Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Dependable Concealing Algorithm of E-apps Repositories Combined with a Robust Blockchain Approach

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

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

[a]*Email: mishall_zubaidie@utq.edu.iq*

Abstract

Managing repository data, whether in terms of security or storage, especially if the data is vast, is thought to be a necessary and crucial problem given the great and quick evolution occurring in the field of technology and the growth in data volume that is dealt with on a daily basis. Thus, we designed an approach in this study that offers storage/repository management in addition to security. Whereas the Whirlpool function and elliptic curve integrated encryption scheme (ECIES) support the security problem in our proposed approach. Furthermore, our approach's security methods are supported by the fast deterministic random bit generator (DRBG). To handle storage for this kind of massive data, a hybrid Blockchain is used to regulate the repository storage. The data is vulnerable to loss or intrusion whether it is stored in databases or using any other conventional centralized technique. As a result, the hybrid form of Blockchain has been determined to be quite suitable for our approach as it allows data distribution across both private and public domains. Upon examination of the suggested approach, it effectively tackled the defense against assaults like Petya, GandCrab, Doxware, SamSam, CryptoWall, and Locky. Furthermore, the lightweight Whirlpool and ECIES findings showed that our approach's performance analysis was highly successful. Based on the result of performance analysis which clarified that the time it takes for the Blockchain to generate a block is believed to be reasonably suitable, ranging from 0.12883 ns to a maximum of 0.1768577 ns. Moreover, the encryption execution time ranged between 0.017 ns and 0.0028 ns. Finally, the decryption execution time was between 0.0053 ns and 0.0016 ns. Therefore, we acquired an efficient approach for data repository administration and control, security, and performance.

Keywords: Big repository data management; ECIES cryptography; DRBG; hybrid Blockchain; Whirlpool function

Citation: M. Al-Zubaidie, D. H. Tahayur, W. A. Jebbar, and R. H. Razzaq, "Dependable Concealing Algorithm of E-apps Repositories Combined with a Robust Blockchain Approach", ARIS2-Journal, vol. 4, no. 2, pp. 32–56, Dec. 2024.

DOI: https://doi.org/10.56394/aris2.v4i2.48

---

* Corresponding author. Email address: mishall_zubaidie@utq.edu.iq

1. Introduction

The benefits and drawbacks of Blockchain/Big Data, the dangers of current attacks involving ransomware in electronic applications, and the significance of our field of study are all presented in this section to help readers develop a thorough and understandable understanding of our subject. These points will be further elaborated upon in the subsections that follow.

Blockchain technology is an evolutionary tool that improves the quality of any system. By providing security, reliability, privacy, and interoperability, this is achieved. The basic idea behind Blockchain is that, unlike a single individual or entity, a vast network of linked computers acts as an electronic record-keeper, known as a ledger, to securely record transactions in an irreversible and impenetrable manner [1]. Big medical data, banking data, agricultural data, or any other type of data is stored securely in the decentralized and immutable ledger of Blockchain technology, which also protects it from attacks that might compromise the integrity of the data [2]. Since the ledger's data is protected against cryptographic characteristics like hashing, electronic signatures, and asymmetrical keys, it cannot be altered [3]. Transparency in the system is further increased by the fact that every Blockchain user will be informed of any slight modifications made to the information exchange due to the decentralized nature of the ledger. Blockchain technology with e-transaction is shown in Figure 1 along with how it is used in electronic applications like e-banking, e-health, electronic agriculture, etc.

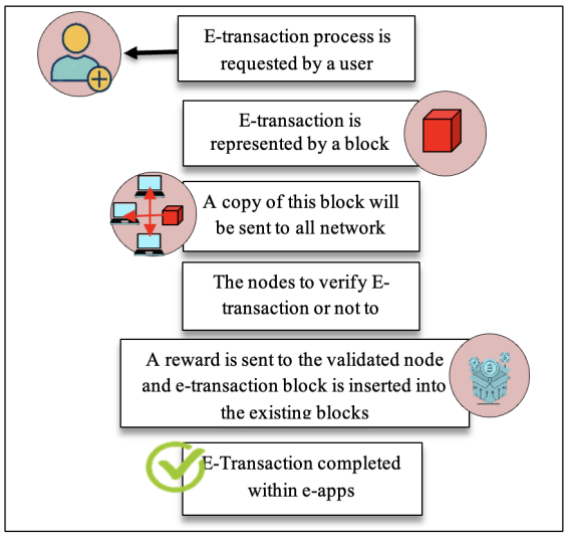


Figure 1: Blockchain mechanism in e-transaction

Table 1 enumerates the various forms of the distributed ledger, including public, private, hybrid, and consortium, while explaining the works of Blockchain.

Table 1: Blockchain categorization

Type of Blockchain	Illustration
Public	The main reason this type of Blockchain is independent is that anyone with an internet connection can utilize it since it is unrestrictive and does not require authorization to access. Open Blockchain technology powers the majority of cryptocurrencies.
Private	It is a kind of distributed ledger that is controlled by a single entity, is limited and needs permission to access. The only people who can access this kind of Blockchain are authorized users.
Hybrid	This type of Blockchain blends public and private components, with some parts under the control of a particular organization and the rest accessible to everyone. While some system components do not need authorization, others must.
Consortium	Wherein certain parts are private and some are public, but they may be regulated by many groups. Decisions regarding network, development, and upgrades are made collectively by consortium members.

Despite all of its benefits, Blockchain technology has some drawbacks that should be taken into account. Here are some of its flaws and vulnerabilities:

- **Issues of the mining process**: A significant quantity of energy and resources are lost during the mining process [4]. Every node on the Blockchain takes part in the proof of work, or the block-mining process that creates the blocks.
- **Issues of storage**: The volume of aggregate data on the Blockchain might surpass the volume of hard disks that are accessible at some point. As more people utilize the system, more data will be generated. Thus, upgrading the hard disk space of the system will also be required.
- **Issues of unchangeability:** The information stored on the Blockchain is immutable. This data cannot be modifiable if something goes wrong during creation.
- **Issues of scalability**: Since every block in the Blockchain has a limited amount of data, its size cannot be extended. This means that, for electronic transfer activities, for instance, which depend on the trustworthiness of every network block, the transfer process could grow extremely long and laborious.

Blockchain technology is undoubtedly the way of the future. There is, however, a need to be conscious of its disadvantages.

The amount of data that is readily available has increased significantly in the modern period; this data is referred to as "Big Data" or "Big Information." There are numerous obstacles and issues that must be addressed as the amount of data grows. Among the most significant issues with using big data are security and privacy [5, 6]. When dealing with sensitive data, such as banking information, agricultural documents, patient records, etc., maintaining confidentiality and guarding against unwanted access is crucial [7]. Apart from security and confidentiality, big data also has challenges with integrated data management and seamless integration with current systems. Blockchain technology can effectively address these issues by enabling access integration gateways with current

systems, such as electronic applications. Systems like healthcare systems deal with a multitude of big data formats, including electronic devices for remote tracking, patient records, and data that may be shared across physicians in the system [8]. Therefore, it is deemed essential to acquire and develop a comprehensive strategy that offers protection, data management, and monitoring. Hash functions and cryptographic algorithms in conjunction with Blockchain access-based systems will achieve the objective of delivering a full strategy that incorporates both security and handling storage professionally [9]. Blockchain technologies are an evolutionary technique that offers systems with security and authority. In order to effectively balance compliance, privacy, and security, Blockchain technology can provide data security and guard against hacking or tampering. This helps to create a dependable and secure environment for exchanging and managing enormous amounts of sensitive data/repositories. This necessitates focusing efforts on creating Blockchain-based approaches and standards and promoting them through cooperation between institutions and stakeholders. 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 [10,11].

Since ransomware attacks have been more frequent recently, there are a variety of concerns connected to the growing number of ransomware attacks that are known as ransomware attack risks. Computer attacks known as "ransomware" target systems and data, encrypt them to prevent users from accessing them, and then demand a ransom to unlock the encryption and allow users to access the data [12]. Attacks using ransomware have increased in frequency over the past few years, posing a serious threat to individuals, companies, and organizations everywhere. These hazards include the potential loss of confidential information, interruptions to services or systems, negative impacts on key business operations and productivity, significant financial losses, and risks to information security and privacy [13, 14]. "Risks of recent malware attacks" describes the threats and perils posed by recent attacks by ransomware on systems and networks. Cyberattacks known as "ransomware" occur when networks and computer systems are breached, files are encrypted, and the attacker then wants a ransom—typically in the form of cryptocurrency like Bitcoin—to unlock and restore the contents. These assaults are considered to be among the most dangerous and serious hazards that people and businesses confront in the world of technology because they have the potential to cause systems to crash, lose data, and lead to major financial losses [15, 16, 17]. Attacks using ransomware present a number of risks, including the loss of private information, breaching of infrastructure and services, jeopardizing security and confidentiality, and negatively impacting the finances and reputation of the targeted businesses [18]. People, companies, and organizations in large numbers have been the victims of this type of attack. Numerous issues have been raised by recent ransomware attacks [15].

