Design of Novel Cryptographic Model Using Zero-Knowledge Proof Structure for Cyber Security Applications

S. Anthoniraj[1*], Rahul Mishra[2], Shweta Loonkar[3], Trapty Agarwal[4], Gunveen Ahluwalia[5], Amandeep Gill[6]

[1]Professor, Department of Computer Science & Engineering (Specialization), School of Engineering & Technology, JAIN (Deemed-to-be University), Bangalore, India
[2]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India
[3]Assistant Professor, Department of ISME, ATLAS SkillTech University, Mumbai, Maharashtra, India
[4]Associate Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Uttar Pradesh, India
[5]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh, India
[6]Dean R&D, Department of R&D, Vivekananda Global University, Jaipur, India
Emails: anthoniraj@jainuniversity.ac.in; rahul.mishra.orp@chitkara.edu.in; shweta.loonkar@atlasuniversity.edu.in; trapty@muit.in; gunveen.ahluwalia.orp@chitkara.edu.in; amandeep.gill@vgu.ac.in

Abstract

Privacy and security in the current modern, digital communication and data transfer-oriented world has become imperative. Most commonly used encryption methods often involve exposing sensitive information, which might be an open gate for potential vulnerabilities. This paper aims to explore the topic of applying ZKPs in cybersecurity in a comprehensive manner. For this purpose, Proposed work will provide an exhaustive description of the basic concepts of Zero-Knowledge Proofs , which refer to both the interactive and non-interactive forms of the product. Additionally, the study will focus on presenting various cryptographic protocols and algorithms utilizing Zero-Knowledge Proofs , such as zk-SNARKs and zk-STARKs . In addition to theoretical studies, Proposed work analyze the practical implementation details of Zero-Knowledge Proofs implementations , cryptographic libraries, programming languages, and frameworks commonly used to create ZKP-based applications . Zero-knowledge proofs enable groundbreaking approaches to address cybersecurity problems with an emphasis on user privacy and data confidentiality. On average, cryptographic operations experienced delays of approximately 10 milliseconds which was not intrusive for real-time systems. The system's throughout remained at a steady average of 100 Mbps all times, so it performed well at processing data despite cryptographic overhead. The packet delivery ratio was constantly high at 98%, implying that most data packets were delivered consistently even over encrypted communication paths.

Keywords: Digital Communication; Privacy; Security; Cryptography; Zero-Knowledge Proofs (ZKPs); Cybersecurity

1. Introduction:

The term Cryptography has its roots in the Greek term "Secret writing." Cryptography is the scientific practice of safeguarding data by utilizing algebraic relationships to transform regular data into unreadable text. Cryptography is used to securely store and transmit confidential information so that only authorized individuals may access or use it. Information submitted by the user is referred to as "Plaintext," [1] whilst the modified or encrypted information is known as "Ciphertext" [2]. Encrypting plaintexts with keys creates ciphertexts, and reversing this process to obtain the original information is known as decryption. The first known usage of cryptography occurred around 3000 B.C. in Egypt, where pictograms were inscribed on a stele. The discovery of the Rosetta Stone in the 19th century aided in deciphering information previously written in pictograms. The scytale cipher evolved from wrapping a parchment strip around a cylinder to rearrange data. The information was disclosed by encasing the parchment strip.

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

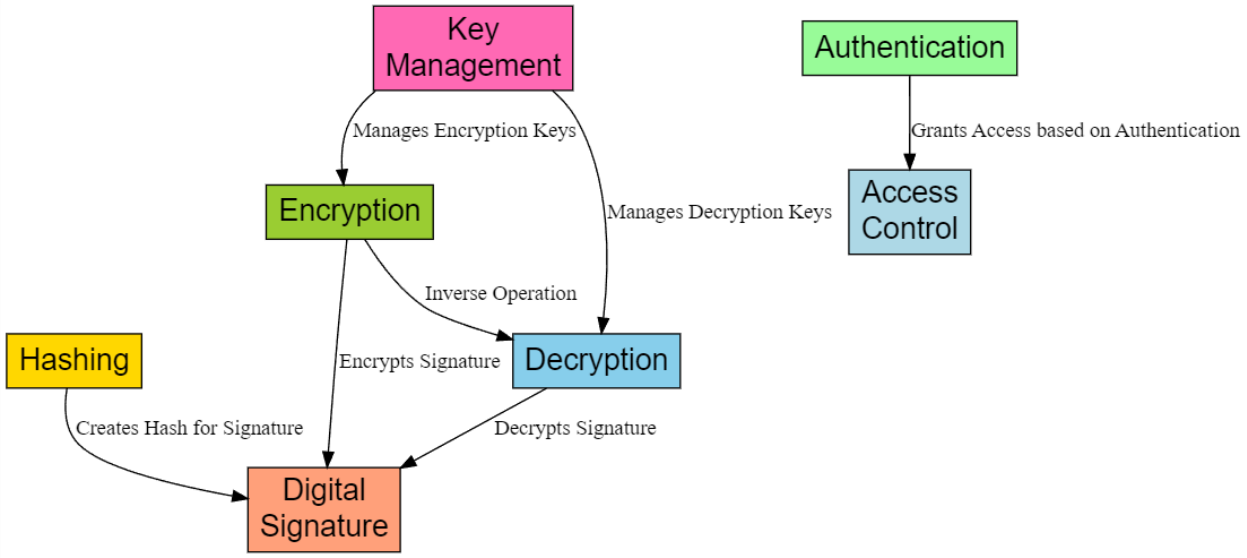

Figure 1: Cryptography in Cybersecurity stages

Gilbert Verman enhanced the approach by introducing a lengthy key and conducting a bitwise XOR operation on the plaintext as shown in Figure 1. The approach was further exposed because of the extended recurring keywords in the secret key. An individual proposed using a random key [3] that matches the length of the message to address the key issue. Each new message was encrypted using a different secret key, and the previous key was no longer used. This technique was referred to as the One-Time Pad. It generates a random cipher to prevent any correlation between the plaintext and ciphertext. The resulting ciphertext was unbreakable. However, this method has two drawbacks: if the information is extensive, such as billions of random characters, a significant number of random keys are required. Generating really random characters can be a challenging process. Key distribution [4] and protection are crucial issues as a new key of the same size as the plaintext is required for every message at both the sender and receiver ends. This approach is suitable for brief messages that need to be transmitted across a low bandwidth channel while maintaining a high level of security.

Chaos-based encryption systems are divided into two categories: analog and digital cryptographic systems. Analog cryptography systems rely on synchronization and can be used in analog channels with additive noise. Cryptographic systems based on chaotic synchronization transport information using single or many random signals. Analog cryptographic systems are classified into many categories based on chaotic dynamics, such as chaos management approaches, chaos masking, chaotic modulation, inverse system approach, and chaos switching. Digital cryptographic systems [5] rely on chaos and are used in computer cryptography. Digital cryptography systems often do not rely on synchronization.

Chaos-based cryptographic methods [6] offer several benefits in comparison to conventional encryption techniques. Traditional encryption systems are limited to integer number fields, but chaos-based cryptographic systems can be defined across continuous number fields. Various types of functions can be used to encrypt the data.

In traditional encryption systems, information needs to be digitized due to their limitation to integer number fields. In contrast, chaos-based encryption systems do not require information to be digitized.

Digital hardware is required for standard encryption systems, but high-speed electrical or optical components such as lasers can be used directly in chaos-based encryption systems [7]. In typical encryption systems, two circuits are required: an analog circuit for broadband modulation and digital circuitry for encryption. In chaos-based encryption, a single circuit is used for both broadband modulation and encryption.

