I. J. Computer Network and Information Security, **2025, 3, 35-53**
Published Online on June 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2025.03.03

Sturdy Blockchain Combined with E-apps Repositories Based on Reliable Camouflaging and Integrating Mechanisms

Rasha Hallem Razzaq
Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq
E-mail: rashahalim.comp@utq.edu.iq
ORCID iD: https://orcid.org/0009-0001-2064-4503

Duaa Hammoud Tahayur
Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq
E-mail: duaahammoud.comp@utq.edu.iq
ORCID iD: https://orcid.org/0009-0006-4438-1994

Wid Alaa Jebbar
Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq
E-mail: widalaa.23co4@utq.edu.iq
ORCID iD: https://orcid.org/0009-0007-6080-3656

Mishall Al-Zubaidie*
Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq
E-mail: mishall_zubaidie@utq.edu.iq
ORCID iD: https://orcid.org/0000-0002-3149-9129
*Corresponding author

Received: 22 June 2024; Revised: 14 February 2024; Accepted: 01 April 2025; Published: 08 June 2025

Abstract: The development of technology around us is going through a rapid and significant state that is almost causing a technological revolution, so one of the most important problems facing us in the current technological era is the management of warehouse data and the growth occurring in the volume of data that is dealt with on a daily basis, whether in terms of its storage or security, especially if the data is huge and large. Therefore, we developed a proposed model in our study that provides security in addition to storage/warehouse management. In our proposed model, the El-Gamal and GLUON functions address the security problem. In addition to supporting other security methods, such as GLUON, which is secure and fast, for encryption. Hybrid Blockchain technology is used in our proposed model to deal with the storage of this type of huge data, and also for the purpose of organizing warehouse storage. Data is exposed to intrusion or loss when using any traditional, centralized technology or when storing it in databases, so we chose the hybrid Blockchain to be an integrated fit with our proposed model, and also because it allows the distribution of data across public and private domains. Our proposed model, upon examination, shows that it effectively dealt with defending against attacks such as NotPetya, GoldenEye, WannaCry, Emotet, Trickbot, Conti, and DarkSide. In addition, the results of lightweight GLUON and El-Gamal showed that the performance analysis of our model was very successful, where the time it takes to create a block was between 0.01 ns and not more than 0.09 ns which is considered too fast for such a system that deals with a big data. As a result, we were able to gain an effective model for data repository control, security, performance, and management.

Index Terms: CSPRNG, El-Gamal Algorithm, GLUON, Hybrid Blockchain, Repository Information Security.

1. Introduction

Blockchain technology enhances the quality of any system via evolution. This is achieved through interoperability, security, reliability, and privacy [1]. Fundamental to Blockchain is the concept that a large network of interconnected

computers serve as a digital record keeper, or what is known as a ledger, securely storing transactions in an immutable and unhackable manner, instead of a single person or institution. Blockchain technology's decentralized, immutable ledger securely stores any kind of data, including big medical and financial institution data, and protects it from assaults that can compromise its integrity [2,3]. The data in the ledger cannot be changed since it is safeguarded against cryptographic features including hashing, digital signatures, and asymmetric keys. Because the ledger is decentralized, every member of the Blockchain will be notified of any minor changes made to the data transaction, which further increases system transparency. Fig. 1 illustrates Blockchain technology and its use in electronic applications such as e-banking, e-health, e-agriculture, etc.

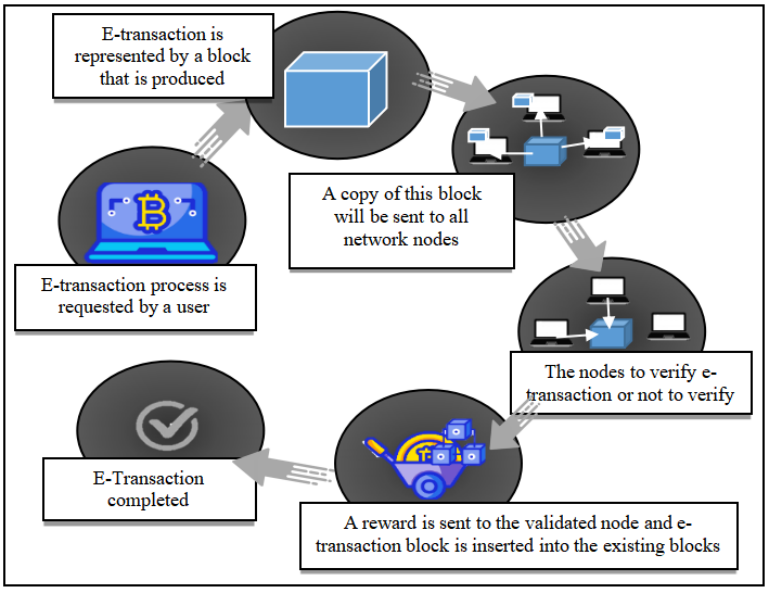

Fig.1. Blockchain workflow

Blockchain technology has several disadvantages that should be considered despite all of its advantages [4-6]. A number of its shortcomings and challenges are as follows:

- Complexity challenges: The complexity and difficulty of understanding Blockchain technology can pose a challenge to its widespread acceptance and utilization.
- Immutability challenges: Although Blockchain's immutability is frequently cited as a positive, it may also be a drawback. It can be challenging to fix bugs or flaws in the code, and since the Blockchain is immutable, intentional alterations or errors may be irrevocable.
- Scalability challenges: Because each block in a Blockchain is limited in size and it takes time for the network to analyze and validate new blocks, Blockchains may find it difficult to manage high transaction volumes. Network congestion and sluggish transaction times may result from this.
- Privacy challenges: Transparent ledgers, in which every transaction is open to the public, are a common feature of Blockchain networks. The potential exposure of users' financial activity may give rise to privacy issues.
- Regulatory Uncertainty Challenges: Regulating Blockchain technology and cryptocurrencies varies greatly throughout states, which may be confusing for consumers and developers and provide compliance issues.
- Wallet vulnerabilities challenge: Blockchain wallets, which are used to manage and store digital assets, are susceptible to theft, hacking, and loss, which might result in money loss.

The future belongs to Blockchain technology, no doubt about it. On the other hand, its drawbacks must also be taken into consideration [6]. In the present day, there is a noticeable growth in the amount of data that is easily accessible; this data is known as "Big Data" or "Big Information." As the amount of data increases, several challenges and problems need to be resolved. Security and privacy are two of the biggest problems in using big data [5]. Confidentiality and preventing unauthorized access are essential when working with sensitive data, such as financial, agricultural, medical, and other information [6,7]. Big data has issues with integrated data management and smooth interaction with existing systems in addition to privacy and security concerns. These problems may be successfully solved by Blockchain technology by providing access integration gateways with existing systems, such electronic apps. Healthcare systems, for example, handle a wide range of big data formats, such as patient records, electronic devices for tracking remotely, and data that can be exchanged between clinicians in the system [8]. For this reason, it is considered necessary to get and create a complete plan that provides monitoring, data management, and protection. A comprehensive solution that efficiently manages storage and guarantees security may be achieved through the combination of Blockchain access-based systems, hash functions, and cryptographic algorithms [9-11]. Blockchain

technology, on the other hand, is a developing technique that provides security and authority to the systems. Blockchain technology may secure data and prevent hacking or manipulation, so successfully combines compliance, privacy, and security. This calls for concentrating efforts on developing Blockchain-based protocols and standards and advancing them via collaboration between organizations and interested parties. Because of this continued attention and successful emphasis, Blockchain technology may be used to protect large amounts of data and gain significant benefits in a variety of areas, including banking, commerce, and health [12].

The term "ransomware" refers to computer assaults that encrypt data and systems, making it impossible for users to access them. The attackers then demand a ransom to decrypt the data and release the users [13,14]. Ransomware attacks have become more common over the past few years, presenting a major risk to people, businesses, and organizations worldwide. These risks include the possibility of losing private data, disruptions to services or systems, detrimental effects on important company functions and output, large monetary losses, and dangers to privacy and information security [15]. The risks and dangers presented by recent ransomware attacks on systems and networks are discussed in "Risks of recent ransomware attacks". When computer systems and networks are compromised, files are encrypted, and the attacker demands a ransom—usually in the form of a cryptocurrency like Bitcoin—to unlock and recover the contents, this type of cyberattack is known as 'Ransomware' [16-18]. Because these attacks have the ability to cause systems to collapse, lose data, and result in significant financial losses, they are regarded as some of the most severe and serious threats that individuals and corporations face in the world of technology [11]. Ransomware attacks include a variety of hazards, such as the loss of confidential data, compromises of systems and services [19,20], compromises of security and privacy, and detrimental effects on the finances and reputation of the enterprises that are the target [21]. Numerous individuals, businesses, and organizations have fallen victim to this kind of assault. Recent ransomware outbreaks bring up several difficulties.

1.1. Importance of Our Research and Problem Statement

The security issue of generating, transmitting, and storing big data in electronic applications has become very important because the larger the data, the more it can affect the performance of security mechanisms. Therefore, when designing any model, lightweight and secure algorithms must be selected. When we discuss managing large amounts of data, we are discussing the security of repository storage. As long as this data is accessible online, it is vulnerable to theft and intrusions. Our work is important because it addresses the challenge of managing and securing the enormous volumes of data generated by e-apps such as e-banking, e-health, e-agriculture, etc. Additionally, Blockchain, big data, and severe ransomware assaults may happen as long as data is created at an increasing rate and enormous data are kept in conventional methods that have dangers and obstacles. By exposing these shortcomings and difficulties, people and organizations may become aware of possible issues and create plans and solutions to deal with them. By being aware of potential constraints, such as repository storage capacity, scalability, mining issues, and the inability to change input data, it is possible to create Blockchain technology and help it overcome its obstacles. Comprehending the obstacles related to privacy, security, compliance, and data management in the context of big data may facilitate the creation of efficacious tactics to safeguard confidential data and ensure adherence to relevant legal and regulatory models. We thus suggested this model for controlling repository storage in addition to security in order to handle these sorts of data. Understanding the challenges associated with privacy, security, compliance, and data management in the context of big data may help develop effective strategies to protect sensitive information and guarantee compliance with applicable legal and regulatory requirements. To manage various sorts of data, we thus proposed this method for managing repository storage in addition to security.