1.1. Significance of Approach Investigation

The significance of our study stems from the need to manage the massive amounts of data produced by e-apps like e-banking, e-health, e-agriculture, etc. When we talk about handling huge data, we are talking about repository storage security. This data is open to loss and attacks as long as it is available online. Additionally, as long as data is being generated at a rising rate and large data is stored using traditional ways that have risks and challenges, Blockchain, big data, and critical ransomware attacks may occur. By bringing these flaws and challenges to light, individuals and groups may grow aware of potential problems and develop strategies and solutions to address them. It can be improved and overcome with the use of knowledge about potential limitations of Blockchain, such

as repository capacity and scalability, mining challenges, and the inability to edit input data. Understanding the challenges associated with privacy, security, compliance, and data governance when it comes to big data can aid in the development of effective strategies to protect sensitive information and guarantee that it is compliant with applicable laws and regulations. In order to handle these kinds of data, we therefore proposed this method for managing repository storage as well as security. Understanding the risks associated with ransomware attacks and how they impact sensitive data, systems, and services improves security and protection and aids in creating strategies to thwart and neutralize these attacks. In general, research with a focus on flaws and challenges can help to improve systems and technology and offer practical solutions to potential problems. Additionally, this research can assist companies and people in protecting their data from potential threats.

1.2. Main Contribution of the Proposed Approach

- The study strategy incorporates security and administration of big data storage. The security aspect of the strategy is supported by proposing of public-key encryption techniques like ECIES, hash functions like Whirlpool, and generators of random numbers like DRBG to integrate in a lightweight proposed approach.
- Data distribution and control with hybrid Blockchain data are 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 Whirlpool algorithm to support block security in e-apps.
- The recommended approach was looked at in order to combat and manage potential security risks including Petya, GandCrab, Doxware, SamSam, CryptoWall, and Locky. To demonstrate our proposal's potential to fend off current threats, we also present security analysis and comparisons between it and earlier approaches.

2. Literature Review

This section will provide an overview of earlier research, including the benefits and drawbacks of the approaches used.

Gope et al. [4] suggested a distributed Internet of Things system design. Then, they provide an anonymous authentication system that can guarantee a number of noteworthy characteristics, including sensor intractability, anonymity, and resistance to replay and clone attacks. Functions, or PUFs, serve as a means of distinguishing individual ICs from counterfeits. However, there are no details in this study about how the authentication process is held, and the authors never mention how the proposed system faces the different types of attacks. Lee et al. [13] proposed a scheme to enhance the security of IoT devices by tagging crucial data from IoT devices with random variables during the information transmission and reception procedures, they mentioned that the suggested technique increased the security of IoT devices. Moreover, joint probability was used to connect the data from IoT devices to which random variables were allocated. But in this study, there is no actual comparison of this system with the other previous systems held, even in the conclusion, they mentioned that in the future they will add a real comparison with the actual systems, thus the claim that the proposed system increases the security is considered not reliable, furthermore, there is no attention paid to the aspects of speed or the accuracy. Tooska et al. [14] presented the first scientific classification of the basic features of ransomware and linked them to the stages of the cyber kill chain. They also presented a parallel classification of the steps of defense against

ransomware (Courses of Action matrix) as a defense model directed using intelligence information. Despite these contributions, they faced some challenges, such as how to apply the proposed classification in practice to detect and deter ransomware attacks in the early stages.

Zeeshan et al. [1] suggested a deep learning-based system to identify distracted driving behavior using a network of convolutional neural networks (CNN). A Blockchain-based multimedia transaction that is safe and impenetrable. Blockchain technology and deep learning combined to identify and convey driver behavior. The suggested CNN-based system was trained using the State Farm inattentive motorist detection dataset. To ensure tamper-proof transmission of multimedia information (video) across the Blockchain, extract hashes using the SHA-256 method. On test data, the suggested CNN-based algorithm outperformed current state-of-the-art techniques with an accuracy of 86.02%. Deep learning and Blockchain computing work together to offer a safe, unchangeable way to identify and share driver behavior. Vilmurugadas et al. [2] created a brand-new approach for keeping an eye on operations and data repositories in cloud environments with software-defined networks (SDNs). There are one hundred mobile IoT nodes in the approach. Activate the flow switch. Controllers based on Blockchain. Authentication Server (AS) is depend on a cloud server detective. After registering with the Authenticity Server (AS), used Harmony Search Optimization (HSO) to retrieve the secret key. Before being sent to the cloud server, information packets from the mobile devices are encrypted using the ECIES method. SHA-256 encrypted hash method is used by the SDN controller to maintain the Blockchain, which stores user signatures and aggregated evidence. A certified investigator is capable of utilizing the Logical Graph of Evidence (LGoE) for identification, evidence collecting, analysis, and report creation using the SHA-256 encrypted hash algorithm. A certified investigator is capable of utilizing the Logical Graph of Evidence (LGoE) for identification, evidence collecting, analysis, and report creation. To show how well the system performed in relation to response time vs user count, the researchers created graphs. The ratio of users to the time it takes to enter evidence. The results of the experimental research showed that the suggested system outperformed the others in terms of accuracy, response time, productivity gain, and overall security parameter modification. Al-Sammak et al. [3] suggested privacy-preserving Blockchain-based approaches for Internet of Things (IoT) big data users. There are three suggested algorithms in the model: 1) To distribute data across all users. 2) To carry out the process of finding data. 3) To confirm the interaction process, they presented a mechanism that secures crucial and potentially private user data on the distributed Blockchain. The Blockchain's size is managed to transfer non-sensitive data to the platform. The suggested Blockchain system offers outstanding Byzantine fault tolerance, as demonstrated by experiments. The ultimate experimental outcomes proved that the algorithms successfully satisfied the performance requirements. They suggested a Blockchain-based strategy to allay large data consumers' worries about security and privacy in Internet of Things-based smart city applications. As part of this approach, they created three algorithms, and they reported on successful experimental outcomes in terms of tolerance for faults and speed.

Abass et al. [7] suggested a way to "ratify text" to resist spy attacks closely. Their method includes the use of "camouflage" letters and the virtual keyboard, which leads to the creation of strong and easy-to-remember passwords. However, their study needs to develop a safety method that has no complexity in the algorithm or the need for special devices, which increases the need to develop a safe entry method. Nannipieri et al. [10] suggested that a series of hybrid cryptographic accelerators called "Crypto-Tile" be designed and put into operation using

the European Processor Initiative (EPI) project methodology. The goal of the EPI project was to create the first completely low-consumption processor family in Europe, catering to the demands of high-performance computing, big data, and the automotive sector. Crypto-tile accelerators are specific to a family of cryptographic algorithms that may perform symmetric encryption, public key encryption, plateau computing, random number generation, and post-quantum encryption. Their idea could have trouble meeting the necessary certification and security requirements, particularly since the industry demands that important safety factors be taken into consideration. Kang et al. [8] proposed to implement an authentication approach based on Blockchain technology to protect the credibility and integrity of patient data. An improved protocol has been developed aimed at overcoming the security issues associated with this area. The challenge was identified that there is a single point of failure in the traditional system used in wireless sensor networks for medical care, which negatively impacts data availability and security. 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 approach may face privacy issues and weaknesses in generated randomness and performance overhead. The existing approaches in [19]-[24] all suffer from the weakness and resistance of Blockchain attacks. Sulaiman et al. [25] proposed the use of the SEIAR partition model to model the dynamics of cybercrime attacks on connected devices on the server, as well as the use of numerical solutions using the BLMA and LMA algorithms to calculate the proposed solutions for the model. They faced some challenges that they could not fully solve, such as not providing full details on how to apply the SEIAR model to real cybercrime attack scenarios, the model and the proposed solutions were not tested on real data or more realistic simulation data, and other challenges.

3. Background Data on Security Technologies and Blockchain

This section deals with basic concepts about the proposed approach.

3.1. Blockchain Concept

Blockchain is a decentralized network designed to store and safeguard data. Its method of operation involves building a series of blocks, each of which uses mathematical hashing techniques to include data related to the blocks before it. Because Blockchain is dispersed among numerous network-connected devices, it is impervious to manipulation and attack. Blockchain technology offers a high degree of security and accelerates systems with many interconnected nodes since it removes the need for third parties and allows for peer-to-peer process execution [2]. A Blockchain is a database consisting of linked chains of blocks. This technology is notable for a number of key features, such as decentralization, security, and transparency. Blockchain data is permanently kept, cryptographically secured, and publicly accessible with challenging alterations. By default, it uses a SHA256 hash to guard against block data modification. Blockchain is frequently employed in electronic projects and applications, such as document management, banking, supply chains, healthcare, and agriculture. Without a dependable central authority to oversee or validate the data, records are kept, guaranteeing data integrity [4]. Standardized test procedures and untrustworthy test libraries present a problem to networked devices. Comprehensive research and analysis are required for Blockchain-based test repositories, and "proof of verification" must be applied to ensure repository administration and accomplish transparency, decentralized management, and security in the exchange and storing of digital data. Blockchain is used to store dispersed data and safeguard access to encrypted information [6, 8].

