ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2479

An Improved Deffie Hellman Scheme for Mitigating an Eavesdropping Attack on a Network

Terfa Samuel Galu[1]; Adekunle A. Adeyelu[2]; Samera Uga Otor
Benue State University, Makurdi, Nigeria

Abstract:- In today's interconnected digital landscape, ensuring data security in transit is paramount amidst the constant threat of adversaries exploiting vulnerabilities in communication channels. This study introduces an enhanced Diffie-Hellman key exchange algorithm designed to bolster data encryption against Man-in-the-Middle (MITM) attacks. The objectives include the development of a novel Diffie-Hellman key exchange model to ensure confidentiality and integrity of data during transit, along with implementing measures to thwart MITM attacks. Additionally, the study integrates a time-based key expiration mechanism within the Diffie-Hellman framework to facilitate secure data transmission while enforcing user authentication. The proposed model was simulated using the Hypertext Preprocessor (PHP) programming language, enabling comprehensive evaluation of performance metrics such as execution time, computational overhead, security strength, and adherence to Burrows-Abadi-Needham (BAN) logic. Rigorous testing and analysis demonstrate the efficacy of the enhanced Diffie-Hellman algorithm in safeguarding data integrity and confidentiality during transit, offering a robust solution against evolving cyber threats.

Keywords:- *Deffie-Hellman, Data Encryption, Data Decryption, Man-In-The-Middle, BAN Logic.*

I. INTRODUCTION

In an increasingly interconnected and digitally dependent world, secure communication is a fundamental prerequisite for safeguarding sensitive information, privacy, and trust. Cryptographic protocols have played a pivotal role in ensuring the confidentiality and integrity of data exchanged over networks [1]. 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].

The Diffie-Hellman key exchange algorithm, developed by Whitfield Diffie and Martin Hellman in 1976, introduced a groundbreaking concept of public key cryptography [3]. 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, in its simplest form, can be understood as the challenge of finding an exponent in modular arithmetic. This problem forms the foundation of the protocol's challenge to eavesdropping and unauthorized access [1].

However, despite its robust theoretical underpinnings, the Diffie-Hellman key exchange is vulnerable to a range of attacks, with the MITM attack being a particularly potent threat [1]. 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 malicious data, or even manipulate cryptographic keys, compromising the security of the communication [4].

Several approaches have been employed to prevent the MitM attacks in the Diffie-Hellman algorithm. Traditionally, monitoring of network traffic patterns and analyzing anomalies, often rely on heuristics and rule-based models. Despite the progress, challenges persist in the realm of MitM attack prevention [5]. Adversaries constantly change their strategies, resulting in complex attacks and shifting threat environments [4][6].

In numerous cryptographic protocols, the Diffie-Hellman algorithm is an essential pillar for secure key exchange. It is, however, vulnerable to a Man-in-the-Middle (MitM) attack, in which an unauthorized opponent intercepts and modifies communication between two parties without their knowledge. The security and integrity of sensitive information exchanged during key exchange are jeopardized by this breach. Current security mechanisms frequently place a greater emphasis on intrusion detection measures. These methods may not properly address the Diffie-Hellman key exchange protocol's particular characteristics and vulnerabilities associated with MitM attacks. It is critical to provide a dependable and efficient mechanism capable of preventing MitM attacks during the Diffie-Hellman algorithm's key exchange. The sophisticated nature of MitM attacks, as well as the necessity to prevent and not only detect MitM attacks, are the primary challenges that must be addressed. Thus, it is on this backdrop that this study proposed an improved secure key exchange using enhanced Diffie-Hellman protocol.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2479

II. LITERATURE REVIEW

A. Overview of Related Work

End-to-end encryption stands as a cornerstone in ensuring secure data transfer between endpoints. However, the persistent threat of Man-in-the-Middle (MITM) attacks poses a significant challenge to its integrity. A notable approach proposed in [7] involves the development of dynamic encryption with implicit key exchange. This innovative solution leverages concepts from graph theory to enhance the security of end-to-end encryption protocols. By applying TAT (Transitive Authentication Tag) labelling over the network, the researchers aimed to eliminate the need for explicit key exchange during transmission. Central to this approach is the notion of implicit key computation using parameters derived from the graph network. This process effectively circumvents the vulnerabilities associated with traditional key exchange methods, thereby thwarting potential MITM attacks. Importantly, this method ensures that message interception is rendered futile, as decryption can only occur at the intended destination.

