The International Journal of Engineering and Science (IJES)
|| Volume || 8 || Issue || 8 Series II || Pages || PP 88-94 || 2019 ||
ISSN (e): 2319 – 1813 ISSN (p): 23-19 – 1805

Securing Data on Transmission from Man-In-The-Middle Attacks Using Diffie Hell-Man Key Exchange Encryption Mechanism

Karim Usman[1], Patrick Obilikwu[2], Kadiri Patrick[3] and Risikatu Karim[4]
[1]*Department of Mathematics and Computer Science, Benue State University, Makurdi, Benue State, Nigeria*
[2]*Department of Mathematics and Computer Science, Benue State University, Makurdi, Benue State, Nigeria*
[3]*Department of Computer Science, Nigerian Army Institute of Technology and Environmental Studies, Makurdi, Nigeria*
[4]*Software Development Unit, Kreative Information Technology Nigeria Limited*
Corresponding Author: Karim Usman

----------ABSTRACT----------
In a world that relies progressively on electronic information and online transactions, a large volume of data is transmitted over the internet on a daily bases. Cyber threats and attacks are steadily increasing. There is, however, a major threat posed by Man-in-the-Middle (MITM) attacks in trying to establish an effective and safe communication line. Most time, these threats and attacks from MITM are targeted at the channel of the transaction to intercept and manipulate vital information being transmitted to a legitimate user. More so for private, confidential, and vital information, the need to secure these data on transmission over the Internet is now a necessity and cannot be overstated. Cryptography is the key method of protecting data and information in a computer system. Today's cryptosystems are divided into two categories: symmetric and asymmetric. The difference lies in the keys used in decryption and encryption. While symmetric cryptography uses the same key for both processes, asymmetric cryptography uses one key (public key) to encrypt data and a different key (private key) to decrypt it. The Diffie Hellman key exchange (DHKE) encryption is one of the renowned asymmetric algorithms, developed by Whitfield Diffie and Martin Hellman in 1976. The DHKE encryption is implemented in the proposed system such that even when MITM can intercept data on transmission, it ensures that the integrity and confidentiality of the data remain intact. The proposed system is capable of encrypting a message and generate the secret key, and while the encrypted message is on transit, the system automatically sends the secret key to the phone number of the legitimate receiver. Therefore, the objectives of this work are; (1) To enhance the confidentiality of transmitted data. (2) To improve the integrity of transmitted data. (3) To ensure the confidentiality and integrity of data on transmission by the implementation of DHKE encryption mechanism. The system developed is highly compatible with MYSQL. Structured System Analysis and Design Methodology (SSADM) was used to design the system while Java Enterprise Edition (JEE) and JBOSS were used to develop a prototype for the proposed system. The system was well tested and the outputs were relatively good.

KEYWORDS- *Cryptosystems, DHKE, MITM, Encryption, SSADM*

Date of Submission: 28-08-2019 Date of acceptance: 13-09-2019

I INTRODUCTION

In a world that relies increasingly on electronic information, data security is more important than ever. Many of the functions of our business and personal life now rely on computers, mobile devices, and the Internet and there's a lot of data out there to protect. As a large amount of data is transmitted over the network, it is preliminary to secure all types of data before sending them [1]. There is, however, a major hindrance in trying to establish an effective and safe communication line: an outside user, not intended to be a part of the connection, might try to steal the information being passed to a legitimate user. Thus, having an internal control mechanism to assure the confidentiality, integrity, non-repudiation, and entity reputation of data in a distributed environment is of paramount importance [2]. Information on transit needs to be protected from being intercepted and accessed by an unauthorized person(s). This phenomenon is referred to as data confidentiality. Data integrity is when there is an absence of any form of alteration on data passing over an unsecured channel from intruders or unauthorized individual. To ensure that the sender of a message is the sender data origin authentication is used. The goal of non-repudiation is to make it able for the receiver to document that the message is sent from the sender, while entity reputation convinces the participants of each other's identity [3].