A traditional encryption scheme generates periodic pseudo-random sequences. To implement these methods, digital hardware is required, and the periodicity is determined by the number of bits used to represent the state of the random number generator. The generation of the pseudo-random sequence is achieved by chaotic dynamics; however, the generated signal is non-periodic. The main disadvantages of the use of chaos-based cryptography are the following:

• Less Bit Error Rate performance than classical cryptosystems
• Power-efficiency and bandwidth-efficiency are poorer than traditional systems

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

1.1 Motivation

Security and privacy are essential aspects of today's era of digital communication and information transmission. Most traditional encryption schemes use sharing models that can expose sensitive information and create vulnerabilities. This paper seeks to explore various encryption methodologies that provide sophisticated security measures without compromising users' privacy and confidentiality aspects. When it comes to exploring the use of Zero-Knowledge Proofs) [8] in cybersecurity, the study is extensive. This model offers an enhancement to the capability of securing cryptographic designs while ensuring that the users' identities remain confidential. ZKP fosters certain aspects that can revolutionize cybersecurity in various domains, including user verification, secured transactions, and identity purposes, among others. The primary aim of this paper is to provide insights into the theoretical orientation, practical-based application, and useful appropriateness of Zero-Knowledge Proofs (ZKPs) [9] in cybersecurity. When implemented, ZKP will provide proof and hence develop a trusted approach towards a solution to the user data. This paper will contribute towards paving a strong understanding and trustworthiness of Zero-Knowledge Proofs (ZKPs) as a reliable and viable means of securing the system while promising strong security measures. If well understood, the research promises to yield crucial insights in fostering further exploration and hence developing useful demands in the future within the sector. The structural layout will involve section 2 for the literature review, Section 3 for the study's design and methods, Section 4 for the results and experiment analysis, and Section 5 for the conclusion and recommendations of further actions.

2. Related Work

One significant obstacle in symmetric key cryptography is the establishment of the secret key between two parties. The [10] individuals pioneered the development of a practical method for creating a shared secret over an unsecure channel. This approach facilitates key exchange via an unsecure channel. However, the technique is vulnerable to man-in-the-middle attacks. The authors expanded the Diffie-Hellman [11] two-party protocol to a multi-party protocol. Multi-party protocols establish secret keys among more than two parties. [12] introduced three key agreement techniques that rely on a single cryptographic assumption. The security of one protocol is directly linked to the security of RSA factoring, upon which it is based. The second one relies on ECC, while the third one is based on discrete logarithm. The Identity based multi-party authenticated protocol [13] cannot be implemented since multi-linear pairing is not available in the literature. [14] [15] introduced an identity-based symmetric key scheme. Nodes in this system can compute a common key without interacting with one other.

With the improvement in processing capacity, the 512-bit key length used in classical cryptography systems is currently considered insecure. Elliptic Curve Cryptographic System (ECCS) is more secure than conventional cryptographic systems when using the same key length. ECC offers a more efficient key distribution mechanism with lower communication costs and less computational overhead than classic cryptographic systems of the same key length. ECC is a different method compared to public key cryptography techniques such as RSA. Conventional public key cryptography relies on the multiplication of extremely large numbers to enhance security. ECC utilizes the characteristics of Elliptic Curve (EC) to create algebraic groups. ECC creates cryptographic keys using algebraic groups. Cryptographic keys in ECC are generated more quickly and offer enhanced security compared to classic methods such as RSA while using the same key length. Trappe et al. [45] introduced a technique for conveying the cryptographic key by incorporating it directly into the multimedia content. The author proposed that an independent method for transferring the key is unnecessary. The authors asserted that integrating the key into the multimedia material enhances the security of the key transfer. The author failed to present evidence about whether the security of the cryptographic system is enhanced by including secret data utilizing Steganography techniques.

[17] introduced a protocol that combines biometric and password authentication to establish a secure session between a mass storage device holding confidential information and a potential user of that information. Researchers in [18] scrutinized the authenticated key agreement mechanism and identified numerous flaws, such as the unauthorized file decryption attack. Table 1 shows the Comparison of Existing work with Merits and Demerits

Table 1: Comparison of Existing work with Merits and Demerits

Study	Focus	Methodology	Key Findings	Demerits

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

[19]	Cryptographic protocols	Theoretical analysis and simulations	Demonstrated the efficiency of zk-SNARKs in privacy- preserving smart contracts.	Limited empirical validation; scalability concerns in real-world deployments.
[20]	Authentication	Comparative analysis of ZKP-based authentication	Compared ZKP- based Authentication schemes and highlighted their effectiveness in privacy protection.	Lack of real- world implementation; potential performance overhead in large-scale systems.
[21]	Data integrity	Empirical study on ZKP-based data integrity checks	Showcased the reliability and efficiency of ZKPs in ensuring data integrity in cloud environments.	Limited scalability in complex data environments; dependency on trusted setup assumptions.
[22]	Privacy preserving transactions	Case studies and simulations	Illustrated the practical implementation of ZKPs in blockchain-based cryptocurrencies.	Potential performance bottlenecks in high-throughput transaction systems; regulatory challenges.

The research on which the Zero-Knowledge Proofs in the field of cybersecurity are the one already being investigated, as it gave several valuable insights; however, for the broadening of the current knowledge, there is a large gap in research regarding overcoming the scalability and efficiency constraints that ZKPs impose when diagnosed on high-throughput systems, commonly utilized in the real world. As theoretical studies and smaller scale simulations have shown, ZKPs have a potential to improve privacy and security of data. However, there has been no thorough examination whether ZKPs are feasible for actual deployment over large scales in networks such as blockchains or cloud environments. Perhaps, the primary limitation for the application of the Zero-Knowledge Proofs into large-scale projects with a priority for performance and scalability is the lack of empirical evidence to support its implementation. This data gap can be filled by wide deployment and general performance testing of the Zero-Knowledge Proof systems on several use cases. The aim of such performance tests is to assess the feasibility of real-world use and the constraints and optimization potential.

3. Design of Zero-Knowledge Proofs Based cryptographic model

While developing a cryptographic model underpinned by Zero-Knowledge Proofs, there are numerous critical elements that need to give due consideration to adequately providing sturdy security and privacy shielding. All of them are schematically depicted in the block diagram of the putative work shown in Figure 2 below.

