International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 998-1004 www.ijaem.net ISSN: 2395-5252

Secure Text Transfer Using Diffie-Hellman Key Exchange Based On Cloud

Jim Mathew Philip[#1], Joyce Thomas M[*2], Jeeva Sarthik A[#3], Aishvarya R[#4]

#1 Assistant Professor, Department of CSE, Sri Ramakrishna Institute of Technology
#2, #3, #4 Students, Department of CSE, Sri Ramakrishna Institute of Technology, Coimbatore,TamilNadu,India

Submitted: 15-03-2021 Revised: 30-03-2021 Accepted: 01-04-2021

ABSTRACT— Encryption is the idea of hiding information that could be private or sensitive in nature within something that appears to be nothing unusual. Anyone who views the ciphertext will have no idea that there is any secret information. Encryption exploits human perception, as humans are not trained to look for files that have information inside of them. What this system does is that it allows the user to send text as a secret message and gives a key to lock the text. This key encrypts the text so that even if the transferred file is compromised by a third party, they would still not be able to read the text. The receiver will require the key to decrypt the encrypted text. The sender shares the key with the receiver which will then be used by the receiver to decrypt the ciphertext given by the user. The Diffie-Hellman key exchange algorithm offers the best of both worlds as it uses public-key cryptography to allow the exchange of a private key which will be used for encryption. By using this method, we can ensure that our secret message is sent secretly without the interference of hackers or crackers. If the sender sends this ciphertext in a public network others will not know what it is, and it will be received by the receiver. The system uses an online database to store all the required information. As the project files and a database file will be stored in the remote MySQL cloud, the project will be accessed in the web browser through a cloud link.

Keywords— Encryption, Decryption, cloud, private key, public key, ciphertext

I. INTRODUCTION

Cloud computing was an important phase in computer science. It provided the resources to solve complex problems that were deemed to be unsolvable by a machine. Cloud computing provided an outstanding platform for optimal utilization of resources that were spread across the planet. It reduced the pressure on manufacturers to build computers with higher processing capabilities. One of the main drawbacks of cloud computing was its standard of security. This project proposes a secure way of storing a file on the cloud using Diffie Hellman. The key exchange algorithm allows the user to decrypt the required file. The main concern in cloud computing is security. The storage of information that is personal and sensitive in nature poses a high-level risk as the information can be stolen or misused by an individual or a group with malicious intent.

The issue is so big that it has discouraged governments and several organizations from migrating their operations onto the web. The age-old method of securing files is redundant when it comes to the cloud scenario. A lot of research and development is required to make the usage of cloud services a safe and secure one.

The Diffie-Hellman key exchange algorithm is so robust that it can take several millions of years for the most powerful computers of all time to crack the ciphertext and read the original message. Our approach uses a standard encryption algorithm and Diffie Hellman for user authentication, in this way the data is stored in the cloud without any unauthorized person misusing it.

The Diffie Hellman key exchange is a way of sharing keys securely over an unsafe network. It was named after two scientists Whitfield Diffie and Martin Hellman. Encryption and Decryption in public-key cryptography are governed by two different keys E and D such that computing D from E is computationally impossible. The encryption key can be made public without displaying the decryption key D. This was one of the main agendas behind the Diffie Hellman key exchange algorithm/protocol. Each user of the proposed system can thereby place the enciphering key in a directory that is public. Any user can send a message to any other user enciphered in such a way

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 998-1004 www.ijaem.net ISSN: 2395-5252

that only the authenticated user can decrypt it. A public-key cryptosystem works similar to a multiple-access cipher.Encryption is one of the widely used methods to protect user information that is sent between a client-server to a server. The information may include passwords, payment information, and other data that could be considered private.

A prime number is a natural number that is greater than 1 and also not formed by multiplying two natural numbers that are smaller than it. The user-defined input parameter in the Diffie Hellman key exchange is the selection of prime numbers. The input parameter must be large enough to withstand the popular attacks against it. The network file system attack is one of the most efficient attacks on 232-bit numbers. It can be proven mathematically that both the sender and receiver are able to generate the same key without knowing each other's private keys.