1.2. Our Contributions

- Design a model for handling the security and storage of repositories. The study model incorporates security and administration of big data storage. The security aspect of the strategy is supported by El-Gamal public-key encryption techniques, GLUON hash functions, and CSPRNG random number generators.
- The administration and security of massive data storage are integrated into the study model by using a hybrid Blockchain. Lightweight El-Gamal, GLUON, and CSPRNG techniques with hybrid Blockchain support the proposed model's security and performance.
- In order to counter and handle possible security threats such as NotPetya, GoldenEye, WannaCry, Emotet, Trickbot, Conti, and DarkSide, the suggested model was examined. We will provide analyses and discussions to demonstrate the acceptability of the proposed model.

2. Related Works

This section will analyze earlier research, including what it showed and the benefits and drawbacks of the methodology used.

Faheem Ahmed Reegu et al. [1] integrated Blockchain technology into electronic health record (EHR) systems in compliance with international and national EHR standards. They suggested that a Blockchain-based system might resolve the problems facing EHR today. It makes it possible for healthcare professionals to manage, control, share, and preserve patient information. They discussed the challenges of integrating EHRs and suggested using Blockchain to

manage records, preserve patient information, and uphold privacy and confidentiality. According to the study, there may be a Blockchain-based model that can help with the problems that exist with present EHR systems. Better comprehension of the present issues and assistance with the correct incorporation of Blockchain technology into EHR. However, they did not use lightweight mechanisms to balance the performance costs when implementing Blockchain technology. Muhammad Kamrul Hassan et al. [2] gave a thorough analysis of Blockchain applications for smart grid safety and energy privacy. To evaluate review topics, gather data, and conduct data analysis, a systematic review process was adhered to. They outlined the main security concerns that big data and the use of Blockchain can assist in resolving for smart grid scenarios. They list and analyze a number of current Blockchain-based research projects as well as their security worries with smart grid implementations. They also discussed cutting-edge research, experiments, and solutions that address security issues with smart grids by utilizing Blockchain technology. Nonetheless, they did not provide threat models in their review to illustrate the severity of attacks on the Blockchain.

Amikumar V. Jha et al. [3] proposed to use of Smart Grid 3.0 synchronous phase communication to improve the security and confidentiality of synchronous phase data. Using the strengths of distributed, decentralized, and hierarchical PDC design, an architecture for a Blockchain-based synchronous communications network is built. Creating a peer-to-peer network of asynchronous communication systems using Blockchain technology. This attempts to solve the cyberattack vulnerabilities found in the traditional TCP/IP based communications network. Synchronous phase data in a smart grid can be made more secure and reliable with the help of the proposed Blockchain-based architecture. The distributed and decentralized architecture of a Blockchain network can enhance the reliability and adaptability of synchronous communication systems. A viable strategy for using Blockchain technology to increase the security and reliability of synchronous phase interactions in smart grid 3.0 is proposed. Nevertheless, their proposal did not focus on managing and securing big data when using Blockchain in electronic applications.

Asif Ali Laghari et al. [4] provided a modular architecture enabled by Blockchain technology for secure and reliable implementation and delivery of services. They acknowledge irreversible and secure ledger storage as well as on-chain and off-chain peer-to-peer (P2P) networks and vehicle-related communications. To facilitate interactions for industrial nodes, the researchers created a data format that is enabled by smart nodes. They mimic the process of transferring data and related information between devices connected to the Internet of Vehicles (IoV). The generation and exchange of powerful nodes may be reduced by up to 56.33%, and computing power costs can be reduced by 37.21% using the proposed BIoV design. Only 41.93% of 47.31% of the resources are used, respectively, for network and IoT constraints. However, the researchers did not rely on a robust encryption algorithm that would prevent attackers from exposing the data.

Mubashir Amjad et al. [5] suggested a Blockchain-based infrastructure for safe data exchange in smart grids. Three important concerns are what the platform seeks to address: User control of data, scalability, and privacy. Participants can access programmable data through Blockchain-based smart contract technology, which ensures that all interactions are authorized and documented in a tamper-resistant chain network. By incorporating an ANN, or artificial neural network, to forecast network speed and delay, their suggested Blockchain platform's performance is further enhanced and the network administrator can tweak the settings. They base their data trading system on Blockchain technology, most especially Hyperledger Fabric. A Blockchain platform is combined with ANN to forecast and maximize network performance. The suggested model enhances the efficiency of data exchange and information sharing in smart grids enabled by Blockchain technology. The platform adjusts to smart grid dynamics with ease. The problem with this infrastructure is that the proposal did not adopt a technology to support randomness, whether for the blockchain parameters or the randomness of encryption. Wu Guangfu et al. [6] created a more comprehensive and accurate risk assessment system that takes into account variables such as reputation and contribution. They proposed a distributed starting node based on a collective hash loop for method selection to reduce single-point failures and improve resilience. To reduce overhead, a deferred view adjustment method is added, which dynamically adjusts the exact moment of view shifts based on the system workload and node state. By adding quota evaluation and better consistent hashing, the Practical Byzantine Failure Tolerance (PBFT) consensus method has been improved. Comparing the proposed method with conventional PBFT, notable gains in system safety and effectiveness were observed. The results show that this technology can be widely used to create more reliable Blockchain systems. However, the researchers did not provide an analytical comparison that illustrates the advantage of the selected Blockchain hash, which is important for security and performance.

Clivent Gerhard Sondakh et al. [7] proposed using the SHA256 hash method to create a data layer on a distributed ledger network. The goal was to improve information security, integrity, and authenticity within the Blockchain network. Setting up the data layer using SHA256 was studied in the study. Include all stages of preparation, evaluation, system development, implementation, evaluation, deployment, and maintenance. They investigated how to integrate a Blockchain data structure for the SHA256 hash algorithm. Through quantifiable gains in security metrics, the researchers demonstrated how well SHA256 provides inaccessible information retention and retrieval. The study examined potential developments in Blockchain technology and their practical implications, which could be facilitated by increasing the security and durability of the SHA256 data layer. However, there is a strong trend towards choosing algorithms other than SHA-256 to balance security and performance, especially in applications that use big data. Louis Frank et al. [8] suggested a fresh method for encrypting Internet of Things devices that rely on trigonometry. Their suggested method provided effective and safe encryption for IoT applications by utilizing the mathematical features of functions that are trigonometric. They created a hardware version of a trigonometry-based encryption system using

specialized cryptographic equipment accelerators, like FPGAs or ASICs, for IoT devices. The electronic architecture employed key generation and administration, encryption/decryption sections, power-saving techniques, and specific components to compute trigonometric functions efficiently. They computed trigonometric functions with minimal processing cost by using techniques like CORDIC. Using exemplary IoT devices, the hardware execution of the trigonometry-based encoding scheme was assessed. The outcomes showed that it was both feasible and successful, suggesting that it may be used for safe and effective encryption in IoT situations with limited resources. However, their scheme is not equipped to repel modern ransomware attacks.

3. An Overview of Security Technologies and Blockchain

This section provides brief overviews of the techniques used in the proposed model.

3.1. Technology of Blockchain

A decentralized network called Blockchain is intended to store and protect data. It works by constructing a sequence of blocks, each of which incorporates information about previous blocks using mathematical hashing algorithms. Blockchain is resistant to manipulation and assault since it is distributed among several network-connected devices [22]. A higher degree of safety is provided to highly secure systems with numerous interconnected nodes by Blockchain technology. Peer-to-peer process execution removes the need for intermediaries, which speeds up these systems. A database made up of connected chains of blocks is called a Blockchain. Numerous important characteristics of this technology, including decentralization, security, and transparency, make it noteworthy. Blockchain data is stored indefinitely, protected by cryptography, and available to the public with difficult modifications. It employs a SHA256 hash by default to prevent block data tampering [23]. Blockchain technology is widely used in electronic projects and applications, including supply chains, finance, document management, healthcare, and agriculture. Data integrity is ensured by the retention of records in the absence of a trustworthy central authority to supervise or verify the data [18]. Networked devices face challenges from standardised test methodologies and unreliable test libraries. Blockchain-based test repositories need thorough investigation and analysis, and "proof of verification" has to be used to guarantee repository management and achieve privacy, decentralization, and transparency in the sharing and keeping of digital data. Blockchain is used to protect access to encrypted data and store distributed data [9,24].

Blockchain technology has drawn a lot of attention from the business and research community for the following reasons:

- Transparency and Auditability: Blockchain technology makes transaction records transparent and auditable. Every member of the network has access to the same data, and once a transaction is entered into the Blockchain, it stays there forever. Participants' trust is increased by this openness and auditability, which also helps to expedite procedures that call for auditing and verification.
- Independent Storage: Blockchain technology makes it simple to store and transfer data to other parties with the consent of the sender. Keeping several copies of this data in various fields is one of the most feasible ways to ventilate data hoarding.
- Traceability and Supply Chain Management: Supply chain end-to-end traceability of products and things is made possible by Blockchain technology. Businesses may confirm the provenance, legitimacy, and state of goods by logging each transaction and movement on the Blockchain. This tracking can guarantee regulatory compliance, deter fraud, and stop counterfeiting.
- Permission: computations manage the entry, storing, and Changes to the information are allowed if everyone involved in the business agrees [1].
- Tokenization and Digital Assets: Tokenization and the creation of digital assets have been made possible by Blockchain technology. Tokens can stand in for a variety of assets, including fractional ownership of tangible items, real estate, cryptocurrency, and intellectual property. Tokenization creates new opportunities for asset management, investment, and liquidity by facilitating the efficient transfer and fractional ownership of assets.
- Financial Inclusion: Blockchain technology has promise in enabling underbanked and unbanked communities in developing nations to access financial services. Decentralized financial systems and Blockchain-based digital identities enable those without access to traditional banking services to safely store and move money, apply for loans, and engage in the global economy.

