Journal of Education for Pure Science- University of Thi-Qar
Vol. 14, No.3 (2024)
Website: jceps.utq.edu.iq Email: jceps@eps.utq.edu.iq

DOI: https://doi.org/10.32792/jeps.v14i3.545

Blockchain and Cryptography Framework of E-Apps with Big Data

Wid Alaa Jebbar [1], Rasha Hallem Razzaq [1], Duaa Hammoud Tahayur[1*] and Mishall Al-Zubaidie[1]

[1] Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq

[*] Corresponding email: duaahammoud.comp@utq.edu.iq

Received 18 /04 /2024, Accepted 02/ 06 /2024, Published 01 / 09 /2024

Abstract:

With the tremendous and rapid evolution taking place in the field of technology and considering the rise in data volume that is dealt with daily, managing this data, whether in terms of security or terms of storage especially if the data is huge, is considered a necessary issue. Therefore, in this research, we established a framework that provides both security and storage/repository management. Where the security issue in the suggested framework is supported by the use of lightweight hash functions and public-key encryption algorithms represented by SPONGENT and elliptic curve cryptography (ECC). Additionally, the fast random number generator is also used to support the security algorithms included in the framework, while managing the repository storage is controlled by the use of a hybrid Blockchain to manage storage for this type of big data. The process of storing this data in databases or any of the traditional centralized methods exposes the data to loss or penetration. After analyzing the proposed framework, it successfully addressed the prevention of malicious within the field of proposed research attacks. Moreover, the performance analysis of the framework proposed was quite effective with the lightweight SPONGENT and ECC results, while the creation of blocks in the storage phase was not more than 0.18 ns. Thus, we obtained an effective framework in terms of security, performance, and terms of data repository management and control.

Keywords: Blockchain, e-apps, hash function, repository security, SPONGENT

1-Introduction

To build a comprehensive and clear view of the topic, this section presents the advantages and disadvantages Blockchain/Big Data offers, the risks of recent ransomware attacks in electronic apps, and the importance of our research topic, this will be explained in the following subsections.

Blockchain is an evolutionary technology that gives any system a qualitative shift for the better. This is done by offering security, dependability, privacy, and interoperability. The fundamental concept of Blockchain is a huge network of interconnected computers serving as a digital record keeper or what is called a ledger, rather than a single person or organization, this network safely logs transactions in an unchangeable and unhackable manner [1]. The decentralized and unchangeable ledger of Blockchain securely stores big medical data, financial institution data, or any data and protects it from threats that compromise data integrity [2]. The data in the ledger cannot be tampered with since it is shielded from cryptographic features like hashing, digital signatures, and asymmetric keys [3]. Additionally, because the ledger is decentralized, every Blockchain member will be aware of any minor changes made to the data transaction, increasing the system's transparency.

Although Blockchain has many advantages, this technology has a few disadvantages to consider. These are a few of its shortcomings and weaknesses:

- **Mining process problems**: In the mining process, a huge amount of materials and energy is wasted [4]. All the nodes in the Blockchain participate in the proof of work, which is the process of mining to produce the blocks.
- **Storage problems**: There may come a moment when the Blockchain contains more aggregate data than the volumes of accessible hard disks. Data will grow as the number of users' increases. Therefore, it will also be necessary to upgrade the system's hard disk space.
- **Unchangeability problem**: The data in the Blockchain cannot be changed or modified. If an error occurs during its creation, this data will never be editable.
- **Ability to scale**: Each block of the Blockchain contains a specific number of data, meaning that the size of the block is fixed and cannot be increased, and since electronic transfer operations, for example, require reliability from all network blocks, this transfer process will become very slow and cumbersome.

The modern era is witnessing a huge increase in the volume of available data which is known as “Big Data” or “Big Information”. As the volume of this data increases, many challenges and problems arise that must be faced and solved. Security and privacy are among the most prominent challenges facing the use of big data [5, 6]. Maintaining confidentiality and protecting against unauthorized access is extremely important, especially when using sensitive data such as financial records, agricultural records, patient records, etc. [7]. In addition to privacy and security, big data faces some problems in managing data in an integrated manner and complying in a harmonious manner with existing systems. The technology used in Blockchain can provide an effective solution to such problems, as access integration portals can be provided with existing systems such as electronic applications. In systems such as healthcare systems, there are a lot of big data forms to deal with, such as patient records, electronic devices for tracking remotely, and the shareable data between doctors in the system [8]. Thus, the need to obtain and build a complete framework that provides both security, managing such data, and monitoring them is considered a critical issue. Blockchain access-based systems combined with cryptographic algorithms alongside the hash functions will hit the goal of providing a complete framework that combines both security and managing storage professionally [9]. Where blockchain technology is an evolutionary technique that provides the systems with security and authority. Blockchain technology can provide data security and protect it from hacking or tampering so that there is an effective balance between compliance, privacy, and security, which contributes to building a reliable and secure environment for exchanging and managing huge sensitive data/repositories. Due to this continued interest and effective focus, Blockchain technology can be used to secure big data and achieve significant benefits in several areas such as finance, trade, and health [10]. Ransomware is a type of computer attack that targets data and systems, encrypts it, prevents users from accessing it, and then demands a ransom in exchange for decrypting it and being able to access user data [11, 12, 13]. Ransomware attacks pose several hazards, such as the loss of confidential data, compromise of systems and services, compromise of privacy and security, and detrimental effects on the targeted organizations' finances and reputation [14, 15]. Numerous organizations, businesses, and people have experienced this kind of assault. Recent ransomware assaults carry several concerns.

The problem statement of our research comes from the importance of managing the large volume of data that is generated from e-apps such as e-health, e-banking, e-agriculture, etc. By managing big data we mean the aspects of security of repository storage. As long as this data is on the internet that means it is vulnerable to attacks and loss. Also, as long as the generating of the data keeps increasing, the storage process using the traditional methods with the vulnerabilities and difficulties, Blockchain, big data may encounter crucial ransomware assaults. Understanding possible drawbacks of Blockchain, such as repository storage capacity, scalability, mining difficulties, and the inability to modify input data, can aid in its improvement and help it get over its obstacles. In terms of big data, comprehending the difficulties with privacy, security, compliance, and data management can help in creating efficient solutions to safeguard sensitive data and ensure adherence to relevant laws and regulations of this data considered too critical. Thus, we suggested this framework to manage both security and repository storage to deal with such types of data. Regarding ransomware attacks, knowing the dangers involved and how they affect sensitive information, systems, and services helps improve security and protection and assists in establishing plans to stop and neutralize these assaults. Research and an emphasis on shortcomings and difficulties can, in general, help to enhance systems and technologies and provide workable answers to possible issues. This research can also help individuals and businesses secure their data and keep it safe from potential dangers. Therefore, our contributions are as follows:

- Establish a framework for managing repository storage and security. Big data storage management and security are built into the research framework. Public-key encryption methods like ECC, hash functions, and random number generators (providing high randomness) are used to support the security component of the framework.
- Data distribution and control with hybrid Blockchain data is dispersed between public and private domains via hybrid Blockchain technology. We replaced the secure hash algorithm (SHA256), which is present by default in the blockchain, with the SPONGENT algorithm to support block security in e-apps.
- To counter and handle possible security threats such as scareware, certber, RaaS, leakware, cryptocurrency, and lockers, the suggested framework was examined. Additionally, we provide security comparisons between our framework and previous works to illustrate the ability of our proposal to repel recent attacks.