[8] devised an implementation of the Diffie-Hellman key exchange method through the use of images that have been concealed through steganography. By employing steganography, the data exchange becomes imperceptible to potential attackers. As a result, there is no necessity for a digital signature or the establishment of a secure channel to execute the key exchange, given that only the two involved parties are privy to this exchange. This approach generates a 128-bit symmetric key between two users without relying on digital signatures or secure channels. Nevertheless, it's important to note that this method is exclusively compatible with bitmap images, particularly those with substantial file sizes, and it is sensitive to image compression techniques.

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 [6]. 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 [9]. 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 [10]. Using clock cycles, the model attained execution time of 10,810,680 Clock Cycles when evaluated.

[11] introduced the Group Security Authentication and Key Agreement Protocol Based on Elliptic Curve Diffie-Hellman Key Exchange (GSAKA-ECDHKE) as a solution to rectify the flaws and vulnerabilities inherent in the LTE network's Evolved Packet System Authentication and Key Agreement Protocol (EPS-AKA). The GSAKA-ECDHKE protocol leverages Elliptic Curve Diffie-Hellman Key Exchange (ECDHKE) and a hash function to create and share secret Elliptic Curve (EC) keys, subsequently employed for the encryption and protection of routing authentication parameters. To validate its security and effectiveness, the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool was employed for thorough security analysis and formal verification. AVISPA's assessments confirmed that GSAKA-ECDHKE successfully mitigates a variety of well-known security threats, including Man-in-the-Middle (MITM) attacks, replay attacks, and Denial of Service (DoS) attacks. Thus, meeting the specified security criteria. Furthermore, the proposed protocol minimizes communication overheads to a significant degree when compared to alternatives. Evaluation indicates that the model yielded operation time (Thash) = 0.067 ms and encryption time (Tenc) = 0.161 ms.

B. Methodology

In the improved secured key-exchange, an augmented approach to key exchange is implemented to fortify security measures. Initially, the Variable Round Hash (VRH) function supplements the original Diffie-Hellman Key Exchange (DHKE) algorithm, ensuring integrity checks for exchanged public keys. However, to further strengthen security, the shared secret key is divided into two parts following the initial key exchange process. The first part of the secret key is exchanged through the established channel using the VRH-enhanced DHKE. Simultaneously, the second part of the secret key is securely transmitted through an alternate, trusted channel, such as the recipient email or phone number. Upon reception at the other end, both segments of the secret key are reassembled to reconstruct the complete shared secret. This approach not only validates the integrity of the exchanged public keys but also disperses the key components across separate channels,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2479

significantly heightening the barrier for potential attackers attempting unauthorized decryption, thereby elevating the overall security of the communication system.

The first process involves the implementation of the improved Diffie-Hellman protocol to enhance data encryption and prevent Man-in-the-Middle attacks. This entails designing a secure data exchange system that employs the Diffie-Hellman protocol to establish secure cryptographic keys. Through this protocol, devices can securely exchange information without being susceptible to eavesdropping or tampering by malicious intermediaries.

The second process introduces a comprehensive security mechanism that combines a time-based key expiration feature, Diffie-Hellman encryption, data binding to the recipient's key, and user authentication. This multifaceted approach enhances the system's resilience against various threats, including unauthorized access and data interception. Key expiration ensures that cryptographic keys are routinely updated, and data binding provides an additional layer of data protection.