3.2. Big Data

Big data is the term used to describe data amounts and types that are too large and complex for traditional data sources. Big data is defined by three main features: volume, velocity, and diversity [2]. The chapter begins by describing the vast quantity of data that is produced and collected from a variety of sources, such as social networks, mobile phones, detectors, hospitals, companies, and other sources that add to this data. The speed at which data is generated and transferred is the second definition of speed. A multitude of sources, including social networks with Internet access, smart gadgets, and sensor data flow, provide massive and continuous volumes of data. As long as plain text data is not the only kind of data that has to be managed, handling data in terms of storage management and system

security support is essential. Images, audio files, and video files are examples of additional data kinds. Big data utilization improves comprehension of occurrences and boosts decision-making effectiveness in a range of industries, including marketing, business, research, medicine, and agriculture [14]. Using specialist techniques and tools, this massive data set may be leveraged to uncover many interesting trends, patterns, and correlations that are obscured by conventional study. Cloud computing refers to the public cloud environment where data is stored on cloud servers via an open network channel. Information that is too large and complicated for conventional technologies to evaluate and manage is sent via this cloud. Large volumes of data must be saved, accessed, and evaluated using certain technology and techniques. "Big data" refers to the vast array of information included in computer systems, including text, photos, music, videos, geographic data, and more. E-apps use a variety of data sources, including social networks, mobile devices, smart applications, detectors, and more, to produce enormous amounts of data rapidly [18,19]. To save, access, and evaluate this data in an appropriate manner, specific tools and methods are needed. Links, patterns, and trends in data that would be hard to identify using conventional analytic models may now be extracted thanks to big data. Moreover, big data has several applications in the electronics industry, including enhancing application performance, user experience, marketing tactics, and intelligent decision-making [4]. Using Blockchain with big data supports the following benefits in any electronic application.

- Blockchain Analysis: Blockchain technology uses a large amount of data that is kept in immutable records. Analyzing this data and extracting valuable insights from it, such as transaction trends and identifying security threats, is made possible by big data.
- Improving operational efficiency: By leveraging big data analytics, Blockchain-based companies can reduce operating costs and improve processing and storage operations.
- Demand forecasting: Companies can use big data-based forecasting methods to assess demand for Blockchain services, which helps in more accurate planning and pricing.
- Rapid detection and confirmation: Big data analysis enables more accurate and timely identification to prevent fraudulent attempts on Blockchain technology.
- Enhancements in Security and Privacy: More sophisticated analysis of large amounts of data can aid in the creation of Blockchain security and privacy protocols that are more efficient.

3.3. Hash Algorithms

A hashing function can handle any type of electronic data, regardless of size; it is essentially a specific formula that divides the data into smaller, fixed-size pieces called hashes [25]. A hash function may be given any kind of digital data, including text, numbers, images, and even videos. The input will next go through a hashing process, in which the function applies a mathematical transformation to the inputted data. The result is a fixed-length string of letters that functions as the compressed form of the original matrilateral and as a unique hash value [26,27]. Like every other method, the hash function has benefits and drawbacks of its own. A synopsis of the two most popular hashing algorithms can be found here.

A. SHA-256

SHA-256, also known as Protect Hash Algorithm 256-bit, is a cryptographic hash function that belongs to the SHA-2 family of hash algorithms. With any length of input message, it produces a fixed-size 256-bit (32-byte) hash method. The SHA-256 algorithm is widely used in many cryptographic applications, including digital signatures, password hashing, and information integrity verification [7]. A padding is applied to the input message length such that it contains 512 bits. The padding ensures that the message's length is predictable and that it may be processed in fixed-size blocks. SHA-256 uses eight initial hash values, which are expressed as 32-bit words (h0 to h7). These values are computed using the first 32 bits of the fractional portions of the square root of the first eight prime integers. The padded text is processed across several rounds, with each of its 512-bit chunks [25]. As the message is processed one block at a time, the hash value is updated after each block. Each 512-bit block is subjected to 64 rounds of operations, which include bit-shifting, modular addition, and bitwise logical operations such as AND, OR, XOR, and NOT. These operations combine the current hash value and the input block to provide an updated hash value. Once every block has been examined, the final hash value may be obtained by concatenating all 32-bit words in the current hash value. The hash generated is a 256-bit value that reflects the input message. It is not possible to compute the actual contents of a message from its hash value since the SHA-256 method is designed to be a one-way function. For greater accuracy, the following are the ways in which SHA-256 is crucial to Blockchain technology:

- Create digital fingerprints: Any digital data, including transactions, blocks, and other data, is transformed into a unique 256-bit hash value using the SHA-256 algorithm. By employing this hash value—which functions as a unique digital signature of the source data—it is then possible to verify the data's integrity.
- Chained blocks: An individual block in a distributed ledger contains both its own data and the hashing algorithm (SHA-256) of the transaction that came before it. Modifying one block's contents will modify the hash value of all sections that precede it because of the ordered linking technique that employs hash values.
- Proof of work (PoW): In certain Blockchain systems, like Bitcoin, SHA-256 hashing is required to determine a precise hash value before a new block may be added to the chain. PoW is a costly computational procedure

that secures the Blockchain against attacks and guarantees its dependability.

- Digital signatures: The Blockchain employs SHA-256 to sign online transactions and confirm their legitimacy. SHA-256 digital signatures confirm the sender's identity and guarantee the integrity of transactions.
- Safety and dependability: SHA-256 contributes to the Blockchain's security and dependability because of its robust security features, which include computational difficulty and uniqueness. It is very difficult to submit bogus data or alter transaction history because of these qualities.

B. GLUON

The GLUON hash function, designed by Daniel J. Bernstein, follows the sponge construction model, which involves absorbing input data, applying a permutation function to the internal state, and then squeezing out the hash value from the internal state. The GLUON hash function is parameterized by two integers: *r* and *c*. These parameters define the internal state size and the rate at which data is absorbed into the state.

The internal state consists of *r+c* bytes, divided into *r* bytes of the capacity and *c* bytes of the rate. This state is initialized to a fixed value. During the absorbing phase, the input message is absorbed into the internal state. The input message is divided into blocks of size *c* bytes each. For each block: XOR the block with the rate portion of the internal state. Apply a permutation function to the internal state, which mixes the input block with the current state. After absorbing the entire input message, the squeezing phase begins [28]. During this phase, the hash value is extracted from the internal state. This can be done by reading *c* bytes from the rate portion of the state at a time and repeating the permutation function to generate more hash output as needed. Like many hash functions, GLUON requires padding to ensure that messages of different lengths produce different hash values. This typically involves appending a bit string to the message to indicate the message length and ensure it's a multiple of the block size. The permutation function operates on the entire internal state and is responsible for mixing the state in a way that ensures cryptographic security. It typically involves a combination of bitwise operations, modular arithmetic, and other cryptographic operations. The GLUON hash function is designed to be highly secure and efficient, with a focus on simplicity and speed. It follows the sponge construction model, which means it absorbs input data in blocks, applies a permutation function to the internal state, and then squeezes out the hash value from the internal state when necessary [29]. One of the notable features of the GLUON hash function is its high performance on modern computer architectures, making it suitable for various applications where both security and speed are important factors. A thorough comparison of the SHA256 and GLUON algorithms is given in Table 1. In addition, Table 2 describes comparison between GLUON and existing hash functions [30].

Table 1. Comparison between SHA256 and the GLUON

Characteristic	SHA256	GLUON
Lightweight	It is a more general-purpose hash function.	It is designed to be more lightweight and efficient, particularly for resource-constrained environments.
Scalability	SHA-256 is a well-established, dependable algorithm that has undergone extensive testing and use.	It might be easier to scale in the years to come if it is developed and accepted in more applications.
Attack Resistance	Less resistance	It is designed to be resistant to various attacks, which are a type of attack that exploits information leakage from the physical implementation of a cryptographic system such as those involving sensitive data or critical infrastructure, where side-channel attacks are a concern.
Cryptanalysis Advancements	Less opportunities for advancements	There may be more opportunities for advancements in the cryptanalysis of GLUON, potentially leading to improved security or performance in the future.
Sponge Construction	Less efficient implementation	The sponge construction used in GLUON allows for efficient implementation and can provide additional security properties, such as resistance to length-extension attacks.
Low Power Consumption	Less energy-efficient	The efficient design of GLUON allows it to have lower power consumption compared to SHA256, making it more energy-efficient, especially in battery-powered devices.
Lower Computational Complexity	Its operations are more complex	The design of GLUON aims to minimize computational complexity, making it more efficient to perform hashing operations.

3.4. El-Gamal Encryption

The Diffie-Hellman key exchange protocol serves as the foundation for the public-key cryptography system known as the El-Gamal algorithm. Taher Elgamal created it back in 1984. The Discrete Logarithm Problem (DLP), which is thought to be difficult to solve computationally, provides the foundation for the security of the El-Gamal method. According to the DLP, it is computationally impossible to obtain the private key x given a prime integer p, a generator g of the multiplicative group modulo *p*, and a public key $y = g^x \bmod p$ [24]. The El-Gamal algorithm includes a number of characteristics and applications, including key exchange, encryption, digital signatures, and homomorphic features. Numerous applications, such as digital signatures, cryptographic protocols, and secure communication, have made extensive use of the El-Gamal algorithm. To maintain system security, it is necessary to carefully control the random

number generation and key creation processes. The encryption algorithm can accomplish the following:

Key Generation:

- Choose a large prime number p and a generator g of the multiplicative group modulo p.
- Select a random private key x from the range [1, p-1].
- Compute the public key y = g^x mod p.

Encryption process:

- To encrypt a message m, the sender:
- Chooses a random number k from the range [1, p-1].
- Computes the ciphertext as c1 = g^k mod p and c2 = m * y^k mod p.
- The ciphertext is the pair (c1, c2).

Decryption Process:

- To decrypt the ciphertext (c1, c2), the receiver:
- Computes s = c1^x mod p.
- Recovers the message as m = c2 / s mod p.