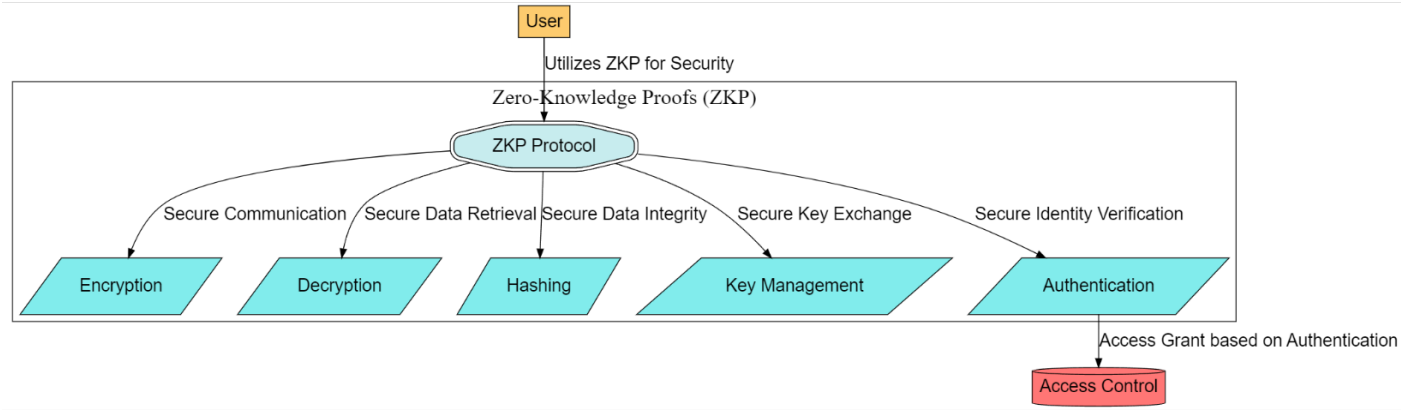

Figure 2: Block Diagram of Proposed work

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

Essentially, this prototype seeks to promote unhackable, trustworthy authentication as well as confirmatory action and identity control without endowing confidentiality on something.

3.1 Cryptographic Primitives Selection:

Selection of cryptographic primitives represents one of the most important parts in the development of robust and secure systems in cybersecurity. This approach is intended to achieve the necessary security properties but, at the same time, to minimize the likelihood of various vulnerabilities and risks. It consists of selecting appropriate mathematical algorithms and techniques as prerequisites. Such selection should be based on the security requirements of particular applications and their limit. Therefore, when it comes to cryptographic models based on Zero-Knowledge Proofs , the selection of the primitives should be mandatory to ensure secure authentication, data integrity verification, and identity management while protecting sensitive information. Thus as an example, the selection of cryptographic hash functions to secure the data integrity features of the system based on ZKPs should be considered. "One-way functions, implemented by cryptographic hash functions, map an arbitrary-length input message to a fixed-size output, denoted as a hash value" . Mathematical representation can be as follows:

$$H(m) = h \quad (1)$$

First of all, the input message is denoted with m, and the hash value produced is denoted as h. Due to prove being based on the ZKPs, the data's integrity is proven due to the required properties of the cryptographic hash function , precisely collision resistance, and preimage resistance. Next, one of the most critical issues in cryptography, based on zero-knowledge proofs framework, remains the confidentiality and authentication of data in the choice of different encryption and signature algorithms . Thus, symmetric encryption, such as AES, is used to encrypt the sensitive data. AES symmetric encryption is more reliable to break, but asymmetric encrypting, such as RSA, is implemented in digital signs and key exchange. Furthermore, iteration in the RSA encryption process occurs when digital signs and key exchange are used, reaching some complexity. Besides, RSA operates when both private and public key shares the modulus. RSA is computationally intense. Asymmetric encryption commonly utilizes a public and a private key pair is used for encryption and decryption, whereas symmetric encryption only employs a single key for both processing unit's stages are shown in Figure 3.

Encryption Stage:

In the previous explanations of the encryption algorithm with RSA encryption, the ciphertext c is calculated by multiplying the original plaintext message with c with the public exponent c and then taking the modulus of the results with r .

$$c = m^e \bmod N \quad (2)$$

Where:

- c is the resulting ciphertext,
- m is the plaintext message,
- e is the public exponent, and
- N is the modulus.

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

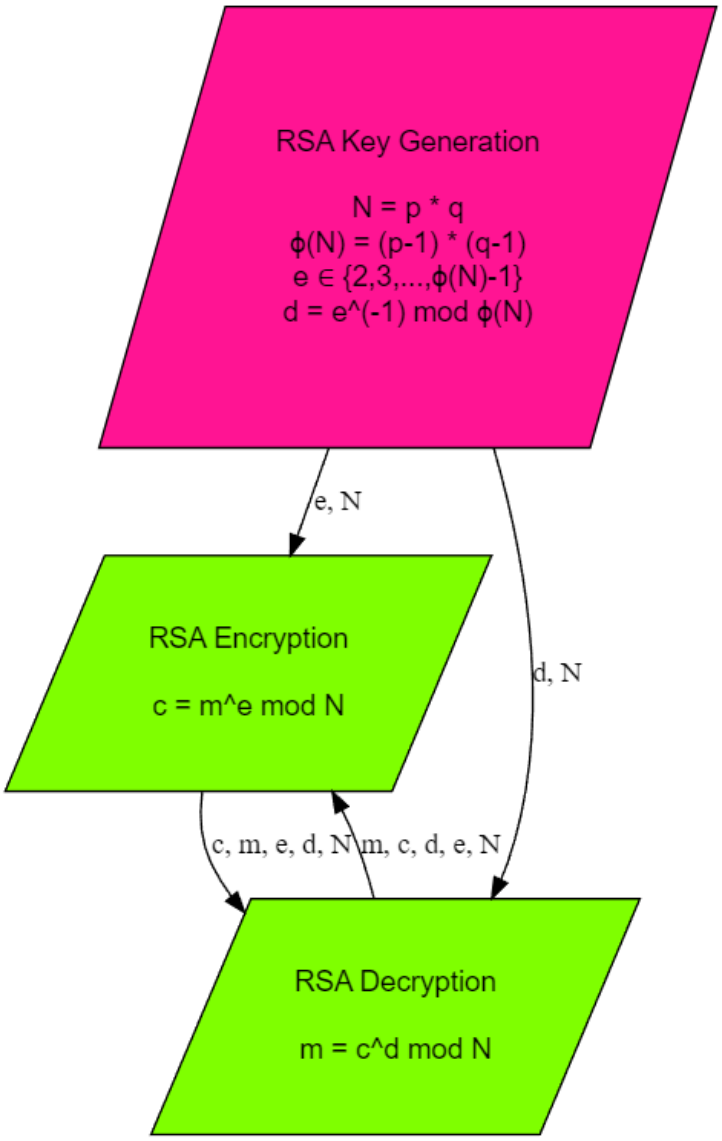

Figure 3: Flowchart of Cryptographic Primitives Selection Stages

Decryption Stage:

Mathematically, Proposed work can write this as:uth code . Once it is generated for the recipient, the recipient must then decrypt the ciphertext using his private key to get back the original plaintext message they received. The ciphertext X is first taken to the power of the private exponent X and then obtain the modulus of the result using X . This process can be expressed mathematically as :

$$m = c^d \text{mod} N \quad (3)$$

Where:

- m is the original plaintext message,
- c is the ciphertext,
- d is the private exponent, and
- N is the modulus.

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

Key Generation:
The RSA method of key generation involves selecting two distinct prime numbers, i and j, calculating the modulus i as the factor of these two integers, selecting the public exponent i, and calculating the private exponent i. The equations being deployed for the creation of keys are as follows:
Modulus Calculation:

$$N = p \times q \tag{4}$$

Totient Function Calculation:

$$\phi(N) = (p-1) \times (q-1) \tag{5}$$

Public Exponent Selection:

$$e \in \{2,3,\dots,\phi(N)-1\} \text{ such that } \gcd(e,\phi(N)) = 1 \tag{6}$$

Private Exponent Calculation (using the Extended Euclidean Algorithm):

$$d = e^{-1} \bmod \phi(N) \tag{7}$$

Where:

- p and q are large prime numbers,
- N is the modulus,
- $\phi(N)$ is Euler's totient function of N,
- e is the public exponent,
- d is the private exponent, and
- gcd denotes the greatest common divisor.