Therefore, the need to protect data on transmission between parties communicating over the Internet is now a necessity that cannot be overstated.

Cryptography is a technique of securing the communication process from attackers. Cryptography is about using protocols that prevent attackers from accessing data, various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation are the base of the modern cryptography [4]. Cryptography is used to convert the readable information (plain text) into unreadable or hidden (cypher text), and only the authorized persons or machines can retrieve or obtain the original texts.

Today's cryptosystems are divided into two categories: symmetric and asymmetric. The difference lies in the keys used in decryption and encryption, symmetric cryptography uses the same key for both of these processes, whereas asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. Symmetric key needs to be changed from time to time to make it more secure and unbreakable to prevent other users from obtaining the plain text. Therefore, the security of any symmetric cryptography system depends on the key exchange protocol used by the system. Key exchange protocol is the way of distributing the keys securely among the users. There are so many ways to exchange keys between users, a user can choose a key and then send it physically (mail or in-person) to the other user. In this work, the Diffie Hellman Key Exchange (DHKE) was implemented to provide enhanced security to encrypted data on transmission from Man in the Middle (MITM) attacks.

Currently, one of the major methods developed by attackers to deceive and manipulate online users is Man-in-the-Middle Attack [5]. MITM attacks is an attack whereby the attacker secretly relays and possibly alters the communications between two parties who believed they are directly communicating with each other. MITM attack can succeed only when the attacker can impersonate each endpoint to their satisfaction as expected from the legitimate ends. Thus, it is necessary to ensure that even when transmitted information is intercepted by MITM, the confidentiality and integrity of that information remained uncompromised. Hence, to enhance the security of transmitted data that travels through an unsecured network, there is the need of a system which provides authentication, verification and encrypted data transfer using DHKE mechanism, hence maintaining data confidentiality.

The Diffie-Hellman key exchange is one of the well-known asymmetric algorithms, formulated by its namesakes Whitfield Diffie and Martin Hellman in 1976. It is referred to in various ways as Diffie-Hellman protocol, Diffie-Hellman handshake, or Diffie-Hellman key negotiation, and commonly shortened to D-H, or DH, for convenience [6]. Diffie Hellman Key exchange is a way of generating a shared secret between two people in such a way that the secret cannot be seen by observing the communication. This technique can help one create an encryption key with someone, and then start encrypting your traffic with that key. And even if the traffic is recorded and later analyzed, there is absolutely no way to figure out what the key was, even though the exchanges that created it may have been visible. Therefore, the general concept is aimed at preventing unauthorized access to transmitted data by MITM, through the implementation of the Diffie Hellman key exchange encryption algorithm.

Therefore, the objectives of this work are; (1) To enhance the confidentiality of transmitted data. (2) To improve the integrity of transmitted data. (3) To ensure the confidentiality and integrity of data on transmission by the implementation of DHKE encryption mechanism. These are the gaps this work hopes to address.

II RELATED WORKS

Prashant and Yogita, [7] proposed an enhanced technique for securing data in cloud computing. In this paper, they designed a "three-way mechanism" because it ensures all the three protection scheme of authentication, data security and verification, at the same time. They implemented the digital signature and Diffie Hellman Key Exchange blended with Advanced Encryption Standard (AES) algorithm to protect the confidentiality of data stored in the cloud. Even if the key in the transmission is hacked, the facility of Diffie Hellman Key Exchange renders it useless, since key in transit is of no use without user's private key, which is confined only to the legitimate user. With the implementation of this proposed three-way mechanism, it becomes tough for hackers to crack the security system, thereby making data stored in the cloud very secured.