2-Literature review

In this section, there will be a review of previous studies, what they presented and what are the advantages and disadvantages of their frameworks as follows.

Wortman et al. [12] proposed a security enhancement model utilizing physical hardware-based techniques to protect consumer electronic devices. The model utilizes a set of physically unclonable functions (PUFs) as potential seeds for pseudorandom number generators (PRNGs). One of the challenges that the model may face is the impact of the use of physical hardware technologies on the performance of electronic devices and their ability to integrate with home automation applications. To determine statistical randomness, entropy, and resilience to cryptographic assaults in the Internet of Things (IoT), Kietzmann and Schmidt [1] examined software and hardware parts. It focused on security, statistics, and operating system integration, using test suites and device performance assessments. Their research suggested dividing OS-level general-purpose random generators from cryptographically safe ones, where SHA256-PRNG is recommended for cryptographic security. However, the drawback of this study is the lack of details about how to use SHA256 to provide security, although they gave a detailed analysis of the performance the security aspect is still not specified.

Hasan et al. [4] aimed to provide a thorough analysis of Blockchain applications about smart grid energy data protection and cyber security perception. Consequently, the researchers outlined the main security problems with smart grid scenarios that Blockchain and big data can resolve. However, this is a theoretical study and never practical with details. Vishwakarma et al. [13] introduced a low-weight Blockchain-based security protocol (LBSV) for safe communication and storage in an ecosystem of Internet vehicles that is supported by the SDN of the next generation. Secure message propagation is achieved by the use of several cryptographic algorithms, such as SHA256 and ECC. They claimed that the LBSV protocol can withstand various assaults that target the privacy of message dissemination. They pointed out that with 85% less computation cost, 55% less storage and transmission cost, and 90% less approval time, LBSV provides appropriate performance.

A model known as the secured image management methodology (MSCCBT-SIM) was published by Padmavathi and Rajagopalan [14] and makes use of Blockchain technology and several strategies to generate multiple stakes. Stakes may be made and encrypted using ElGamal public key encryption, which is based on emperor penguin enhanced (EPO-EPKC). Many experiments were carried out, and the outcomes were examined using various measurements, to confirm the functionality of the MSCCBT-SIM model. However, the ElGamal algorithm will be very expensive if used to encrypt big data and thus increase performance overhead. Koshiba et al.

[5] focused on changing the mindset surrounding the security-performance trade-off. However, the researchers considered their suggested system to be quite secure just because it relies on the difficulty of a unique variation of the discrete logarithm issue, and never went through the attacks analysis.

Thantharate and Thantharate [7] proposed a comprehensive Blockchain framework called “ZeroTrustBlock" to exchange health information securely and privately. This framework aims to overcome issues related to interoperability, security, and privacy in existing healthcare data management systems. Integration with existing systems such as electronic healthcare records can be difficult. Additional integration gateways or APIs may be required to ensure compatibility and seamless communication between ZeroTrustBlock and other systems. To build a strong Blockchain architecture for COVID-19 data, Gopalakrishnan and Basarkod [9] proposed an effective Blockchain and lightweight data encryption model with a re-encryption mechanism. Using Blockchain, encrypting data, and storing it in the interplanetary file system may be computationally and storage expensive, and this is considered one of the challenges facing the proposed model.

Nannipieri et al. [10] proposed the design and implementation of a set of hybrid cryptographic accelerators, named “Crypto-Tile”, within the framework of the European processor initiative (EPI) project. The EPI project aimed to develop Europe's first fully low-consumption processor family, meeting the needs of big data, high-performance computing, and the automotive industry. Their proposal may have difficulty complying with the required security and certification standards, especially in the automotive market requires critical safety aspects to be taken into account. Vishwakarma et al. [3] suggested smart grid-NG, a thorough smart grid architecture with Blockchain. According to their performance analysis, throughput is enhanced by 60%, calculations overhead, and energy consumption are decreased by 70%, and the consensus delay is down to 80%. With all these parameters and appropriate results, their paper never addressed the execution in real-time as a parameter, because with their proposed idea they presented to enhance the work of Blockchain, the parameter of overall time the system needed to complete the processes was considered a huge issue. Kang et al. [8] proposed to implement an authentication framework based on Blockchain technology to protect the credibility and integrity of patient data. Instead, the researchers propose using Blockchain technology to achieve mutual authentication between different parties without relying on central servers. The medical data exchanged in their proposed framework may face privacy issues and weaknesses in generated randomness and performance overhead.

3-Blockchain and repositories protection technologies

3.1-Blockchain

Blockchain is a distributed network for protecting and storing data. Its work is based on creating a chain of blocks, each of which contains data connected to the previous blocks using mathematical hashing techniques. Blockchain is resistant to attack and manipulation since it is distributed across many devices connected to the network. In systems that consist of a lot of nodes that are connected together, blockchain technology provides these systems with a high level of security [2] and speeds up these systems as the existence of third parties is eliminated and all the execution of the processes is peer to peer. A database made up of interconnected chains of blocks is called a blockchain. This technology has several important characteristics, including transparency, security, and decentralization. Data on Blockchain is secured by cryptographic techniques, stored permanently, and made publicly available with difficult modifications. It relies on a SHA256 hash [16] by default to prevent block data from being modified. Blockchain is widely used in electronic applications and projects including health services, supply chains, banking, agriculture, and document management that require security. Records are maintained, ensuring data integrity, without the need for a reliable central authority to supervise or verify the data [4]. Blockchain-based test repositories must be comprehensive and studied, and “proof of verification” must be used as a method to verify repository management and achieve transparency, decentralization, and security in the transfer and storage of digital information. Blockchain is used as a means to protect access to encrypted data and to store scattered data [6, 8].

3.2- SPONGENT hash function

The term SPONGENT represents a specific type of lightweight hash function, which accepts inputs with variable length and uses permutation technique on the inputs to produce the fixed-length output, where this type of function provides hash values with the length 128-bit, 160-bit, 224-bit, and 256-bit. SPONGENT function aims to stop weakness arising from the mathematical operations representing the hashing operation [17]. Because this type of function relies on simple mathematical operations, it helps systems with limited resources. Also, it does not need a lot of power to complete the hashing process, where it provides security with an easy and smooth hashing operation. The hashing process is based on state $b = r + c \geq n$, where r refers to the rate, *c* is the capacity, and *n* represents its size. The final hash value is produced by using the internal state of the function [16, 18]. For scenarios where efficiency is paramount, SPONGENT offers a portable and secure hashing solution. Table 1 describes the main differences and security preferences of SPONGENT over SHA256.