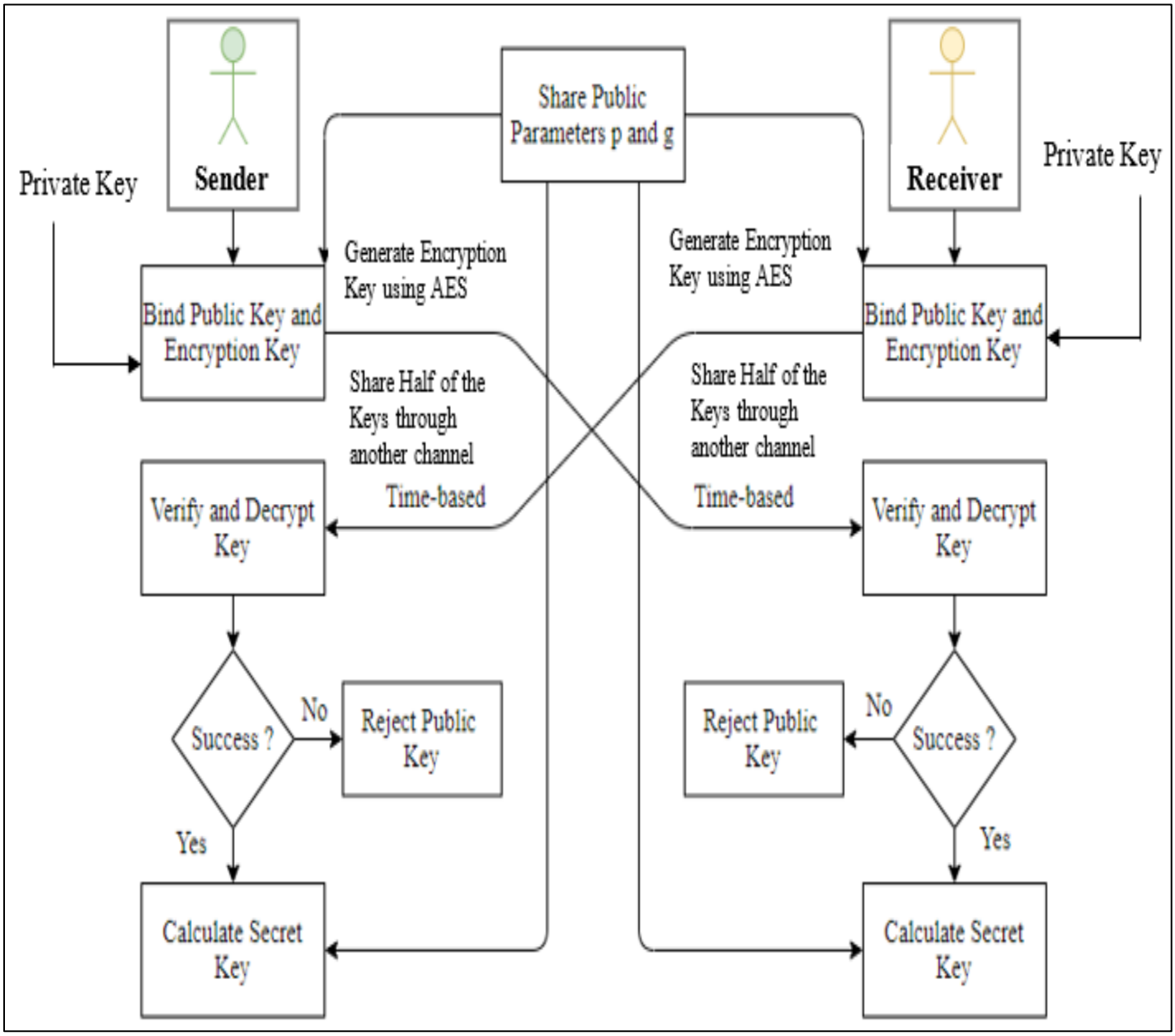

Fig 1: Improved Diffie-Helman Key Exchange Protocol

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2479

III. RESULTS

➢ *The Results are as Shown. Figure 2 to 6.*

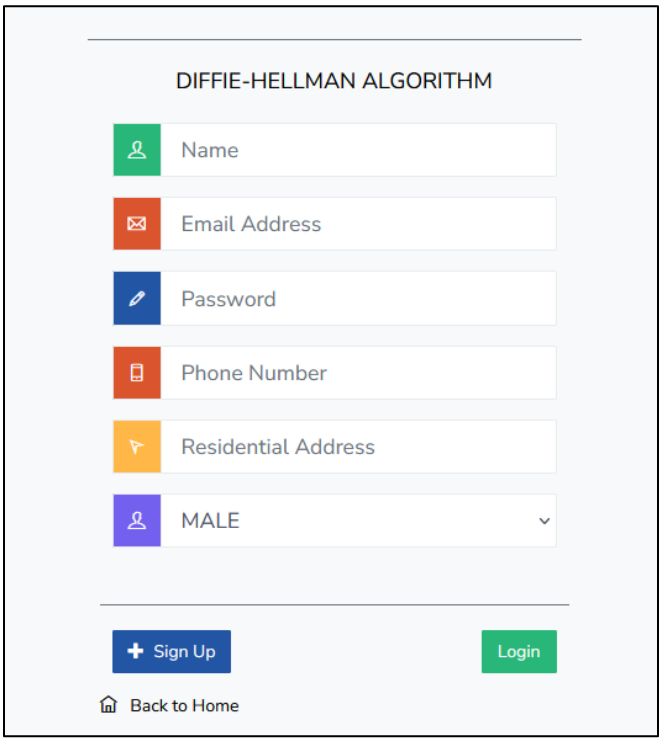

Fig 2: Registration Page

Figure 2 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 supplying the necessary information, the user is redirected to supply login credentials as shown on figure 3.