Aboho et al., [5] proposed a technique to improve the security features of One Time Password (OTP) from Man in the Middle attacks. Man in the Middle (MITM) attacks have been a major challenge in e-Commerce as users' confidential information are intercepted and manipulated by fraudsters. OTP is an already existing security framework for online banking and transactions, however, this OTP is susceptible to a MITM attack. The proposed technique, seek to address the security challenges of online banking as well as buying/paying for services online by encrypting the OTP before it is sent. They implemented the newly proposed technique by combining the Diffie Hellman Key Exchange (DHKE) encryption and Advanced Encryption Standard (AES) algorithm. The proposed security model ensures that the OTP is encrypted with DHKE and further scrambled with the AES before it is sent to the user's registered mobile number. With the

implementation of this proposed security model, if eventually the OTP is intercepted by MITM, it is the encrypted data that will be captured and not the original content. This will provide a secured transaction using OTP during online banking and e-Commerce.

Syeda Farhana et al. [8] came up with a technique to enhance the security of encrypted data on transmission over the network. The proposed system seeks to address the security challenges associated with data already encrypted with any of the cryptography algorithms like DES, triple DES and AES etc. However, the transmission of encrypted data directly through the network is not much secure. Accordingly, they introduced watermarking algorithms, where data (plain text) is inserted as watermark in an image. The digital watermarking is the process of embedding information into a digital (image) signal which may be used to verify its authenticity or the identity of its owners. Another technology used is the discrete wavelet transform, where an image signal can be analysed by passing it through an analysis filter bank. They implemented the proposed system by using Cryptography and Steganography methods to increase the security of the data while transmitting through networks. Before embedding the plain text into the image, the plain text is encrypted with the Advanced Encryption Standard (AES) algorithm. The encrypted text is embedded into an image using a steganographic technique using Discrete Wavelet Transform (DWT) method and the resultant image is transmitted to the receiver. At the receiver's end, from the image, the encrypted text is extracted by using the DWT method and the result is decrypted using AES.

Vinothini et al. [9] proposed a modified architecture for Secure Sockets Layer (SSL) to improve the confidentiality, authenticity and integrity information transiting the internet. The modified architecture of the internet seeks to reduce the possibility of attacks that can be sent across the network. In their research work, they study and tried to know the various attack methods, and then came up with an appropriate security solution. They provided harder encryption by combining SSH with Diffie Hellman encryption to enhance the public key encryption security protocol, such that it can be implemented into any network to provide better security. The enhanced hardness in the modified security architecture was done with an improved Diffie-Hellman encryption algorithm. The improvement was achieved by adding some more security codes into the current algorithm.

Shashikant Kuswaha et al. [1], observed that various types of cryptographic algorithms provide high security to information on networks, but they also have some drawbacks. This informed their decision to develop an enhanced security architecture to protect information transmitted over the network. They implemented the new hybrid system through a combination of two cryptographic algorithms AES and RSA. The integration of AES with RSA is to enhance security for input mode as text and image. The research work also outlines the possible weaknesses within the current AES encryption algorithm, especially against algebraic based cryptanalysis. Therefore, to minimize algebraic attacks on AES, the need for integrating AES with RSA was proposed. This new hybrid cryptographic technique was designed for better security along with integrity.

S. Grace Sophia and S. Prabakeran, [9] worked on "Implementation of key Aggregate Cryptosystem with and Diffie Hellman Key Exchange Algorithm for Secured Data Sharing in Cloud Computing". The proposed system describes the public-key cryptosystems that give fixed size cypher texts classes that represent the high performance of decryption of keys are available for all the cypher text that is created. The data Owner can release a fixed-size of a single key and the remaining files that are encrypted remain confidential. These single key can be sent to others otherwise stored in a card with a limited number of storage devices. The AES and Diffie Hellman Key Exchange Algorithm was used to improve the security of this technique.

Iman ALMomani et al. [10] Bluetooth version "Bluetooth 2.1+EDR" adopts a Secure Simple Pairing (SSP) procedure which is a secure method for establishing a Bluetooth connection that uses Diffie-Hellman public-key cryptography in its communication. Despite the high-security mechanism provided by this method, it is still vulnerable to attacks, especially Man-In-The-Middle (MITM). Several solutions have been proposed to tackle this vulnerability but the process of securing the exchange of public keys in SSP was not taken into consideration, consequently, this threatens the complete pairing process. In this work, a new method for securing the exchange of public keys between the communicating Bluetooth devices that uses the SSP method is introduced. The details of the proposed method which is an Enhancement to the SSP (ESSP) and how security is assured are illustrated. Moreover, a case study is presented to demonstrate the effectiveness of the proposed ESSP. The paper finally discusses the security strength of the proposed ESSP against different types of MITM attacks as compared to other related work.