Table 1. Comparison between SHA256 and the SPONGENT [18]

Aspect	SHA256	SPONGENT
Security	It is regarded as secure. With SHA-256, it is exceedingly difficult to alter the data and obtain the same hash value.	It was created with security in mind as well, adhering to a particular plan to thwart vulnerabilities. But compared to the well-known SHA-256, it could not have the same degree of cryptanalysis (testing for flaws) because it is a younger design.
Efficiency	Although efficient, it may use more resources and be slower than SPONGENT, particularly on devices with little processing power.	It demonstrates remarkable efficiency. Because of its deliberate design to be small and light, it works well with devices that have limited power or computing capacity.
Use	Strong security and widespread use make it a popular choice for a variety of security applications, including file verification, password protection, and digital signatures.	Designed to be more specifically utilized in resource-constrained contexts where efficiency is essential, such as embedded systems and sensor networks.

The unique demands will determine which SHA-256 and SPONGENT are best for users' applications. SHA-256 is a fantastic option if security is your top priority. SPONGENT might be a better option if you require a quick and effective hashing solution for a device with minimal resources.

3.3-ECC encryption

Elliptic Curve Cryptography was developed in 1985 using an elliptical curve as the cryptographic technique. Each user or device using ECC has two keys: a public key and a private key. ECC is a type of public-key encryption [19]. The equation "$y2 = x3+ax+b$" is the elliptic curve over which the mathematical operations of ECC are specified, where $4a3+27b2 \neq 0$. Each value of '*a*' and '*b*' results in a unique elliptic curve. A private key is a random integer, while a public key is a point on the curve. Multiplying the private key by the generator point *G* on the curve yields the public key. The domain parameter of ECC is composed of the generator point *G*, the curve parameters '*a*' and '*b*', plus a few other constants. Algorithm 1 presents the ECC encryption.

Algorithm 1. Elliptic curve cryptography encryption

```
Input: Parameters field of an elliptic curve ($p$, $E$, $P$, $n$), Public key ($Q$), Plaintext ($m$)
Output: $C_{i1}$and $C_{i2}$ ciphertexts
Begin
    1. Represents the message $m$ as a point $M$ in $E$ ($F_p$)
    2. Selects $k \in R^{[1, n-1]}$
    3. Calculates $C_{i1} \longleftarrow K_p$
    4. Computes $C_{i2} \longleftarrow M + kQ$
    5. Return $C_{i1}$ and $Ci_2$
End
```

3.4-PRNG algorithm

An approach known as a pseudorandom number generator (PRNG) is used to produce a string of numbers that closely resembles the output of a genuine random number generator, which is used to produce actual random numbers. The output produced by PRNG execution is not completely random as it depends on a starting value (seed) that defines the generation sequence [1]. The PRNG output will ultimately begin to repeat when it exhibits the same pattern as previously after a given amount of time. Cryptographic applications typically demand an unexpected output, particularly when examining historical outputs. Unless the cycle length is extremely long, deterministic generators, or PRNGs, have short durations for certain beginning values, which makes it simple to anticipate the output of a PRNG. PRNG seeds can be produced using traditional methods, either through software or utilizing hardware. For software-based PRNGs, the seed generation process is as simple as calling an arbitrary procedure. In a hardware context, an initial combination of values can be fixed and contained in memory, or the seed can be produced using initial inputs obtained during the manufacturing process [12, 20].

4- A Proposed Methodology for Secure Repositories Access

Enterprise applications, or e-apps, produce enormous volumes of data, which can be difficult to manage efficiently. A special approach to managing e-apps big data records and repositories is provided in the suggested framework which is shown in the next subsections. Figure 1 shows the workflow of the proposed framework.

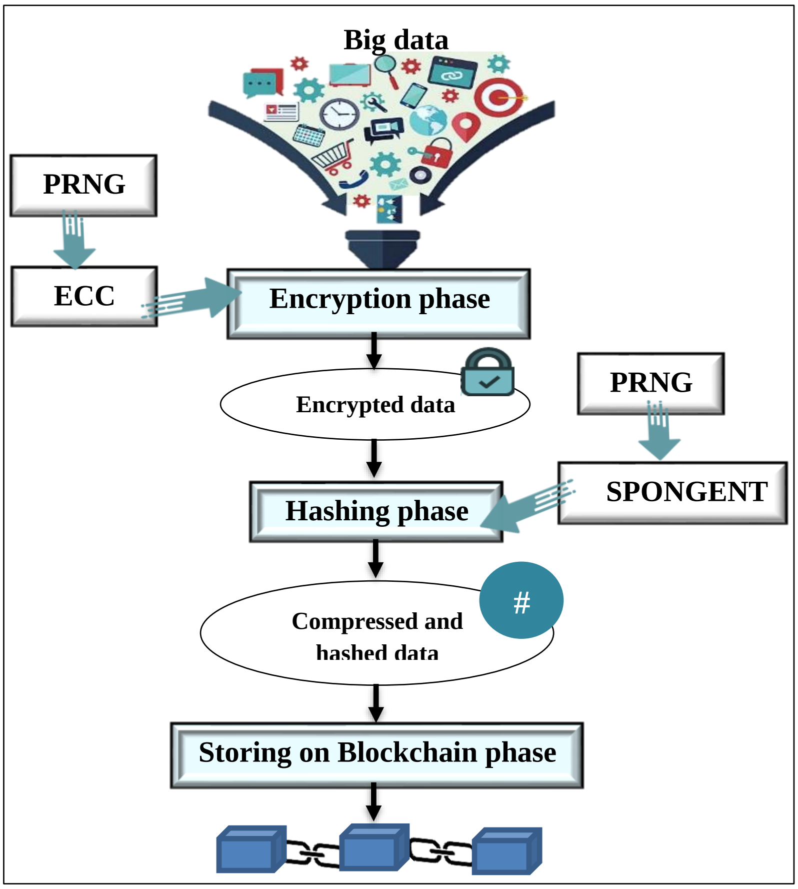


Figure 1. Workflow of the proposed framework

4.1-Using hybrid Blockchain

Hybrid Blockchains offer a reusable, scalable, and secure way to manage big volumes of data. Big data and hybrid Blockchain are two powerful technologies that can complement one another. Especially since this kind of Blockchain incorporates the best features of both private and public Blockchains, for systems that deal with such a type of data where data integrity and trust are crucial. We adopted utilizing this kind of Blockchain in the suggested framework for the following reasons:

1- Providing security: This type of blockchain provides the frameworks and systems with high security because it combines characteristics of both public and private Blockchains.

2- Partition of the work: Because some parts of this type of blockchain are public, while the others are private; thus, the work of such a blockchain is portioned, and the speed of work will be enhanced. This improves e-transaction speeds and scalability.

3- Storage technique: Hybrid Blockchain stores only the important data, where the stored data is the hashes and symbols that represent the actual data and not the data itself. This provides the framework with a high speed for implementing the processes. Also, it provides data integrity and reduces cost because the actual data is stored outside the Blockchain while only hashes are stored in the hybrid Blockchain.