3.2. Big Data Concept

Big data refers to data types and quantities that are too complicated and vast for standard data sources. Three primary characteristics—volume, velocity, and variety—define big data [4]. Firstly, the volume describes the enormous amount of data generated and gathered from various sources, including social media sites, smart devices, detectors, hospitals, businesses, and other sources that contribute to this data. The second definition of speed is the speed at which data is created and sent. Massive and constant amounts of data are generated from a variety of sources, such as social networks with Internet connections, smart devices, and sensor data flow. It is crucial to deal with data in terms of storage management and system security support, provided that regular text data does not constitute the only type of data that needs to be handled. Other types of data include images, audio files, and video files. Using big data enhances understanding of events and makes decision-making more efficient in a variety of fields, such as marketing, commerce, science, medical, and agriculture. This enormous data set can be used to identify numerous informative trends, patterns, and relationships that are hidden by traditional research by using specialized methods and tools.

The public cloud environment, where data is stored on servers in the cloud through an open network path, is known as cloud computing. This cloud delivers information that is too big and complex for traditional technologies to assess and handle. Certain technologies and tools are required in order to store, retrieve, and evaluate enormous amounts of data. Within the context of electronic programs, "big data". This data contains a wide variety of information, such as text, images, audio, videos, geographic data, etc. E-apps generate vast volumes of data quickly by utilizing a range of data sources, such as social media, mobile devices, smart apps, detectors, and more. Certain instruments and techniques are required in order to properly save, retrieve, and assess this data. Big data makes it possible to extract links, patterns, and trends from data that are otherwise impossible to find with traditional analysis techniques. Furthermore, big data can be used in the electronics sector for a variety of purposes, such as improving application performance, user experience, marketing strategies, and helping with astute decision-making [4].

3.3. Hash Function Concept

Any kind of digital data, no matter how big or little, can be processed into smaller, fixed-size data pieces called hashes using a special formula called a hash function [19]. This hash acts as the fingerprint equivalent of the input. Figure 2 depicts a basic hashing procedure. The operation of it is then explained.

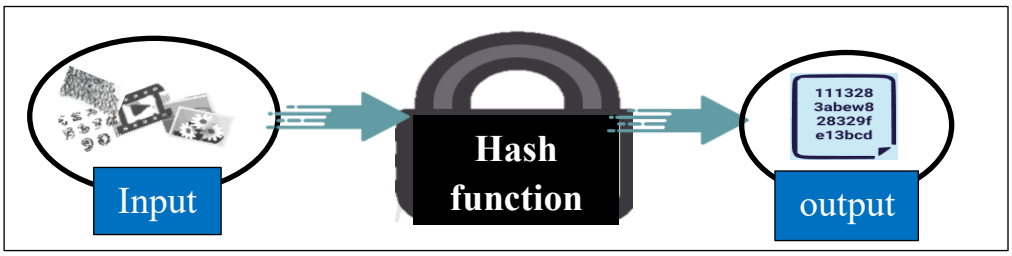


Figure 2: Hash function technique

Any kind of digital data, including numbers, text, images, and even movies, can be fed into a hash function. After that, what is entered will go via the hashing process, in which the function applies a mathematical

transformation to the entering data. The result is a fixed-length character string that functions as the original matrilateral's compressed version as well as a unique hash value. The hash function offers benefits and drawbacks of its own, much like any other method. A brief description of two of the more popular hashing functions follows.

3.3.1. SHA-256 Algorithm

The National Security Agency (NSA) created a unique variant of the SHA-2 algorithm [1]. Any type of electronic data, including communications and documents of any size, can be included. The procedure uses a complex mathematical algorithm to slice and blend data in a specific way. The outcome is the same information previously, but it is now represented by a distinct hash value of 32 bytes (256 bits) [20]. SHA-256 offers the following features:

- **Sensitivity to inputs:** A minor alteration in input causes a significant alteration in output. Because of this characteristic, it is challenging to alter data without clearly changing the hash value.
- **Scalability:** There are no problems or performance lags when using SHA256 on big input sizes. It is appropriate for applications handling high volumes of data because of this functionality.
- **Security:** Using a hash value to recreate the original data is extremely challenging, if not impossible. It is therefore a reasonably suitable function for maintaining data integrity. If there is data alteration, the hash will change and a warning will occur.
- **Commonly Used:** For a number of security applications, such as password protection and digital signatures—which verify the authenticity of communications or documents—SHA-256 is a popular choice. Hashed passwords can be used to securely store passwords and file verification—that is, to confirm that a file was downloaded and was not altered during transport. This is an alternative to keeping the password in plain text.
- **Flexibility:** SHA256 is applicable to a wide range of tasks, including file integrity checks, digital signatures, and cryptocurrency applications.

3.3.2. Whirlpool Algorithm

The cryptographic hash function Whirlpool was created by Paulo S. L. M. Barreto and Vincent Rijmen. It was among the five finalists in the NIST hash function competition, which saw the SHA-3 algorithm, now known as Keccak, chosen as the new standard [21]. Whirlpool is still regarded as a reliable cryptographic hash function even if it was not chosen. Whirlpool generates hash values in different sizes, offering 160, 256, 384, and 1n3 512 bits as options. The greater the defense against brute-force attacks, the bigger the hash size. Security was the main consideration in its design. It is immune to several cryptographic assaults because it has a robust internal structure with many rounds and a sophisticated mixing mechanism. Whirlpool is appropriate for a variety of cryptographic applications due to its high security features and reasonable computational performance [22]. Without compromising efficiency or security, Whirlpool can handle a broad range of input lengths, from brief messages to enormous data chunks. Whirlpool is still used in many security-critical applications, such as digital signatures, data integrity verification, and password hashing, even though its use is not as widespread as that of some other cryptographic hash functions, such as SHA-256. Table 2 provides a careful comparison between the SHA256 and Whirlpool algorithms.

Table 2: SHA256 and Whirlpool comparison

Feature	SHA256	Whirlpool
Safety	It is thought to be safe. It is very difficult to change the data and get the same hash value when using SHA-256.	It was also designed with security in mind, using a specific strategy to prevent vulnerabilities. However, because it is a more recent design than the well-known SHA-256, it might not have the same level of cryptanalysis (testing for vulnerabilities).
Efficiency	Despite being efficient, it could be slower and consume more resources than Whirlpool, especially on devices with little computing power.	It is quite effective. Owing to its purposeful compact and lightweight design, it functions effectively with devices that possess restricted power or processing capability.
Use	It is a well-liked option for many security applications, such as digital signatures, password protection, and file verification, because of its strong security and broad use.	Especially made to be used in situations with limited resources where effectiveness is crucial, like embedded systems and sensor networks.

The optimal SHA-256 and Whirlpool will depend on the user's particular requirements. SHA-256 is a great choice if security is the user's primary concern. While if the need is a rapid and efficient hashing solution for a device with limited resources, Whirlpool might be a better choice.

3.4. ECIES Encryption

It is a type of cryptography created by Curve N. Koblitz and Miller in 1985. They used an elliptical curve as their encryption technique. A public key and a private key are available to EVERY user or device utilizing ECIES. Public-key encryption comes in the form of ECIES [23]. The elliptic curve over which the ECIES mathematical operations are given is y2 = x3+ax+b, where 4a3+27b2 ≠ 0. An elliptic curve is produced for every value of 'a' and 'b'. A point on the curve represents a public key, while a random number represents a private key. The public key is obtained by multiplying the generator point G on the curve by the private key. The domain parameter of ECIES is composed of the generator point *G*, the curve parameters '*a*' and '*b*', plus a few other constants [24]. Algorithm 1 presents the ECIES encryption. The ECIES algorithm provides suitable security for electronic applications, and because it is a public key algorithm, it greatly supports scalability issues, which qualifies this algorithm to work in the security of large organizations.

Algorithm 1: Elliptic curve cryptography encryption

Input: Initialize parameters: ***P, N***, ***G, d, and m***

Where: ***P***: prime number that determine the size of the cryptographic keys and impacts the security level of the encryption scheme.

N: The number of times must be added *G* to itself in order to obtain the identity element.

G: It generates all other points on the curve through repeated addition. It should have prime order and be chosen carefully to avoid certain vulnerabilities.

d: Private key

M: message to be encrypted.

Output: Ciphertext (C_1, C_2)

Begin

1. **Generate a Private Key**: a random integer d such that $1<d< n$, which will be the private key.
2. **Compute Public Key**: Compute the corresponding public key Q as $Q=d\times G$, where × denotes point multiplication.
3. **Input Message**: Encode the message to be encrypted into a point M on the elliptic curve.
4. **Choose Randomness**: Generate a random integer k such that $1<k<n$.
5. **Compute Temporary Point**: Compute the temporary point $C_1= k \times G$.
6. **Compute Shared Secret**: Compute the shared secret point $S= k \times Q$.
7. **Compute Cipher Point**: Compute the cipher point $C_2 =M+S$ where + denotes point addition.
8. **Output Cipher**: The ciphertext consists of the pair (C_1, C_2).