II. LITERATURE SURVEY

Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing - Prashant Rewagad , Yogita Pawar - This paper proposes a three-way mechanism that involves authentication, data security, and verification all at the same time. Digital signature and Diffie Hellman key exchange are combined with the Advanced Encryption Algorithm (AES) to secure the data which is stored in the cloud. Even if the key is hacked the application of Diffie hellman makes it useless for the hacker. The proposed system makes it difficult for hackers to break the secured system, thereby ensuring the protection of data that is stored in the cloud.

Provably Secure Authenticated GroupDiffie–Hellman Key Exchange - Emmanuel Bresson, Olivier Chevassut, David Point cheval - This method extends the cryptographic method by considering a group of members exchanging a shared secret value and providing standard treatment for it. Concurrency introduces technical difficulties when it comes to security analysis. Prevention of active attacks is done by adding authentication to the key exchange protocol. Active attacks are easier to perform and have more scope for destruction as middleware enables data exchange between a large number of components that form a multicast group.

Password-Authenticated Key Exchange between Clients -JinWook Byun Ik Rae Jeong, Dong Hoon Lee, Chang-SeopParkol - This paper suggests two C2C-PAKE schemes. one in a cross-realm and the other one in a single-server setting. The security notions and the type of possible attacks are defined according to the new framework. Due to the rapid change in modern communication systems, a secure client-to-client channel is required. This paper proves that their scheme is secure against all the attacks considered in this paper. The password-authenticated key exchange is based on two different passwords without any pre-shared secret. Authentication that relies on passwords is a popular method especially when it comes to the client-server model due to its easy to memorize property. A password that is selected from a small space allows the hacker to launch a dictionary attack. The proposed schemes are based on cross-realm authentication based on the Kerberos system.

A Faster Software Implementation of the Supersingular Isogeny Diffie-Hellman Key Exchange - Armando Faz-Hernández , Julio López, Eduardo Ochoa-Jiménez , Francisco Rodríguez-Henríquez - This paper introduces a more efficient approach for elliptic curve operation nP+ [k]Q. This plan achieves a 1.4x speed-up compared to the regularly used three-point ladder algorithm that is generally used in the phase that is a shared secret. The algorithm yields a 1.7x acceleration in the key generation phase.

This approach provides an optimized evaluation of the point tripling formula and also discusses several algorithmic and implementation techniques that lead to better performance. No secret values were used to index the lookup tables or separate the execution of any function.

Multisignatures Using Proofs of Secret Key Possession, as Secure as the Diffie-Hellman Problem - Ali Bagherzandi , StanisławJarecki - This paper shows how to produce secure multisignatures in the proof of secret key possession. Multisignatures are applied when there are a moderate number of signers such as the distribution of certificate authorities. The multisignatures in the free setting have a slower rate of verification than the one in the key registration model. This paper proposes two multisignature schemes in the key verification model.

Integrating Diffie-Hellman key exchange into the digital signature algorithm - L. Harn , M. Mehta , Wen-Jung Hsin - This paper proposes three different protocols that integrate the Diffie Hellman key exchange along with the digital

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 998-1004 www.ijaem.net ISSN: 2395-5252

signature authentication for the authenticated distribution of keys. The original Diffie Hellman key exchange did not provide an authentication security mechanism for the public keys that were exchanged. The one-round protocol supports applications that are not interactive like a secure email transmission. The two-round protocol supports interactive applications. The three-round protocol is similar to the two-round protocol in such a way that it includes the confirmation of keys. One-round and two-round protocols cannot prevent key-replay attacks as they do not have the security layer of key confirmation. Unknown key-share attacks can be prevented by key confirmation. The proposed protocols prevent the key-replay attack and the known-key attack.

Applied Cryptography and Network Security - Raphael C. , W. Phan , Bok-Min Goi - This paper proposes ways to protect EKE-U from external attacks and make a strong case for the EKE-U scheme to prove its potential as a very secure n-party PAKE. This paper shows that the EKE-U is vulnerable to different attacks like an offline dictionary attack, an online dictionary attack, and the impersonation attack. This paper proves that the key privacy is not provided by the original and strengthened EKE-M variants.

