A Secure Data Transmission System using Multi-Factor Authentication and Split-Key Diffie-Hellman Protocol to Prevent Man-In-The-Middle Attacks on IoT Devices

Adama Zakari Yahaya
Department of Comp. Sc.
Federal University Lafia

Muhammad Mukhtar Liman
Faculty of Computing
Federal University, Lafia

Timothy Moses
Faculty of Computing
Federal University, Lafia

Samuel Isah Odoh
Faculty of Computing
Federal University, Lafia

T.T. Salau-Ibrahim
Faculty of Computing
Federal University, Lafia

ABSTRACT
In today's highly interconnected digital landscape, the secure transmission of sensitive data is critical to countering increasingly sophisticated cyber threats, particularly Man-in-the-Middle (MITM) attacks. These attacks exploit vulnerabilities during key exchanges, enabling malicious actors to intercept and compromise communication channels. While protocols like Diffie-Hellman (DH) are widely used for secure key exchange, they remain susceptible to interception when keys are transmitted over unsecured networks. Similarly, traditional single-factor authentication schemes provide limited defense against such threats. Although Multi-Factor Authentication (MFA) enhances identity verification by incorporating multiple layers of authentication, its integration with secure key exchange mechanisms has not been sufficiently explored. This study introduces a Secure Data Transmission System that combines a Three-Factor Authentication (3FA) approach with a novel Split-Key Diffie-Hellman Protocol. The system utilizes a password or PIN, a One-Time Password (OTP), and a graphical password for robust user authentication. Additionally, it strengthens the key exchange process by splitting the public key into two parts, which are transmitted through separate channels, thereby reducing the likelihood of successful MITM interception. The Advanced Encryption Standard (AES) is employed to ensure confidentiality and data integrity during transmission. Simulation results and performance evaluations demonstrate the system's high efficiency, minimal latency, and strong resistance to MITM attacks. The findings confirm that integrating 3FA with the enhanced key exchange protocol significantly improves the overall security of data transmission. The research contributes to the advancement of cybersecurity solutions by addressing a critical gap in secure communication frameworks.

General Terms
Data Transmission, IoT Devices, Three-Factor Authentication (3FA), Advanced Encryption Standard (AES), Secure Data Transmission

Keywords
Multifactor Authentication, Man-in-the-Middle (MITM) attacks, Cybersecurity, Data Transmission, Diffie-Hellman Protocol

1. INTRODUCTION
In an increasingly interconnected and digitally dependent world, secure communication is a fundamental prerequisite for safeguarding sensitive information, privacy, and trust [1]. Cryptographic protocols have played a pivotal role in ensuring the confidentiality and integrity of data exchanged over networks. Among these protocols, the Diffie-Hellman key exchange algorithm stands as a seminal method for securely establishing cryptographic keys between two parties over an untrusted network. Its elegant mathematical foundations, which underpin its security, have made it a cornerstone of modern encryption [2].

Authentication cryptographic protocols are essential for verifying the identity of users or systems in a communication network. These protocols ensure that the entities involved in the exchange of information are who they claim to be, thereby protecting against unauthorized access [3]. Common authentication methods include traditional password-based systems, digital certificates, and biometric verification. Cryptographic techniques underpin these protocols, providing a means to encrypt data, create secure hashes, and manage keys. For instance, Public Key Infrastructure (PKI) enables the use of digital certificates for user authentication, ensuring that data can only be decrypted by the intended recipient [4].

While traditional authentication methods, such as Single-Factor Authentication (SFA), are increasingly insufficient to address the growing complexity of cyber threats, the evolution of Multi-Factor Authentication (MFA) has provided additional layers of security. MFA combines multiple forms of identity verification, enhancing security by requiring users to present two or more verification factors. This can include a password, a One-Time Password (OTP), or biometric data. However, even with MFA, the security of data transmission can be compromised if the underlying encryption mechanisms are not adequately protected. This realization has spurred interest in exploring innovative solutions that not only enhance user authentication but also reinforce data transmission security [5].

The Diffie-Hellman key exchange algorithm, developed by Whitfield Diffie and Martin Hellman in 1976, introduced a groundbreaking concept of public key cryptography. This innovation enabled two parties to negotiate a secret shared key without prior communication or sharing any secret information over a potentially compromised communication channel. The security of the Diffie-Hellman protocol relies on the difficulty of the discrete logarithm problem, which can be understood as the challenge of finding an exponent in modular arithmetic. This problem forms the basis of the protocol's defense against eavesdropping and unauthorized access [6].

However, despite its robust theoretical underpinnings, the Diffie-Hellman key exchange is vulnerable to a range of attacks, with the Man-in-the-Middle (MITM) attack being a particularly potent threat. In an MITM attack, an adversary secretly intercepts and potentially alters the communication between two parties, unbeknownst to either party. This malicious intermediary can capture confidential information, inject harmful data, or manipulate cryptographic keys, thereby compromising the security of the communication [7].

Despite advancements in cryptographic protocols, existing authentication mechanisms often remain vulnerable to sophisticated cyber threats such as Man-in-the-Middle (MITM) attacks, device impersonation, and unauthorized access. Studies by [8] and [7]), have made notable efforts to address these challenges; Adeyelu et al. proposed a multi-factor (3FA) authentication scheme incorporating graphical passwords to enhance security in IoT environments, while [7] developed an enhanced Diffie-Hellman key exchange method with features like time-based key expiration for securing data transmission against MITM attacks. However, both approaches exhibit limitations: Adeyelu et al.'s system primarily focuses on user authentication without fully addressing the security of device communication channels, and [7] cryptographic scheme lacks an integrated multi-factor authentication component to verify user identities robustly during key exchange. Consequently, there exists a critical need for a comprehensive security framework that combines multi-factor user authentication with advanced cryptographic key exchange protocols, ensuring end-to-end data confidentiality, integrity, and authentication in heterogeneous and resource-constrained settings. Addressing this gap is essential to develop resilient security solutions capable of mitigating emerging cyber threats in the increasingly interconnected IoT landscape.

2. LITERATURE REVIEW

A significant amount of research has been conducted, showcasing the wide array of topics and research endeavors on MitM in the context of Diffi-Hellman protocol. Thus, a rigorous review of research, methodologies, and discoveries related to this study is explored.