End

3.5. DRBG Algorithm

An approach known as a deterministic random bit generator (DRBG) 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 DRBG execution is not completely random as it depends on a starting value (seed) that defines the generation sequence [1]. The DRBG 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 DRBGs, have short durations for certain beginning values, which makes it simple to anticipate the output of a DRBG. DRBG seeds can be produced using traditional methods, either through software or utilizing hardware. For software-based DRBGs, 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 [13].

4. Suggested Approach to Safe Repositories 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 approach's workflow is depicted in Figure 3.

4.1. Hybrid Blockchain as a Base

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 type of data where trust and data integrity are critical, as this type 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 reasons listed below: Providing security: This type of Blockchain provides the approaches and systems with high security because it combines characteristics of both public and private Blockchains.

1. **Work partitioning**: 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.
2. **Storage method:** Only the most crucial data is saved on a hybrid Blockchain; this data is composed of hashes and symbols that point to the real data 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.

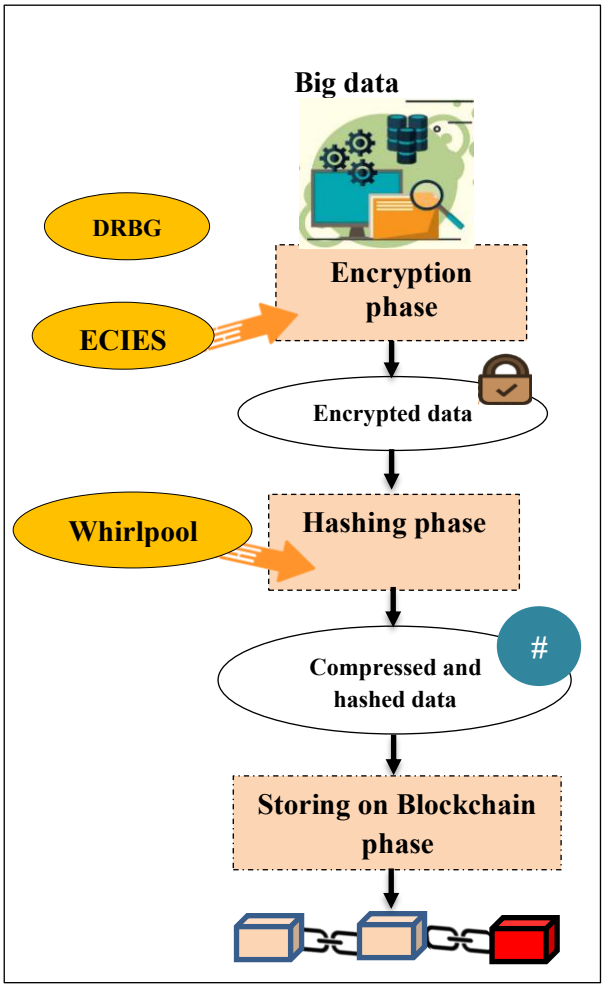


Figure 3: Proposed approach workflow

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 can 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, based on a seed value, pseudorandom number generators can accomplish the desired randomization by generating a random series of numbers. This is why, in our suggested method, we merged the DRBGs with Whirlpool, a kind of hash function, and the public key encryption represented by the ECIES described above. This allowed us to get a degree of unpredictability that is ideal for our suggested method. In our suggested method, we generate high randomness for the condensed message that comes out of the hashing process by using DRBG with Whirlpool. In addition, our method generates highly random private and public keys using DRBG and ECIES to enable robust Blockchain block encryption.

4.3. Utilizing Whirlpool to Secure Blocks

The lightweight Blockchain approach is a methodology for installing Blockchain in a lightweight and resource-efficient way, with the goal of improving the functionality and responsiveness of mobile Blockchains and environments 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 Whirlpool algorithm is one of the key components of our approach that may be used to achieve trustworthy integrity in a lightweight Blockchain solution. Whirlpool allows for the integrity storage of both transaction logs and data repositories on the Blockchain. To maintain data integrity before it is stored, the Whirlpool hashes can be employed twice—once for each block in a chain and once again for the data repository. Within the block, mixing, transformation, and deduction operations are used to achieve the required integrity. As a result, information is reliably and securely stored on the Blockchain; similar steps are then repeated for each new block. It was therefore selected as the block data integration algorithm.

4.4. Blocks Encryption

To use the lightweight hybrid Blockchain, the ECIES algorithm is used to encrypt blocks in the lightweight Blockchain. Blocks can be collections of huge data records or electronic application records. The block is converted to the appropriate format for data. Using other formats or converting the data to a bit format may be necessary at this point, depending on the requirements of the algorithm and the internal structure of the lightweight Blockchain. Our method generates randomness using DRBG before encrypting the data. Then, it leverages this randomness to generate private and public keys using the ECIES algorithm for each valid member of the network. The proposed 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. Compared to ElGamal and RSA, the cryptographic operations of the ECIES method use appropriate rapid encryption algorithms. In addition, compared to other key algorithms, the ECIES method generates relatively tiny keys (160, 192, 224, 256, 384, and 512 bits), which will minimize the amount of storage space needed for these keys. In our

approach, we choose the ECIES algorithm because it strikes a balance between solid security and performance overhead. Block data cryptography steps are illustrated in Algorithm 2.

Algorithm 2: Blocks encryption algorithm

Inputs:

- Public key of block ***K*** ← Public key… Where the key (160, 192, 224, 256, 384, or 512 bits).
- Private key of block ***P*** ← Private key …. Where the key (160, 192, 224, 256, 384, or 512 bits).
- ***D*** ← The big data desire to encrypt.

Outputs:

- ***X*** ← The encrypted blocks data.
- ***L*** ← The decrypted blocks data.
- ***H*** ← Hash value.

Start

1. **Keys creation using DRBG phase**
2. S ← **DRBG** seed
3. ***K*** ← S+ Random values generation (160, 192, 224, 256, 384, or 512 bits).
4. P ← S+ Random values generation (160, 192, 224, 256, 384, or 512 bits).
5. **Encryption and decryption phase:**
6. **D** ← The big data desire to encrypt.
7. ***X***← ECIES (***K***). (***D***) *as bytes*.
8. L← ECIES (P). (***X***) *as bytes.*
9. **Hash value calculation phase:**
10. ***H*** = Whirlpool Hash. Hash (***X***. **DRBG**)
11. **Data storing in the repository phase**:
    a. Storing ("Encrypted data: ", ***X***)
    b. Archive ("Decrypted data: ", ***L***)
    c. Archive ("Hash value: ", ***H***)

4.4. The Proposed Methodology for our Approach

This section will explain our proposed approach, which is based on the process of combining DRBG, Whirlpool hashes, the ECIES encryption algorithm, and LZ27 in a hybrid Blockchain-based environment. This type of combination ensures the system's confidentiality, integrity, security, privacy, simplicity of data transfer, and proper data management.

Initially, the LZ77 data compression method is used to minimize the size of sent data and save storage space in the hybrid Blockchain. The data is separated into small blocks, and the LZ77 method is applied to each one separately. Duplicate data is sought for and represented using reference statements, reducing the amount of data required in the hybrid Blockchain. The second step ECIES cryptography is used to ensure the safety and security of data exchanged via the Blockchain. Compressed data is encrypted using ECIES 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 disguise data on the Blockchain, so only those with the private key may decrypt it. This enables only authorized people to access the data. Following that, algorithms in the Blockchain ecosystem are coordinated in a harmonious manner. The compressed and encrypted data is combined with Blockchain Whirlpool hash routines to generate a hash set for each block. The Blockchain is signed using the Whirlpool message digest, which includes PRING to support robust hashes and ensure that the data has not been edited or modified.

Our proposed approach protects data stored on hybrid Blockchain technology by ensuring its authenticity and anonymity. Our strategy provides great efficiency in terms of performance, security, and privacy of information, dependability, ease of transmitting information, and anonymity. Data compression decreases storage space and increases access speed, while the ECIES encryption technique protects data from illegal access. We use Blockchain hash functions and digital hashing to maintain data security. Along with that, our hybrid Blockchain architecture facilitates data transfer. Only authorized parties can gain access to the Blockchain, obtain compressed data, and decrypt it with the private key. This simplifies and ensures data retrieval, hence boosting the methodology's productivity and overall experience for users. Figure 4 depicts the workflow processes of the suggested approach, whereas Figure 5 depicts the important characteristics of our proposed approach and the benefits of this strategy.

