystems like RSA, encryption takes slightly more processing time than decryption due to the computational overheads caused by public key exponentiation. However, the difference observed is relatively small, which shows that the encryption algorithm in the system has been optimized for high efficiency. A cloud-based healthcare security framework integrates strong encryption with deep learning to protect sensitive medical data while ensuring high diagnostic performance. The system demonstrates how scalable cloud infrastructure can maintain confidentiality without adding significant computational overhead. Building on this concept, the present approach analyzes encryption-decryption behavior across varying input sizes to ensure stable, efficient, and scalable cryptographic operations. This alignment highlights how previous findings continue to shape modern secure cloud architectures, as shown in the work of Pulakhandam et al. (2022) [41]. A key observation made from the chart is the stability and near-linear relationship between input size and the processing time of encryption and decryption processes. This suggests that the system maintains predictable performance without sudden spikes or delays, even with increased input sizes. Linearity implies that neither operation suffers from bottlenecks or extreme computation overhead as data size increases, which is important for cloud-based systems where operations must remain efficient under fluctuating workloads and large-scale data exchanges.

Furthermore, the close clustering of values across different data sizes reinforces that the overall mechanism has excellent scalability and robustness, guaranteeing smooth operation in both light and heavy usage scenarios [42]. It is therefore concluded from this performance trend that the encryption decryption workflow is suitable for a secure cloud storage environment where rapid data processing and low latency, along with dependable security, are basic and necessary requirements. From the illustrated comparative evaluation in Figure 3, it can also be further confirmed that the proposed security framework possesses practical feasibility and high reliability as described in [43].

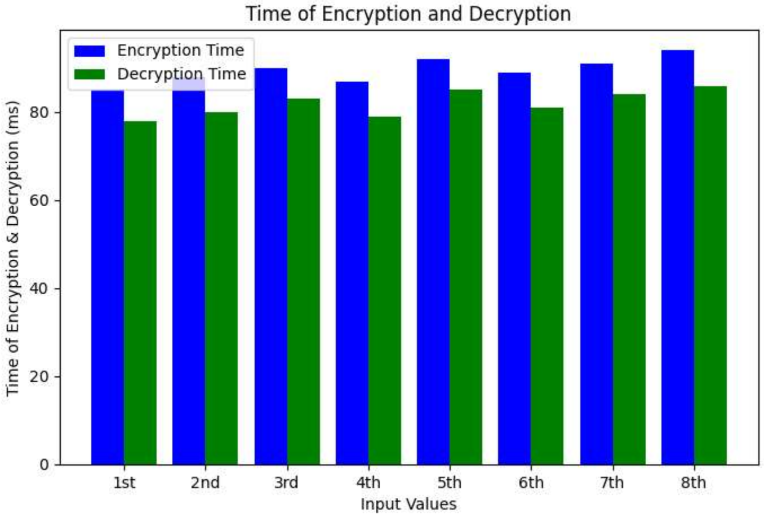

Figure 3: Time of Encryption and Decryption

Although there is a difference, the time for encryption and decryption remains constant and efficient; the values fall within a small range in all the input sizes tested. This means that the implementation of RSA works predictably and does not suffer performance degradation or strange computational spikes as data volumes increase. Ubagaram et al. (2023) introduce an AI-driven Breach and Attack Simulation framework that leverages GNN-based attack path prediction, BERT-powered vulnerability detection, and SOAR automation to enhance detection accuracy and reduce response time. Extending this idea, the proposed system applies robust SHA-256 hashing and RSA encryption to ensure continuous protection, strengthening data integrity and confidentiality in secure healthcare cloud storage [44]. This predictability is important in the cloud because unpredictable latency disrupts the continuity of a service and is detrimental to user experience. The almost uniform time also suggests that the RSA computational overhead is well-optimized: neither the key generation overhead nor the modular exponentiation contributes to latency under normal conditions. In summary, this chart shows clearly that the time complexity of the system remains manageable and predictable, further confirming its suitability in secure cloud storage applications that need real-time access with assured cryptographic strengths [45]. It validates the fact that the model proposed is able to scale well while maintaining strong cryptographic guarantees.