Table 2. Comparison between hash functions and the GLUON

Hash function	*n*	*c*	*r*	Preimage	Collision	Second preimage	Process, µm	Area (GE)	Cycles
Hash-One	160	160	1	160	80	80	0.18	1006	324/162
Hash-One	160	160	1	160	80	80	0.18	2130	14/7
SPONGENT	176	160	16	144	80	80	0.13	1329	3960
SPONGENT	176	160	16	144	80	80	0.13	2190	90
D-QUARK	176	160	16	160	80	80	0.18	1702	704
D-QUARK	176	160	16	160	80	80	0.18	2819	88
PHOTON	160	160	36	124	80	80	0.18	1396	1332
PHOTON	160	160	36	124	80	80	0.18	2117	180
GLUON	160	160	16	160	80	80	0.18	2799	50

3.5. CSPRNG Algorithm

A crucial component of cryptography and computer security is a Cryptographically Secure Pseudo-Random Numbers Generator, or CSPRNG. Its goal is to generate random numbers suitable for use in cryptography methods that demand a high level of statistical unpredictability and randomness. A CSPRNG algorithm's overall functionality may be summed up as follows:

- To start the CSPRNG, a seed value is chosen. Several sources, including encrypted copies of unexpected data, user-provided input, and randomness from the system (e.g., mouse movements, keyboard scheduling, disk events), can be used to construct this seed.
- The seed value is used to initialize the internal state of the CSPRNG algorithm.
- The underlying setting of the CSPRNG results in a stream of non-random numbers. If one were to look at these statistics without knowing about the internal condition, they would appear arbitrary and unpredictable.
- CSPRNG algorithms regularly reseed either on a regular basis or in reaction to specific events, in order to avoid the produced sequence from being duplicated.
- Certain cryptographic characteristics, such statistical randomness, resistance to prediction, unpredictability, and resilience to cryptographic attacks, are required of a CSPRNG.

Typical CSPRNG algorithms consist of: Fortuna is a robust and highly secure CSPRNG. Yarrow: Developed by the late Bruce Schneier and others, it also strives for robust security and unpredictability. AES-CTR_DRBG: Based on the usage of AES encryption in counters mode, this well-liked and efficient encryption technique. Daniel J. Bernstein's stream cipher ChaCha20 is widely used as the core of CSPRNGs due to its speed and security [26]. Building cryptographic systems requires using pre-established CSPRNG algorithms from trustworthy cryptographic libraries since creating a secure CSPRNG is challenging and prone to mistake. Regular security audits and upgrades are also necessary to preserve the integrity of digital signature systems [27]. The primary role of CSPRNG in Blockchain is the creation of safe encryption keys and digital signatures.

- CSPRNG is used in the block generation process to generate the block ID and an odd number that links the previous block to the current block, ensuring the chain's integrity.
- CSPRNG is used to create the private keys of the sender and receiver during the agreement building procedure.

Transactions may then be safely signed using these keys. Add a new block. In order to generate random values throughout the mining process, PoW models rely on CSPRNG.

The following difficulties arise while implementing CSPRNG in e-apps:

- In order to maintain a high degree of security and unpredictability, premium seed sources are needed.
- The initial seed has to be refreshed frequently to ensure that the numbers generated are unexpected.
- Preserve a balance between security and performance, as frequent restocking may diminish system efficacy.
- CSPRNG has to be connected with the other Blockchain protocol components in order to preserve the overall dependability of the network.

4. A Tried-and-True Methodology to Safe Storage Access

Large amounts of data are produced by enterprise apps, or e-apps, and managing this data effectively can be challenging. Our proposed strategy, which is shown in the following subsections, offers a unique method for handling huge data records and repositories for e-apps. The suggested model's process is displayed in Fig. 2.

4.1. Hybrid Blockchain Utilization

Big data management is made reusable, scalable, and safe with the use of hybrid Blockchains. Hybrid Blockchain and big data are two potent technologies that work well together. Especially for systems that deal with such a sort of data where trust and data integrity are critical, since this form of Blockchain combines the best aspects of both public and private Blockchains. We decided to use this form of Blockchain in the recommended method for the features listed below:

- By combining both permissioned and permissionless capabilities, for example, a hybrid model enables the Blockchain architecture to be customized and adapted to particular requirements.
- By fusing elements of public and private Blockchains, this kind of Blockchain offers strategies and systems with a high level of security.
- Interoperability between various Blockchain networks and between Blockchain and conventional systems can be facilitated by a hybrid Blockchain.
- Because this kind of Blockchain has portions that are public and others that are private, the work on it is divided up, which will speed up the process. This enhances the scalability and speed of e-transactions.
- Only the most crucial data is saved on a hybrid Blockchain; the data that is recorded consists of hashes and symbols rather than the actual data itself. This gives the process implementation technique a high rate of speed. Because only hashes are saved in the hybrid Blockchain and the actual data is stored outside of it, it also offers data integrity and lowers costs.
- A hybrid method can be less expensive than implementing a totally private or fully public Blockchain infrastructure, depending on the use case.

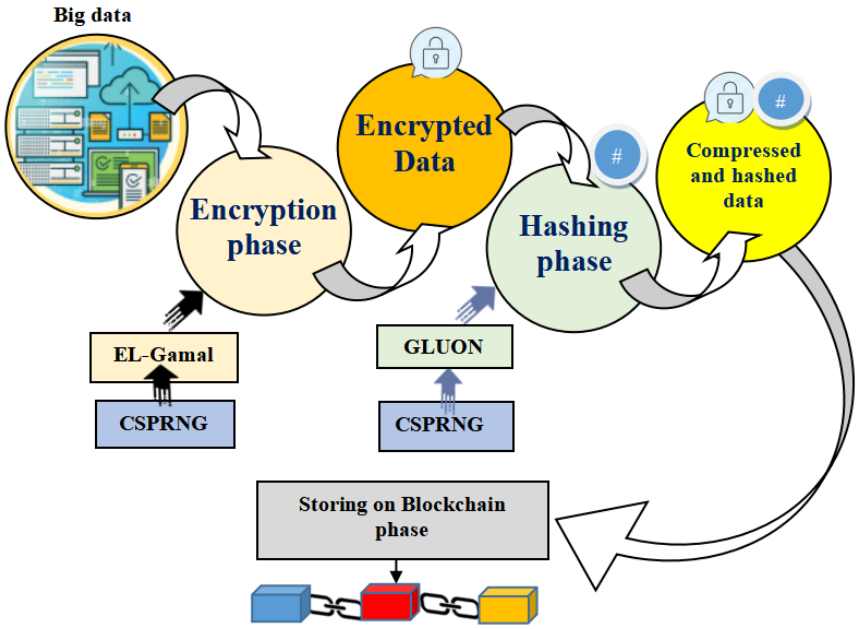

Fig.2. Workflow of the proposed model

4.2. Ensuring Adequate Unpredictability for Blocks

The term "randomness in blocks" refers to the element of uncertainty that is added during the creation of a new block in a Blockchain system. Because block construction is random, malicious actors find it difficult to predict or manipulate the outcome. Cryptographic hash functions may be used to create this unpredictability. They take various inputs, such as timestamps and hashes from earlier blocks, and produce an output that appears random. Then, this output is used in the block creation process. Additionally, depending on a seed value, pseudorandom number generators can accomplish the desired randomization by generating a random series of numbers. A Blockchain's seed might originate from a variety of sources, including system time or validator input. Despite not being entirely random, CSPRNGs can be cryptographically safe when used appropriately. For this reason, in our suggested method, we merged the CSPRNGs with GLUON, a kind of hash function, and the public key encryption represented by the El-Gamal previously described. This gave us a degree of unpredictability that is ideal for our suggested method. In our suggested model, we generate high randomness for the hashed message's condensed form using CSPRNG and GLUON. In order to provide robust encryption of Blockchain blocks, our solution also generates private and public keys with good randomness using CSPRNG with El-Gamal.

4.3. Using Blocks with GLUON

The lightweight Blockchain model is a methodology for installing Blockchain in a lightweight and resource-efficient way, with the goal of improving the functionality and responsiveness of mobile Blockchain and settings with limited resources. This method increases the efficiency of Blockchain data operations and storage by utilizing some updated tools and technology. Secure and protect sensitive data when it comes to large online applications by reliably integrating big data repositories and web application logs. Trusted integrity is used by data records and repositories to safeguard stored data and ensure that it cannot be altered by adversaries. The GLUON algorithm is one of the key components of our method that may be used to provide trustworthy integrity in a lightweight Blockchain solution. With GLUON, data repositories and transaction logs may both be securely maintained on the Blockchain. To maintain data integrity prior to storage, the GLUON hashes can be employed twice (previous hash and current hash) at the level of individual blocks in a chain or at the data repository level. Within the block, mixing, transformation, and deduction operations are used to provide the required integrity. As a result, information is reliably and securely stored on the Blockchain; similar steps are then repeated for each new block. We discovered that the GLUON method offers greater security than the SHA256 algorithm after reviewing current studies. As a result, it was selected as the block data integration algorithm. A Blockchain's block structure may incorporate GLUON hashing as follows:

- A Blockchain's block header is an essential component as it holds data about the block, including the date, the hash of the previous block, and the Merkle root of the transactions in the block. The block header hash in a Blockchain based on GLUON may be calculated using the GLUON hash function, which would result in a reduced hash size than SHA-256.
- In order to produce a Merkle tree structure within each block, the transactions are usually hashed using a cryptographic hash function. The hash of each transaction might be calculated using the GLUON hash function, which could lead to a smaller Merkle tree and perhaps quicker Merkle tree traversal and verification.
- Blockchains frequently keep track of the current state of the network (such as account balances, contract storage, etc.) using a state tree or Merkle Patricia tree. The block header usually contains the root hash of this state trie. It may be possible to lower the amount of storage and transmission needed for this data by utilizing GLUON to compute the state root hash.
- The miners would have to locate a nonce value that, when hashed with the block header using the GLUON function, yields a hash value that satisfies the desired difficulty if the Blockchain employed a PoW consensus method. When compared to SHA-256, the PoW mining process could be quicker and more effective with GLUON's reduced hash size.
- Validators are chosen on a Proof-of-Stake (PoS)-based Blockchain according to the quantity of bitcoin they have staked. The scalability and fairness of the PoS consensus process may be enhanced by using the GLUON hash function to calculate the hash-based weights or random validator selection.
- The lower block header and transaction hashes in a GLUON-based Blockchain would help lightweight or mobile clients since they would need less bandwidth and storage to synchronize and validate the Blockchain.