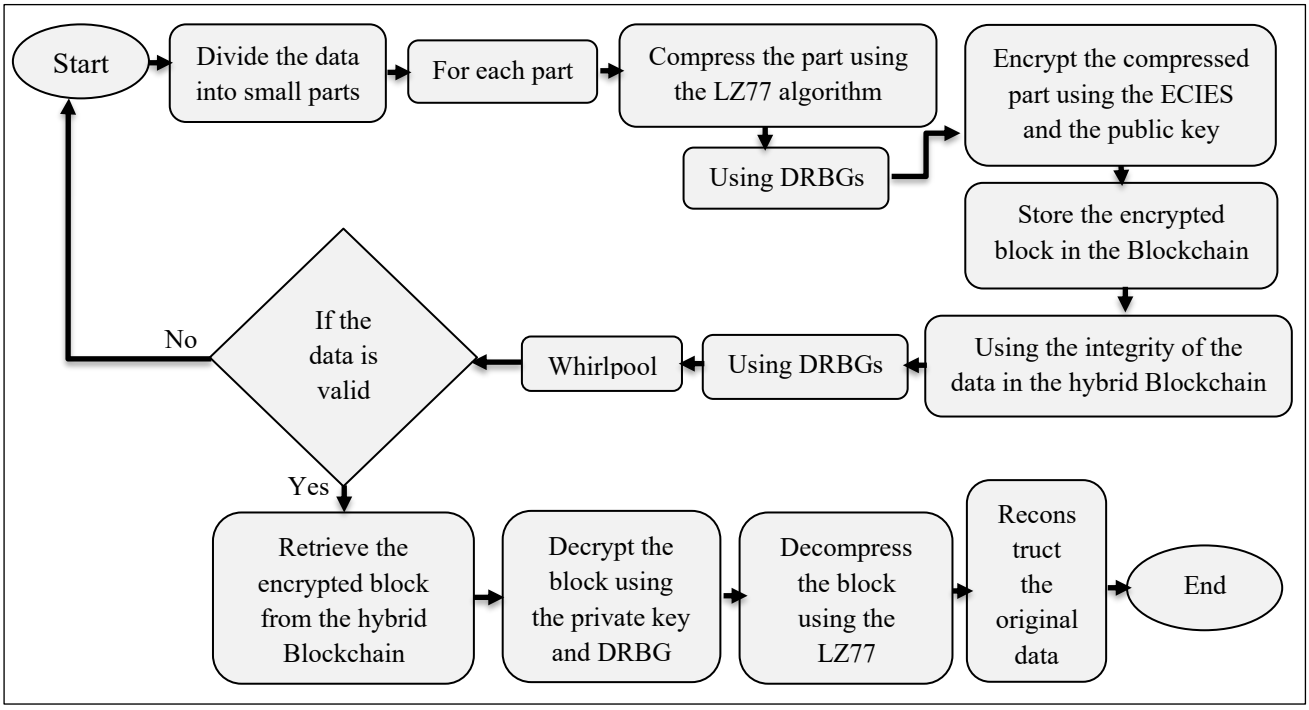


Figure 4: A diagram of the workflow steps of our proposed approach

Important characteristics		
It provides a high and additional layer of security and confidentiality through its use of encryption and randomization algorithms (ECIES, DRBG) together, which are known for their strength in protecting data.	It provides storage space in the blockchain by compressing data and reducing its size, and this allows large amounts of data to be stored.	By using Whirlpool hash functions with DRBG, it ensures the integrity of data within the hybrid blockchain from unauthorized change.

Figure 5: Important characteristics of our proposed approach

5. Results and Analyses

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

5.1. Performance Assessments

We present a thorough performance study of all the algorithms in our recommended method, with implementations of the algorithms shown in Figures 6, 7, 8, 9, 10, 11, 12, 13, and 14. The Ubuntu 20 operating system and Java language formed the basis for the working environment. In 64-bit architecture, 16 GB of RAM, and Intel (R) Core(TM) i5-2540M CPU @ 2.60 GH clock speed were also noted. To completely analyze all the algorithms of the suggested technique, we ran them 50 times. The application of the ECIES method to assess the encryption and decryption processes is depicted in Figure 6. Figure 6 shows that the encryption processes take not more than 0.0117441 ns to complete, while the decryption processes execution time was 0.0117441 ns.

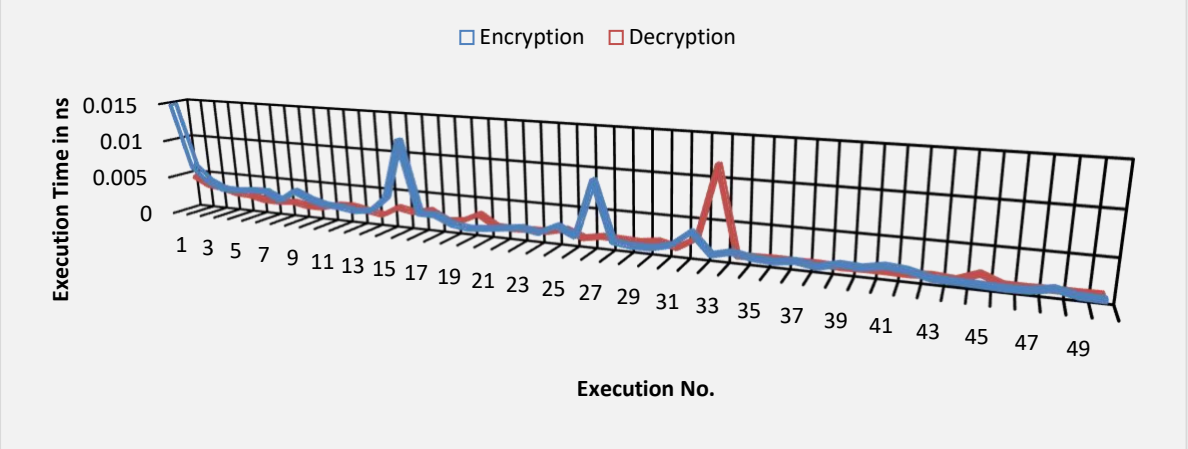


Figure 6: Assessment of ECIES cryptography

The ECIES algorithm's public and private key generation execution time is depicted in Figure 7. It can be observed that the public key must conduct point multiplication in ECIES, it takes longer to execute than the private key, where at the highest level the public key will not take more than 0.00242406 ns.

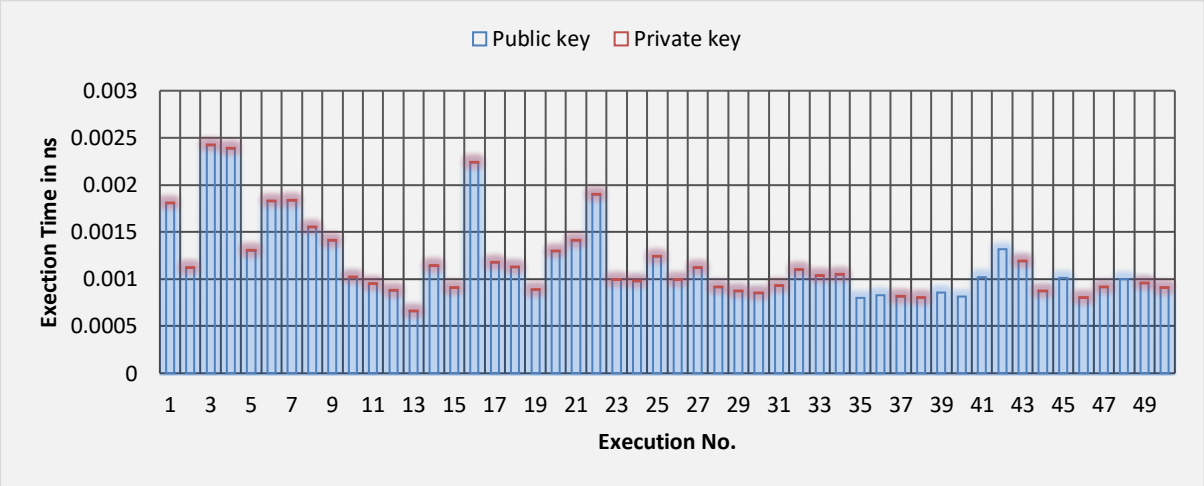
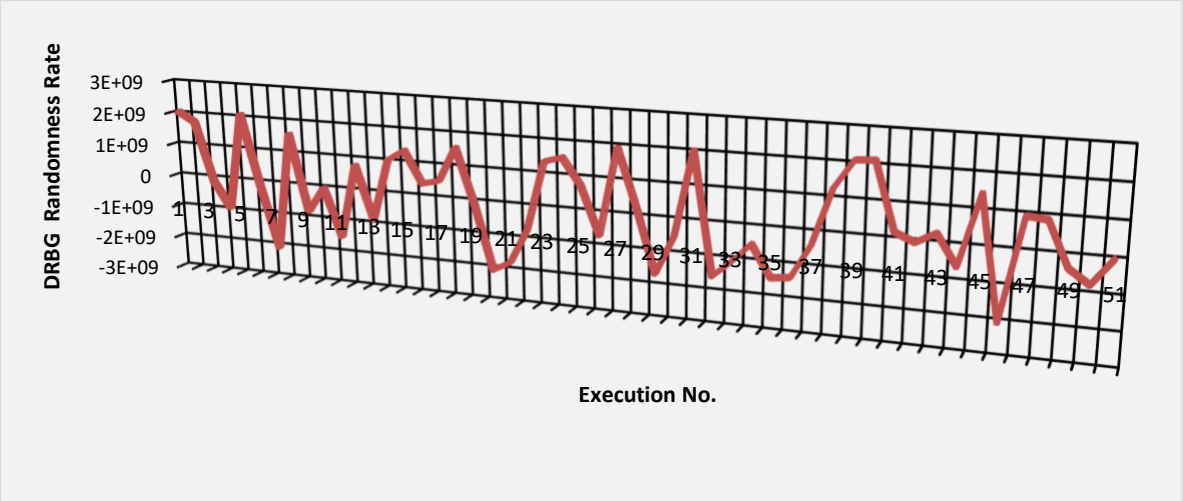


Figure 7: Execution time evaluation for ECIES keys

DRBG algorithm's performance analysis is shown in Figures 8 and 9. Figure 8 displays the possible range of random numbers for each execution, and Figure 9 displays the DRBG algorithm's execution time after fifty



iterations. Figure 9 illustrates how quickly randomization may be generated with DRBG.