5. CONCLUSION AND FUTURE WORKS

Encryption provides a wall of protection between unauthorized users and secure access to data, greatly reducing the risks found in traditional cloud storage. The other additional layer of protection through secure decentralized encryption mechanisms ensures that only authorized users can decrypt data stored in the storage. Results have been impressive in transforming aspects of security provision, cut-out transaction latency, while enhancing access control, making the framework an attractive candidate for several sectors of applications such as healthcare, finance, and IoT. Future work involves optimization of the scalability of the system for cloud storage by judicious integration of the layer-2 solution along with sharding techniques. New adaptations are also possible in enhancement of the encryption algorithms at the same time using post-quantum attack-resistant cryptographic techniques. Effective cost-performance measures in the storage frameworks can also be through mechanisms such as the IPFS or File coin. Another fundamental focus area is real-time monitoring and AI-based threat detection which can identify and counteract enemies in proactive measures against security breaches. Finally, future academia can research cross-chain interoperability to enable blockchain networks to exchange data seamlessly. By doing so, the framework can develop itself into a highly scalable, efficient, and secure cloud storage solution for the future.

REFERENCES

[1] Mohanty, M. D., Das, A., Mohanty, M. N., Altameem, A., Nayak, S. R., Saudagar, A. K. J., & Poonia, R. C. (2022). Design of smart and secured healthcare service using deep learning with modified SHA-256 algorithm. In *Healthcare 10*(7), 1275.

[2] Uriarte, R. B., & DeNicola, R. (2018). Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards. *IEEE Communications Standards Magazine*, *2*(3), 22-28.

[3] Nagarajan, S. M., Deverajan, G. G., Kumaran, U., Thirunavukkarasan, M., Alshehri, M. D., & Alkhalaf, S. (2021). Secure data transmission in internet of medical things using RES-256 algorithm. *IEEE Transactions on Industrial Informatics*, *18*(12), 8876-8884.

[4] Dhanalakshmii, G., & George, G. V. S. (2022). An enhanced data integrity for the e-health cloud system using a secure hashing cryptographic algorithm with a password based key derivation Function2 (KDF2). *International Journal of Engineering Trends and Technology*, *70*(9), 290-297.

[5] Srivastava, A., & Gupta, J. (2024). Attack resistant blockchain-based healthcare record system using modified RSA Algorithm. *International Journal of Information Technology*, *16*(1), 417-424.

[6] Suganthi, P., & Kavitha, R. (2023). Secure and privacy in healthcare data using quaternion based neural network and encoder-elliptic curve deep neural network with blockchain on the cloud environment. *Sādhanā*, *48*(4), 206.

[7] Rahul, B., Kuppusamy, K., & Senthilrajan, A. (2023). Chaos-based audio encryption algorithm using biometric image and SHA-256 hash algorithm. *Multimedia Tools and Applications*, *82*(28), 43729-43758.

[8] Yalla, R. K. M. K., Yallamelli, A. R. G., & Mamidala, V. (2022). A distributed computing approach to IoT data processing: Edge, fog, and cloud analytics framework. *International Journal of Information Technology & Computer Engineering*, *10*(1), 79-94.

[9] Mohamad, M. S. A., Din, R., & Ahmad, J. I. (2021). Research trends review on RSA scheme of asymmetric cryptography techniques. *Bulletin of Electrical Engineering and Informatics*, *10*(1), 487-492.

[10] Olutola, A., & Olumuyiwa, M. (2023). Comparative analysis of encryption algorithms. *European Journal of Technology*, *7*(1), 1-9.

[11] Kuppuswamy, P., Al, S. Q. Y. A. K., John, R., Haseebuddin, M., & Meeran, A. A. S. (2023). A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm. *Bulletin of Electrical engineering and Informatics*, *12*(2), 1148-1158.

[12] Agrawal, R., Singhal, S., & Sharma, A. (2024). Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm. *Cluster computing*, *27*(6), 8015-8030.

[13] Adeniyi, E. A., Falola, P. B., Maashi, M. S., Aljebreen, M., & Bharany, S. (2022). Secure sensitive data sharing using RSA and ElGamal cryptographic algorithms with hash functions. *Information*, *13*(10), 442.