3.2 ZKP Protocol Based Path Selection:

In the case of cryptographic applications, it is necessary to choose the proper Zero-Knowledge Proof protocol for ensuring the desired security level and efficiency. As a powerful, and highly used, ZKP protocol, Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, shortly known as zk-SNARK, is famous for its usage in the shortening verification and short proofs. Using cryptographic primitives such as elliptic curve pairing and precisely polynomial interpolation for producing short proofs of computational statements, the zk-SNARK method is expanded in this paper using the flow-chart that shows the proposed ZKP Protocol Based Path Selection in Figure 4.

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

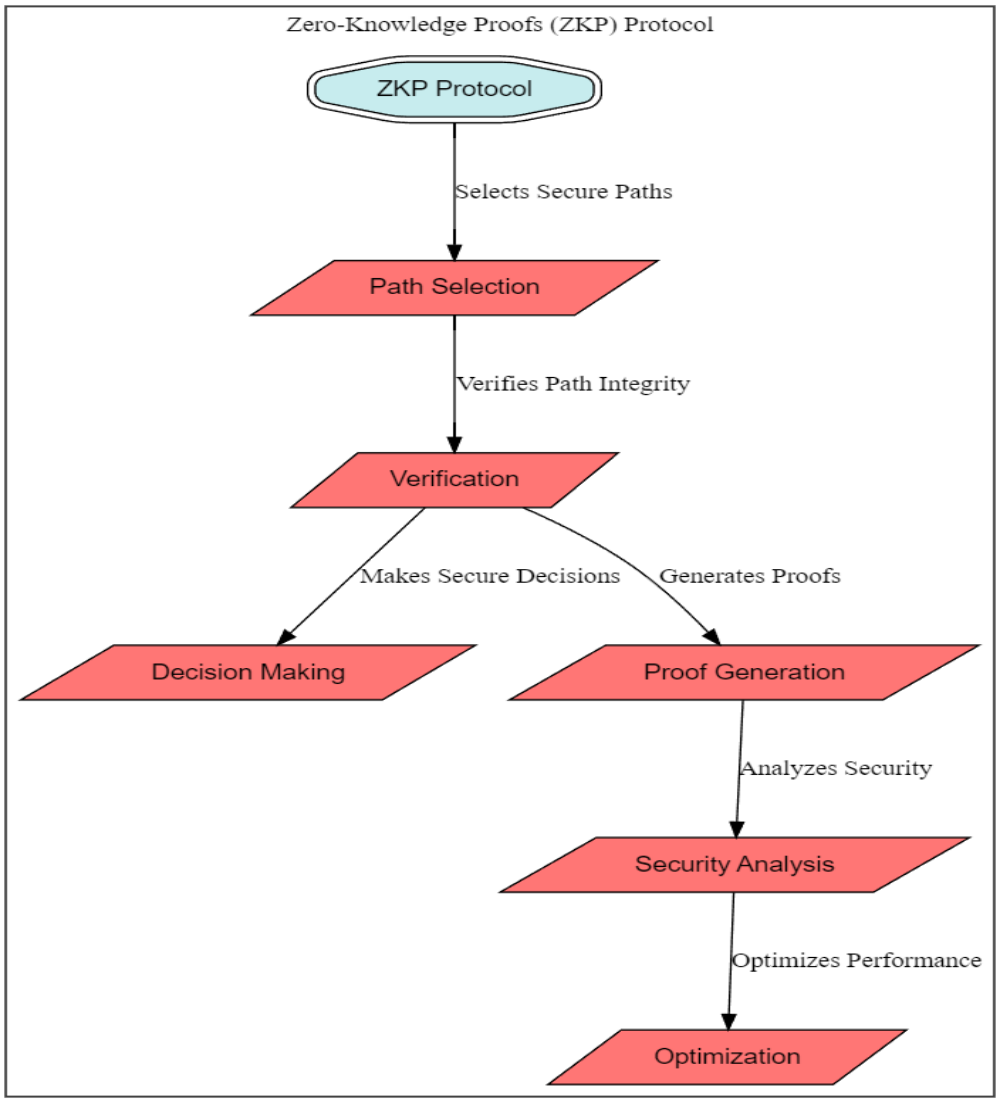

Figure 4: Flowchart of proposed ZKP Protocol Based Path Selection

Establishment: The establishment phase entails the production of common reference strings and parameters that are necessary for the generation and verification of proofs. Proposed work will refer to the common reference string as r, and the parameters that are formed throughout the setup process will be denoted by params..

CRS, params ← Setup () (8)

Establishment: This stage involves the creation of common reference strings and all parameters required to make and confirm proofs. Proposed work shall use two generic names – r to indicate the common reference string and params to indicate all parameters created during the setup. Key Generation: Meanwhile, Proposed work carry out the parties' key generation process to create prover and verifier public and secret keys. The public key will be designated as T, and the secret key as X.

$pk, sk \leftarrow$ KeyGen (params) (9)

The prover is responsible for constructing a concise proof π in order to indicate that they are aware of a witness w for a certain assertion ϕ presented to them.

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

$$\pi \leftarrow \text{Prove}\ (\phi, w, sk) \quad (10)$$

For the purpose of proof verification, the verifier uses the public key pk to determine whether or not the proof π is valid in comparison to the statement ϕ.

$$\text{Validity} = \text{Verify}\ (\phi, \pi, pk) \quad (11)$$

This is accomplished through the zk-SNARK protocol, where the prover convinces the verifier that a given statement is true without revealing any extra knowledge about the verification party . The zk-SNARK protocol is used to provide ZKP-based cryptographic models for businesses, allowing them to a wide range of security assurances and proof verification capabilities.

$$\phi = \text{ComputeStatement(path)} \quad (12)$$

Therefore, it is appropriate for a wide variety of use cases in the cybersecurity industry. The prover's computational statement to prove knowledge of is represented by the letter ϕ. Frequently, this statement pertains to the characteristics of the path to be taking through the network. Additionally, it determines whether the route is appropriately valid and adheres to certain parameters.

$$w = \text{GenerateWitness (path)} \quad (13)$$

The ultimate goal for zk-SNARK protocols is to minimize the number of proofs generated as people keep generating the proofs. At the same time, the validity of the proves is of importance. This is for the sake of efficiency. Thus, the presentation of computational claims and witnesses must be sufficiently efficient to avoid the need for a large proof size.

$$\pi = \text{OptimizeProofSize}\ (\phi, w) \quad (14)$$

Using ZKP protocol-based path selection, users can build channels with confidentiality and integration on communication networks that are secure and time-efficient. The security of the zk-SNARKs from adversarial attacks is assured by the mathematical and cryptographical methods under which these techniques are established. Zk-SNARKs are thus a breakthrough in cybersecurity and can therefore be used to maintain privacy and trust on network communications.