4.2-Providing suitable randomness for blocks

While discussing Blockchain-based systems, randomness in blocks refers to the element of uncertainty added while a new block is being created. Malicious actors find it challenging to anticipate or control the result of block formation due to randomness. This randomness can be achieved by using cryptographic hash functions, where these functions accept different inputs like timestamps, and hashes from previous blocks, and turn them into an output that looks random. The process of creating blocks then makes utilization of this output. Also, pseudorandom number generators can achieve the goal of randomness based on a seed value, these methods produce a random sequence of integers. When utilized properly, PRNGs can be cryptographically secure even though they are not completely random. This is why in the proposed framework we combined both SPONGENT (which is a type of hash function) with the public key encryption represented by the ECC explained above, alongside the PRNGs, we obtained a level of randomness that is quite suitable for the proposed framework. In the proposed framework, we use PRNG with SPONGENT to produce high randomness for the condensed message resulting from the hashing process. Also, the framework uses PRNG with ECC to generate private and public keys with high randomness to support strong encryption of blockchain blocks.

4.3-Applying SPONGENT with blocks

To enhance the functionality and responsiveness of Blockchains and environments with restricted resources, the lightweight Blockchain framework is a methodology for deploying Blockchain in a lightweight and resource-efficient manner. This approach makes use of some upgraded tools and technologies to increase the effectiveness of Blockchain data storage and operations. Integrating big data repositories and web application logs in a reliable manner sensitive data must be secured and protected when it comes to huge web apps. One of the important elements in the framework that can be utilized to accomplish reliable integrity in a lightweight Blockchain framework is the SPONGENT algorithm. Transaction logs and data repositories can both be integrity and stored on the Blockchain with SPONGENT. The SPONGENT hashes can be used twice (previous hash and current hash) at the level of individual blocks in a chain or at the data repositories level to support data integrity before it is stored. To accomplish the desired integrity, mixing, transformation, and deduction operations are applied within the block. Consequently, data is consistently and securely within the Blockchain, these procedures are repeated over subsequent blocks.

4.4- Encryption of blocks

To encrypt blocks in the lightweight Blockchain by employing the ECC algorithm within the hybrid Blockchain. Blocks might be groups of electronic application records or large data records. The block is transformed into the proper data format. This stage could involve utilizing alternative formats or transforming the data to bit format, based on the algorithm's specifications and the lite Blockchain's internal organization. Before encrypting the data, the framework uses PRNG to generate randomness and then uses this randomness to generate private and public keys for each legitimate member of the network using the ECC algorithm. Depending on the security needs and internal design of the lightweight Blockchain, the framework can use a public key to encrypt blocks and a private key to decrypt blocks. The ECC algorithm's cryptographic operations involve the usage of suitable fast encryption functions compared with ElGamal and RSA. Also, the ECC algorithm generates relatively small keys (160, 192, 224, 256, 384, and 512 bits) compared to other key algorithms, which will reduce the storage size required for these keys. We chose the ECC algorithm in the framework because it balances performance overhead with robust security. Algorithm 2 shows the steps of block data cryptography.

Algorithm 2. Block data encryption and decryption algorithm

```
Algorithm inputs:
- Assign "$PK$" as the puplic key.
- Assign "$D$" as the wanted data to encrypt.
Algorithm outputs:
- "$E$" as the encypted data, "$D$" as the decoded data and "$H$" as the value of hash.
start
1. Using PRNG to generate randomness is "RND"
    Generating the public key:
   $PK \longleftarrow kQ.\text{RND}$
Generating the private key:
   $PR \longleftarrow RND$
2. Prepare the data:
   D ⟵ entered data
3. The step of converting the desired data into bytes:
  D_bytes ⟵ D.encode('utf-8')
 4. Encrypting data:
  E ⟵ ECC_Cipher (PK). encrypt(D_bytes)
 5.Calculating the hash value:
  H = SPONGENT_Hash (). hash(E.RND)
 6. Decrypting the data:
  D ⟵ ECC_Cipher (PR). decrypt(E)
 7. Authentication of the hash value:
  H = SPONGENT_Hash (). hash(E.RND)
 8. Archving data in the repository:
     Archive("Encrypted data: ", E)
     Archive("Decrypted data: ", D)
     Archive("Hash value: ", H)
```

4.4-Proposed framework methodology

The proposed framework will be clarified in this section, where this framework is based on the process of combination of PRNG, SPONGENT hashes, ECC encryption algorithm, and LZ27 in an environment based on a hybrid blockchain. This type of combination providing the system with confidentiality, integrity, privacy, and ease of data transfer and managing the data correctly.

1- First, the LZ77 data compression algorithm is employed to reduce the size of transmitted data and save storage space in the hybrid Blockchain. The data is divided into small blocks, and then the LZ77 algorithm is applied to each block individually. Duplicates in data are searched for and represented by reference statements, which reduces the amount of data used in the hybrid Blockchain.

2- Secondly, ECC cryptography is applied to provide confidentiality and protection of the data sent in the Blockchain. Compressed data is encrypted utilizing the ECC encryption (after adding sufficient randomness to strengthen the anonymity of the data during the application of the algorithm), using private and public keys. The public key is utilized to conceal data in the Blockchain, therefore only those who have the private key can decrypt the data. This enables only authorized people to access the data. After that, the work of algorithms in the Blockchain environment is coordinated harmoniously. The compressed and encrypted data is joined using Blockchain SPONGENT hash functions to calculate a hash set for each block. The Blockchain is signed using the SPONGENT message digest with using PRING to support robust hashes, to guarantee that the data has not been modified or changed.

Through the proposed framework, data stored on hybrid blockchain technology is safeguarded by preserving its integrity and confidentiality. The approach ensures high efficiency in aspects of performance, providing privacy, reliability, ease of data transfer, and confidentiality. Data compression reduces storage space and improves access speed, while the implementation of the ECC encryption algorithm secures the data from unauthorized access. We utilize blockchain hash functions and digital hashing to maintain data integrity. In addition, the proposed hybrid blockchain system allows for easy data transfer. Only authorized parties can access the blockchain, retrieve the compressed data, and decrypt it using the private key. This makes data retrieval easy and reliable and contributes to improving the effectiveness of the framework and the overall user experience. Figure 2 shows the workflow steps of the proposed framework and Figure 3 shows the advantages of this framework.