Figure 8: Assessment of randomness range using DRBG

Figure 9: Execution time of randomness numbers for DRBG

In order to illustrate the benefit of Whirlpool256 and the significance of incorporating it into our strategy, we also assessed hashing methods. The hash rates of the Whirlpool256 and SHA256 algorithms in each implementation are displayed in Figure 10. We observe that hash rates are higher for the Whirlpool256 method than for SHA256. Additionally, Figure 10 illustrates how each SHA256 and Whirlpool256 hash function is implemented. According to the figure, Whirlpool256 performs better than SHA256, where the level of hashing rate to the Whirlpool algorithm was between 0.172164 and 0.12883, while SHA256 hashing rate was less in variation, it was between 0.159893 and 0.176857.

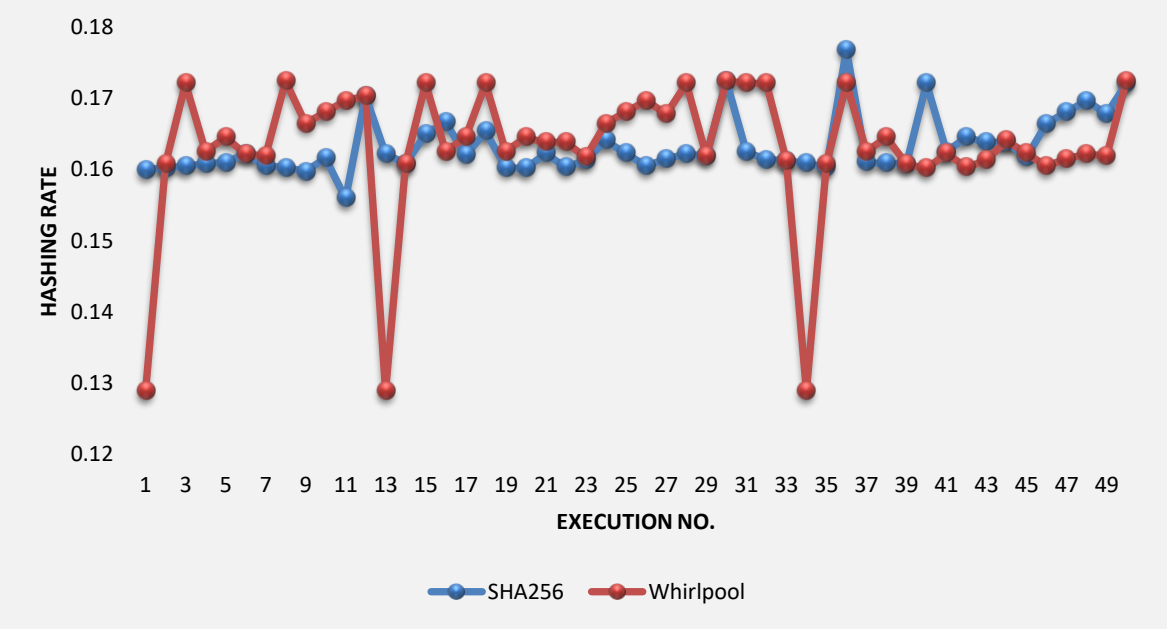


Figure 10: Analysis of SHA256 and Whirlpool256 rates' performance

Figure 11: Execution time of Whirlpool256 and SHA256

The time it takes the Blockchain to generate a block is shown in Figure 12. With such a system, the time it takes is thought to be fairly good, ranging from 0.12883 ns to no more than 0.176857 ns.

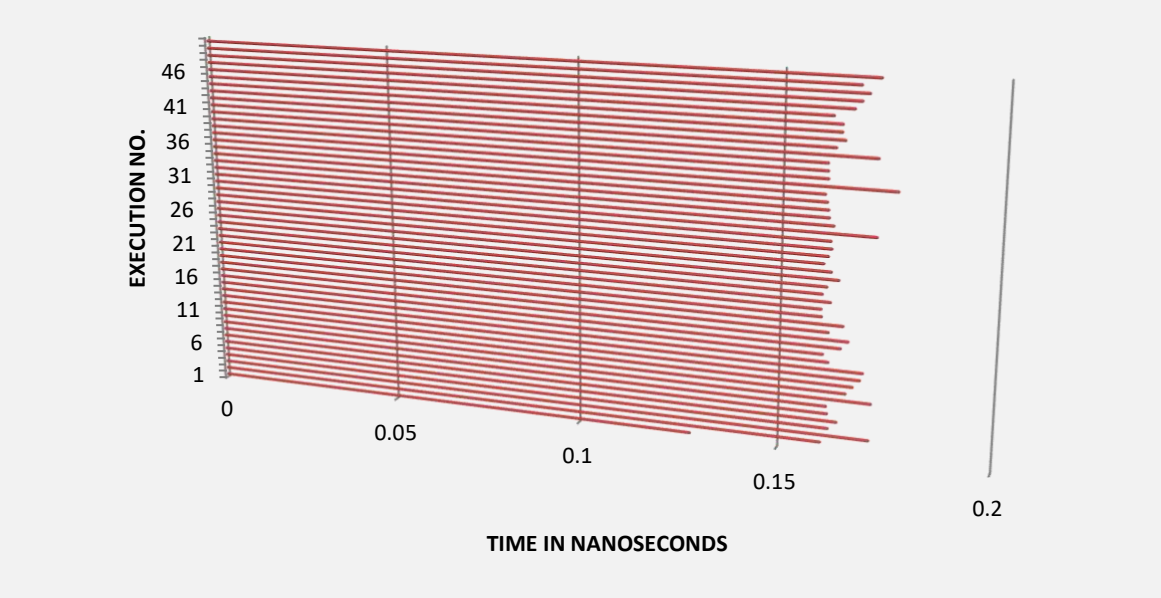


Figure 12: Blocks time period in nanoseconds

The results of a text's compression and decompression processes are shown in Figure 13. We observe that these procedures stand out for their great performance, which is good news for the ECIES algorithm's encryption and decryption processes.

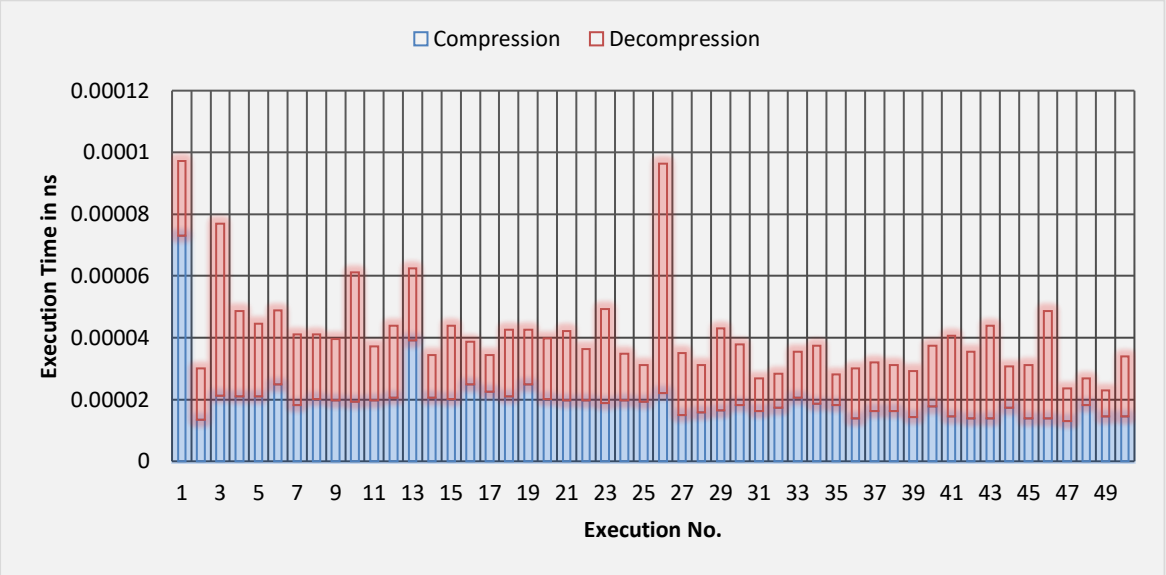


Figure 13: LZ77 execution time for 50 times

Finally, Figure 14 illustrates the whole functionality of the suggested method, encompassing encryption and decryption functions for both SHA256 and Whirlpool256. This is achieved by incorporating ECIES (encryption or decryption), hash functions (SHA256 or Whirlpool256), DRBG, LZ77 (compression or decompression), and Block into each implementation. Figure 14 makes it abundantly evident that the suggested method using Whirlpool256 performs better for encryption and decryption than SHA256. Where the SHA256 encryption execution time was 0.018 ns and 0.00327 ns, while the whirlpool encryption execution time was between 0.017 ns and 0.0028 ns. While SHA256 decryption execution time was 0.0059 ns and 0.00206 ns, while the Whirlpool decryption execution time was between 0.0053 ns and 0.0016 ns.