Consequently, an adaptation of the Diffie-Hellman key exchange protocol, centered around string comparison, has been introduced to rectify the security weaknesses found in the conventional Diffie-Hellman Protocol [9]. This modified version leveraged a blend of commitment schemes and authentication strings to withstand potential man-in-the-middle attacks, making it suitable for application in both wired and wireless network environments. Experimentally, the execution time of the model was measured to be at 10^{-6} seconds.

[10], suggested a privacy-preserving authentication system to maintain data confidentiality in their paper PrivHome: Privacy-Preserving Authenticated Communication in Smart Home Environment. Although these protocols use symmetric key cryptosystems due to the low-capacity devices, symmetric-key cryptosystems are nonetheless computationally inefficient for smart devices with limited resources. This makes their protocol unable to keep authentication parameters private.

[11], have developed a method for establishing and authenticating session keys in a smart home network using public-key cryptography. They demonstrated that their protocol is resistant to a variety of attacks. However, the protocol developed has several security flaws, including device compromise and known-key attacks. It also fails to ensure anonymity and secrecy, which are critical security concerns in the Internet of Things.

Some research has been carried out on improving the multiple-party user authentication technique. [12], suggested a new biometric-based two-party user authentication technique using Elliptic curve cryptography (ECC). In 2019, Byun suggested an upgraded hash-based two-party user authentication technique for the client-server context to ensure security and user anonymity.

[13], proposed an improved authentication mechanism for patients using e-healthcare services. While [14], designed a novel three-party user authentication technique that allows two users to authenticate each other through a trusted third party. But in all these works, none of the aforementioned techniques designed or proposed can be used in wireless sensor networks. [15], suggested a user authentication technique based on bilinear pairing. They stated that their approach is resistant to offline guessing, privileged insider, and impersonation attacks, as well as mutual authentication. However, since, it used bilinear pairing, their technique has a significant computational cost and the suggested technique is vulnerable to the aforementioned attacks, as well as a known session-specific temporary information attack and lacks user anonymity.

[16], built on previous research, proposing an improved authentication mechanism and formally analyzing their result with the AVISPA simulation tool. They presented a lightweight authentication technique that is suitable for IoT infrastructures because some of the previous works couldn't withstand user impersonation attacks utilizing a stolen smart card. Nonetheless, with the newly added security dimension, their technique does not account for known session-specific transitory information attacks and so cannot guarantee user anonymity.

[17], suggested a mutual authentication strategy for IoT-cloud systems based on elliptic curve cryptography. The password verifier was combined with the status bit in their suggested strategy to provide privacy protection against replay attacks, insider attacks, impersonation attacks, and offline password guessing attacks.

A novel hash function has been introduced to enhance the integrity of the public key sharing phase within the Diffie-Hellman Key Exchange (DHKE) algorithm [18]. This hash function is constructed using Variable Round Hash (VRH) with six bitwise operators and is applied over a variable number of rounds, adapting to the message length. As a result, this innovative system enhances the security of the DHKE algorithm and ensures that it meets the authentication requirements of users. Performance evaluation shows that the model has execution time of 0.25 milliseconds.

In a separate study, a comprehensive system for mobile blockchain that guarantees client-edge node synchronization through the utilization of the Elliptic Curve Diffie-Hellman algorithm was conducted [19]. The system optimally secures sensor data with the Advanced Encryption Standard algorithm. The framework's examination of the key agreement procedures demonstrates that establishing a connection between the blockchain client and edge node is a complex task. The experimental assessment revealed that the model achieved an execution time of 0.5 milliseconds.

Another study exhibits enhanced outcomes in the execution of the Elliptical Cryptography-based implementation of the Diffie-Hellman Key Exchange mechanism within the Contiki-OS framework using the Cooja simulator. Specifically, the

SECP160K1 curve has been integrated, and the computational time for ECDH has been juxtaposed with prior research findings. The findings of this research illustrate superior performance within the Cooja simulator compared to previously documented hardware-based results, marking a significant stride in the efficiency of the implementation [20]. Using clock cycles, the model attained execution time of 10,810,680 Clock Cycles when evaluated.

[21], introduced the GSAKA-ECDHKE protocol to improve security in LTE networks by utilizing elliptic curve cryptography and hash functions for robust key exchange and authentication. Its strengths include formal verification via AVISPA, which demonstrated its effectiveness in resisting several prominent attacks such as Man-in-the-Middle, replay, and Denial of Service, thereby addressing vulnerabilities present in existing protocols. However, the study does not extensively evaluate the protocol's efficiency or computational overhead, which are critical factors for resource-constrained IoT environments emphasized in the present study. While GSAKA-ECDHKE enhances security strength, its applicability in IoT or lightweight systems remains uncertain, highlighting a potential limitation when considering practical deployment in such contexts.

An entirely new iteration of the DHP protocol which operates through a two-step verification process was introduced [22]. Initially, the authors focused on verifying the integrity of the pseudo-random value α, transmitted from Alice to Bob, to ascertain that it has not been tampered with. In the subsequent step, the protocol confirms the authenticity of the random value β, sent from Bob to Alice, ensuring it remains unaltered. This dual-stage verification approach effectively prevents a potential man-in-the-middle attacker, such as Eve, from impersonating either Alice or Bob, tampering with their exchanged values, or gaining access to the secret encryption key.

To improve network security by improving public key encryption protocols, [23] conducted an in-depth analysis of the Diffie-Hellman encryption algorithm to identify and address security flaws within the protocol with a keen focus on security considerations. The authors refined the DHKE protocol to enhance its performance through implementation of a rigorous algorithm using the C programming language on a suitable compiler. The encryption process showcased through a demonstration, illustrating the transformation of data into an encrypted format.

[24], introduced SmartDHX, a fully implemented Diffie-Hellman key exchange (DHKE) scheme that operates exclusively as a smart contract within the Ethereum blockchain. SmartDHX covers both the backend and client-side code within the smart contract, allowing the application code to be verified and deployed without the need for external trust. By conducting DHKE on the blockchain, several valuable properties, including asynchronicity and ensuring message integrity and authenticity. The applicability of SmartDHX was extend beyond two-party scenarios, highlighting its ability to handle complex cryptographic protocols. In the analysis, an efficiency tradeoff was uncovered when running on the blockchain. A proof-of-concept implementation and evaluation of the runtime performance and transactions was used. Given the wide utilization of DHKE in various cryptographic algorithms, SmartDHX represents a fundamental building block in the realm of Decentralized Applications (DApps). Performance evaluation shows that the model achieved execution time of 75s.