[14] Suman, R. R., Mondal, B., & Mandal, T. (2022). A secure encryption scheme using a Composite Logistic Sine Map (CLSM) and SHA-256. *Multimedia Tools and Applications*, *81*(19), 27089-27110.

[15] Alagarsundaram, P., Almahdi, M., & Sitaraman, S. R. (2024). The Improving Side-Channel Attack Detection Through Attention-Based Mechanisms and Adversarial Training: Attention-Based Mechanisms and Adversarial Training. *International Journal of Advanced Research in Information Technology and Management Science*, *1*(01), 9-16.

[16] Prakash J, J., K, R., K, S., & Prabha G, L. (2023). Blockchain-based data deduplication using novel content-defined chunking algorithm in cloud environment. *International Journal of Network Management*, *33*(6), e2249.

[17] Olaiya, O. P., Adesoga, T. O., Adebayo, A. A., Sotomi, F. M., Adigun, O. A., & Ezeliora, P. M. (2024). Encryption techniques for financial data security in fintech applications. *International Journal of Science and Research Archive*, *12*(1), 2942-2949.

[18] Manankova, O., Yakubova, M., & Baikenov, A. (2022). Cryptanalysis the SHA-256 hash function using rainbow tables. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *10*(4), 930-944.

[19] Gudivaka, B. R., Izang, A., Muraina, I. O., & Gudivaka, R. L. (2024). The Revolutionizing Cloud Security and Robotics: Privacy-Preserved API Control Using ASLL-LSTM and HAL-LSTM Models with Sixth Sense Technology: Cloud Security and Robotics. *International Journal of Advanced Research in Information Technology and Management Science*, *1*(01), 100-109.

[20] Kumar, S., Bharti, A. K., & Amin, R. (2021). Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. *Security and Privacy*, *4*(5), e162.

[21] Chen, Z., Gu, J., & Yan, H. (2023). HAE: A hybrid cryptographic algorithm for blockchain medical scenario applications. *Applied Sciences*, *13*(22), 12163.

[22] Alserhani, F. M. (2024). Integrating deep learning and metaheuristics algorithms for blockchain-based reassurance data management in the detection of malicious IoT nodes. *Peer-to-Peer Networking and Applications*, *17*(6), 3856-3882.

[23] Kodadi, S., Deevi, D. P., Allur, N. S., Dondapati, K., & Chetlapalli, H. (2024). AI-driven unified channel management in cognitive radio IoT networks: Integration of OFDM, SDN, MRC, RIS, and cloud computing. *Journal of IoT in Social, Mobile, Analytics, and Cloud*, *6*(4), 395-412.

[24] Najm, H., Hassan, R., & Hoomod, H. K. (2021). Data authentication for web of things (WoT) by using modified secure hash algorithm-3 (SHA-3) and Salsa20 algorithm. *Turkish Journal of Computer and Mathematics Education*, *12*(10), 2541-2551.

[25] Sharma, D. M., Shandilya, S. K., & Satapathy, S. C. (2023). Maximizing blockchain security: Merkle tree hash values generated through advanced vectorized elliptic curve cryptography mechanisms. *Concurrency and Computation: Practice and Experience*, *35*(23), e7829.

[26] Ayyadurai, R., Parthasarathy, K., Panga, N. K. R., Bobba, J., & Padmavathy, R. (2024). A multilevel analysis of corporate tax compliance: The moderating roles of governance managerial gender and multilevel predictive modelling with AI. *International Journal of Research in Commerce and Management Studies, 6*(5), 403-423.

[27] Mahida, A. (2024). Secure data outsourcing techniques for cloud storage. *International Journal of Science and Research (IJSR)*, *13*(4), 181-184.

[28] Sevin, A., & Osman Mohammed, A. A. (2024). Comparative Study of Blockchain Hashing Algorithms with a Proposal for HashLEA. *Applied Sciences*, *14*(24), 11967.

[29] Saredyy, M. R, & Pushpakumar, R. (2024). Integrating AI and deep neural networks to explore organizational culture's role in enhancing employee performance and loyalty in human resource management. *ISIR Journal of Business and Management Studies (ISIRJBMS)*, *1*(2), 8-16.