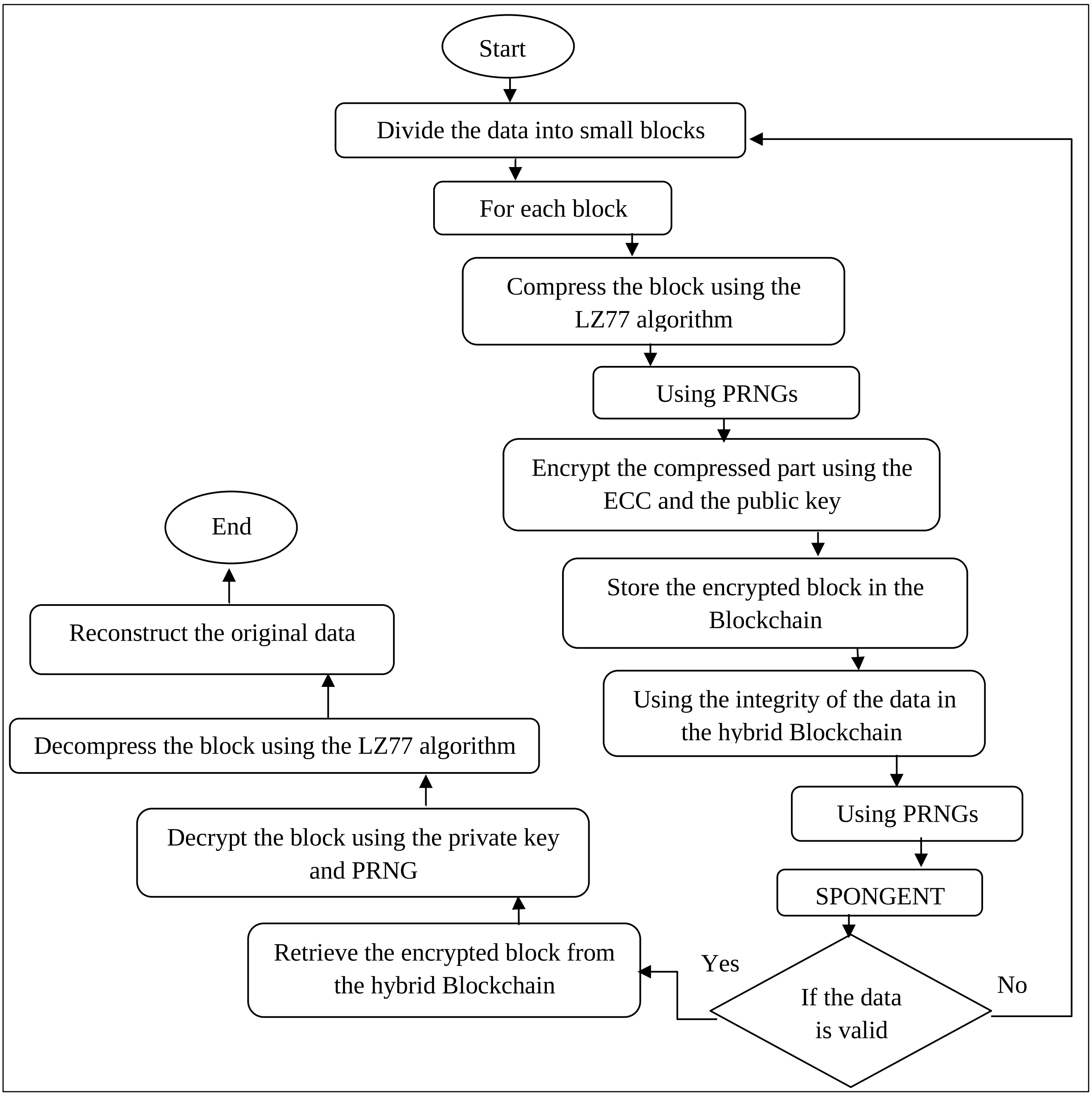
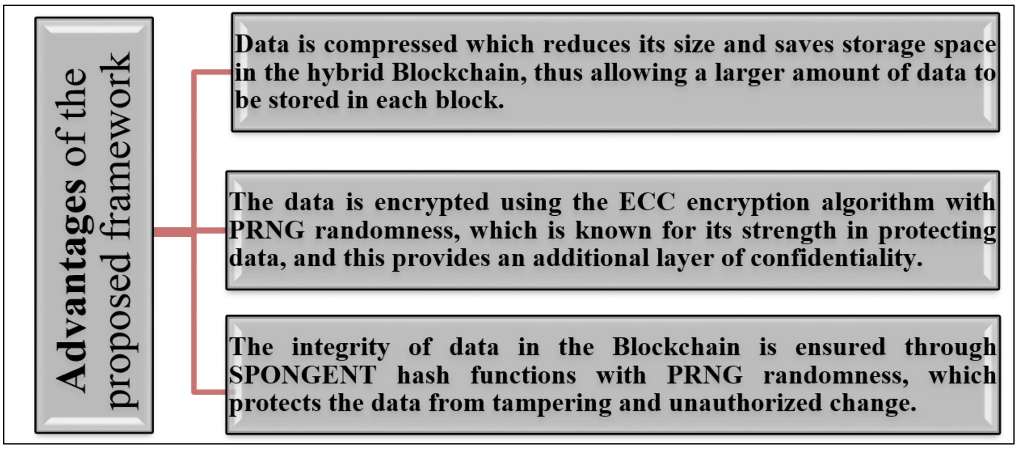

Start
Divide the data into small blocks
For each block
Compress the block using the LZ77 algorithm
Using PRNGs
Encrypt the compressed part using the ECC and the public key
Store the encrypted block in the Blockchain
Using the integrity of the data in the hybrid Blockchain
Using PRNGs
SPONGENT
If the data is valid
Yes
No
Retrieve the encrypted block from the hybrid Blockchain
Decrypt the block using the private key and PRNG
Decompress the block using the LZ77 algorithm
Reconstruct the original data
End

Figure 2. Workflow steps of the proposed framework



Advantages of the proposed framework

Data is compressed which reduces its size and saves storage space in the hybrid Blockchain, thus allowing a larger amount of data to be stored in each block.

The data is encrypted using the ECC encryption algorithm with PRNG randomness, which is known for its strength in protecting data, and this provides an additional layer of confidentiality.

The integrity of data in the Blockchain is ensured through SPONGENT hash functions with PRNG randomness, which protects the data from tampering and unauthorized change.

Figure 3. Advantages of the proposed framework

5-Results and Analyses

In this section, the evaluation and assessment of the proposed framework will be presented, where the analyses rely on two main aspects, the performance evaluation and the security analysis, as clarified next.

5.1-Performance results

Comprehensive performance analysis for all the algorithms in the suggested framework, Figures 4, 5, 6, 9, 10, 11, 12, 13, and 14 shows algorithms implementations. The working environment was based on the Java language within the Ubuntu 20 system, the processor speed is Intel (R) Core (TM) i5-2540M CPU @ 2.60 GH, the RAM is 16 GB and the system type is 64-bit. We run all the algorithms of the proposed framework 50 times to evaluate them thoroughly. Figure 4 shows the implementation of the ECC algorithm to evaluate the encryption and decryption operations. We notice from Figure 4 that the encryption operations (0.015 ns) require more time to execute than the decryption operations (0.012 ns).