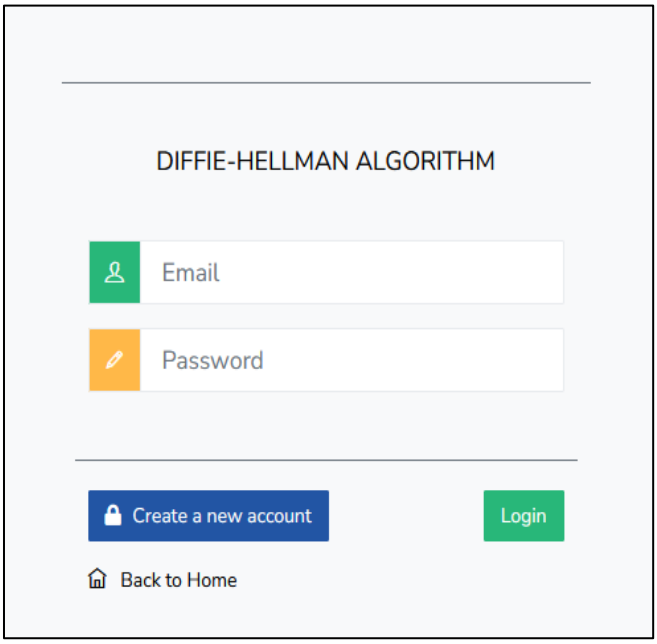

Fig 3: Login Page

Figure 3 which represents the user login page, where the user of the system is expected to supply their email address and password before proceeding to the user dashboard. 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.

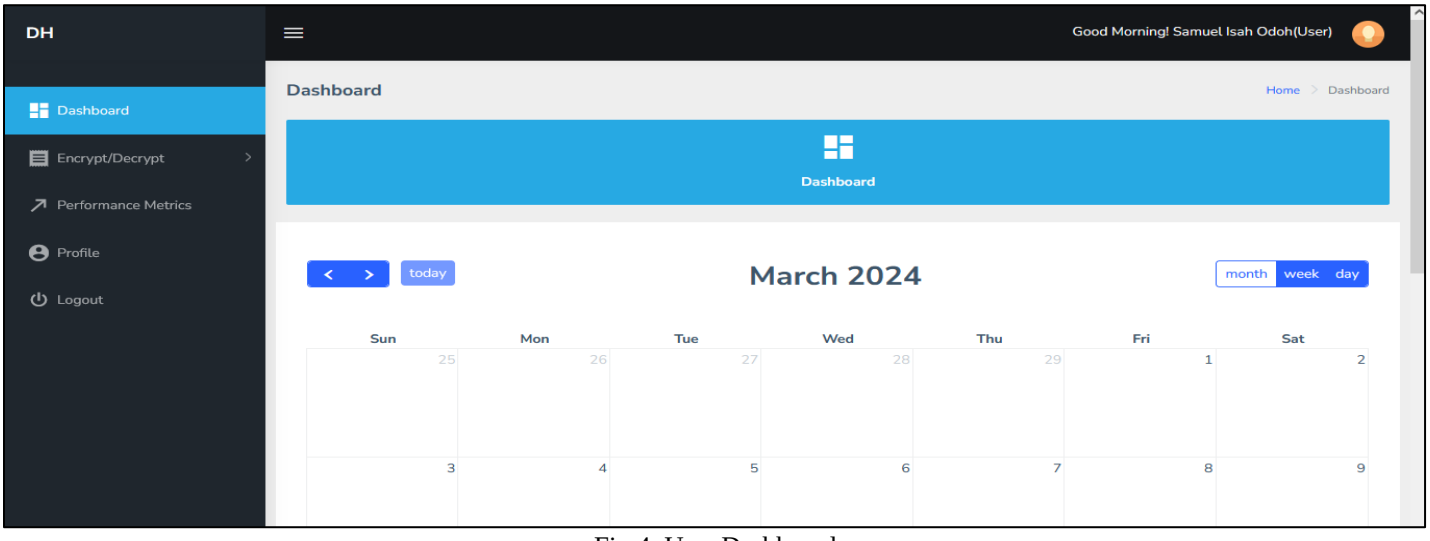

Fig 4: User Dashboard

Figure 4 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.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2479