3.3 System Architecture Design:

In this cryptographic model, the zk-SNARK protocol is defined as ZeroKnowledge of Succinct Non-Interactive Argument of Knowledge. The primary function of this protocol is to ensure that the communication taking place between the two entities 'A' and 'B' would be secure. On the other hand, the model is vulnerable to a man-in-the-middle attack explanation attack or a rail there which is the eavesdropper 'C'. This attack takes place because the communication between "A" and "B" is intercepted and the eavesdropper "C" manages to impersonate the two parties exchange while modifying the response messages without detecting. This weakness occurs due to the fact that the public keys that were exchanged between 'A' and 'B' were intercepted and then replaced with the public key of the 'C' s public key the public key of "A" is referred to term A and the public key of "B" is denoted by " B" and the public key of the attacker under the letter "C". The secret key 'K' is calculated for both 'A' and 'B' legitimacies the model was the exponentiation modulo a prime number 'q'. These calculations are demonstrated in the following formula:

$$K_A = (Y_B)^{X_A} \quad \text{mod} q \quad (15)$$
$$K_B = (Y_A)^{X_B} \quad \text{mod} q$$

$$K_C = (Y_A)^{X_C} \quad \text{mod} q \quad (16)$$
$$K_C' = (Y_B)^{X_C'} \quad \text{mod} q$$

This is because the private keys of 'C' are also denoted by the letters 'C' and 'C'. As a result, 'C' will be capable of decrypting and reading the intended message that is being sent and received by 'B' and 'C', thereby editing and re-encrypting it without them knowing of it. This will compromise the secrecy and integrity of the message. In general, the man-in-the-middle attack serves to interfere with the security guarantees of the zk-SNARK protocol. It does so by abusing the existing weaknesses in the key exchange process . Messages in cryptographic systems cannot be effectively guaranteed integrity and access. This can be done by establishing robust authentication mechanisms that

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

ensure messages' source and secure channels for key exchange. A relevant framework is important to enable all these precautions with a reasonable level of certainty .

3.4 Proof Generation and Verification Mechanisms:

The zk-SNARK protocol is integrated into the cryptographic protocol proposed here to enhance the level of security related to the communications of entities A and B. First, at the start of the initialization, user A forwards a message to the Authentication Server that has to include the transmission of the identifiers IDA and IDB. . Afterwards, at the second stage of the initialization, Authentication Server must perform the authentication and the key exchange. AS produces a random number u1 and XORs it with the password u1 of A, sends the result to u. The same is implemented for B – the same process is done with IDA sent to B and the functioning hash of IDA concatenated through XOR.

$$N1 \oplus PA \rightarrow A \quad (17)$$

The public key YA is computed by A, and then it is transmitted to B along with the hash of YA that is concatenated with $N1$ for the purpose of verifying its freshness.

$$N1 \oplus PB \parallel H(N1 \oplus PB \parallel IDA) \rightarrow B \quad (18)$$

For confirmation and key calculation purposes, A computes the session key K by using Y B and its private key X A , whereas B computes K using Y A and its private key X B :

$$YA||H(YA||N1) \rightarrow B \quad (19)$$
$$YB \parallel H(YB \parallel N1) \rightarrow A$$

Upon receiving the message from A and verifying that it is still fresh, B computes its public key represented by Y B and transmits it to A with the hash of Y B for refreshing the message.

$$K_A = (YB)^{XA} \mathrm{mod} q \quad (20)$$
$$K_B = (YA)^{XB} \mathrm{mod} q$$

Where AS uses XOR with the hash of XOR appended with IDA to send a message to B in order to check if the people sending them a message is who they say they are , this is done as follows; B always checks if there is no impersonation attempted by comparing the calculated hash to the one received. Which shows that the sending person is the one they say they are . The scenario-based proof generation and verification mechanisms are shown in Figure 5.

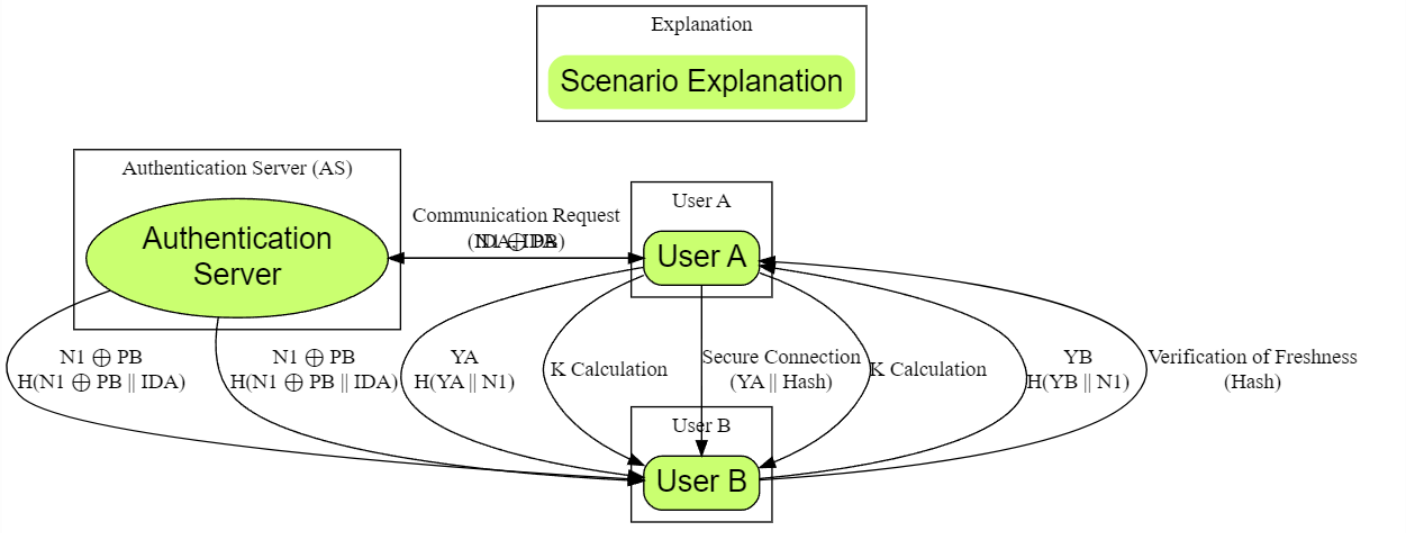

Figure 5: Scenario Based Proof Generation and Verification Mechanisms

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

As part of the process of establishing a secure connection, A transmits its identification to B, along with the hash of the nonce and its public parameter X, which guarantees that the information is both current and genuine. For the purpose of sender authentication, B checks the freshness of the message that was sent from A and computes the hash of XOR concatenated with IDA.

For the purpose of ensuring safe communication, both A and B compute the common secret key K. Through the incorporation of the zk-SNARK protocol into the communication process, this protocol guarantees robust authentication, freshness verification, and confidentiality, hence strengthening the security of the data exchange that takes place between entities A and B.

$$K = K_A = K_B \tag{21}$$

4 Experimental Results and Analysis

One chaotic system is used to permute pixel positions, and another chaotic system is used to change pixel values. Both of these chaotic systems are utilized by the picture encryption system that is now under investigation. As the test image, a Color Lena image with dimensions of 256 × 256 was utilized. When it comes to the Pixel position permutation stage, the Lorenz, Chen, and Lu chaotic systems are applied. As seen in Figure 6, the original photograph that was used for the work is displayed. The image was altered by permuting the positions of the pixels through the use of a chaotic system such as Lorenz, Chen, or Lu, and the outcome was presented in Figure 7. Figure 8 presents the image that was obtained when it was spread on the screen.