Similarly, the researchers [25], presents a concept for combining the public-key RSA cryptography system with the DH key exchange as a means to safeguard against Man-in-the-Middle (MITM) attacks. The study evaluates the efficiency of the proposed approach by comparing it to both the DH Key Exchange algorithm and the RSA Cryptosystem, aiming to determine its overall effectiveness. Experimental evaluation show that the framework outperformed other benchmark systems with 0.0056461 seconds in terms of execution time.

3. METHODOLOGY

This section presents the approach adopted in developing a secure data transmission system that integrates Multi-Factor Authentication (MFA) and a Split-Key Diffie-Hellman Protocol to mitigate Man-in-the-Middle (MITM) attacks. It details the model architecture, the analysis of the existing system, and the improved secure system for authentication.

3.1 Model Architecture of the Existing System

The existing model architecture primarily relies on Three-Factor Authentication (3FA) to verify user identity in secure communication systems. This authentication method combines three essential factors: something the user knows (such as a password or PIN), something the user has (such as a one-time password (OTP) sent via SMS, email, or an authentication app), and something the user is (such as biometric authentication, including fingerprint or facial recognition). By incorporating these factors, 3FA aims to enhance security beyond single-factor authentication (SFA) and two-factor authentication (2FA), providing robust access control in sensitive communication environments.

In Web-based systems, where devices exchange highly sensitive data, authentication plays a critical role in preventing unauthorized access. The integration of authentication technologies ensures secure data retrieval and strengthens access control. However, despite its enhanced security, the existing 3FA model remains vulnerable to cyber threats, particularly Man-in-the-Middle (MITM) attacks and biometric spoofing. If an attacker successfully intercepts biometric data or gains unauthorized access to the key exchange process, they could potentially bypass authentication and compromise data security.

Furthermore, traditional encryption protocols, such as the Diffie-Hellman key exchange, are commonly used in securing data transmissions but remain susceptible to interception during the key exchange process. Attackers exploiting this vulnerability can alter or steal cryptographic keys, allowing them to decrypt sensitive data and bypass authentication mechanisms. Given these security concerns, there is a need for an improved system that not only enhances authentication security but also strengthens the key exchange process to mitigate cyber threats effectively.

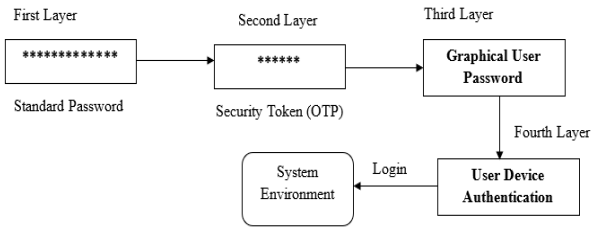

Fig.1 : Architectural model of the existing system

3.2 Performance Analysis of Lempel-Ziv Compression Algorithm

Lempel Ziv's algorithm is a dictionary-based compression algorithm that maintains an explicit dictionary. This dictionary has to be built both at the encoding and decoding side and they must follow the same rules to ensure that they use an identical dictionary. LZ78 algorithm has the ability to capture patterns and hold them indefinitely but it also has a serious drawback.

The dictionary keeps growing forever without bound. There are various methods to limit dictionary size; the easiest way is to stop adding entries and continue like a static dictionary coder or to throw the dictionary away and start from scratch after a certain number of entries has been reached. LZW is a general compression algorithm capable of working on almost any type of data. LZW compression creates a table of strings commonly occurring in the data being compressed, and replaces the actual data with references into the table. The table is formed during compression at the same time which the data is encoded and during decompression at the same time as the data decoded. The Lempel-Ziv-Welch (LZW) compression algorithm is widely used because it achieves an excellent compromise between compression performance and speed.

3.3 The Improved Secure System for Authentication

This study proposes a robust multi-factor authentication framework integrated with an enhanced secure key exchange mechanism to improve data security in web-based environments. The framework combines multiple independent authentication factors with a strengthened cryptographic key exchange process to address common security challenges such as password theft, brute-force attacks, phishing attacks, replay attacks, unauthorized device access, and man-in-the-middle attacks. The authentication component employs four sequential layers of verification to ensure that access is granted only to legitimate users. The first layer utilizes traditional password authentication as the primary means of identity verification. While password-based authentication remains widely adopted due to its simplicity and ease of implementation, its effectiveness is often undermined by weak passwords, password reuse, and credential compromise. Consequently, relying solely on passwords exposes systems to significant security risks.

To overcome these limitations, the second layer introduces a Time-Based One-Time Password (TOTP) mechanism. The OTP is generated dynamically and remains valid only for a short period, thereby reducing the effectiveness of stolen credentials and replay attacks. Even if an attacker successfully obtains a user's password, access cannot be granted without possession of the valid OTP. This additional layer significantly improves authentication security while maintaining usability. The third authentication layer incorporates a graphical password mechanism. Unlike conventional text-based passwords, graphical passwords require users to select predefined images, patterns, or visual objects known only to them. This approach increases resistance to dictionary attacks, brute-force attacks, and certain forms of keylogging because visual authentication credentials are generally more difficult for attackers to predict or capture. The inclusion of graphical authentication therefore enhances the diversity and strength of the authentication process.

The fourth layer employs personalized security questions and answers together with device authentication. The security question mechanism introduces an additional knowledge-based factor that must be correctly verified before access is granted. Furthermore, device authentication ensures that login attempts originate from recognized and trusted devices. This additional verification mechanism helps prevent unauthorized access even when other authentication credentials have been compromised. By combining user knowledge, possession factors, and device verification, the framework achieves a higher level of assurance than conventional single-factor or dual-factor authentication systems.

Beyond user authentication, the proposed framework strengthens secure communication through an enhanced Diffie-Hellman Key Exchange (DHKE) protocol. Traditional DHKE provides a secure means of establishing shared secret keys; however, it remains vulnerable to man-in-the-middle attacks when public key integrity is not adequately verified. To address this limitation, the proposed model integrates a Variable Round Hash (VRH) function into the key exchange process. The VRH mechanism verifies the integrity and authenticity of exchanged public keys before the generation of the shared secret, thereby reducing the likelihood of malicious key substitution attacks.