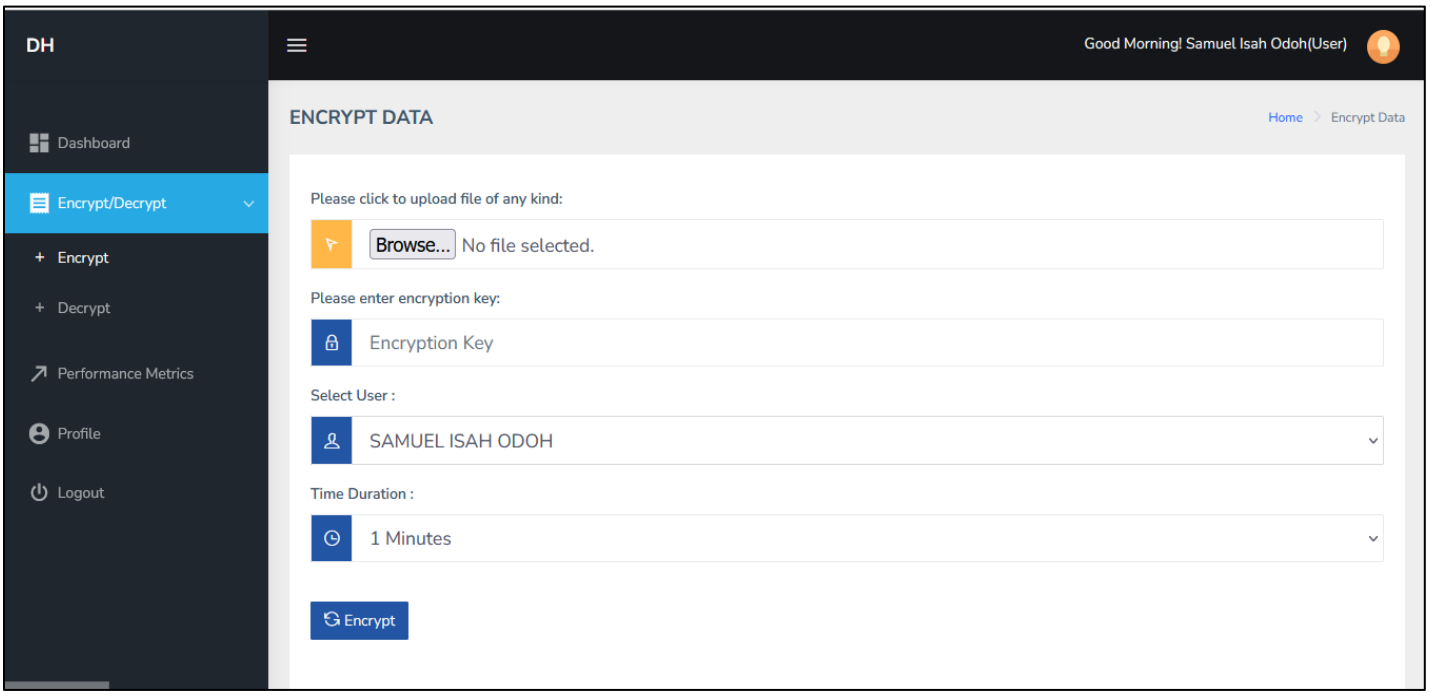

Fig 5: Encrypt Data

Figure 5 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.