Efficient and Secure Authenticated Key Exchange UsingWeakPasswords - Jonathan Katz , Rafail Ostrovsky , Moti Yung - This paper proposes a 3-round protocol for password-only authenticated key exchange and provides rigorous proof of how secure the proposed protocol is, based on the Diffie-hellman key exchange algorithm. The proposed protocols assume public parameters that can be hardcoded when the protocol is finally implemented. The proposed protocol is practical and provably secure based on cryptographic calculations.

III. EXISTING SYSTEM

Cryptographic algorithms in general are categorized on the basis of the number of keys that are used for encryption and decryption. A few examples of these algorithms include secret key cryptography that uses a single key for both encryption and decryption, public-key cryptography that uses a different key each for encryption and decryption , and a hash function that irreversibly encrypts the information.

IV.PROPOSED SYSTEM

The Diffie Hellman algorithm utilizes the public key technique to facilitate the sharing of the private key used for encryption. The protocol involves two users selecting very large prime numbers on the condition that one can generate the other. Both users select their private keys. The public keys are later generated using a modulus-based mathematical formula. The public key is later shared over an unsafe network. The shared secret key is later generated by each of the users that help in decrypting the message safely and securely. The user information is saved on a free cloud-based online database named Remote MySQL.

A.Use Case Diagram

A Use case diagram is a way of representing a system from an end user's perspective. They help us to visualize the expected behavior of the system. A use case diagram consists of three main components, the use case, actor, and the system. It helps us to view the various relationships between the user and the system.

- Both the users agree upon two prime numbers.
- Both the users have private keys of their own.
- The public keys generated are shared with each other.

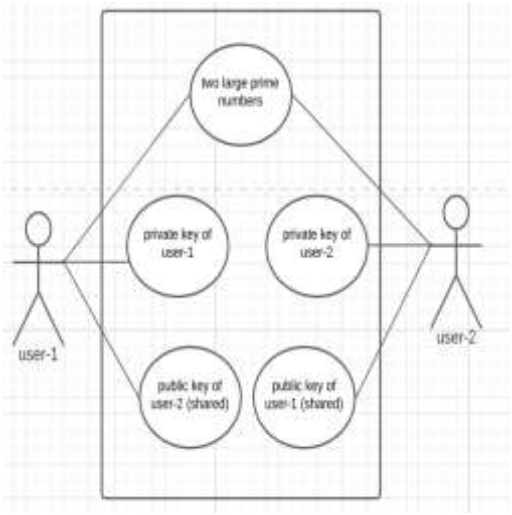

Fig 1: Use Case Diagram

B.Sequence Diagram

A sequence diagram is an interaction diagram that is used by software developers and business professionals to better understand the user requirements or is used for documentation purposes.

- The prime number and the private number are generated by both the users.
- The generated public key is shared with each other.
- The final secret key generated will be used in the safe and secure transmission of the message.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 998-1004 www.ijaem.net ISSN: 2395-5252

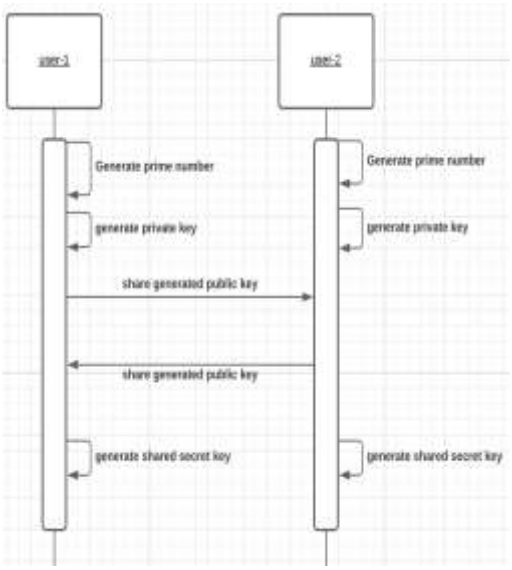

Fig 2: Sequence Diagram

C.State Diagram

State diagrams are used by software engineers and business professionals to describe the behavior of the particular system that they are working on. They introduce a level of reasonable abstraction.