Image1

Figure 6(a): Original Image

Figure 6(b): Encryption Key

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

Figure 6(c) Separation of Red Green and Blue component

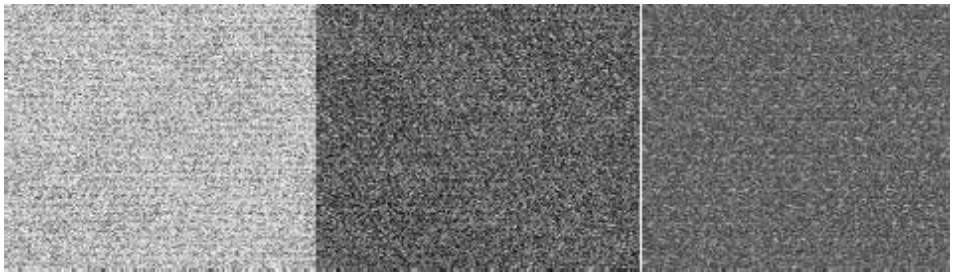

Figure 6(d): Confused Red, Green and Blue Component

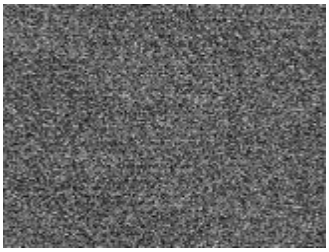

Figure 6(e): Pixel permuted Image

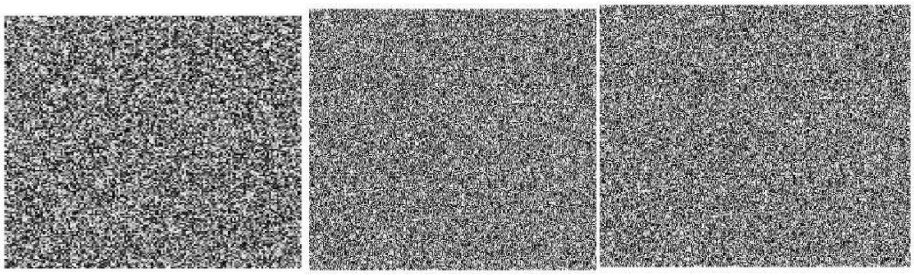

Figure 6(f): Pixel values changed after diffusion

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

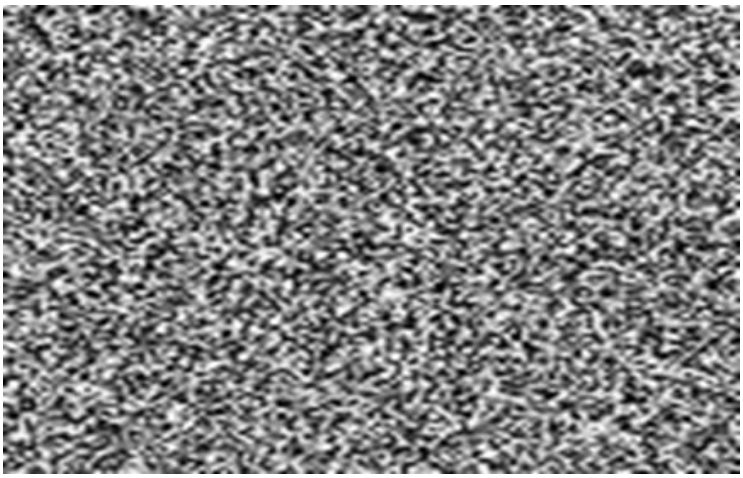

Figure 6(g): Encrypted Image

Figure 6(h): Decrypted Image

The test results involve analyzing 20 distinct photographs sized 256 × 256, then presenting the encrypted and decrypted images obtained. Figures 7 illustrate the encryption and decryption processes utilizing chaotic encryption. The associated confusion and diffusion images are also included.