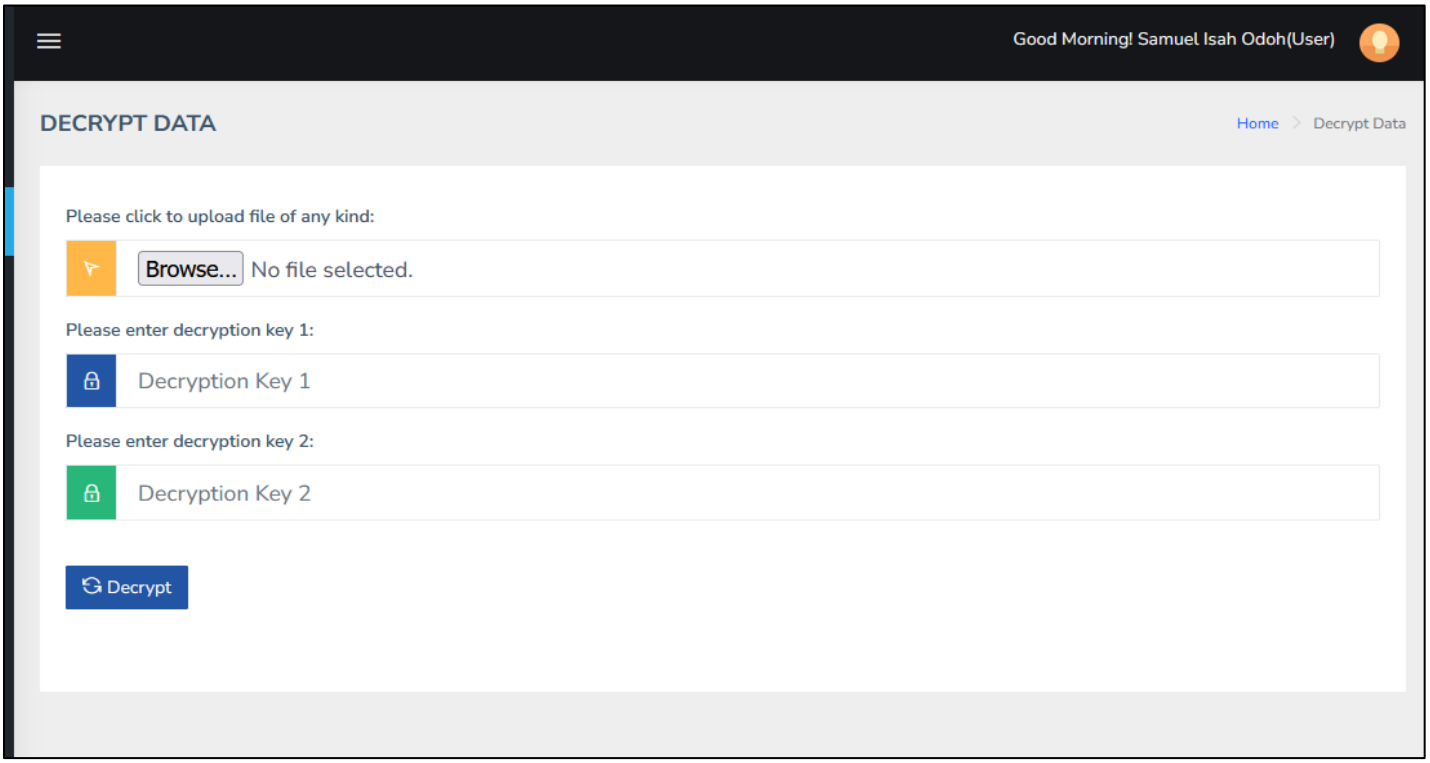

Fig 6: Decrypt Data

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2479

Figure 6 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.

A. *Formal Security Analysis*

This section provides the detailed formal security analysis of the proposed security scheme using the BAN-Logic. It first describes the basic notation of BAN-Logic that is used to analyze the proposed scheme's secure authentication and correctness.

Table 1: BAN-Logic Expressions

Rule Number	Rule Description	Logic Expression
1	Authentication: If a user successfully logs in, then the system considers the user authenticated.	$Auth(U,S) \rightarrow Auth_{U,S}$
2	Key Exchange: If a user initiates a key exchange securely, then both the user and the system possess a shared secret key.	$KeyExchange(U,S) \wedge SecureDH(U,S) \rightarrow SharedKey_{U,S}$
3	Encryption: If a user selects a document, provides keys, and the communication is secure, then the keys are bound to the document.	$SelectDoc(U,S) \wedge ProvideKeys(U,S) \wedge SecureComm(U,S) \rightarrow BindKeys_{U,S}$
4	Private Key Expiry Check: Before decryption, the system checks if the private key shared with the recipient has expired. If expired, access is denied. Otherwise, proceed with decryption.	$CheckExpiry(R,S) \wedge \neg Expired(R,S) \rightarrow DecryptDocR,S$
5	Key Confidentiality: The system ensures the confidentiality of secret keys during generation, transmission, and storage.	Confidentiality(K,S)
6	Document and Key Integrity: The system verifies the integrity of documents and secret keys to detect any tampering or alteration.	$Integrity(D,S) \wedge Integrity(K,S)$
7	Secure Communication: The system ensures that communication channels used for key exchange, encryption, and decryption are secure against eavesdropping and tampering.	SecureComm(U,S)
8	Key Management: The system implements proper key management practices for generation, storage, distribution, and revocation of secret keys.	KeyManagement(S)
9	Access Control: The system enforces access control mechanisms to ensure that only authorized users can access documents and secret keys.	AccessControl(U,S)

B. *Informal Security Analysis*

The implementation of the Improved Diffie-Hellman Key Exchange Algorithm not only aimed to establish a secure shared key between communicating parties but also addresses various security threats such as unauthorized access, man-in-the-middle (MITM) attacks, and others.