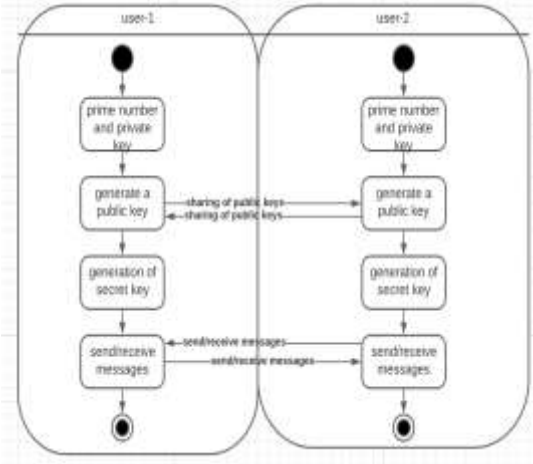

Fig 3: State Diagram

V. WORKING PRINCIPLE

The block diagram given below gives a visual representation of how the proposed system works. The proposed system uses the Diffie Hellman key exchange algorithm for the safe and secure transfer of information.

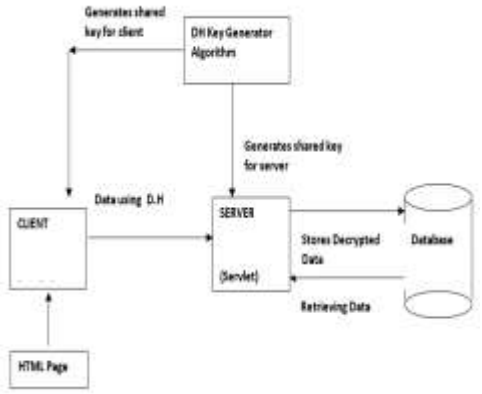

Fig 4: Block Diagram

The user will have to register on the application then login to the user portal. The client-side browser will accept the user information and send it to the server(servlet) for further processing. The server makes use of the Diffie Hellman key generator to generate keys that help in the encryption of the data.

The encrypted data is later stored in the cloud-based online database. The Diffie Hellman key generator sends a key to the client-side to allow the user to decrypt the message. The server retrieves the required data and keys from the online-based cloud database.

VI. EXPERIMENTAL SETUP

The proposed application uses the object-oriented programming language java version 8. The IDE used is the NetBeans IDE version 8.0.1. HTML is dynamically generated using Java Server Pages(JSP). The data is stored in a cloud service called Remote MySQL. SQLyog a powerful MySQL GUI tool is installed for its powerful features like autocomplete and query building.

VII.RESULTS

As a result, our application has successfully implemented the Diffie Hellman key exchange protocol that enables users to send and receive textual data safely and securely.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 998-1004 www.ijaem.net ISSN: 2395-5252

Fig 5: Home Page

The above image displays the home page of the application.The below screenshots will provide a walkthrough about the working of the application.

Fig 6: Registration page

Fig 7: Login page

In order to use the application, the user will have to register with their details. After registration, the user can log in to start using the application.

Fig 8: Send/Receive page

Fig 9: Message details page

Fig 10: Parameters page

The user will choose whether to send or receive a message. When the user clicks on the send button, the user is directed to the message details page where the user will have to enter the receiver's username and the message to be sent. When the send button is clicked, the parameters that need to be input will be shown to the user.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 998-1004 www.ijaem.net ISSN: 2395-5252

Fig 11: Message sent confirmation page

Fig 12: Receiver login page

When the Diffie Hellman key Exchange button is clicked the textual message will be sent to the receiver and the other generated parameters will also be shown to the sender.

Fig 13: Receiver inbox

Fig 14: Selecting a message

Once the receiver logs in to the application and clicks on the receiver button, he will be directed to the inbox page. On the inbox page, the receiver can enter the id of the message and click on the extract button to extract the key. The extracted key will be displayed to the receiver. When the receiver enters the key and clicks on the view button, the sent message will be displayed.