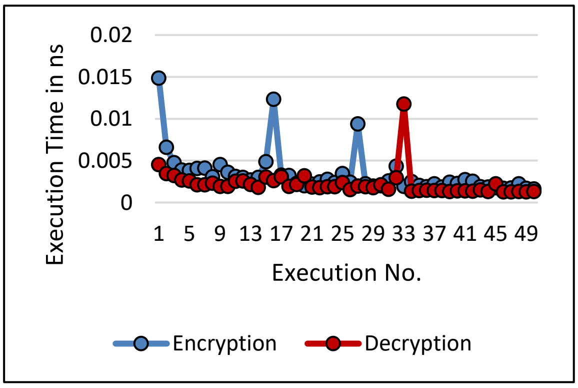


Figure 4. Evaluation of ECC algorithm

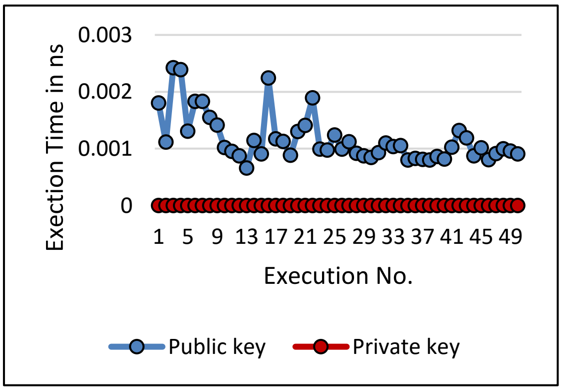
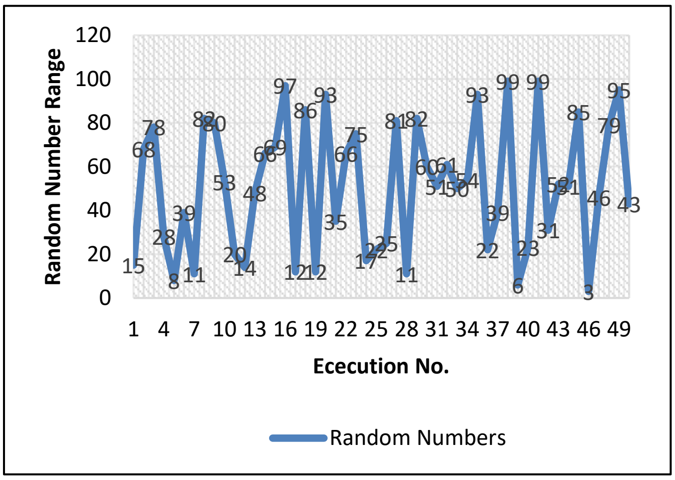


Figure 5. Exection time evaluation for ECC keys

Figure 5 shows the execution time for generating public and private keys for the ECC algorithm. We note that the public key requires more execution time than the private key because the key needs to perform point multiplication in ECC.

Figures 6 and 7 are an evaluation of the performance of the PRNG algorithm. Figure 6 shows the range of random numbers that can be obtained during each execution, while Figure 7 shows the execution time for fifty times for the PRNG algorithm. We note from Figure 7 that PRNG does not consume much time to generate randomness.



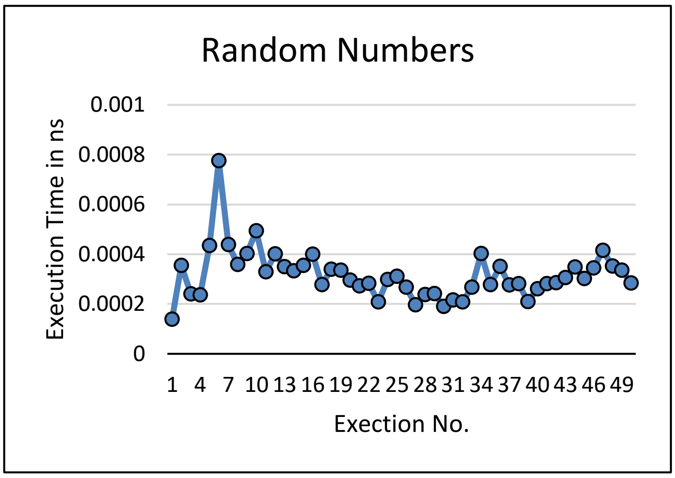
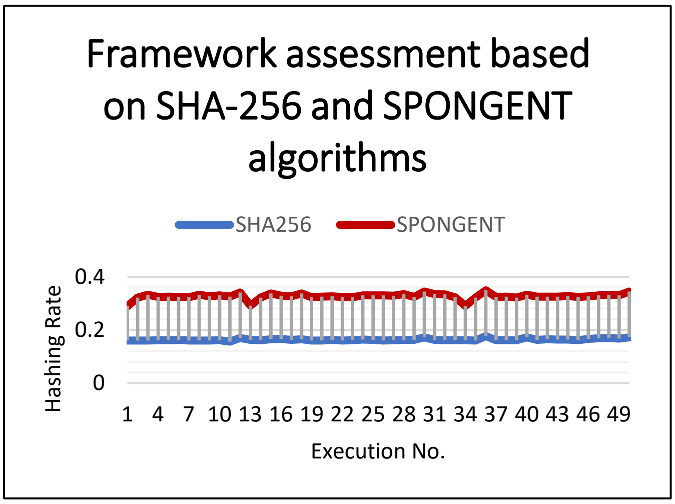


Figure 6. PRNG evaluation of random range numbers

Figure 7. Exection time for PRNG

We also evaluated hashing algorithms to demonstrate the advantage of SPONGENT256 and the importance of including it in the framework. Figure 8 shows the hash rate of the SHA256 and SPONGENT256 algorithms in each implementation. We note that the SPONGENT256 algorithm achieves better hash rates than SHA256. Also, Figure 9 shows the implementation of each hash function for SHA256 and SPONGENT256. From the figure, the performance of SPONGENT256 is better than SHA256 because SPONGENT256 performs lightweight operations compared to the SHA algorithm.



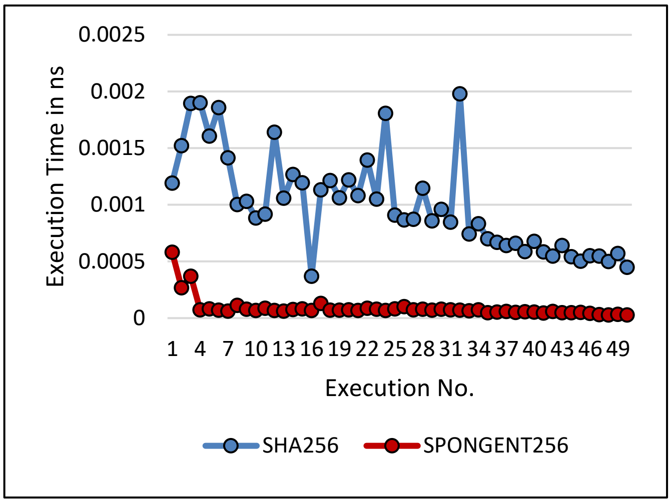
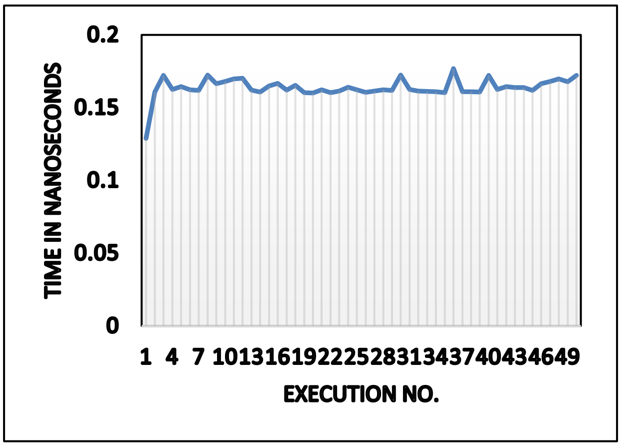


Figure 8. Performance of SHA and SPONGENT rates **Figure 9. Execution time for hash functions**

Figures 10 depict the time it takes for the Blockchain to create a block. Where the time it takes to was between 0.12 ns and not more than 0.18 ns which is considered quite good with such a system. Figure 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 on the encryption and decryption operations in the ECC algorithm.