III THE PROPOSED MODEL

In this work, the proposed system is designed to secure data in transit. The system allows would-be users to send messages to their emails addresses. It can be used by organisations in sending secure files to their clients and employees. Messages sent through the system are encrypted to prevent its content from Man in the Middle attacks (MITM). While the encrypted message is on transit, the secret key does not go along with the message, as it is sent through a different channel to the legitimate user. The MITM attacks have become so

sophisticated that they can access intercept data and manipulate its content before releasing it. This informed the use of Diffie Hellman Key Exchange algorithm (DHKE) to enhance the securing of the transmitted data.

The implementation of DHKE in the proposed system will enable the system to encrypt data and automatically generate a secret key. The DHKE mechanism improves the integrity and enhances the confidentiality of the encrypted message to be sent. Now, if an attacker succeeds to intercept the transmitted data, they would not be able to decode it because they don't have the key to decrypt it. DHKE algorithm is a complex mathematical algorithm, thus making it impossible to decrypt without the key. The system sends the secret key to the legitimate user through another channel of communication to the user phone number. The concept is this, even if the MITM intercepts the encrypted data, he would not have the key to access it vice-versa, therefore, rendering the captured data useless to the attacker.

IV DIFFIE HELLMAN KEY EXCHANGE PROTOCOL

For instance, Alice and Bob want to agree on a shared secret key using the Diffie–Hellman key exchange algorithm, they will generate the shared key as shown in Table 1 below.

Table 1: An illustration of how a shared secret key is generated using the Diffie Hellman Key Exchange Protocol

Process	Parameters
Alice and Bob agree on two numbers: p and g	p is a large prime number g is the generator or the base
Alice privately picks a secret number a	Alice's secret number = a
Bob privately picks a secret number b	Bob's secret number = b
Alice computes her public key; $x = g^a \bmod p$	Alice's public number = x
Bob computes his public key; $y = g^b \bmod p$	Bob's public number = y
Alice and Bob exchange their public keys, to be used for private generations of a common key.	(Alice knows p, g, a, x, y) (Bob knows p, g, b, x, y)
Alice computes the secret key $k_a = y^a \bmod p$	$k_a = (g^b \bmod p)^a \bmod p$ $k_{a=(}g^b)^a \bmod p$ $k_{a=} g^{ba} \bmod p$
Bob computes the secret key $k_b = x^b \bmod p$	$k_b = (g^a \bmod p)^b \bmod p$ $k_{b=(}g^a)^b \bmod p$ $k_{b=} g^{ab} \bmod p$
By the laws of algebra, Alice's key k_a is the same with Bob's key k_b Or $k_a = k_b = k$	Now Alice and Bob both know the secret value k

Source [6][11]

V DIFFIE–HELLMAN ALGORITHM

Let **p** be a large prime and assume that **α** is a primitive element of $\mathbf{Z_p}$, **p** and **α** are publicly known [11].

1. Alice choose**s a** $(0 \leq a \leq -2)$ at random.
2. Alice computes $\mathbf{x} = \mathbf{g^a} \bmod \mathbf{p}$ and sends it to Bob.
3. Bob chooses **b** $(0 \leq b \leq -2)$ at random.
4. Bob computes $\mathbf{y} = \mathbf{g^b} \bmod \mathbf{p}$ and sends it to Alice.
5. Alice computes $(\mathbf{g^b})^{\mathbf{a}} \bmod \mathbf{p}$ whereas Bob computes $(\mathbf{g^a})^{\mathbf{b}} \bmod \mathbf{p}$.