4.4. Concealing Blocks

In order to encrypt the blocks in the in the lightweight Blockchain, El-Gamal algorithm was employed in the proposed method, in most circumstances, El-Gamal algorithm is not intended to encrypt large amounts of data. However, in the case of our suggested method, we have developed it to accomplish this goal in the following way: we employ CSPRNG to create randomness, which is then used to generate private and public keys using the El-Gamal algorithm for each authorized user on the network. Blocks can be big data records or collections of electronic application records. The block is changed to reflect the correct data format. Depending on the requirements of the algorithm and the internal structure of the lightweight Blockchain, this step may entail using alternate formats or converting the data to bit format. Prior to the data's encryption, our method can employ a public key for block

encryption and a private key for block decryption, depending on the security requirements and internal architecture of the lightweight Blockchain. In contrast to RSA, the cryptographic operations of the El-Gamal algorithm use appropriate rapid encryption algorithms. Additionally, compared to other key methods, the El-Gamal algorithm generates very small keys, which will minimize the amount of storage space needed for these keys. We choose El-Gamal algorithm because it strikes a balance between solid security and performance overhead. Block data cryptography steps are illustrated in Algorithm 1.

Algorithm 1: Encryption process of the blocks

Start

Step 1: Key Generation through randomness generation

- generates El_Gamal keys by utilizing CSPRNG for the randomness (RND):
- P ← RND large prime,
- Q ← RND public key
- H ← RND private key

Step 2: data preparation

- D ← entered data

Step 3: data conversion to bytes

- *DB* ← *D*. encode ('utf-8')

Step 4: Encrypting data:

- *E* ⟵ El-Gamal_ Cipher (*Q*). encrypt (*DB*)

Step 5: Hashing process

- *H* = GLUON_ Hash (). Hash (*E.RND*)

Step 6: Decrypting the data:

- *D* ⟵ El-GamalCipher (*H*). decrypt (E)

Step 7: Authentication of hashing

- *H* = GLUON_Hash (). Hash (*E.RND*)

Step 8: sending data to the repository:

- send("Encrypted data: ", *E*)
- send("Decrypted data: ", *DB*)
- send("Hash value: ", *H*)

End

4.5. Suggested Model Methodology

This section will clarify our proposed paradigm, which is based on the combination of CSPRNG, GLUON hashes, the EL-GAMAL encryption algorithm, and LZ27 in a hybrid Blockchain context. This type of combination ensures the system's confidentiality, integrity, security, privacy, simplicity of data transfer, and proper data management.

Initially, the LZ77 compression data method is used to minimize the size of sent data and save space for storage in the hybrid Blockchain. The data is separated into tiny segments, and the LZ77 method is applied to each one separately. Duplicates in data are identified and expressed via reference statements, reducing the amount of data required in the hybrid Blockchain. Second, El-Gamal cryptography is used to offer confidentiality and safety of the data supplied across the Blockchain. Packed information is encrypted using EL-GAMAL encryption (after adding enough randomness to increase the data's anonymity during the algorithm's application), with private and public keys. The public key is used to conceal data on the Blockchain, and only those with the private key can decrypt it. This allows only authorized users to access the data. Following that, the work of algorithms in the Blockchain ecosystem is coordinated smoothly. The compacted and encrypted data are combined with Blockchain GLUON hash functions to generate a hash set for each block. The Blockchain has been authenticated with the GLUON message digest and PRING to support robust hashes, ensuring that the data has not been edited or altered.

Our suggested architecture protects data stored on hybrid Blockchain technology by ensuring its integrity and confidentiality. Our methodology guarantees excellent efficiency in terms of performance, privacy and security, dependability, ease of data transfer, and secrecy. Data compression decreases storage space and increases access speed, while the EL-GAMAL encryption technique protects data from illegal access. We use Blockchain hash functions and digital hashing to ensure data integrity. In addition, our hybrid Blockchain system facilitates data transfer. Only authorized parties can access the Blockchain, get compressed data, and decrypt it with the private key. This simplifies and improves data retrieval, contributing to the model's effectiveness and overall user experience. Fig 3 depicts the workflow phases for the suggested paradigm.

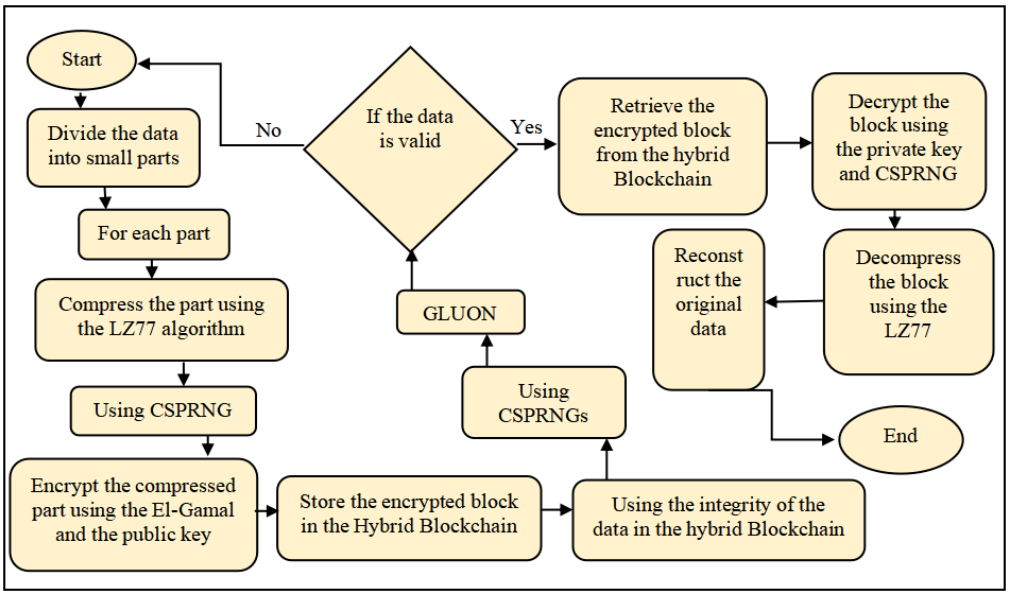

Fig.3. Workflow stages for the suggested model

5. Outcomes and Evaluations

This part will provide the evaluation and assessment of the suggested strategy. The analyses rely on two primary components, which will be explained later: the security analysis and the performance evaluation.

5.1. Outcomes of Performance

We present a thorough performance study of all the algorithms in our proposed model, with implementations of the algorithms shown in Figs. 4-11. The Ubuntu 20 system's Java language formed the basis for the working environment. Its 64-bit architecture, 16 GB of RAM, and Intel (R) Core (TM) i5-2540M CPU @ 2.60 GH clock speed were also noted. To fully assess the suggested model, we execute each of its 50 algorithms 50 times. The El-Gamal technique is implemented in Fig. 4 to assess the encryption and decryption processes. We notice from Fig. 4 that the encryption operations require more time to execute than the decryption operations.

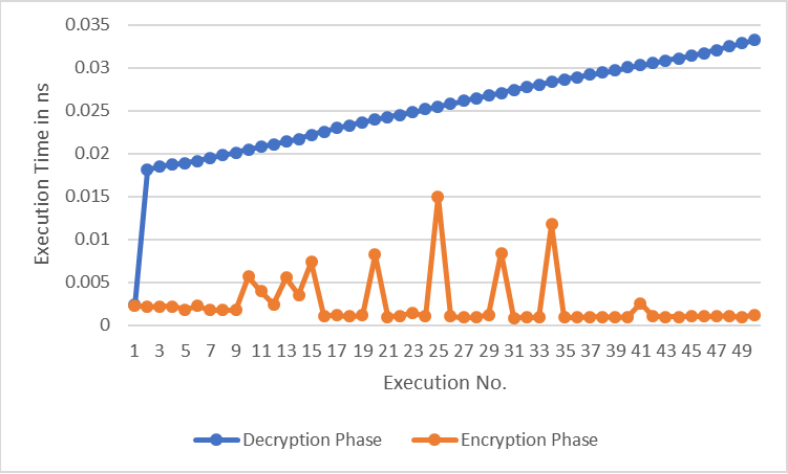

Fig.4. Evaluation of El-Gamal algorithm

Fig. 5 shows the execution time for generating public and private keys for the El-Gamal algorithm. We note that the private key requires more execution time than the public key because the private key generation involves additional steps such as checking for the validity of the chosen private key (ensuring it's within the correct range and satisfies necessary conditions like coprimality with $p-1$).

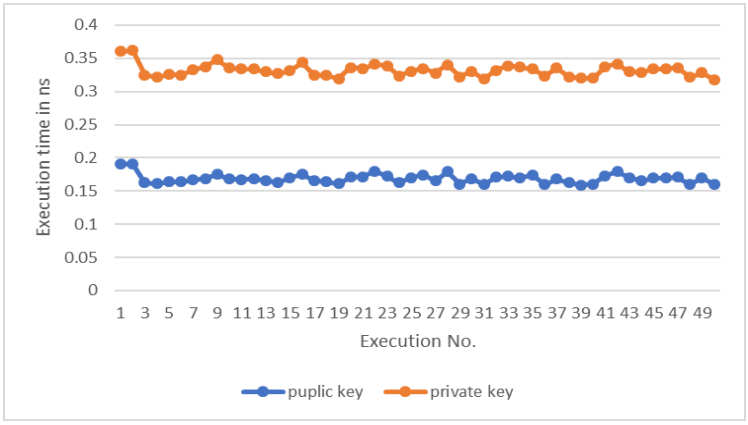

Fig.5. Execution time evaluation for El-Gamal keys

Fig. 6 and 7 are an assessment of the performance of the CSPRNG algorithm. Fig. 6 shows the average of random numbers that can be obtained during each execution which can be reach up to 290 randomness, while Fig. 7 shows the execution time for fifty times for the CSPRNG algorithm range is so fast and never take long time. We note from Fig. 7 that CSPRNG does not consume much time to generate randomness, it was not more than 0.0005 ns.