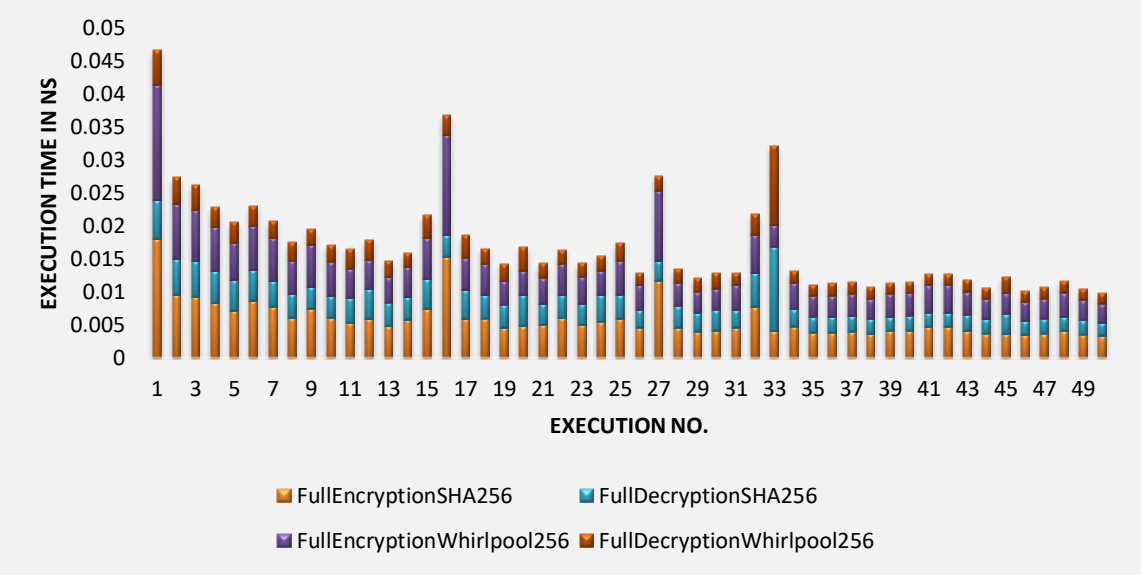


Figure 14: Comprehensive valuation of the suggested method using both SHA256 and Whirlpool256 with encryption and decryption

5.2. Security Evaluation

This part of our research provides high-security analyzes of our proposed approach against ransomware and malware attacks, and we also explain in detail how data is exposed to these attacks and how our proposed methodology addresses them robustly and robustly.

5.2.1. Analysis of the Ability of the Proposed Approach to Repel Ransomware Attacks

In this subsection of our study, we present some of the types of ransomware and how our proposed approach addresses them.

- **CryptoWall**

  It appeared for the first time in 2014 and is one of the most dangerous and widespread types of ransomware in previous years. It spreads through social engineering methods, tainted emails, and malicious websites. Once it reaches the victim's device, it encrypts all documents and files on the hard disk using strong encryption algorithms. It displays a ransom message to the victim and requests a ransom payment. If the ransom is not paid, the victim will lose his important data permanently. Our methodology combats this type of attack in a strong and robust way because it uses the ECIES encryption algorithm, as this algorithm is difficult to hack due to its high security strength.

- **Locky**

  It appeared for the first time in 2021. It is a type of ransomware, which is a malicious program and is considered the most advanced and dangerous among the attacks mentioned in our study. This attack is spread via infected websites, security vulnerabilities in software, and via email as well. It encrypts all files on the hard disk as soon as they reach the victim's systems, closes the desktop, and displays a message to the victim, and then the hackers demand ransom in digital currencies such as Bitcoin, for example. In order to confront such malicious programs, very secure systems with a high security methodology must be used, and this is what our methodology provides through its use of strong and strong encryption algorithms that are difficult to be penetrated by these malicious programs, as well as its use of hybrid Blockchain technology that is highly efficient in protecting data, because it makes

copies. Encrypted backups are distributed across a decentralized network and are available for recovery in the event of an attack.

- **Petya**

  It appeared for the first time in 2016 and is a malicious program (malware), and its updated version called "NotPetya" was discovered in 2017. This malicious program spreads via email, security vulnerabilities in systems and programs, and malicious software attached to documents, and once it reaches the system. The victim encrypts part of the boot sector, which leads to the failure of the boot process, and also encrypts the data on the hard disk. After that, the stage of demanding ransom in exchange for decryption begins. We have taken great care in our methodology to combat such malicious programs by using (Whirlpool256) a highly random encryption algorithm to provide a reliable and immutable record. In general, when exposed to such attacks, the ransom should not be paid, and the competent authorities should be notified to assist and solve the problem.

- **GandCrab**

  This attack appeared in 2018 and is a type of ransomware, and it was one of the most widespread malicious programs at that time. These attacks spread through malicious email attachments, misleading online advertisements, and bombed links. Once the victim's system is accessed, the attack encrypts his data and files on the device. The hacker then demands a ransom payment in encrypted currencies in order to decrypt the code. We worked hard to make our methodology resistant to such attacks and thwart them by using the highly randomized Whirlpool256 algorithm. This algorithm creates a unique digital signature for each file, ensuring that files are not altered during transfer. Prevention and advance preparation are the best solutions to repel cyberattacks in general.

- **Doxware**

  These attacks have appeared recently and are a type of ransomware attack, and differ from the traditional type of ransomware attacks in the way they work, where pirates penetrate the victims' computer systems and access their confidential and personal data and private messages. Instead of demanding ransom, the pirates blackmail the victims and threaten to publish them if the ransom is not sent. Our proposed approach to confront and interact with these attacks uses hybrid Blockchain technology and encryption of random public keys, so it is difficult for hackers and intruders to access all data and encrypt it securely.

- **SamSam**

  This attack appeared in 2016, and it is one of the ransomware attacks. This attack seeks to threaten and reveal customers' personal information, as it targets institutions and companies in various fields and works to penetrate their computer systems and completely encrypt the data, and the customer cannot recover his data until after paying the ransom, so we focused, as part of our proposed research, on confronting such attacks through the use of high-security encryption algorithms, such as the (ECIES) encryption algorithm, which attackers have difficulty cracking, and this is considered one of the strengths of our proposed approach.

5.2.2. Security of the Proposed Approach and Comparison of Attacks

The proposed approach for our research is based on the hash function (Whirlpool256), the use of random DRBG, public key encryption (ECIES256), and LZ77, in order to enhance and improve the security of the proposed system. In this section of our study, we will explain how Blockchain technology works and its power in protecting customer data from cyberattacks and other risks. Using hybrid Blockchain technology in our proposed approach provides a secure distribution of data between the private and public sectors, and this increases the security of our methodology. Table 3 below shows some comparisons between our proposed methodology and other methodologies in terms of their response to cyberattacks, especially in previous studies ([7], [14], and [25]-[29]).