- Mitigation of MITM Attacks: Measures are in place to prevent and detect man-in-the-middle (MITM) attacks. Techniques such as digital signatures, certificates, or session identifiers are utilized to verify message integrity and detect tampering by intermediaries.
- Secured Multiple Channels: Separate channels are established for sharing the 16-digit key, with one channel designated for the public key and another for the private key. The public key resides within the system, while the private key is shared via the user's email address.
- Private Key Time Expiration: To mitigate the risk of privileged insider attacks, private keys have a limited validity period. This reduces the window of opportunity for malicious insiders to misuse keys.
- Defense against Offline Password Guessing: The algorithm includes measures to defend against offline password guessing attacks. Key stretching techniques, such as bcrypt or scrypt, are employed to slow down password cracking attempts.
- Protection against Stolen Mobile Devices: Measures are implemented to protect against stolen mobile devices. Remote key revocation and device wiping mechanisms are supported, allowing users to revoke access to keys and erase cryptographic materials stored on lost or stolen devices.
- Sharing of 16-Digit Key: The 16-digit key, comprising both public and private keys, is transmitted through multiple channels. The public key, which is part of the 16-digit key, is stored within the system, while the private key is shared via the user's email address. This approach ensures secure transmission and storage of cryptographic materials while minimizing the risk of unauthorized access.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2479

Table 2: Comparison of the Proposed Scheme with other Relevant Schemes based on Security Features

Security Features	Thwe & Htet, (2019)	Fan et al., (2021)	Khader & Lai, (2015).	Xing et al., (2019)	Usman et al., (2019)	Proposed Scheme
Man in the middle attack	Yes	Yes	Yes	Yes	Yes	Yes
Secured Multiple Channels for Secret and Public Key Sharing	No	No	No	No	Yes	Yes
Private Key Time Expiration	No	No	No	No	No	Yes
Resistance to user impersonation attack	Yes	Yes	No	Yes	Yes	Yes
Secure login and password change phase	Yes	No	Yes	Yes	Yes	Yes
Privileged insider and offline password guessing attack	Yes	Yes	Yes	Yes	Yes	Yes
Resistance to stolen mobile device attack	Yes	No	No	No	No	Yes
User Experience	Yes	Yes	Yes	Yes	Yes	Yes

➢ *The Result on Table Two Below Represents the Performance of the Implemented System.*

Table 3: Performance of the Implemented System

Filename	File Size	Expiry Time	Expiry Status	Execution Time	Public Key	Status
Data1_enc	2.5 MB	2024/03/15 02:26:03	Active	0.507318 seconds	09876543	Encrypt
Data1_dec	3.1 MB	2024/03/15 02:26:03	Active	1.439523 seconds	0987654345346458	Decrypt
Data1_enc	514.46 KB	2024/03/16 02:27:07	Active	0.614509 seconds	11111111	Encrypt
Data1_dec	685.96 KB	2024/03/16 02:27:07	Active	0.993508 seconds	1111111185513884	Decrypt

As shown on table two above the user of the system has to submit a valid 16-digit number before they can have access into the encrypted data.

IV. DISCUSSION

After successfully implementing and achieving the objectives outlined in the research topic, it's essential to provide a comprehensive discussion of the results. The developed system integrates various security measures to address critical challenges in data encryption and transmission, with a focus on preventing Man-in-the-Middle (MITM) attacks, ensuring data confidentiality and integrity, incorporating time-based key expiration, and complying with BAN logic principles.

The improved Diffie-Hellman key exchange model serves as the cornerstone of the system, facilitating secure communication between parties while mitigating the risk of unauthorized interception or tampering. By leveraging robust cryptographic techniques and secure key exchange protocols, the system establishes a secure shared secret between communicating entities, thereby safeguarding sensitive information from potential attackers.

In addition to the enhanced key exchange mechanism, the system employs a separate channel for transmitting decryption keys of encrypted data in transit. This approach enhances security by minimizing the exposure of sensitive information during transmission, thereby reducing the risk of interception or unauthorized access. By segregating key transmission from data transmission, the system fortifies its defense against potential attacks, ensuring the confidentiality and integrity of transmitted data.

Furthermore, the incorporation of a time-based key expiration feature, coupled with the Diffie-Hellman algorithm, enhances the security of data encryption and key management. By associating data with recipient-specific keys and enforcing user authentication, the system mitigates the risk of unauthorized access and ensures that decryption keys remain valid only for a specified duration. This feature adds an extra layer of security, reducing the likelihood of key compromise and enhancing overall data protection.