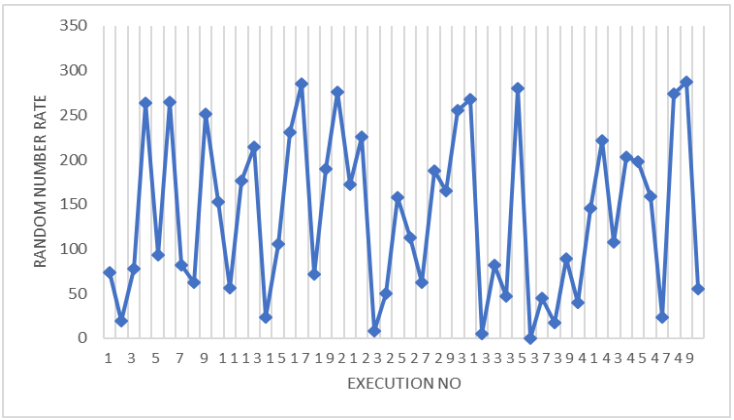

Fig.6. CSPRNG evaluation of random number range

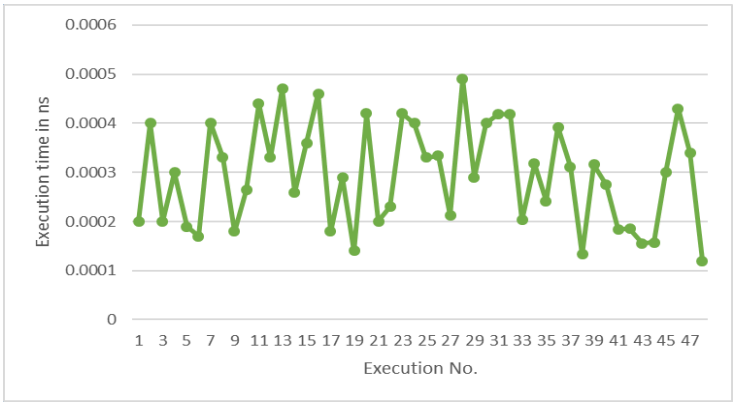

Fig.7. Execution time for CSPRNG random numbers

We also prepared an assessment of the hashing algorithms to illustrate the advantage of GLUON256 and the importance of embedding it in our model. Fig. 8 shows the hash rate of the SHA256 and GLUON256 algorithms in each implementation. We see that the GLUON256 algorithm perform better hash rates than SHA256.

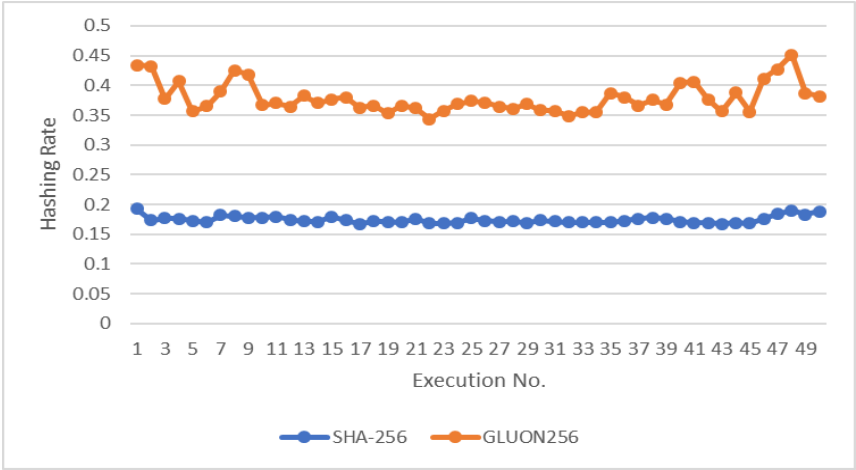

Fig.8. Performance analysis of SHA256 and GLUON256 rates

Also, Fig. 9 shows the implementation of each hash function for SHA256 and GLUON256. From the figure, we note the hashing rate was up to 0.02 while the GLUON256 is higher by 0.45, while the time it took for each algorithm was, 0.15 ns for GLUON256 while it was 0.20 ns for SHA256. In conclusion the performance of GLUON256 is quite better than SHA256, where

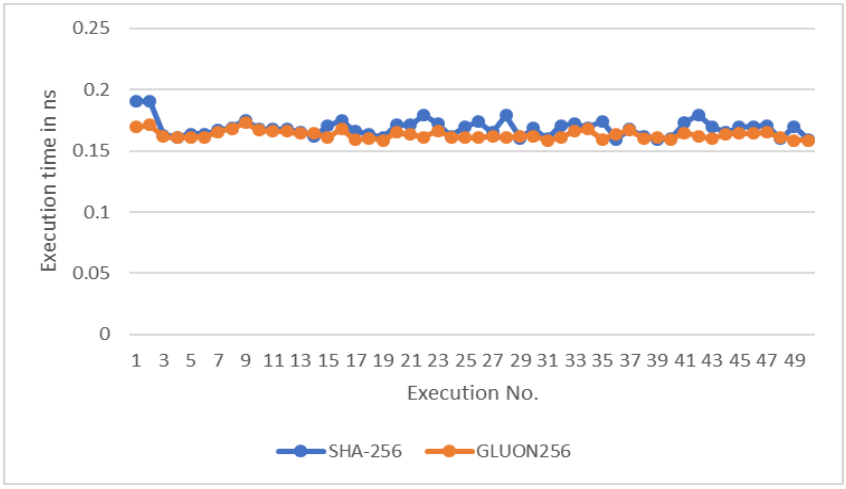

Fig.9. Execution time for both SHA256 and GLUON256

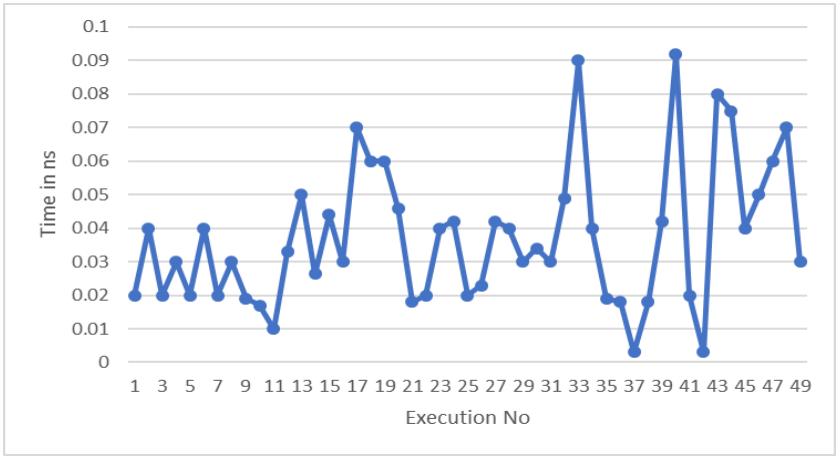

Fig.10. Blocks time interval in nanoseconds

Fig. 10 depict the time it takes for the Blockchain to create a block. Where the time it takes to the creation was between 0.01 ns and not more than 0.09 ns which is considered quite suitable with such a system.

Fig. 11 displays the performance of compression and decompression operations for a text. We note that these operations are distinguished by their high performance, which reflects positively for the encryption and decryption

operations in the LZ77 algorithm.

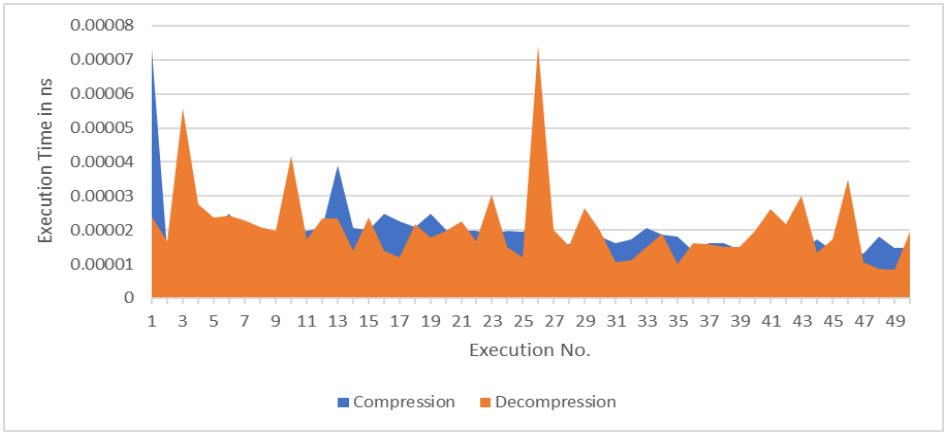

Fig.11. Execution time for LZ77 algorithm

Finally, Fig. 12 shows the full performance of the proposed model with encryption and decryption operations for both SHA256 and GLUON256, as each implementation includes El-Gamal (encryption or decryption), hash (SHA256 or GLUON256), CSPRNG, LZ77 (compression or decompression) and Block. It is clear from Fig. 12 that the proposed model with GLUON256 is better for encryption and decryption than SHA256.