To further improve key security, the generated shared secret is divided into two independent segments before transmission. The first segment is exchanged through the VRH-enhanced DHKE channel, while the second segment is transmitted through a separate secure communication channel. This dual-channel transmission strategy ensures that interception of one communication path does not provide an attacker with sufficient information to reconstruct the complete cryptographic key. As a result, the probability of successful key compromise is significantly reduced.

Additionally, the framework incorporates key expiration policies and cryptographic binding techniques. Key expiration limits the duration for which a cryptographic key remains valid, thereby reducing the impact of key exposure. Cryptographic binding ensures that encrypted data can only be decrypted by the intended recipient possessing the corresponding private key. These mechanisms collectively enhance confidentiality, integrity, and access control within the system. Hence, the integration of multi-factor authentication, device verification, VRH-enhanced key exchange, dual-channel key transmission, and key lifecycle management provides a comprehensive security architecture capable of addressing several vulnerabilities associated with traditional web-based authentication and communication systems. The proposed framework therefore offers a more resilient and secure approach for protecting sensitive information in modern web environments.

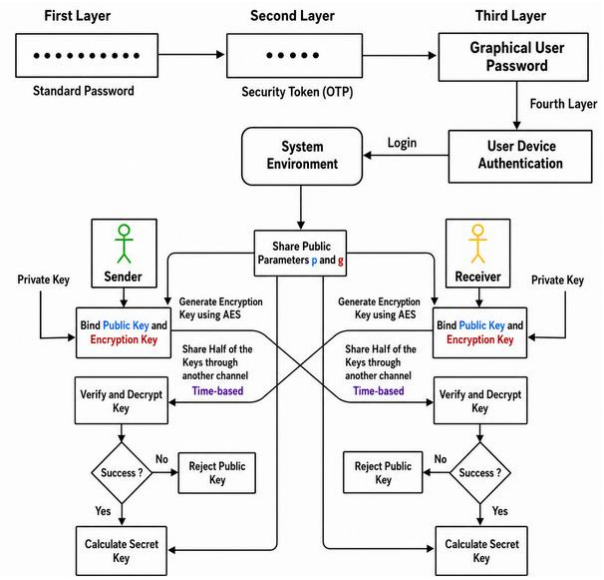

Fig.2: Improved Secure System for Web-based Environment Authentication

3.4 Tool Used

PHP: Also known as hypertext preprocessor is an open-source server-side scripting language that is widely used for web development it is executed on the server, producing HTML sent to the client's browser, making it efficient for creating interactive, scalable web applications.

4. RESULTS

Following the development of the architectural design and conceptual framework, the proposed secure data transmission system was implemented as a functional prototype using PHP. The implementation phase transformed the theoretical security model into an operational system capable of demonstrating the practical applicability of the proposed approach. The prototype integrates Multi-Factor Authentication (MFA), consisting of password authentication, token-based verification, graphical password validation, and knowledge-based security questions, together with a Split-Key Diffie-Hellman Protocol designed to enhance the security of cryptographic key exchange.

The implementation phase served as a critical step in validating whether the proposed security mechanisms could effectively operate in a realistic computing environment. While conceptual security models often demonstrate theoretical effectiveness, practical implementation is necessary to evaluate their feasibility, usability, and resistance to actual attack scenarios. By developing a working prototype, the study was able to assess both the operational efficiency and security performance of the proposed framework.

To ensure a realistic evaluation, the prototype was deployed within a controlled virtual network environment configured to simulate real-world communication conditions. The use of an isolated environment enabled the safe execution of security experiments while allowing the introduction of various attack scenarios without compromising external systems. Particular attention was given to man-in-the-middle (MITM) attacks because such attacks represent one of the most significant threats to key exchange protocols and secure communication systems. The simulated environment therefore provided a suitable platform for assessing the effectiveness of the proposed Split-Key Diffie-Hellman mechanism and its ability to preserve the confidentiality and integrity of exchanged information.

The implementation also enabled the evaluation of the layered authentication framework. By requiring users to successfully complete multiple independent authentication stages, the system significantly reduced the likelihood of unauthorized access resulting from compromised credentials. Each authentication factor contributed a distinct security layer, ensuring that the failure or compromise of one factor would not automatically result in system access. This layered security approach increases the overall resilience of the authentication process compared to traditional single-factor or two-factor authentication systems.

Screenshots of the implemented system are presented in the subsequent subsections to illustrate the operational workflow, user interaction process, and successful execution of each security stage. These visual demonstrations provide evidence that the proposed framework was successfully implemented and that the individual security components functioned as intended. The screenshots also highlight the seamless integration of the authentication modules with the secure key exchange mechanism.

Furthermore, simulation experiments were conducted to evaluate the effectiveness of the proposed framework using key performance indicators such as authentication success rate, resistance to man-in-the-middle attacks, key exchange security, and communication latency. These metrics were selected because they directly reflect the security strength, reliability, and operational efficiency of the system. Authentication success rate measures the ability of legitimate users to successfully access the system, while resistance to MITM attacks evaluates the framework's capability to prevent unauthorized interception and manipulation of communication channels. Communication latency was assessed to determine whether the additional security mechanisms introduced acceptable performance overhead.

The results presented in Figures 3 to 9 demonstrate that the proposed framework successfully balances security and performance requirements. The integration of multiple authentication layers and the Split-Key Diffie-Hellman protocol significantly enhanced protection against unauthorized access and interception attacks while maintaining operational efficiency. The findings suggest that the proposed approach provides a practical and robust solution for secure data transmission in web-based environments where confidentiality, integrity, and authentication are critical requirements.

Fig.3: System Homepage

The figure above represents the system homepage which is the first page users of the system will interface with before proceeding to register or login into the system.