Fig 15: View message

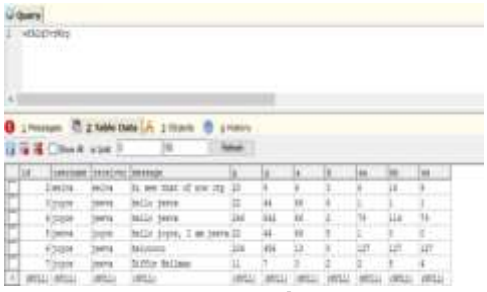

Fig 16: Database

The user details and the message parameters can be viewed in the database. The user information is stored in the cloud-based database in a safe and secure manner.

VIII. CONCLUSION

The use of the Diffie Hellman key exchange protocol helps us to override the problems of key agreement and key exchange. It must be taken into consideration that the key exchange protocol does not involve any sort of encryption or decryption. The textual information can be exchanged between the users through an insecure network once the keys have been successfully exchanged.

IX.FUTURE WORKS

The Diffie Hellman key exchange is one of the most secure key exchange protocols, however, with the ever-increasing number of mobile devices with limited computational resources it is important to reduce the computational load on the mobile devices. In the future, we would like to implement a modified Diffie Hellman protocol along with three-party authenticated schemes that reduce the client exponential computation up to 50 percent.

ACKNOWLEDGEMENT

The authors are deeply grateful to The Honourable Principal and Faculties of Sri Ramakrishna Institute of Technology, Coimbatore for providing the necessary support, guidance, and facilities for the preparation of this paper.

REFERENCES

[1] Prashant Rewagad , Yogita Pawar,"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 , 2013, pp. 437-439 , 10.1109/CSNT.2013.97.

[2] Bresson, E., Chevassut, O., &Pointcheval, D. (2007). "Provably secure authenticated group Diffie-Hellman key exchange". ACM Transactions on Information and System Security, 10(3), 10–es. doi:10.1145/1266977.1266979

[3] Byun, J. W., Jeong, I. R., Lee, D. H., & Park, C.-S. (2002). "Password-Authenticated Key Exchange between Clients with Different Passwords". Lecture Notes in Computer Science, 134–146. doi:10.1007/3-540-36159-6_12

[4] Faz-Hernandez, A., Lopez, J., Ochoa-Jimenez, E., & Rodriguez-Henriquez, F. (2017). "A Faster Software Implementation of the Supersingular Isogeny Diffie-Hellman Key Exchange Protocol". IEEE Transactions on Computers, 1–1. doi:10.1109/tc.2017.2771535

[5] Bagherzandi, A., &Jarecki, S. (2008). "Multisignatures Using Proofs of Secret Key Possession, as Secure as the Diffie-Hellman Problem." Security and Cryptography for Networks, 218–235. doi:10.1007/978-3-540-85855-3_15

[6] Harn, L., Mehta, M., &Hsin, W.-J. (2004). "Integrating Diffie–Hellman Key Exchange into the Digital Signature Algorithm (DSA)". IEEE Communications Letters, 8(3), 198–200. doi:10.1109/lcomm.2004.825705

[7] Zhou, J., Yung, M., & Bao, F. (Eds.). (2006). "Applied Cryptography and Network Security". Lecture Notes in Computer Science. doi:10.1007/11767480

[8] Katz, J., Ostrovsky, R., & Yung, M. (2009). "Efficient and secure authenticated key exchange using weak passwords". Journal of the ACM, 57(1), 1–39. doi:10.1145/1613676.1613679

[9] Chien, H.-Y. (2017). "Using the Modified Diffie–Hellman Problem to Enhance Client Computational Performance in a Three-Party Authenticated Key Agreement". Arabian Journal for Science and Engineering, 43(2), 637–644. doi:10.1007/s13369-017-2725-6

[10] Gadhavi, L., Bhavsar, M., Bhatnagar, M., &Vasoya, S. (2016). "Design of efficient algorithm for secured key exchange over Cloud Computing. 2016 6th International Conference".Cloud System and Big Data Engineering (Confluence). doi:10.1109/confluence.2016.7508110