[30] El-Attar, N. E., El-Morshedy, D. S., & Awad, W. A. (2021). A new hybrid automated security framework to cloud storage system. *Cryptography*, *5*(4), 37.

[31] Shrivastava, P., Alam, B., & Alam, M. (2024). An anonymous authentication with blockchain assisted ring-based homomorphic encryption for enhancing security in cloud computing. *Cluster Computing*, *27*(10), 13675-13691.

[32] Narla, S. (2024). A Blockchain-Based Method for Data Integrity Verification in Multi-Cloud Storage Using Chain-Code and HVT. *International Journal of Modern Electronics and Communication Engineering (IJMECE)*, *12*(1), 1216-1237.

[33] Rawal, B. S., Aleti, S. N., & Reddy, S. (2022). Optimization of SHA 256 with finetune pipeline and parallel processing with split techniques. *Mathematical Statistician and Engineering Applications*, *71*(3s), 460-472.

[34] Doan, T. V., Psaras, Y., Ott, J., & Bajpai, V. (2022). Toward decentralized cloud storage with IPFS: opportunities, challenges, and future considerations. *IEEE Internet Computing*, *26*(6), 7-15.

[35] Gangadharaiah, S., & Shrinivasacharya, P. (2024). Secure and efficient public auditing system of user data using hybrid AES-ECC crypto system with Merkle hash tree in blockchain. *Multimedia Tools and Applications*, *83*(29), 72301-72320.

[36] Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S., Vasamsetty, C., & Padmavathy, R. (2024). Context-aware decision making and real-time feature extraction for adaptive healthcare and environmental systems. *History of Medicine Studies, 20*(1), 1-10.

[37] Narayanan, U., Paul, V., & Joseph, S. (2022). Decentralized blockchain based authentication for secure data sharing in Cloud-IoT: DeBlock-Sec. *Journal of Ambient Intelligence and Humanized Computing*, *13*(2), 769-787.

[38] Sharma, K., Agrawal, A., Pandey, D., Khan, R. A., & Dinkar, S. K. (2022). RSA based encryption approach for preserving confidentiality of big data. *Journal of King Saud University-Computer and Information Sciences*, *34*(5), 2088-2097.

[39] Radhakrishnan, P., Ganesan, S., Musam, V. S., Musham, N. K., & Kurunthachalam, A. (2024). Testing hypotheses in IoT business intelligence: Leveraging big data analytics and advanced techniques. *International Journal of Information Technology & Computer Engineering, 12*(4), 226-242.

[40] Ugochukwu, N. A., Goyal, S. B., Rajawat, A. S., Islam, S. M., He, J., & Aslam, M. (2022). An innovative blockchain-based secured logistics management architecture: utilizing an RSA asymmetric encryption method. *Mathematics*, *10*(24), 4670.

[41] Pulakhandam, W., Vallu, V. R., Chaluvadi, A., & Hemnath, R. (2022). Securing healthcare data with AES encryption and cloud storage: A CNN approach for heart disease classification in Google Cloud. *International Journal of Research and Analysis in Science and Engineering*, *2*(3), 35-50.

[42] Eddy, T. T. M., Georges, B. B., Salomon, N. E. P., & Boniface, E. M. V. (2024). Birth Certificates Delivery, Traceability and Authentication Using Blockchain Technology. *International Journal of Advanced Computer Science and Applications*, *15*(9), 555-568.

[43] Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., & Kumar, N. (2022). Blockchain-enabled cybersecurity efficient IIOHT cyber-physical system for medical applications. *IEEE Transactions on Network Science and Engineering*, *10*(5), 2466-2479.

[44] Ubagaram, C., Dyavani, N. R., Jayaprakasam, B. S., Mandala, R. R., Garikipati, V., & Kumar, V. (2023). Ethical hacking and penetration testing: Strengthening cyber defense with AI-driven breach and attack simulation. *International Journal of Information Technology & Computer Engineering*, *11*(1), 230-236.

[45] Ghayvat, H., Pandya, S., Bhattacharya, P., Zuhair, M., Rashid, M., Hakak, S., & Dev, K. (2021). CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications. *IEEE Journal of Biomedical and Health Informatics*, *26*(5), 1937-1948.