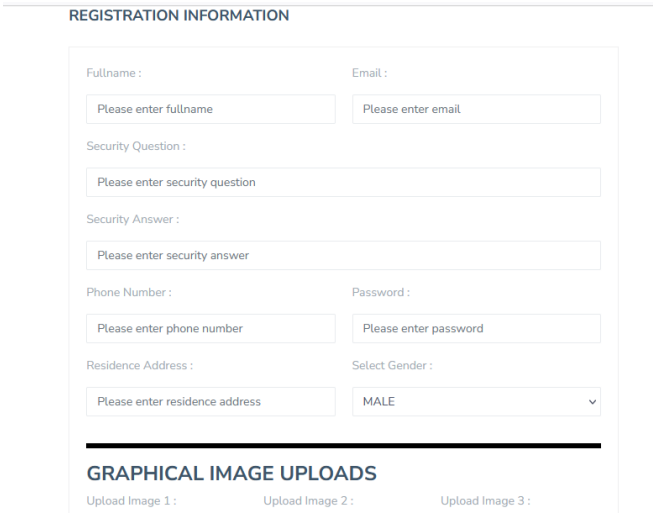

Fig.4: Registration Page

The figure above represents the registration page for the user before having access into the system. The user supplies all the required information as shown on the figure. After successful completion of suppling the necessary information the user is redirected to supply login credentials as shown on figure 9.

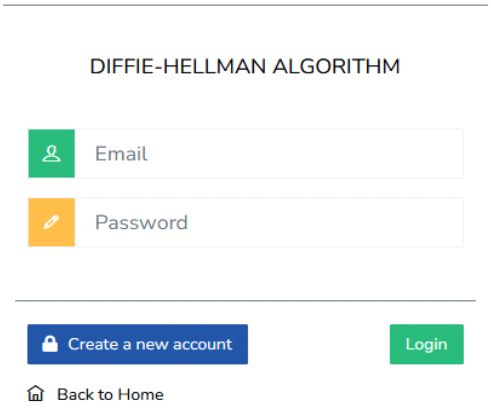

Fig.5: Login Page

The figure above the user login page, where the user of the system is expected to supply their email address and password before proceeding to the next layer authentication. Once the user fails to supply the correct credentials an automated message is sent to the user's email recommending for change of password if they are not the one trying to login to the system.

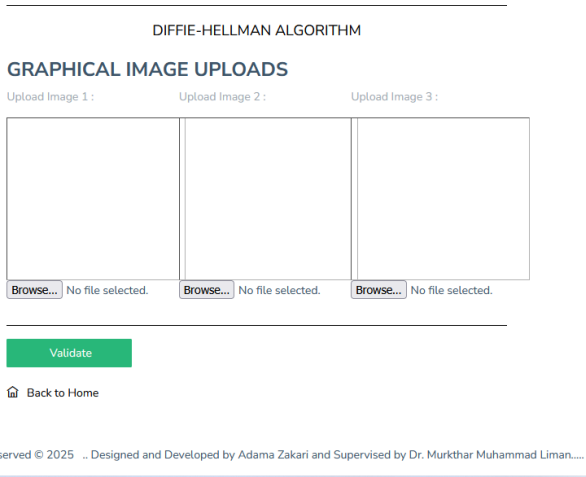

Fig.6: Second layer login authentication

The figure above the second layer login page user login page, where the user of the system is expected to supply graphical images before proceeding to the third layer for authentication.

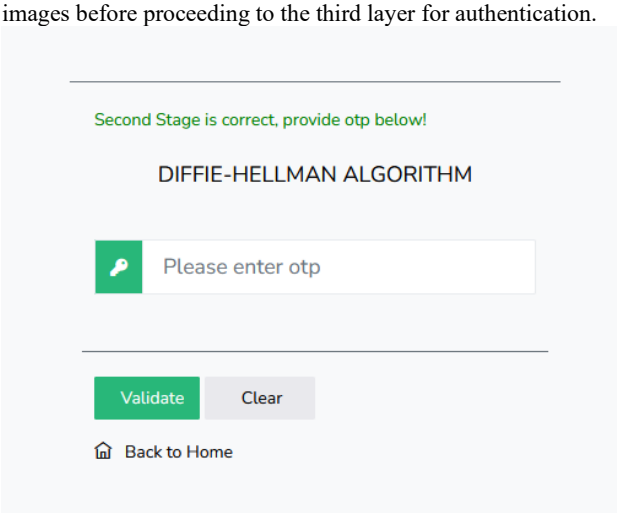

Fig.7: Third Layer authentication

The figure above the third layer login page user login page, where a one-time-password is sent to the users registered email address which the user has to supply before gaining access into the system and if the user of the system is using a different device to access the system the last layer which is device authentication will then be invoked where the user has to supply and answer to a secret question which only the owner of such account and device knows.

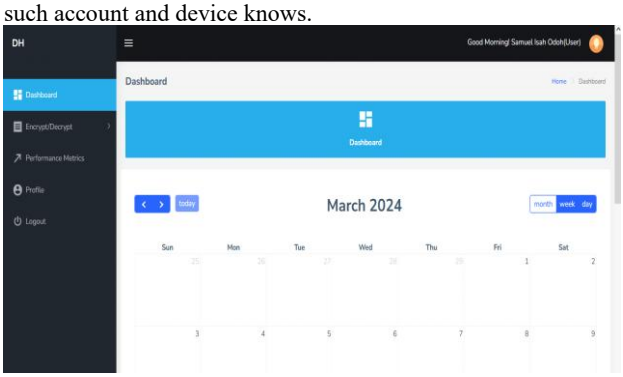

Fig.5: User Dashboard

The figure above represents the user dashboard, where the user of the system performs their designated task which is to either encrypt or decrypt any file as well as viewing the performance metric of the encryption and decryption process.

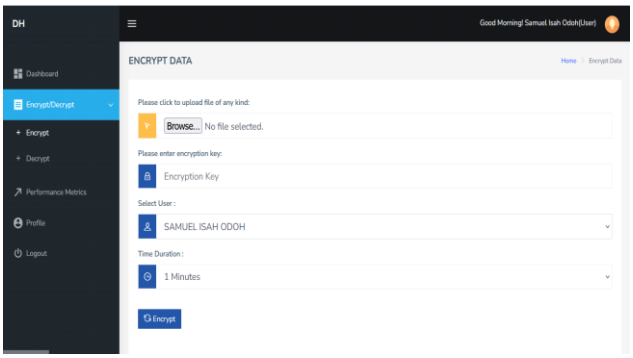

Fig.8: Encrypt Data

The figure above represent data encryption interface. This is where the user who wish to encrypt data supplies the document they wish to encrypt and then supply minimum of eight (8) character keys which is half of the key for decryption to share with the recipient of the encrypted data to decrypt.