In other words, both Alice and Bob compute thesame key $\mathbf{g^{ab}} \bmod \mathbf{p}$.

VI METHODOLOGY

The methodology adopted for this work is the Structured System Analysis and Design Methodology (SSADM), which the researcher chooses because of its numerous benefits. SSADM uses a formal methodical approach to the analysis and design of information systems. It is an open methodology based on the waterfall model by which an information system design can be arrived at. The SSADM can be thought to represent a pinnacle of the rigorous document led approach to system design and contrast with more contemporary rapid application development methods such as Dynamic Systems Development Method (DSDM). One of the main features of SSADM is the intensive user involvement in the requirements analysis stage. This approach does not allow users to proceed to the next stage without completing or sign off the previous stage. Adequate and relevant UML diagrams such as a class diagram, use case diagram, activity diagram and deployment diagrams were generated which makes the coding process quite easy and straightforward.

The proposed system is designed in such a way that the key is generated first using the Diffie Hellman key exchange algorithm. The generated key is then used to encrypt the file. Once the encrypted file is sent, the key does not go along with the file in the same channel, instead, it passes through a different channel. Even

when MITM intercept the encrypted data on transmission, they will not be able to decode it since the key is not in their possession Or when the key is intercepted, it is useless to the attacker. At the end of the recipient, they can only decode the message only when they have the shared key. Accordingly, when the encrypted data is sent to the email address of the recipient, the key will be sent to the phone of the recipient. The key is what is now use to decrypt the data. Figure 1 below is the schematic diagram of the proposed system.

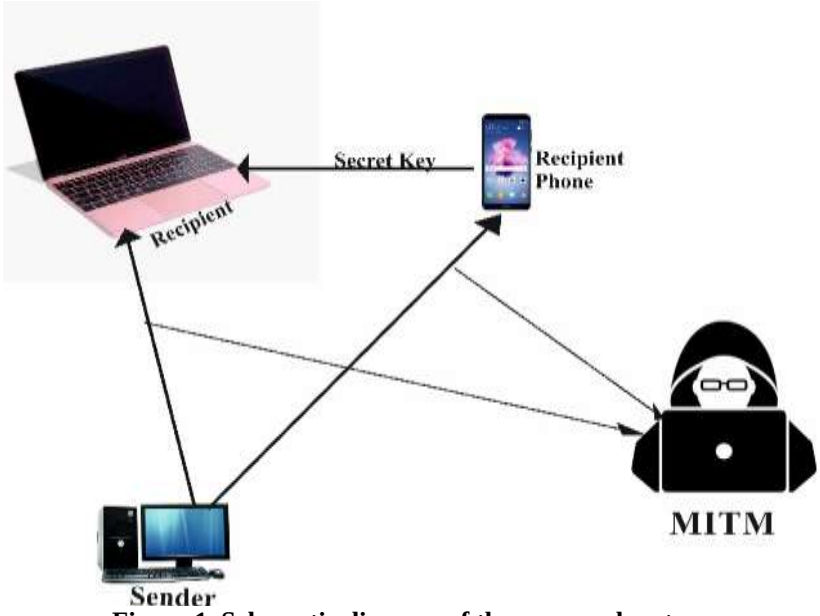

Figure 1. Schematic diagram of the proposed system

VII IMPLEMENTATION AND RESULTS

In implementing the proposed system, the researcher uses a laptop with the following processor configuration: Intel(R) Celeron(R) CPU N2840 @ 2.16GHz, RAM of 4GB and Hard disk of 500GB. The Operating System is Windows 10 64-bit. Also, Java was used for front-end programming, while MySQL was utilized for database management.

In testing the proposed system, Figure 2 below display the options for user login in, this is after the user must have registered. The user will have to provide their Username and Password to access the system.

Figure 2. User Login Interface

Upon successful logging, the data encrypting interface represented by Figure 3, is displayed. This enables the users to locate the data he intends to send and then encrypt it with the generated key. The user can now prepare to send it to the email of the legitimate receiver.