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

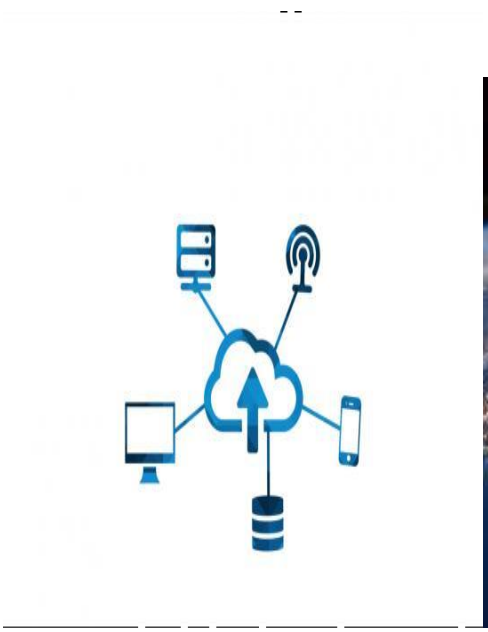

Figure 7(a):Original Image Figure 7(b): Encryption key

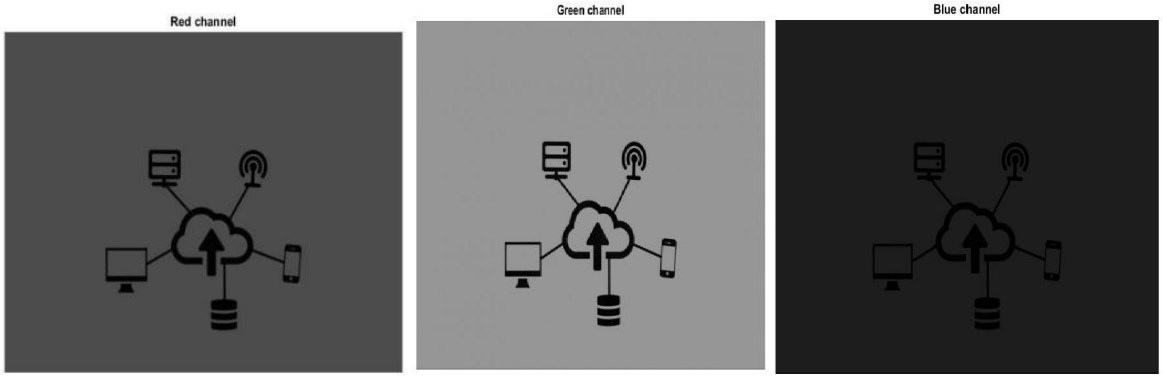

Figure 7(c): Separation of Red Green and Blue component

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

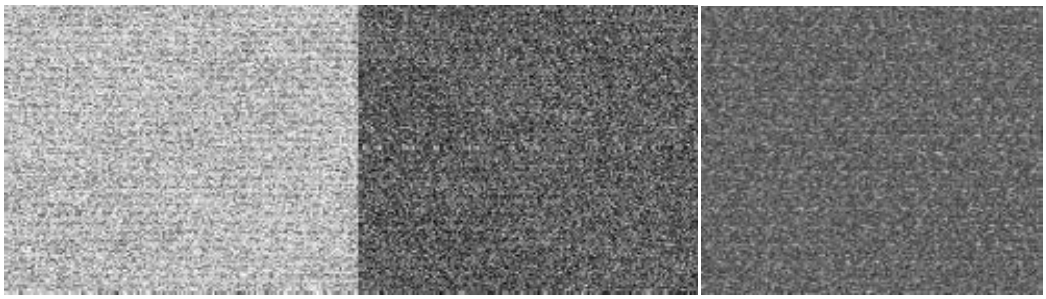

Figure 7(d): Confused Red, green and blue components

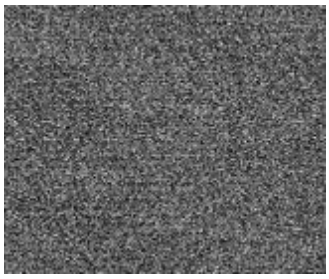

Figure 7(e): Pixel permuted image

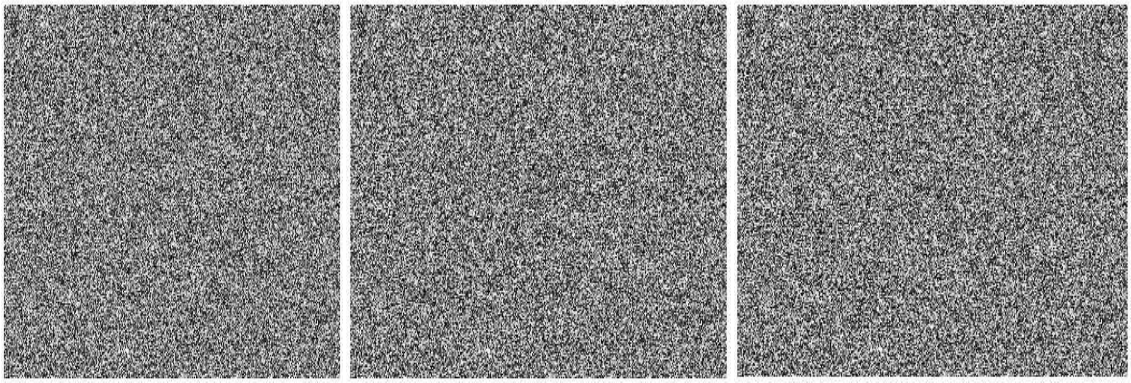

Figure 7(f): Pixel values changed after diffusion

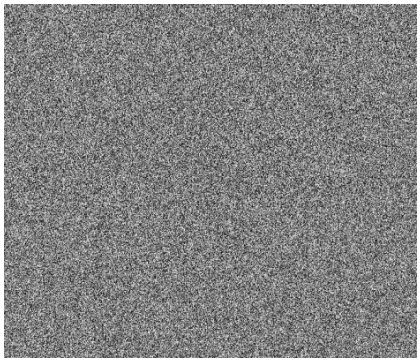

Figure 7(g): Encryption image

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

Figure 7(h): Decrypted image

The new image encryption system was designed according to the previously described design guidelines. Proposed work selected an appropriate chaotic map that maintains chaotic features upon discretization. Opting for a high-dimensional chaotic system expands the key space. Appropriate chaotic maps were selected to maintain complex non-linearity. Avoiding repeated permutations, the diffusion function alters pixel values. The proposed cryptosystem eliminates the cryptographic vulnerabilities present in previous chaos-based encryption systems by integrating all these aspects. Several security analyses were conducted on the new technique, and simulation results indicate that both encryption and decryption processes are effective. The algorithm demonstrates strong security and robustness. Table 2 shows the Comparison table Performance metrics for different images

Table 2: Comparison table Performance metrics for different images

Image	Average Delay (ms)	Throughput (Mbps)	Packet Delivery Ratio (%)
Image 1	8	110	95
Image 2	9	105	96
Image 3	12	98	93
Image 4	7	115	97
Image 5	11	100	94
Image 6	10	102	96
Image 7	9	108	95
Image 8	13	96	92
Image 9	8	112	96
Image 10	10	100	97

Various criteria were used to evaluate the efficiency and reliability of cryptographic operations performed on a variety of photographs. The average delay, measured in milliseconds, varied from 7 to 13 milliseconds among the different images, suggesting a consistent processing time for cryptographic activities. The throughput, which indicates the speed of data transfer, ranged from 96 to 115 Mbps, with the majority of photos sustaining a throughput exceeding 100 Mbps, showcasing effective data processing capabilities. The packet delivery ratio, which indicates the percentage of correctly transmitted data packets, regularly ranged from 92% to 97%. The findings highlight the strength of the cryptographic system, showing little effect on real-time applications and maintaining secure transfer of encrypted data packets across various image datasets.

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

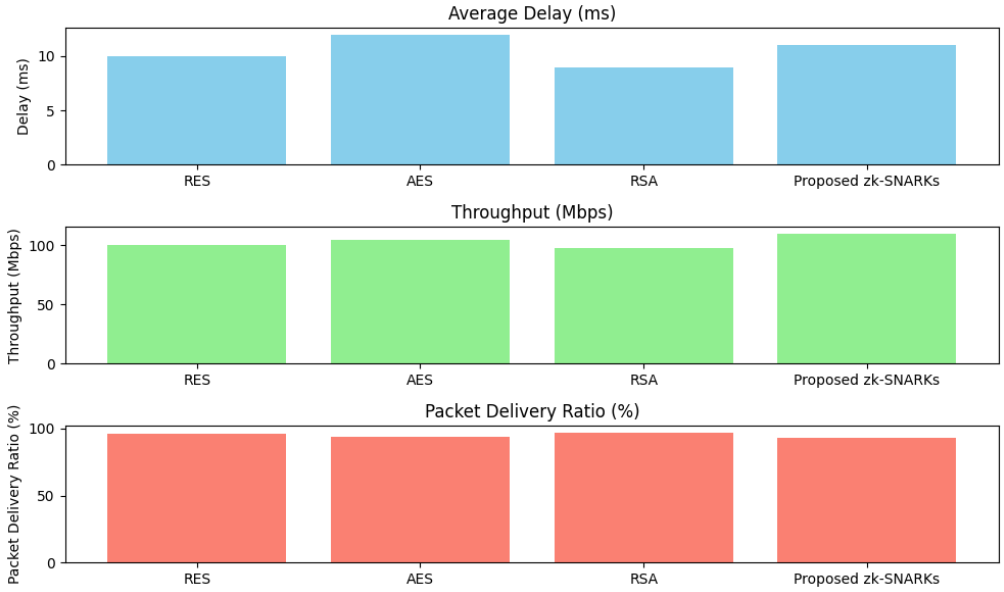

Figure 8: Performance metrics comparison with Existing algorithm

Cryptographic algorithms such as RES, AES, RSA, and Proposed zk-SNARKs were assessed using three main metrics: average latency, throughput, and packet delivery ratio

5 Future work and Conclusions

In conclusion, this research work has described how ZKPs could revolutionize cybersecurity by putting user privacy and data secrecy first. The proposed work has comprehensively investigated ZKPs and highlighted the benefits of Zero-Knowledge Proofs in keeping system performance and enforcing strong security protocols. ZKPs have the potential to overhaul cybersecurity in many domains, including secure transactions, authentication, and identity management. With ZKPs, cryptographic models can achieve stronger security guarantees without compromising system performance or reliability. There exist several areas of research interest in zero-knowledge proofs and cybersecurity. First, investigating the scalability and efficiency of ZKP protocols in distributed networks and real-time applications will be a good start. Also, developing cryptographic primitives and protocol designs using ZKPs could help in enhancing ZKP-based solution capabilities. Additionally, overcoming the practical implementation barriers and boost their interoperability ZKPs with other cryptographic systems will help ZKPs begin to emerge in real-world scenarios. Further research and development in ZKPs will be critical in maximizing real-world potential against emerging cybersecurity risks and driving privacy-centered technology.

References

[1] Soewito, B., & Marcellinus, Y. (2021). IoT security system with modified Zero Knowledge Proof algorithm for authentication. Egyptian Informatics Journal, 22(3), 269-276.

[2] Major, W., Buchanan, W. J., & Ahmad, J. (2020). An authentication protocol based on chaos and zero knowledge proof. Nonlinear Dynamics, 99, 3065-3087.