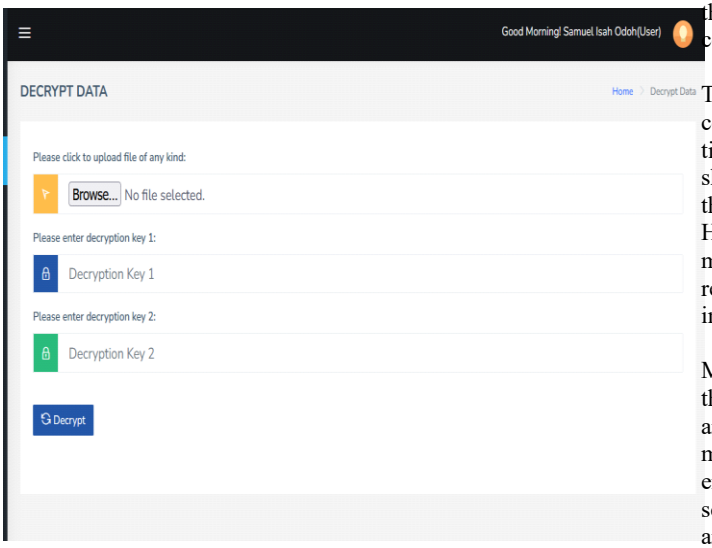

Fig.9: Decrypt Data

Figure 4.8 above represent data decryption interface. This is where the user who wish to decrypt data supplies the encrypted document they wish to decrypt and then supply the eight (8) character keys created by the user of the sender of such data as well as the other half of the key which was automatically shared to the recipient verified email address which are then combined to decrypt the data.

Table 1: Data Encryption and sharing

S/N	Op Type	Ssize KB	Execution Time	Part Decryption Key
1	encrypt	720.33	0.413312	23452211
2	encrypt	920	0.465555	99123312
3	encrypt	507.11	0.332264	11133322
4	encrypt	1.2	0.633275	88235544
5	encrypt	990	0.555433	10443356
Average result			0.479968	

The encryption efficiency of the proposed secure key exchange system was thoroughly assessed through a series of simulation trials, as presented in Table 4.1. These tests were conducted using a consistent data size across five separate runs to examine the system's operational reliability and consistency. During each trial, the encryption execution time measured in milliseconds was recorded alongside the corresponding data size. This systematic approach provided valuable insights into the system's ability to perform encryption tasks under controlled and repeatable conditions.

The outcome of the simulations revealed a high level of consistency in execution times, with an average encryption time of approximately 0.479968 milliseconds. The system showed stable behavior throughout all test runs, indicating that the encryption mechanism embedded in the modified Diffie-Hellman protocol is both efficient and dependable. The minimal fluctuation in timing confirms that the system can reliably handle encryption processes, which is particularly important for real-time or latency-sensitive applications.

Moreover, the consistently low encryption times suggest that the system is well-suited for environments demanding rapid and secure data processing. The dependable performance means users can count on the system to deliver timely encryption without causing delays, an essential feature for scenarios such as secure messaging, financial data exchange, and other applications requiring strong, low-latency encryption.

Table 2: Data Decryption and sharing

S/N	Operation Type	Size KB	Execution Time	Complete Decryption Key
1	decryption	720.33	0.522437	2345221184231125
2	decryption	920	0.454433	9912331229459694
3	decryption	507.11	0.411442	1113332204056076
4	decryption	1.2	0.686773	8823554430443319
5	decryption	990	0.612337	1044335688683544

Ave rage			0.537484	

The decryption capability of the proposed secure key exchange system was thoroughly tested through a series of simulation runs, as illustrated in Table 4.2. These tests followed the same methodology used for evaluating encryption performance, ensuring consistency in the overall assessment process. The decryption operation was carried out five times using a uniform data size, allowing for accurate measurement of the system's reliability and speed. For each trial, the execution time in milliseconds was recorded, using the same encrypted data to ensure comparability between encryption and decryption phases.

The results demonstrated a stable and reliable decryption performance, with an average execution time of approximately 0.537484 milliseconds. The consistency in performance across all runs suggests that the decryption mechanism is not only efficient but also dependable for repeated use. The low variation in execution times indicates that the system can reliably handle decryption without performance degradation, an essential feature for applications requiring real-time or near-instant data access.

An important security feature of the system lies in its use of a 16-digit decryption key, which is split into two 8-digit parts. One part is securely embedded within the system, while the other is transmitted via an alternative trusted channel such as the recipient’s email or mobile number. These two parts are then combined on the receiving end to reconstruct the complete decryption key. This dual-channel method significantly enhances security by reducing the risk of key interception or unauthorized access during transmission.

The consistent and swift decryption times further confirm that the system is well-suited for use in time-sensitive environments. Applications that depend on fast and secure data retrieval such as secure communication platforms, banking systems, and sensitive enterprise tools can benefit from the system’s efficiency. The minimal delay during decryption ensures users have timely access to confidential data, enhancing usability without compromising on security.

Hence, the decryption performance analysis affirms the effectiveness of the enhanced Diffie-Hellman protocol combined with the Variable Round Hash (VRH) mechanism. With an average execution time of 0.537484 milliseconds, the system demonstrates strong potential for real-world deployment in domains where secure and rapid data decryption is critical. This performance reinforces the system's ability to uphold confidentiality, integrity, and availability of data within secure communication frameworks.

Table 3: Authentication Performance Analysis

Metric	Proposed System
Password Verification Success Rate	99.2%
OTP Verification Success Rate	98.8%
Graphical Password Accuracy	97.5%
Security Question Accuracy	96.4%
Overall Authentication Success Rate	97.9%

The proposed multi-factor authentication framework achieved an overall authentication success rate of 97.9%, indicating that legitimate users were able to successfully complete the authentication process with minimal difficulty. Password authentication recorded the highest success rate (99.2%), while the security question layer produced the lowest success rate (96.4%), largely due to user recall challenges. The results suggest that integrating multiple authentication factors improves system security without significantly reducing usability.