Table 3: Comparison of attack response, between our proposed approach and existing approaches

Attacks / Approches	Petya	GandCrab	Doxware	SamSam	CryptoWall	Locky
[7]	Lower	Lower	Lower	Beneficial	Insufficient	Lower
[14]	Insufficient	Lower	Insufficient	Lower	Beneficial	Durable
[25]	Beneficial	Lower	Durable	Lower	Durable	Lower
[26]	Lower	Durable	Durable	Lower	Durable	Insufficient
[27]	Lower	Lower	Insufficient	Insufficient	Durable	Durable
[28]	Lower	Insufficient	Insufficient	Lower	Beneficial	Lower
[29]	Durable	Lower	Beneficial	Lower	Durable	Insufficient
Proposed approach	Durable	Durable	Durable	beneficial	Durable	Durable

5.3. Discuss the Limitations of the Proposed Approach

Proposing any approach may contain some limitations. Although we have made an effort to propose a robust approach that provides high security and satisfactory performance at the individual and organizational levels, there are some limitations that may arise from our proposal. First, the randomness provided by the DRBG algorithm may be sufficient to resist attacks in the field of this research, which may be insufficient for attacks that will appear in the future. Second, the proposed approach may be designed to deal with big data and extended applications in large organizations, as our proposed approach may not be suitable for small organizations that rely on little data, that is, the proposed approach may be expensive to perform due to the use of several algorithms such as ECIES, DRBG, Whirlpool, Blockchain and others. Third, the use of a hash algorithm without signature mechanisms may cause security problems for sensitive applications, such as e-banking applications. Fourth, our approach does not address the issue of hiding large data stored on remote servers. Fifth, our approach may be limited in terms of managing, sorting, and archiving large data in server databases. Sixth, the difference in applying the proposed approach to different operating systems may reveal unstudied results, as the results of the proposed approach were applied to the Ubuntu 20 system.

6. Conclusion

Every organization that uses an e-app must have an approach in place for safely and efficiently managing storage data. Furthermore, in order to gain an advantage economically, ransomware attacks have multiplied and are increasingly often launched against programs that use repository-sensitive data, such as e-banking, e-health, and e-agriculture. In this research, we proposed a technique that gives adequate efficiency alongside defense against ransomware attacks of the current period. The employment of hash algorithms (Whirlpool), public-key encryption methods (ECIES), and appropriate randomization helps to alleviate the security vulnerability in data repositories. However, this form of storage for data is handled by a hybrid Blockchain. It makes perfect sense to adopt a hybrid

Blockchain since it allows us to transfer data between the public and personal sectors while storing it in repositories. This paper provided attack analysis on ransomware such as Petya, GrandCrab, CryptoWall, SamSam, Doxware, and Locky. Our approach thus strikes an appropriate compromise between confidentiality and speed. After doing a performance evaluation, we concluded that the Whirlpool256 methodology outperforms the SHA256 method. We also find that our strategy can fight off ransomware attacks in our study field based on security analysis and comparison to earlier studies. In the future, we plan to investigate cryptographic algorithms like XSalsa20 and signatures like Ed25519 to see whether they may help us develop this method. Furthermore, we will look into optimal solution algorithms like jellyfish, artificial bee colonies, and yellow saddle goatfish for archival information extraction.

References

[1] M. Z. Khan, M. U. Khan, O. Irshad, O., and R. Iqbal, "Deep learning and Blockchain fusion for detecting driver's behavior in smart vehicles," *Internet Technology Letters*, *3*(6), e119, 2020. https://doi.org/10.1002/itl2.119.

[2] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Materials Today: Proceedings*, *37*, 2653-2659, 2021. https://doi.org/10.1016/j.matpr.2020.08.519.

[3] I. L. H. Alsammak, M. F. Alomari, I. S. Nasir, and W. H. Itwee, "A model for Blockchain-based privacy-preserving for big data users on the internet of thing," *Indones. J. Electr. Eng. Comput. Sci*, *26*(2), 974-988, 2022. https://doi.org/10.11591/ijeecs.v26.i2.pp974-988.

[4] P. Gope, and T. Hwang, "Untraceable sensor movement in distributed IoT infrastructure," *IEEE Sensors Journal*, *15*(9), 5340-5348, 2015. https://doi.org/10.1109/JSEN.2015.2441113.

[5] T. Koshiba, B. Zolfaghari, and K. Bibak, "A tradeoff paradigm shift in cryptographically-secure pseudorandom number generation based on discrete logarithm," *Journal of Information Security and applications*, *73*, 103430, 2023. https://doi.org/10.1016/j.jisa.2023.103430.

[6] J. Wang, J. Chen, Y. Ren, P. K. Sharma, O. Alfarraj, and A. Tolba, "Data security storage mechanism based on Blockchain industrial Internet of Things," *Computers & Industrial Engineering*, *164*, 107903, 2022. https://doi.org/10.1016/j.cie.2021.107903.

[7] I. A. M. Abass, L. F. Hussein, and A. B. Aissa, "New Textual Authentication Method to Resistant Shoulder-Surfing Attack," *International Journal of Advanced Computer Science and Applications*, *13*(1), 2022. https://doi.org/10.14569/IJACSA.2022.0130161.

[8] T. Kang, N. Woo, and J. Ryu, "Enhanced Lightweight Medical Sensor Networks Authentication Scheme Based on Blockchain," *IEEE Access,* 2024. https://doi.org/10.1109/ACCESS.2024.3373879.

[9] C. A. 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. https://doi.org/10.1002/ett.4653.

[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*, 2023. https://doi.org/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. https://doi.org/10.1016/j.procs.2024.05.078.

[12] 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), 1-19, 2024. https://doi.org/10.58496/MJCS/2024/005.

[13] S. H. Lee, and Y. S. Jeong, "Information authentication selection scheme of IoT devices using conditional probability," *Indian Journal of Science and Technology*, volume 9, issue 24, pages 1-7, 2016. https://dx.doi.org/10.17485/ijst/2016/v9i24/95991.

[14] T. Dargahi, A. Dehghantanha, P. N. Bahrami, M. Conti, G. Bianchi, L. Benedetto, "A Cyber-Kill-Chain based taxonomy of crypto-ransomware features," *Journal of Computer Virology and Hacking Techniques*, *15*, 277-305, 2019. https://doi.org/10.1007/s11416-019-00338-7.

[15] M. Wazid, A. K. Das, and S. Shetty, "BSFR-SH: Blockchain-enabled security framework against ransomware attacks for smart healthcare," *IEEE Transactions on Consumer Electronics*, *69*(1), 18-28, 2022. https://doi.org/10.1109/TCE.2022.3208795.

[16] O. Delgado-Mohatar, J. M. Sierra-Cámara, and E. Anguiano, E. "Blockchain-based semi-autonomous ransomware," *Future Generation Computer Systems*, *112*, 589-603, 2020. https://doi.org/10.1016/j.future.2020.02.037.

[17] A. Lakhan, O. Thinnukool, T. M. Groenli, and P. Khuwuthyakorn, "RBEF: ransomware efficient public Blockchain framework for digital healthcare application," *Sensors*, *23*(11), 5256, 2023. https://doi.org/10.3390/s23115256.

[18] 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. https://doi.org/10.1007/s11277-021-08800-w.

[19] M. Al-Zubaidie, "Implication of lightweight and robust hash function to support key exchange in health sensor networks," *Symmetry*, *15*(1), 152, 2023. https://doi.org/10.3390/sym15010152.

[20] Z. Wang, X. Dong, Y. Kang, and H.Chen, "Parallel SHA-256 on SW26010 many-core processor for hashing of multiple messages," *The Journal of Supercomputing*, *79*(2), 2332-2355, 2023. https://doi.org/10.1007/s11227-022-04750-7.

[21] F. Al-Shareefi, and Z. Al-Barmani, "Comparing two cryptographic hash algorithms: SHA-512 and whirlpool-a case study on file integrity monitoring," In *BIO Web of Conferences* (Vol. 97, p. 00093). EDP Sciences, 2024. https://doi.org/10.1051/bioconf/20249700093.

[22] S. Chen, J. Guo, E. List, D. Shi, and T. Zhang, "Diving deep into the preimage security of AES-like hashing," In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 398-426). Cham: Springer Nature Switzerland, 2024. https://doi.org/10.1007/978-3-031-58716-0_14.

[23] 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.

[24] D. Li, J. Li, X. Di, and B. Li, "Design of cross-plane colour image encryption based on a new 2D chaotic map and combination of ECIES framework," *Nonlinear Dynamics*, *111*(3), 2917-2942, 2023. https://doi.org/10.1007/s11071-022-07949-8.

[25] M. Sulaiman, M. Waseem, A. N. Ali, G. Laouini, and F. S. Alshammari, "Defense strategies for epidemic cyber security threats: modeling and analysis by using a machine learning approach," *IEEE Access*, 2024. https://doi.org/10.1109/ACCESS.2024.3349660.

[26] R. Seth, A. Sharaff, J. M. Chatterjee, and N. Z. Jhanjhi, "Ransomware Attack: Threats & Different Detection Technique," In *Information Security Handbook* (pp. 157-176). CRC Press, 2022.

[27] T. R. Reshmi, "Information security breaches due to ransomware attacks-a systematic literature review," *International Journal of Information Management Data Insights*, *1*(2), 100013, 2021. https://doi.org/10.1016/j.jjimei.2021.100013.

[28] H. Le Bouder, *Symmetric cryptography applied in different contexts: physical attacks and ransomware* (Doctoral dissertation, Université de Rennes), 2023.

[29] J. A. Gómez Hernández, "Crypto-ransomware: Crypto-ransomware can be detected and deleted from time to time by archiving files," *IET Information Securi*ty, 2022. https://doi.org/10.1049/ise2.12042.