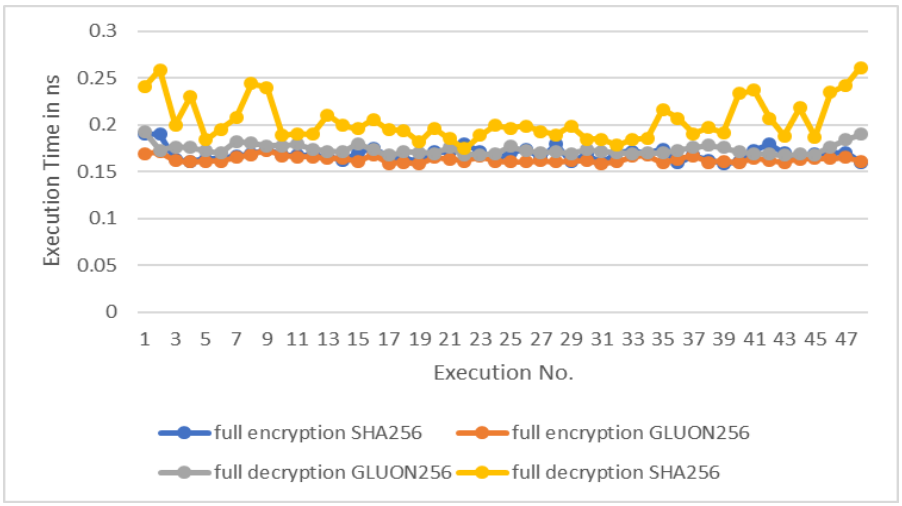

Fig.12. Full performance analysis of the proposed model with both SHA256 and GLUON256

5.2. Assessment of Security

This section provides a security analysis of our proposed model against recent ransomware attacks.

A. Assessment of the Proposed Model for Resistance of Ransomware Threats

- NotPetya; It is among the world's most serious and sophisticated cyber threats. It is a sophisticated form of ransomware that is intended to cause substantial harm to the targeted computers. It infiltrates computer systems, encrypts data, and then demands that the user pay a ransom to acquire the decryption key. Furthermore, the malware ruins the operating system of the target device, rendering it inoperable. Our suggested architecture mitigates this threat by utilizing hybrid Blockchain technology, which is a highly effective storage and encryption solution.
- GoldenEye: It is among the most dangerous cyberattacks. This attack uses a unique combination of harmful tools and technologies. The attack begins with malware penetrating the target computers via security flaws. The malware then encrypts the files on the target device with high encryption. Following that, the malware damages part of the device's operating system, rendering it useless. Finally, the spyware demands a ransom for the encryption key. Our hybrid Blockchain architecture mitigates this threat by creating several backup copies of the files contained within it.
- WannaCry: It is a ransomware assault, one of the largest ever. WannaCry has been connected to the Houthis, a skilled criminal outfit with ties to North Korea. It takes advantage of EternalBlue, a weakness in the Windows operating system. Once hacked, WannaCry encrypts and holds the user's files hostage. WannaCry displays a

message asking for a payment to obtain the encryption key for their files. If the ransom is not paid, WannaCry has threatened to permanently erase the encrypted files. The WannaCry attack is thought to have cost billions of dollars around the world. Maintaining up-to-date backups of critical data is critical in combating this threat, and our suggested strategy employs hybrid Blockchain technology to back up and store data. Customers should additionally be made aware of the dangers of questionable messages and links and advised not to open them.

- Emotet: It is one of the most dangerous malware attacks seen in recent years. The assault begins with sending bogus emails containing harmful attachments or links. When user open the attachment or click the link, the virus is activated and begins to install itself on user's device. Emotet then downloads and installs other software, including adware, ransomware, and botnets. Emotet employs advanced techniques to disguise and connect to command and control servers in order to acquire more instructions. Once installed on the device, Emotet spreads throughout the network, gaining access to user and company data. Our solution is more secure than Emotet's, as it employs a hybrid Blockchain and CSPRNGs design.
- Trickbot: It is a sophisticated malware and Trojan designed to steal victims' financial details and data. Trickbot is delivered through fraudulent emails that include harmful attachments or URLs. When user open the attachment or click the link, the virus is activated and starts to install on user's device. Trickbot downloads and installs extra components to enable espionage and data theft. Trickbot especially targets victims' financial and banking information. Because such assaults are the first to be halted by backups, we were able to prevent them by including hybrid Blockchain and encryption approaches into our methodology structure.
- Conti: It is a criminal organization that specializes in ransomware. Conti is among the most dangerous and effective malware for extortion and data theft. Conti is distributed using a variety of techniques, including phishing emails and remote access assaults. When the device is compromised, Conti encrypts the user's files and holds them for ransom. Conti shows the victim a message asking for a ransom to retrieve the encryption key for their files. If the ransom is not paid, Conti threatens to either publish or permanently delete the stolen data. Conti uses innovative tactics to conceal and navigate through the targeted networks. Conti has been identified as being affiliated with a well-known Russian criminal organization. It is opposed by our system, which is based on strong encryption methods and uses Blockchain technology to store backups. We must also educate users about the dangers of suspicious messages and links, encouraging them not to open them, cooperating with security agencies, and reporting any suspicious activity.
- DarkSide: It is a ransomware that has emerged as one of the most hazardous infections. DarkSide was created by a Russian criminal outfit that specializes in cyber spoofing. DarkSide is distributed using a variety of techniques, including phishing emails and security flaws. When a machine is compromised, DarkSide encrypts and holds the user's files hostage. DarkSide presents a message asking that the victim pay a ransom to obtain the encryption key for their files. If the ransom is not paid, DarkSide threatens to either publish or permanently erase the stolen data. DarkSide assaults are mitigated by keeping up-to-date and trustworthy backups of critical data, which our proposed methodology provides thanks to Blockchain data storage and two-factor authentication for the encryption technologies utilized in our methodology.

B. Comparing Security Measures of Existing Models

In this phase, we will look at the topic of safety in the setting of hybrid Blockchain, particularly our suggested architecture. It uses CSPRNG randomness, LZ77, hash function (GLUON256), and public key encryption (EL-GAMAL256) to improve the safety of the system. The suggested hybrid Blockchain enables the sharing of information between both the public and private sectors, increasing the model's security. Table 3 provides some security comparisons between the proposed model and prior studies' models [31-37] for repelling attacks.

Table 3. Ransomware threats comparisons

Attacks	[31]	[32]	[33]	[34]	[35]	[36]	[37]	Proposed model
NotPetya	Yes					Yes	Yes	Yes
GoldenEye	Yes					Yes		Yes
WannaCry	Yes						Yes	Yes
Emotet		Yes			Yes			Yes
Trickbot		Yes			Yes			Yes
Conti			Yes		Yes			Yes
DarkSide		Yes		Yes			Yes	Yes

6. Conclusions

Nowadays, ransomware attacks have spread widely and rapidly, as they are now frequently launched against precise and sensitive data in warehouses through the use of some applications such as e-health, e-agriculture, e-banking, etc. Therefore, every institution or company that uses an electronic application must rely on a strategy that provides a way to manage warehouse data effectively and securely. In this study, we proposed a model that provides

comprehensive protection against ransomware attacks in our current era, as well as providing appropriate performance. Through our use of hash functions (GLUON), the security vulnerability in data warehouses was mitigated, as well as the use of sufficient randomness and public key encryption methods (El-Gamal). In our proposed model, we used hybrid Blockchain technology for the purpose of managing and storing this type of data, because it logically gives our model flexibility in sharing and storing data between the private and public sectors in warehouses. Our model provides a good balance between speed and security, by analyzing ransomware attacks such as NotPetya, GoldenEye, WannaCry, Emotet, Trickbot, Conti, and DarkSide that were covered during our study. As a result, we concluded that the SHA256 technology provides lower performance than the GLUON256 technology, after we conducted a performance evaluation. At the end of our research, we also conclude that our proposed model can address ransomware attacks based on comparisons with previous research and security analysis. We set before us a future vision for developing this study by investigating some algorithms such as yellow goatfish algorithms, bee colonies, and signatures such as Ed25519, optimal solution algorithms such as jellyfish/crocodile, and analyzing encryption algorithms such as Ed25519. This vision contributes to the development of our study very significantly.

References

[1] F.A., Reegu, S. Mohd, Z. Hakami, K.K Reegu, and S. Alam, "Towards Trustworthiness of Electronic Health Record System using Blockchain," *Annals of R.S.C.B.*, 25(6), 2425-2434, 2021. Retrieved from http://annalsofrscb.ro

[2] M.K., Hasan, A. Alkhalifah, S. Islam, N.B.M. Babiker, A.K.M.A. Habib, A.H.M. Aman, and M.A. Hossain, 2022. Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations. *Wireless Communications and Mobile Computing*, p.9065768, 2022. https://doi.org/10.1155/2022/9065768.

[3] A.V. Jha, B. Appasani, D.K. Gupta, B.S. Ainapure, & N. Bizon, "A Blockchain-Enabled Approach for Enhancing Synchrophasor Measurement in Smart Grid 3.0," *Sustainability*, 15, 14451, 2023. https://doi.org/10.3390/su151914451.

[4] A. A. Laghari, A.A. Khan, R. Alkanhel, H. Al-Mannai, and S. Borwis, "Lightweight-BIoV: Distributed Ledger Technology (BDLT) for the Internet of Vehicles (IoVs)," *Electronics*, 12(3), 677, 2023. https://doi.org/10.3390/electronics12030677.

[5] M. Amjad, J. Taylor, Z. Huang, M. Li, and C.S. Lai, "Improving the performance of the information and data exchange platform that supports Blockchain technology for smart grids," *Electronics*, 12(6), 1405, 2023. https://doi.org/10.3390/electronics12061405.

[6] W. Guangfu, Xin Lai, Daojing He, Sammy Chan, Xiaoyan Fu. "Improving Byzantine Fault Tolerance Based on Quota Evaluation and Consistent Hashing," *Peer-to-Peer Netw. Appl.*, 17, 1963–1975, 2024. https://doi.org/10.1007/s12083-024-01700-3.

[7] C.G. Sondakh, R. Ardiansyah, Y.Y. Joefrie, D.S. Nangreni, and M.Y. Pusadan, "Implementing the Data Layer in a Blockchain Network Using the SHA256 Hash Algorithm," *Advancing Sustainable Science, Engineering, and Technology (ASSET)*, 6(1), pp. 0240204-01 - 0240204-06, 2024. https://doi.org/10.26877/asset.v6i2.18103.

[8] L. Frank, "Hardware implementation of trigonometry-based encryption for IoT devices", *Cryptography and Communications*, February 2024. https://doi.org/10.1007/s12095-024-0378-9.

[9] R. H. Razzaq, and M. Al-Zubaidie, "Formulating an advanced security protocol for Internet of medical Things based on blockchain and fog computing technologies," *Iraqi Journal for Computer Science and Mathematics*, 5(3), 723-734, 2024. https://doi.org/10.30880/ijcsm.2024.05.03.046.