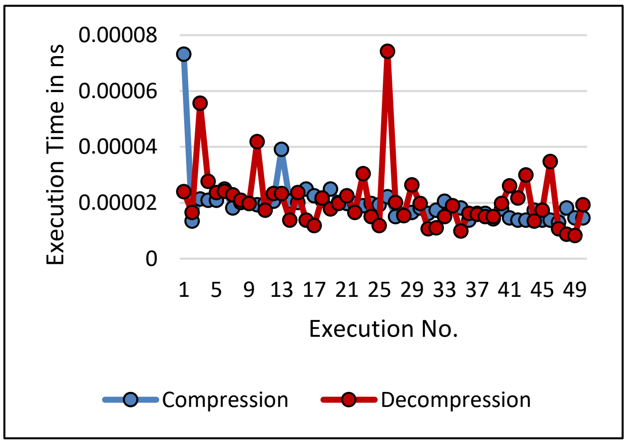


Figure 10. Blocks time interval in nanoseconds **Figure 11. Execution time for LZ77 algorithm**

Finally, Figure 12 shows the full performance of the proposed framework with encryption and decryption operations for both SHA256 and SPONGENT256, as each implementation includes ECC (encryption or decryption), hash (SHA256 or SPONGENT256), PRNG, LZ77 (compression or decompression) and Block. It is clear from Figure 12 that the proposed framework with SPONGENT256 is better for encryption and decryption than SHA256.

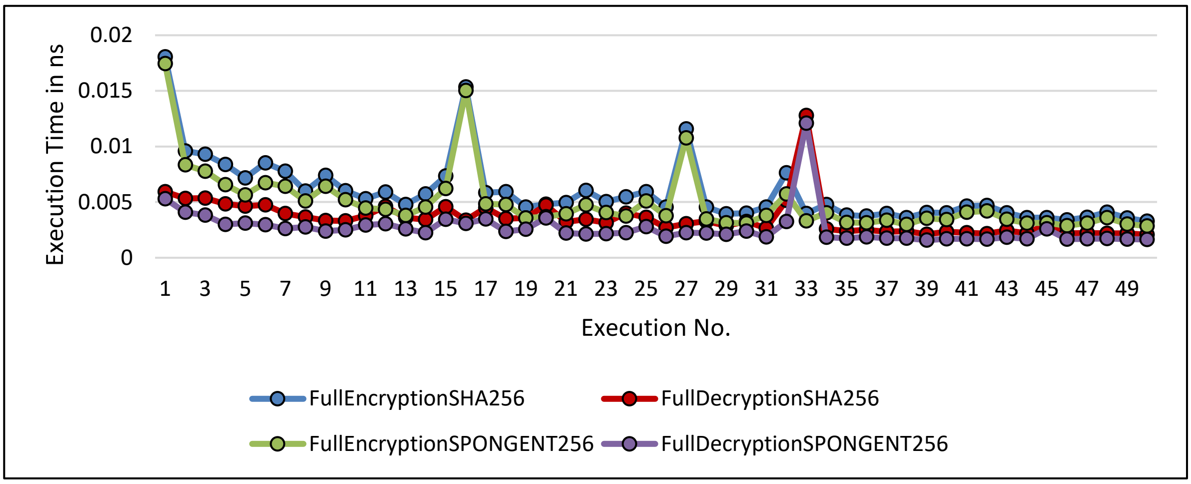


Figure 12. Full performance analysis of the proposed framework with both SHA256 and SPONGENT256

5.2-Security analysis

This section provides a security analysis of the proposed framework against recent ransomware attacks.

5.2.1- Ransomware attacks

- **Crypto**

  These attacks target the victim's files and encrypt them using a strong encryption algorithm. After the files are encrypted, the victim is presented with a message asking the user to pay a ransom to obtain the decryption key that restores the files to their original state. These attacks are very common and may affect ordinary users and businesses alike. In the proposed framework, we avoid these attacks by using the ECC encryption algorithm, as it is difficult to decrypt the user's data files, whether a client or an administrator, and thus the data is secure and cannot be hacked.

- **Lockers**

  Locker ransomware attacks generally target the victim's device. These attacks lock down all or part of the system, preventing access to files and content stored on the targeted device. When the attack is carried out, the victim is presented with a locked page requiring them to pay a ransom to unlock the system and regain access. To obtain the ransom, the victim is directed to specific payment methods, usually requesting payment in untracked digital currencies (such as Bitcoin) as they are difficult to track. In the proposed framework, we counter these attacks by using Blockchain technology to create encrypted backups of data. These copies are distributed across the decentralized network and are available for recovery in the event of a ransomware attack.

- **Scareware**

  Scareware is the term for malicious software designed to instill fear and panic in its users. Typically, they are portrayed as fraudulent security software alerts and warnings that demand large payments from customers to obtain the program or resolve the said issues. The primary objective is to steal financial and personal data from users and swindle them. To prevent Scareware attacks that try to deceive users into doing undesirable things, the framework uses SPONGENT256 to offer a trustworthy and unchangeable record of transactions and data.

- **Cerber**

  This kind of ransomware encrypts the victim's device's files and requests payment for their decryption (often in the form of cryptocurrencies like Bitcoin). Cerber can interrupt systems and cause data loss, and it targets both companies and regular consumers. The framework employs the PRNG with SPONGENT256 to thwart Cerber assaults. For every encrypted file, a distinct digital signature can be generated using the SPONGENT256 method. As a result, SPONGENT256 with high randomness can be used to confirm that files have not been altered during transport and to check their integrity after downloading.

- **RaaS**

  It refers to a business strategy that makes it possible for hackers to buy or rent ransomware and utilize it in their intrusions. It implies that ransomware tools and procedures are now available to hackers without requiring them to be developed from scratch, increasing the quantity and complexity of attacks. RaaS assaults are less likely since the technology is dispersed and decentralized, which keeps systems and data from being concentrated in one location. Hybrid Blockchain makes it harder for hackers to access and encrypt all of the data since it distributes and stores the data over several networked devices. The proposed framework uses hybrid Blockchain and randomness public key encryptions to interface with RaaS assaults.