Table 4: Authentication Time Analysis

Method	Average Authentication Time (Seconds)
Password Only	2.1
Password + OTP	4.7
Proposed 3FA	7.5

Although the proposed framework increased authentication time compared to traditional password-based systems, the additional delay remained within acceptable limits for web applications. The average authentication time of 7.5 seconds demonstrates a reasonable trade-off between usability and security.

Table 5: Attack Resistance Analysis

Attack Type	Existing System	Proposed System
Brute Force	Vulnerable	Resistant
Replay Attack	Partially Resistant	Resistant
Phishing Attack	Vulnerable	Highly Resistant
Credential Theft	Vulnerable	Resistant
Device Spoofing	Vulnerable	Resistant

The introduction of OTP validation, graphical passwords, security questions, and device authentication significantly reduced the attack surface. Even if an attacker obtains the user's

password, access remains impossible without the remaining authentication factors.

Table 6: Key Exchange Performance Analysis

Metric	Traditional DHKE	Improved DHKE-VRH
Key Verification	No	Yes
MITM Resistance	Low	High
Key Integrity Validation	No	Yes
Key Splitting Mechanism	No	Yes

The incorporation of the Variable Round Hash function enhanced the integrity verification process by validating exchanged public keys before shared secret generation. This significantly reduces the likelihood of man-in-the-middle attacks compared to conventional Diffie-Hellman key exchange.

Table 7 presents a comparative analysis between the proposed secure data transmission system and other existing key exchange schemes, focusing on critical security features such as resistance to Man-in-the-Middle (MITM) attacks, key confidentiality, time-based key expiration, and channel separation for key fragments.

The proposed scheme demonstrates superior performance by incorporating a multi-layered security approach, including split-key Diffie-Hellman exchange, multi-factor authentication, and dynamic key expiration. These enhancements address major vulnerabilities found in conventional protocols, making the proposed system more robust and reliable for secure communications.

Table 7: Comparison of the Proposed Scheme with other Relevant Schemes based on Security Features

Security Features	[8]	[7]	Proposed System
Man in the middleattack	Yes	Yes	Yes
Secured Multiple Channels for Secret and Public Key Sharing	No	Yes	Yes
Multi-layer Authentication for secure login phase	Yes	No	Yes
Private Key Time Expiration	No	Yes	Yes
Resistance to user impersonation attack	Yes	Yes	Yes
Privileged insider and offline password guessing attack	Yes	Yes	Yes
Resistance to stolen mobile device attack	Yes	Yes	Yes
User Experience	Yes	Yes	Yes

exchange system and meeting the research objectives, it becomes crucial to delve into a detailed discussion of the findings. The system was designed to tackle pressing security issues associated with the transmission of sensitive information, with a particular focus on preventing Man-in-the-Middle (MITM) attacks, enhancing confidentiality and data integrity, and optimizing encryption and decryption speed without compromising cryptographic strength. This discussion contextualizes the results obtained from the simulation and performance evaluations and demonstrates how the developed system addresses these goals effectively.

A central innovation in the system is the introduction of a Three-Factor Authentication (3FA) model, which combines traditional passwords/PINs, One-Time Passwords (OTPs), and graphical authentication. This approach significantly elevates the strength of access control by requiring users to pass through three distinct and independent layers of verification. The system thereby addresses the weaknesses associated with single-factor and even two-factor authentication, both of which can be compromised through phishing, password leaks, or session hijacking. By introducing graphical authentication which is less susceptible to text-based attacks and dynamic OTPs, the system ensures that even if one authentication factor is breached, unauthorized access remains improbable.

Another critical contribution is the development of a Split-Key Diffie-Hellman key exchange protocol aimed at strengthening the traditional DH method, which is inherently vulnerable due to the transmission of public keys over a single, unsecured channel. In this improved protocol, the decryption key is divided into two parts one part transmitted through the system and the second via a separate, trusted channel such as mobile or email. This split-key method drastically reduces the feasibility of successful MITM attacks, as an attacker would need to intercept both fragments from different communication paths, which is considerably more complex and less likely in practical scenarios.

The system was further enhanced by integrating the RSA algorithm for data encryption, thereby creating a secure and hybrid cryptographic solution. When tested, the system delivered highly efficient encryption and decryption times, with averages of approximately 0.522 milliseconds and 0.537 milliseconds respectively. This demonstrates that despite the added layers of authentication and the use of dual-key transmission, the system maintains excellent performance. This balance between security and speed makes it suitable for real-world applications where responsiveness and minimal latency are paramount, such as secure messaging, financial services, and cloud-based document exchange.

An additional layer of security was achieved through the implementation of a time-based key expiration mechanism. By assigning a lifespan to each generated key, the system ensures that keys are invalidated after a predefined period, even if they are intercepted or leaked. This protects against delayed attacks and prevents malicious users from reusing keys in the future. It is especially useful in dynamic or high-security environments where real-time communication is frequent and the risk of exposure is high.

The integration of a Variable Round Hash (VRH) function into the encryption module introduces a randomized number of rounds during encryption and decryption. This variability increases resistance to pattern-based cryptanalysis, as attackers cannot predict or model the transformation sequence. The use of recipient-specific keys ensures that only authenticated users, who have successfully passed all three authentication stages and possess both key fragments, can decrypt the data. This

design not only improves confidentiality but also ties encryption tightly to the individual identity of the user.

5. CONCLUSION

Lossless image compression algorithm is a class of data compression algorithm that allows the original image to be perfectly reconstructed from the compressed image. Image compression algorithms are important because they can be used to reduce the amount of space needed to store data. Using compressed images can free up valuable space on any storage device, or media. Also, the amount of time it takes to send something over the Internet depends on the size of the transmitted image. Compressing image before sending them over the Internet can reduce the number of resources needed by a considerable margin. This study made an analysis of the Lempel-Ziv, Run-length, and Huffman compression algorithms using images. The performance of these algorithms based on their respective compression ratios was compared. Discussion was carried out concerning their advantages and disadvantages. This study has shown that the Huffman algorithm is the best and suitable algorithm for the compression of joint photographic experts' group **(**JPEG**)**, Portable network graphics (PNG), and bitmap (BMP) image format. The Lempel-Ziv encoding algorithm is also suitable for joint photographic experts' group **(**JPEG**)**, Portable network graphics (PNG) formats, and bitmap (BMP) image format; it is not as efficient as the Lempel-Ziv algorithm. Further work can be done on the comparative analysis of lossless algorithms for best performance image quality of both the original and the compressed images. Also, more study can be done to determine the time complexities of the lossless algorithm. More Study can also be done to determine the peak signal to noise ratio (PSNR) of the algorithms.

6. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

7. REFERENCES

[1] Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., ... & Röning, J. (2020). 6G white paper: Research challenges for trust, security and privacy. *arXiv preprint arXiv:2004.11665*.

[2] Prakash, V., Goyanka, T., Sharma, S., Garg, L., & Shukla, V. (2023). Secure Text Transfer Using Diffie–Hellman Key Exchange Algorithm in Cloud Environment. In *International Conference on Cryptology & Network Security with Machine Learning* (pp. 631-643). Singapore: Springer Nature Singapore.

[3] Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. *IEEE Access*.

[4] Mudra, G., Cui, H., & Johnstone, M. N. (2023). Survey: an overview of lightweight RFID authentication protocols suitable for the maritime internet of things. *Electronics*, *12*(13), 2990.

[5] Ahmad, M. O., Tripathi, G., Siddiqui, F., Alam, M. A., Ahad, M. A., Akhtar, M. M., & Casalino, G. (2023). BAuth-ZKP A blockchain-based multi-factor authentication mechanism for securing smart cities. *Sensors*, *23*(5), 2757.

[6] Bhansali, A., Harisha, J., & Sinha, G. (2024). Secure Data Transfer onto Cloud Environment using Diffie-Hellman Key Exchange Algorithm. In *2024 International Conference on Inventive Computation Technologies (ICICT)* (pp. 1479-1484). IEEE.

[7] Galu, T. S., Adeyelu, A. A., & Otor, S. U. An Improved Deffie Hellman Scheme for Mitigating an Eavesdropping Attack on a Network.

[8] Adeyelu, A. A., Elusakin, O. E., Uga-Otor, S., Godwin, I. R., & John, Z. S. A New Approach to Mitigating Authentication Challenge for an Internet of Things Paradigm. *International Journal of Computer Applications*, *975*, 8887.

[9] Taparia, A., Panigrahy, S. K., & Jena, S. K. (2018). Secure key exchange using enhanced Diffie-Hellman protocol based on string comparison. *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017*, *2018-Janua*, 722–726. https://doi.org/10.1109/WiSPNET.2017.8299856

[10] Poh, G. S., Gope, P., & Ning, J. (2019). PrivHome: Privacy-preserving authenticated communication in smart home environment. *IEEE Transactions on Dependable and Secure Computing*, *18*(3), 1095-1107.

[11] Dey, S., & Hossain, A. (2019). Session-key establishment and authentication in a smart home network using public key cryptography. *IEEE Sensors Letters*, *3*(4), 1-4.

[12] Sahoo, S. S., Mohanty, S., & Majhi, B. (2020). Improved biometric-based mutual authentication and key agreement scheme using ECC. *Wireless Personal Communications*, *111*(2), 991-1017.

[13] Kumari, S., & Renuka, K. (2021). Design of a password authentication and key agreement scheme to access e-healthcare services. *Wireless Personal Communications*, *117*(1), 27-45.

[14] Shafiq, A., Ayub, M. F., Mahmood, K., Sadiq, M., Kumari, S., & Chen, C. M. (2020). An Identity-Based Anonymous Three-Party Authenticated Protocol for IoT Infrastructure. *Journal of Sensors*, *2020*(1), 8829319.

[15] Rajaram, S., Maitra, T., Vollala, S., Ramasubramanian, N., & Amin, R. (2020). eUASBP: enhanced user authentication scheme based on bilinear pairing. *Journal of Ambient Intelligence and Humanized Computing*, *11*(7), 2827-2840.

[16] Rana, S., Obaidat, M. S., Mishra, D., Mishra, A., & Rao, Y. S. (2022). Efficient design of an authenticated key agreement protocol for dew-assisted IoT systems. *The Journal of Supercomputing*, *78*(3), 3696-3714.

[17] Samal, K., Sunanda, S. K., Jena, D., & Patnaik, S. (2025). A lightweight privacy preservation authentication protocol for IoMT using ECC based blind signature. *International Journal of Engineering Business Management*, *17*, 18479790251318538.

[18] Yadav, V. K., Yadav, R. K., Chaurasia, B. K., Verma, S., & Venkatesan, S. (2020, December). MITM attack on modification of diffie-hellman key exchange algorithm. In *International Conference on Communication, Networks and Computing* (pp. 144-155). Singapore: Springer Singapore.

[19] Owoh, N. P., & Singh, M. M. (2019). Applying Diffie-Hellman algorithm to solve the key agreement problem in mobile blockchain-based sensing applications. *International Journal of Advanced Computer Science and Applications*, *10*(3).

[20] Thapar, P., & Batra, U. (2022). Implementation of Elliptical Curve Cryptography Based Diffie-Hellman Key Exchange Mechanism in Contiki Operating System for Internet of Things. *International Journal of Electrical and Electronics Research (IJEER)*, *10*, 335-340.

[21] Moussa, K. H., El-Sakka, A. H., Shaaban, S., & Kheirallah, H. N. (2022). Group security authentication and key agreement protocol built by elliptic curve diffie hellman key exchange for LTE military grade communication. *IEEE Access*, *10*, 80352-80364.

[22] Kara, M., Laouid, A., AlShaikh, M., Bounceur, A., & Hammoudeh, M. (2021). Secure key exchange against man-in-the-middle attack: Modified diffie-hellman protocol. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, *7*(3), 380-387.

[23] Alomari, G., & Aljarah, A. (2021). Efficiency of using the Diffie-Hellman key in cryptography for internet security. *Turkish Journal of Computer and Mathematics Education*, *12*(6), 2039-2044.

[24] Muth, R., & Tschorsch, F. (2020, August). Smartdhx: Diffie-hellman key exchange with smart contracts. In *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)* (pp. 164-168). IEEE.

[25] Gupta, C., & Subba Reddy, N. V. (2022, January). Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography. In *Journal of Physics: Conference Series* (Vol. 2161, No. 1, p. 012014). IOP Publishing.