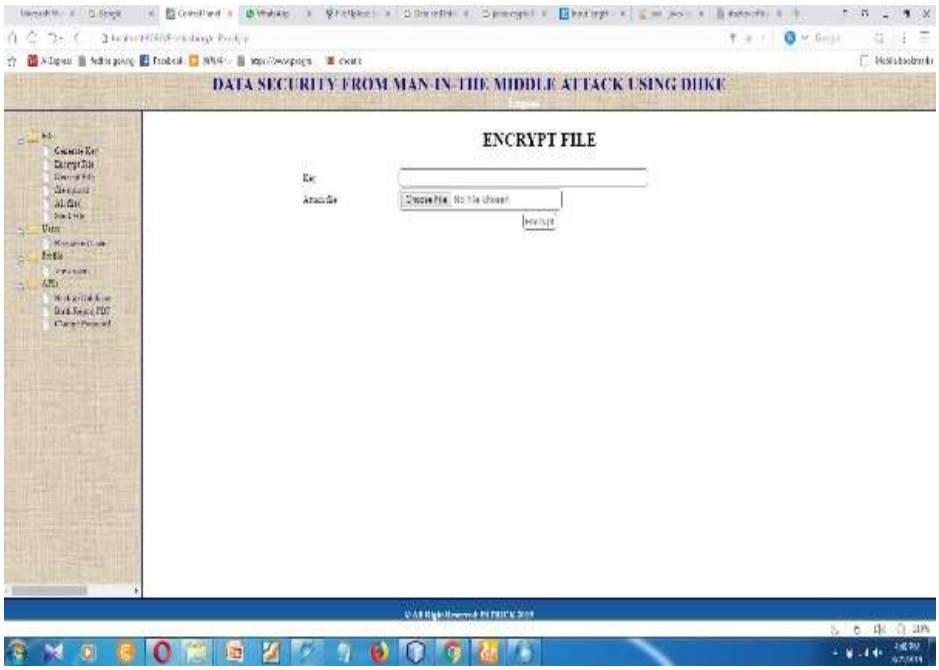

Figure 3. Data Encryption Interface

Under the send file menu, the compose mail interface is displayed in figure 4 below. The users now enter the recipient e-mail address, the subject of the mail to be sent and little write up in the content area. The encrypted file is then attached before sending. The proposed system will also notify the user when the message is successfully sent.