[10] W. A. Jebbar, and M. Al-Zubaidie, "Transaction-based blockchain systems security improvement employing micro-segmentation controlled by smart contracts and detection of saddle Goatfish," *SN Computer Science*, 5(7), 898, 2024. https://doi.org/10.1007/s42979-024-03239-9.

[11] A. Janarthanan, and V. Vidhusha, "Cycle-Consistent Generative Adversarial Network and Crypto Hash Signature Token-based Blockchain Technology for Data Aggregation with Secured Routing in Wireless Sensor Networks," *International Journal of Communication Systems*, 37(4), e5675, 2024. https://doi.org/10.1002/dac.5675.

[12] M. Al-Zubaidie, and W. A. Jebbar "Providing Security for Flash Loan System Using Cryptocurrency Wallets Supported by XSalsa20 in a Blockchain Environment," *Applied Sciences*, 14(14), 6361, 2024. https://doi.org/10.3390/app14146361.

[13] R. Vatambeti, E. P. Krishna, M. G. Karthik, and V. K. Damera, "Securing the medical data using enhanced privacy preserving based Blockchain technology in Internet of Things," *Cluster Computing*, 27(2), 1625-1637, 2024. https://doi.org/10.1007/s10586-023-04056-0.

[14] V. S. Marichamy, and V. Natarajan, "Blockchain based securing medical records in big data analytics," *Data & Knowledge Engineering*, 144, 102122, 2023. https://doi.org/10.1016/j.datak.2022.102122.

[15] S. Shree, C. Zhou, and M. Barati, "Data protection in internet of medical things using Blockchain and secret sharing method," *The Journal of Supercomputing*, 80(4), 5108-5135, 2024. https://doi.org/10.1007/s11227-023-05657-7.

[16] E. R. D. Villarreal, J. García-Alonso, E. Moguel, and J. A. H. Alegría, J. A. H. "Blockchain for healthcare management systems: A survey on interoperability and security," IEEE Access, 11, 5629-5652, 2023, https://doi.org/10.1109/ACCESS.2023.3236505.

[17] I. Keshta, Y. Aoudni, M. Sandhu, A. Singh, P. A. Xalikovich, A. Rizwan, and S. Lalar, "Blockchain aware proxy re-encryption algorithm-based data sharing scheme," *Physical Communication*, 58, 102048, 2023, https://doi.org/10.1016/j.phycom.2023.102048.

[18] G. Tripathi, M. A. Ahad, and G. Casalino, "A comprehensive review of Blockchain technology: Underlying principles and historical background with future challenges," *Decision Analytics Journal*, 100344, 2023, https://doi.org/10.1016/j.dajour.2023.100344.

[19] R. H. Razzaq, M. Al-Zubaidie, and R. G. Atiyah, "Intermediary Decentralized Computing and Private Blockchain Mechanisms for Privacy Preservation in the Internet of Medical Things," *Mesopotamian Journal of CyberSecurity*, 4(3), 152-165, 2024. https://doi.org/10.58496/MJCS/2024/020.

[20] W. A. Jebbar and M. Al-Zubaidie, "Transaction Security and Management of Blockchain-Based Smart Contracts in E-Banking-Employing Microsegmentation and Yellow Saddle Goatfish," *Mesopotamian journal of Cybersecurity*, vol. 4, no. 2, pp. 71-89, 2024, https://doi.org/10.58496/MJCS/2024/005.
[21] W. L. Shiau, X. Wang, and F. Zheng, "What are the trend and core knowledge of information security? A citation and co-citation analysis," *Information & Management*, 60(3), 103774, 2023. https://doi.org/10.1016/j.im.2023.103774.
[22] A. T. Oyewole, C. C. Okoye, O. C. Ofodile, and C. E. Ugochukwu, "Cybersecurity risks in online banking: A detailed review and preventive strategies application," *World Journal of Advanced Research and Reviews*, 21(3), 625-643, 2024, https://doi.org/10.30574/wjarr.2024.21.3.0707.
[23] M. Al-Zubaidie, "Implication of lightweight and robust hash function to support key exchange in health sensor networks," *Symmetry*, 15(1), pp. 152, 2023. https://doi.org/10.3390/sym15010152.
[24] M. Al-Zubaidie and G. S. Shyaa, "Applying detection leakage on hybrid cryptography to secure transaction information in e-commerce apps," *Future Internet*, 15(8), 262, 2023. https://doi.org/10.3390/fi15080262.
[25] M. Al-Zubaidie, and R. A. Muhajjar, "Integrating Trustworthy Mechanisms to Support Data and Information Security in Health Sensors," *Procedia Computer Science*, *237*, 43-52, 2024. https://doi.org/10.1016/j.procs.2024.05.078.
[26] J. P. Arockiasamy, L. E. Benjamin, and R. U. Vaidyanathan, "Beyond Statistical Analysis in Chaos-Based CSPRNG Design," *Security and Communication Networks*, *2021*(1), 5597720, 2021. https://doi.org/10.1155/2021/5597720.
[27] S. Jain, M. A. Rios, and B. Cambou, "Enhancing True Random Number Generation in MRAM Devices Through Response Adjustment," In *Science and Information Conference* (pp. 438-454). Cham: Springer Nature Switzerland, 2024. https://doi.org/10.1007/978-3-031-62273-1_28.
[28] J. Daemen, D. Kuijsters, S. Mella, and D. Verbakel, "Propagation properties of a non-linear mapping based on squaring in odd characteristic," *Cryptography and Communications*, 1-15, 2024. https://doi.org/10.1007/s12095-024-00711-4.
[29] J. Chen, R. G. Edwards, and W. Mao, "Graph Contractions for Calculating Correlation Functions in Lattice QCD," In *Proceedings of the Platform for Advanced Scientific Computing Conference* (pp. 1-10), 2023. https://doi.org/10.1145/3592979.3593409.
[30] P. M. Mukundan, S. Manayankath, C. Srinivasan, and M. Sethumadhavan, "Hash-one: A lightweight cryptographic hash function," *IET Information Security*, 2016. https://doi.org/10.1049/iet-ifs.2015.0385.
[31] M. Waqas, M. A. Khuhro, U. Saeed, K. Kumar, N. Mirbahar, Ruqiya, " Security Awareness on Ransomware Threats Detection and their Protection Techniques," *International Journal of Advanced Trends in Computer Science and Engineering*, 2021. https://doi.org/10.30534/ijatcse/2021/701022021.
[32] R. Tate, and C. Bates, "Deterrence Thru Transparent Offensive Cyber Persistence," *JSTOR*, Vol. 7, No. 4, pp. 227-246, 2022. https://www.jstor.org/stable/48703302.
[33] K. A. Williams, *Conti Ransomware Gang: An Analysis of the Group's Motives and Methods*, (Doctoral dissertation, Utica University), 2022.
[34] A. D. Westbrook, "A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets and Defending National Security," *NYUJL & Bus.*, 18, 391, 2021.
[35] J. A. Gómez Hernández, *Crypto-ransomware: Analysis and early detection based on the use of trap files*, (Doctoral dissertation, University of Granada) 2022. https://digibug.ugr.es/bitstream/handle/10481/76803/94887%281%29.pdf?sequence=4&isAllowed=y.
[36] Q. Zhong, and Q. Kang, "Ransomware Detection with Opcode Analysis and GAN-Based Unsupervised Learning," *Research Square*, 2024. https://doi.org/10.21203/rs.3.rs-3819158/v1.
[37] K. Stoddart, "Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers," *In Cyberwarfare: Threats to Critical Infrastructure*, Cham: Springer International Publishing, pp. 351-399, 2022. https://doi.org/10.1007/978-3-030-97299-8_6.

Authors' Profiles

Rasha Hallem Razzaq: She received her bachelor's degree in computer science in 2010. The subject of the bachelor's thesis is devoted to the study of search engines. She is currently studying for a master's program in the Department of Computer Science at University Thi-Qar, Iraq. Her research topics include medical security systems, information storage, Blockchain encryption techniques, and medical information security.

Duaa Hammoud Tahayur: She obtained a bachelor's degree in computer science from the University of Thi-Qar, Iraq, in 2021, and she is currently studying for a master's degree in information and data security at the University of Thi-Qar, Iraq, for the current year 2024. Her current scientific interests are digital signature algorithms to secure, verify, and preserve data as well as Blockchain and optimization.

Wid Alaa Jebbar: She received her bachelor's degree in cybersecurity in Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Iraq, in 2014. The theme of the bachelor's thesis is devoted to the study of wireless sensor network security. She is currently studying a master's program at Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Iraq. Her research topics is all about the security of Blockchain system in terms of loans and money transaction.

Mishall Al-Zubaidie: He received the bachelor's degree in computer science from Basrah University, Iraq, in 2004, and the master's degree in security of the wireless network from Basrah University, Iraq, in 2010. He obtained the Ph.D. degree with the School of Agricultural, Computational and Environmental Sciences, Faculty of Health, Engineering, and Sciences, University of Southern Queensland, Toowoomba, QLD, Australia, in 2020. His current research interests are public key algorithms, authenticating and authorizing users in electronic health record (EHR), both security and efficiency in wireless sensor network, Public-Key cryptography, Lightweight hash functions, Anonymity and pseudonymity techniques, Keys exchange/agreement algorithm in health systems, Security in IoT and smart cities, Cybersecurity in the health sector, Research in Cybersecurity, Cybersecurity Programs and Policies, Security, and privacy challenges in smart cities, Security and Forensics, Blockchain and Integrity Techniques.

How to cite this paper: Rasha Hallem Razzaq, Duaa Hammoud Tahayur, Wid Alaa Jebbar, Mishall Al-Zubaidie, "Sturdy Blockchain Combined with E-apps Repositories Based on Reliable Camouflaging and Integrating Mechanisms", International Journal of Computer Network and Information Security(IJCNIS), Vol.17, No.3, pp.35-53, 2025. DOI:10.5815/ijcnis.2025.03.03