- **Leakware**

  It refers to a particular kind of attack that seeks to reveal or makes threats to reveal private or sensitive information about people or organizations. If a ransom is not paid, victims can be blackmailed by having their information sold to outside parties or made public. All information stored on blocks or even in repositories is fully protected in the proposed framework by encrypting all this data and then applying a hash to all the encrypted data, which makes it very impossible for an attacker to penetrate users' devices.

5.2.2- Security comparisons

In this section, we will illustrate the issue of security in the context of hybrid Blockchain, specifically within the proposed framework. It relies on the use of PRNG randomness, LZ77, hash function (SPONGENT256), and public key encryption (ECC256) to enhance the security of the system. The use of the proposed hybrid Blockchain provides data distribution between private and public sectors, which increases the security of the framework. Table 2 below shows some security comparisons between the proposed framework and the approaches of previous studies ([10], [12], and [14]) in terms of repelling ransomware attacks.

Table 2. Attack comparisons

Attacks	MSCCBT-SIM [14]	P2M-Sec [12]	Crypto-Tile [10]	Proposed framework
Scareware	Weak	Middle	Middle	Strong
Cerber	Middle	Good	Strong	Strong
RaaS	Weak	Weak	Weak	Strong
Leakware	Middle	Strong	Middle	Good
Crypto	Strong	Middle	Good	Strong
Lockers	Good	Middle	Weak	Strong

6-Conclusion

The establishment of a framework offering a solution for safe and effective data management is a requirement for every organization that uses an e-app. Also, ransomware attacks have become common and are carried out against applications that use sensitive data, such as e-banking, e-health, e-agricultural, etc., to gain financial benefits. In this paper, we proposed a framework that provides high performance and security against modern ransomware attacks. The utilization of public-key encryption algorithms (ECC), hash functions (SPONGENT), and high randomness support the security issue in the data repositories. On the other hand, a hybrid Blockchain is used to manage the storage of this kind of data. The usage of a hybrid Blockchain is highly appropriate since it provides our framework with the capability of sharing data between the public and private sectors while storing this data in repositories. This paper discussed assault analysis such as scareware, certber, ransomware, leakware, RaaS, and lockers. As a result, our framework provides a balance between performance and security. During the performance analysis, we will conclude that our framework with SPONGENT256 provides the best performance of the SHA256. Also, through security analysis and comparisons with previous studies, we conclude that our framework is capable of repelling ransomware attacks within our research field. To develop this framework in the future, we intend to expand the analysis of ransomware attacks further. Furthermore, we intend to analyze different signature algorithms.

REFERENCES

[1] P. Kietzmann and T. C. Schmidt, "A Guideline on Pseudorandom Number Generation (PRNG) in the IoT," *ACM Comput*, vol.54, no. 6, 2021, doi: 10.1145/3453159.

[2] S. A. Yousiff, R. A. Muhajjar, and M. H. Al-Zubaidie, "Designing a Blockchain approach to secure firefighting stations based Internet of Things," *Informatica*, 47(10), 2023.

[3] L. Vishwakarma, D. Das, S. K. Das and C. Becker, "SmartGrid-NG: Blockchain protocol for secure transaction processing in next generation smart grid," *ACM International Conference Proceeding Series*, pp. 174 - 185, 2024, doi: 10.1145/3631461.3631554.

[4] M. K. Hasan, A. Alkhalifah, S. Islam, N. B. M. Babiker, A. K. M. Ahasan Habib, A. H. Mohd Aman, and Md. A. Hossain, "Blockchain technology on smart grid, energy trading, and Big Data: Security issues, challenges, and recommendations," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 26, 2022, doi.org/10.1155/2022/9065768.

[5] T. Koshiba, B. Zolfaghari and K. Bibak, "A tradeoff paradigm shift in cryptographically-secure pseudo-random number generation based on discrete logarithm," *Journal of Information Security and Applications*, *73*, 103430, 2023.

[6] A. Alabdulatif, I. Khalil and M. Saidur Rahman, "Security of Blockchain and AI-empowered smart healthcare: Application-based analysis," *Applied Science*, 12(21), 11039, 2022.

[7] P. Thantharate and A. Thantharate, "ZeroTrustBlock: Enhancing security, privacy, and interoperability of sensitive data through ZeroTrust permissioned Blockchain," *Big Data and Cognitive Computing*, *7*(4), 165, 2023.

[8] T. Kang, N. Woo and J. Ryu, "Enhanced lightweight medical sensor networks authentication scheme based on Blockchain," *IEEE Access*, vol. 12, pp. 35612 - 35629, 2024.

[9] C. Avula Gopalakrishna and P. I. Basarkod, "An efficient lightweight encryption model with re-encryption scheme to create robust Blockchain architecture for COVID-19 data," *Transactions on Emerging Telecommunications Technologies*, *34*(1), e4653, 2023.

[10] P. Nannipieri, L. Crocetti, S. Di Matteo, L. Fanucci and S. Saponara, "Hardware design of an advanced-feature cryptographic tile within the European processor initiative," *IEEE Transactions on Computers*, pp. 1-14, 2023, doi: 10.1109/TC.2023.3278536.

[11] 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.

[12] P. Wortman, W. Yan, J. Chandy and F. Tehranipoor, "P2M-based security model: security enhancement using combined PUF and PRNG models for authenticating consumer electronic devices," *IET Computers & Digital Techniques*, *12*(6), 289-296, 2018.

[13] L. Vishwakarma, A. Nahar, and D. Das, "LBSV: Lightweight Blockchain security protocol for secure storage and communication in SDN-enabled IOV," *IEEE Transactions on Vehicular Technology*, *71*(6), 5983-5994, 2022.

[14] U. Padmavathi and N. Rajagopalan, "Blockchain-enabled emperor penguin optimizer-based encryption technique for secure image management system," *Wireless Personal Communications*, *127*(3), 2347-2364, 2022.

[15] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications" *Security and Communication Networks*, 2019, 2019, doi: 10.1155/2019/3263902.

[16] B. Mouad and H. Abdellatif, "Performance evaluation of orange Pi 4 in SHA256 computation for Blockchain mining," *In 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud)*, IEEE, pp. 236-241, August 2023.

[17] S. E. Abed, R. Jaffal, B. J. Mohd and M. Al-Shayeji, "An analysis and evaluation of lightweight hash functions for Blockchain-based IoT devices," *Cluster computing*, 24, 3065-3084, 2021.

[18] Y. Huang, J. Mu, Y. Wang and R. Zhao, "A Review of Authentication Methods in Internet of Drones," *In 2023 International Conference on Networking and Network Applications (NaNA)*, IEEE, pp. 7-12, August 2023.

[19] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "REISCH: Incorporating lightweight and reliable algorithms into healthcare applications of WSNs," *Applied Sciences*, 10(6), 2007, 2020.

[20] W. 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*, 4(2), 71-89, 2024.