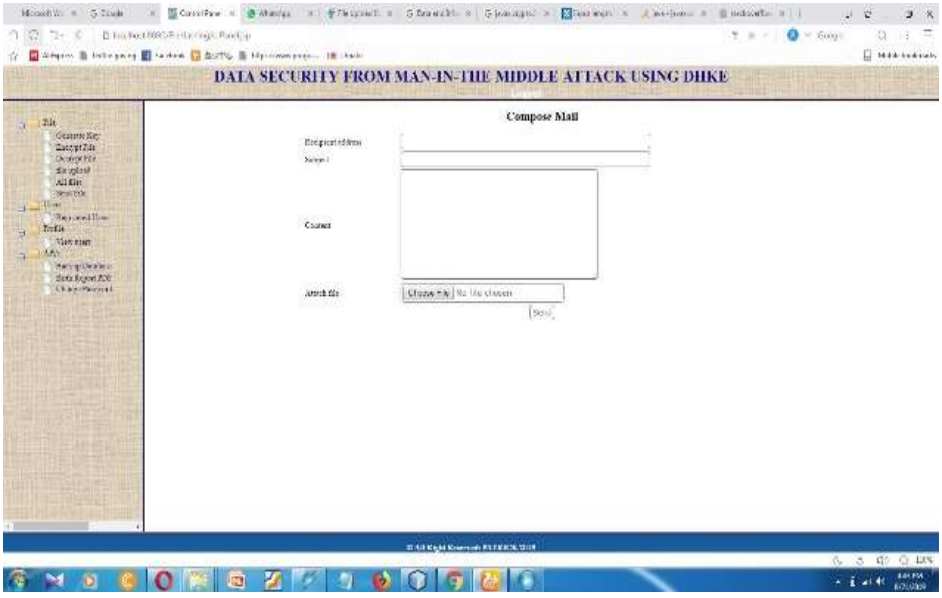

Figure 4. Mail Sending Interface

VII CONCLUSION

The research is very useful in many governmental and non-government institutions around the globe where securing confidential information while sending it has become important. In Nigeria for instance, it will be useful for Military, all Para-Military and tertiary institutions. The military and paramilitary can use it in sending their confidential, secret and top-secret operational data to their various operation commanders or units commanders securely from being intercepted by the adversaries. In Nigeria, tertiary institutions such as the

Universities, Polytechnics and Colleges of Education have portals that serve as a platform where the institutions are managed. However, these portals are not equipped with secured data transmission mechanism. The proposed system can be integrated with these portals to securely send data of students, academic and non-academic staff to the would-be client for legitimate transactions.

Deploying the proposed system into these portals, will not only eliminates the possibility of alteration in the data on transit by MITM but also ensures that the confidentiality remains intact as it reaches its destination. The findings of this research are also very useful to all the commercial banks, examination bodies and small & medium scale businesses all over the globe.

REFERENCES

[1]. Shashikant Kuswaha, Praful B. Choudhary, Sachin Waghmare and Nilesh Patil (2015). Data Transmission using AES-RSA Based Hybrid Security Algorithms. International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169.

[2]. Jitender Kumar (2012). Data Security and Encryption in a Network environment. International Research Journal of Management Science & Technology (http:www.irjmst.com).

[3]. Tange, H. (2012). SPDH – A Secure Plain Diffie–Hellman Algorithm. Journal of Cyber Security and Mobility, 1(2-3).

[4]. Prateek Kumar Singh, Pratikshit Tripathi, Rohit Kumar and Deepak Kumar (2017). Secure Data Transmission. International Research Journal of Engineering and Technology e-ISSN: 2395-0056 p-ISSN: 2395-0072.

[5]. Aboho D Moses, Karim Usman, Awuhe T. Richard and Engr. Ikerave A. Fredrick (2016). Integration of Deffie Hellman Key Exchange Encryption and Advanced Encryption Standard Algorithm for Securing SMS based One-time Password from Man in the Middle (MITM) Attacks. International Journal of Advanced Studies in Computer Science and Engineering Volume 5, Issue 5.

[6]. Maryam Ahmed and Habeeb Omotunde (2012). Diffie Hellman and its Use in Secure Internet Protocols. International Journal of Engineering Science and Innovative Technology.

[7]. Prashant Rewagad, Yogita Pawar (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. International Conference on Communication Systems and Network Technologies.

[8]. Syeda Farhana Tasneem, S Durga Bhavani and K. Suresh Babu (2014). Secure Data Transmission Using Cryptography and Steganography.International Journal of Emerging Trends in Electrical and Electronics (IJETEE – ISSN: 2320-9569).

[9]. S. Grace Sophia and S. Prabakeran (2016). Efficient and Secure Data Sharing Using AES and Diffie Hellman Key Exchange Algorithm in cloud. Middle-East Journal of Scientific Research 24 (Special Issue on Innovations in Information, Embedded and Communication Systems): 126-131.

[10]. Iman Almomani, Mohammed Al-Saruri and Mousa AL-Akhras (2011).Secure Public Key Exchange against Man-In-The-Middle Attacks during Secure Simple Pairing (SSP) in Bluetooth. World Applied Sciences Journal 13 (4): 769-780, 2011 ISSN 1818-4952.

[11]. Rupa Ganjewar (2010). Diffie Hellman Key Exchange. Department of Electrical and Computer Engineering, University of California, Santa Barbara, CA 93106.

Karim Usman" Securing Data on Transmission from Man-In-The-Middle Attacks Using Diffie Hell-Man Key Exchange Encryption Mechanism" The International Journal of Engineering and Science (IJES), 8.8 (2019): 88-94