The simulation and evaluation of the proposed model, implemented using the PHP programming language, yielded promising results in terms of performance and security. Metrics such as execution time, computational overhead, security strength, and compliance with BAN logic principles were assessed to gauge the effectiveness and efficiency of the system. The simulation demonstrated efficient key exchange, encryption, and decryption processes, with minimal computational resources required. Additionally, the system's compliance with BAN logic rules validated its effectiveness in mitigating security risks and ensuring the confidentiality, integrity, and availability of data during transit.

V. CONCLUSION AND RECOMMENDATION FOR FUTURE WORKS

In conclusion, this study focused on strengthening authentication security for the Internet of Things (IoT) by mitigating the risks associated with man-in-the-middle (MitM) attacks. To achieve these objectives, a multipronged approach was used, which began with a thorough analysis of the various three-factor authentication (3FA) systems that are currently in

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR2479

use within the IoT, establishing basic design requirements and principles. Next, a new 3FA algorithm was developed, closely adhering to these identified prerequisites, and was implemented using the PHP programming language. Rigorous performance assessments using benchmark 3FA metrics were carried out, highlighting the algorithm's strong points. Finally, by outlining essential design requirements, this study established a strong basis for developing a resilient solution. Further research and development efforts should focus on enhancing system capabilities and addressing emerging threats to ensure ongoing effectiveness and relevance.

REFERENCES

[1]. S. Srilaya and S. Velampalli, "Cryptography: The Key Technology for Security Management," *Int. J. Res. Anal. Rev.*, vol. 7, no. 1, pp. 621–629, 2020.

[2]. A. M. Banaamah and I. Ahmad, "Intrusion Detection in IoT Using Deep Learning," *Sensors*, vol. 22, no. 21, 2022, doi: 10.3390/s22218417.

[3]. M. R. Mishra and J. Kar, "a Study on Diffie-Hellman Key Exchange Protocols," *Int. J. Pure Apllied Math.*, vol. 114, no. 2, pp. 179–189, 2017, doi: 10.12732/ijpam.v114i2.2.

[4]. H. M. Ahmed and R. W. Jassim, "Enhanced Diffie-Hellman Algorithm for Data Transmission Security," pp. 316–335, 2020.

[5]. M. Kara, A. Laouid, M. AlShaikh, A. Bounceur, and M. Hammoudeh, "Secure Key Exchange Against Man-in-the-Middle Attack: Modified Diffie-Hellman Protocol," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 7, no. 3, p. 380, 2021, doi: 10.26555/jiteki.v7i3.22210.

[6]. P. P. Thwe and M. Htet, "Prevention of Man-In-The-Middle Attack in Diffie-Hellman Key Exchange Algorithm using Proposed Hash Function," *Int. J. Adv. Sci. Res. Eng.*, vol. 05, no. 10, pp. 192–203, 2019, doi: 10.31695/ijasre.2019.33560.

[7]. J. O. Odeh, "Totally Antimagic Total Labelling of a Complete Bipartite Graph and its Application in End-to-End Encryption Totally Antimagic Total Labelling of a Complete Bipartite Graph and its Application in End-to-End Encryption," no. January, 2024.

[8]. A. Khaldi, "Diffie-hellman key exchange through steganographied images," *Rev. Direito, Estado e Telecomunicacoes*, vol. 10, no. 1, pp. 147–160, 2018, doi: 10.26512/lstr.v10i1.21504.

[9]. N. P. Owoh and M. M. Singh, "Applying Diffie-Hellman algorithm to solve the key agreement problem in mobile blockchain-based sensing applications," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 3, pp. 59–68, 2019, doi: 10.14569/IJACSA.2019.0100308.

[10]. P. Thapar and U. Batra, "Implementation of Elliptical Curve Cryptography Based Diffie-Hellman Key Exchange Mechanism in Contiki Operating System for Internet of Things," *Int. J. Electr. Electron. Res.*, vol. 10, no. 2, pp. 335–340, 2022, doi: 10.37391/IJEER.100245.

[11]. K. H. Moussa, A. H. El-Sakka, S. Shaaban, and H. N. Kheirallah, "Group Security Authentication and Key Agreement Protocol Built by Elliptic Curve Diffie Hellman Key Exchange for LTE Military Grade Communication," *IEEE Access*, vol. 10, no. July, pp. 80352–80364, 2022, doi: 10.1109/ACCESS.2022.3195304.