[3] Boubakri, W., Abdallah, W., & Boudriga, N. (2021). ZAO-AKA: a zero knowledge proof chaotic authentication and key agreement scheme for securing smart city cyber physical system. Wireless Networks, 27(6), 4199-4215.

[4] Yang, R., Gao, H., Si, F., & Wang, J. (2024). Advancing User Privacy in Virtual Power Plants: A Novel Zero-Knowledge Proof-Based Distributed Attribute Encryption Approach. Electronics, 13(7), 1283.

[5] Vandana Roy. "An Effective FOG Computing Based Distributed Forecasting of Cyber-Attacks in Internet of Things" Journal of Cybersecurity and Information Management, Vol. 12, No. 2, 2023 ,PP. 8-17.

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

[6] Al-Aswad, H., El-Medany, W. M., Balakrishna, C., Ababneh, N., & Curran, K. (2021). BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. Arab Journal of Basic and Applied Sciences, 28(1), 154-171.

[7] Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. Journal of Information Security and Applications, 80, 103678.

[8] Moya, C. V., Bermejo Higuera, J. R., Bermejo Higuera, J., & Sicilia Montalvo, J. A. (2023). Implementation and Security Test of Zero-Knowledge Protocols on SSI Blockchain. Applied Sciences, 13(9), 5552.

[9] Moya, C. V., Bermejo Higuera, J. R., Bermejo Higuera, J., & Sicilia Montalvo, J. A. (2023). Implementation and Security Test of Zero-Knowledge Protocols on SSI Blockchain. Applied Sciences, 13(9), 5552.

[10] Ren, Z., Yan, E., Chen, T., & Yu, Y. (2024). Blockchain-based CP-ABE data sharing and privacy-preserving scheme using distributed KMS and zero-knowledge proof. Journal of King Saud University-Computer and Information Sciences, 101969.

[11] V. Roy. "Breast cancer Classification with Multi-Fusion Technique and Correlation Analysis" Fusion: Practice & Applications, Vol. 9, No. 2, 2023 ,PP. 48-61.

[12] P. Kumar, A. Baliyan, K. R. Prasad, N. Sreekanth, P. Jawarkar, V. Roy, E. T. Amoatey, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5713092, 15 pages, 2022. https://doi.org/10.1155/2022/5713092

[13] Chaeikar, S. S., Alizadeh, M., Tadayon, M. H., & Jolfaei, A. (2022). An intelligent cryptographic key management model for secure communications in distributed industrial intelligent systems. International Journal of Intelligent Systems, 37(12), 10158-10171.

[14] Surinder Kaur , Shivani Mankotia , Pooja Bharadwaj, Study of Multi-Prime RSA, Fusion: Practice and Applications, Vol. 1 , No. 1 , (2020) : 40-48 (Doi : https://doi.org/10.54216/FPA.010105)

[15] Harsh Jain , Parv Bharti , Arun Kumar Dubey , Preetika Soni, Identification of Facial Expressions using Deep Neural Networks, Fusion: Practice and Applications, Vol. 2 , No. 1 , (2020) : 22-30 (Doi : https://doi.org/10.54216/FPA.020101)

[16] Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks, 27(2), 1515-1555.

[17] Gadde, S., Amutharaj, J., & Usha, S. (2023). A security model to protect the isolation of medical data in the cloud using hybrid cryptography. Journal of Information Security and Applications, 73, 103412.

[18] Bhagat, V., Kumar, S., Gupta, S. K., & Chaube, M. K. (2023). Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. Concurrency and Computation: Practice and Experience, 35(1), e7425.

[19] Chen, Z., Jiang, Y., Song, X., & Chen, L. (2023). A survey on zero-knowledge authentication for internet of things. Electronics, 12(5), 1145.

[20] Mohamed, N. N., Yussoff, Y. M., Saleh, M. A., & Hashim, H. (2020). Hybrid cryptographic approach for internet ofhybrid cryptographic approach for internet ofthings applications: A review. Journal of Information and Communication Technology, 19(3), 279-319.

[21] R.Pandi Selvam, Performance of MAODV and ODMRP Routing Protocol for Group Communication in Mobile Ad Hoc Network, International Journal of Wireless and Ad Hoc Communication, Vol. 1 , No. 1 , (2020) : 26-32 (Doi : https://doi.org/10.54216/IJWAC.010104)

[22] M. Ilayaraja, Particle Swarm Optimization based Multihop Routing Techniques in Mobile ADHOC Networks, International Journal of Wireless and Ad Hoc Communication, Vol. 1 , No. 1 , (2020) : 47-56 (Doi : https://doi.org/10.54216/IJWAC.010105)

[23] Sharma, N. (2017). A Review of Information Security using Cryptography Technique. International Journal of Advanced Research in Computer Science, 8(4).

[24] Subramani, S., & Svn, S. K. (2023). Review of security methods based on classical cryptography and quantum cryptography. Cybernetics and Systems, 1-19.

[25] Logunleko, K. B., Adeniji, O. D., & Logunleko, A. M. (2020). A comparative study of symmetric cryptography mechanism on DES AES and EB64 for information security. Int. J. Sci. Res. in Computer Science and Engineering, 8(1).

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024

[26] Andino Maseleno, Design of Optimal Machine Learning based Cybersecurity Intrusion Detection Systems, Journal of Cybersecurity and Information Management, Vol. 0 , No. 1 , (2019) : 32-43 (Doi : https://doi.org/10.54216/JCIM.000103)

[27] Ahmed A. Elngar , Salah-ddine KRIT, Performance Analysis of Machine Learning based Botnet Detection and Classification Models for Information Security, Journal of Cybersecurity and Information Management, Vol. 0 , No. 1 , (2019) : 44-53 (Doi : https://doi.org/10.54216/JCIM.000104)

[28] Kapoor, V., & Yadav, R. (2016). A hybrid cryptography technique for improving network security. International Journal of Computer Applications, 141(11), 25-30.

[29] Miriam, H., Doreen, D., Dahiya, D., & Rene Robin, C. R. (2023). Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. Intelligent Automation & Soft Computing, 35(2).

[30] Abualkishik, A. Z., & Alwan, A. A. (2022). Trust aware aquila optimizer based secure data transmission for information management in wireless sensor networks. Journal of Cybersecurity and Information Management, 9(1), 40-51.

[31] Vandana Roy. "An Improved Image Encryption Consuming Fusion Transmutation and Edge Operator." Journal of Cybersecurity and Information Management, Vol. 8, No. 1, 2021 ,PP. 42-52.

[32] Zaki, A. M., Abdelhamid, A. A., Ibrahim, A., Eid, M. M., & El-Kenawy, E. S. M. (2024). Metaheuristic Optimization for Enhancing Cyber Security Index Prediction: A DTO+ FGW Approach with MLP Integration. International Journal of Advances in Applied Computational Intelligence, 4(2), 15-5.

[33] Reem N. Yousef, Marwa M. Eid, Mohamed A. Mohamed, Classifsication of Diabetic Foot Thermal Images Using Deep Convolutional Neural Network, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 1 , (2023) : 17-32 (Doi : https://doi.org/10.54216/JISIoT.080102)

[34] Ahmed Abdelhafeez, Hoda K. Mohamed, Skin Cancer Detection using Neutrosophic c-means and Fuzzy c-means Clustering Algorithms, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 1 , (2023) : 33-42 (Doi : https://doi.org/10.54216/JISIoT.080103)

Doi : https://doi.org/10.54216/JCIM.140110
Received: January 09, 2024 Revised: March 12, 2024 Accepted: June 09, 2024