Application of Diffie-Hellman Key Exchange for Secure Text Transfer

Nikesh Singh[1], Prof.Saravanan C[2]

[1]*PG Student, Master of Computer Applications, RV College of Engineering®, Karnataka, India*

[2]*Assistant Professor, Master of Computer Applications, RV College of Engineering®, Karnataka, India*

Abstract-Cloud security is one of the concerns in the cloud computing domain. Keeping personal and sensitive information in a third-party storage system poses a high risk of data theft and misuse of data by anyone with malicious intent. This threat is so disgraceful that it has hampered governments and many other large organizations to move their operations to the cloud base. Traditional methods of accessing files and information are excellent in the cloud environment. Extensive research is underway in this field to make the cloud safer and more reliable. During this time of behemoth research, some of the emerging trends include AES encryption and the Diffie Hellman Key Exchange. The storage system is so powerful that it can take millions of years and even the most powerful computers in modern times to crack the code and read the file.

Keyword: - *Diffie Hellman Algorithm, Encryption, Decryption, Public Key, Secure Text, Security, Private Key, Key Exchange Policy*

1. INTRODUCTION

In cryptography, exchanging keys is a way of sending a key between a sender and the person who receives it. Key exchange issues on how to send a message so no one can understand the message other than the sender and the recipient. The process is one of the cryptographic of the first public key. Contracts used to create a private key between each other through a security channel. The protocol itself is compressed to rotate buttons for example: we can make the key together instead of sharing data while the exchange is key. We use the algorithm for exchanging information on a public channel to creates the secret of an encounter between two circles that can use it for private communication. Diffie-Hellman is worth using in the communication of information as well is widely used for archiving or archiving in the long term. In a cryptographic protocol having a key exchange is the first problem. Personal development, people try to hide data from other people in order to compose formation. This is thought to be the original and subtle form of encryption, but it is only about half the size of cryptography. The other part is the scale reproducing the original message from its hidden structure. Cryptography is like a normal message but no one but the particular recipient will understand the message. At that time most of the cryptosystems were private symmetric key cryptosystems. In this case two clients Alice and Bob choose a key, which is their private key and then use the key in the private key cryptosystem to transmit personal information to the public channel. We are investigating public key cryptography relating to the Diffie-Hellman key Exchange Protocol, which is the very first concept behind public key cryptography. In the Diffie-Hellman key protocol, two anonymous clients can set up a private but controversial key for their symmetric key system. Diffie-Hellman (1976) main protocol was the first effective way to create a shared secret over an insecure communication channel. In modern cryptography, we think the key is only private. So, if there are multiple keys, then the hardest cryptosystem opponent. We will create a general protocol for the exchange of keys in groups. We choose the key that is the automorphism group in the highest group of the automorphism group.

2. LITERATURE REVIEW

Key establishment agreements are among the most important security measures whereby one or more parties can encrypt their communications over an unsecured network. This paper is concerned with the risk of a single-party multivariate logistic regression (K-CI) procedure. The latter can happen when the enemy has received a long-term key for a loyal party, and presents a risk - but often overlooked - threat, since a successful counterfeit attack may have a far greater effect than learning from future negotiations. Our aim is to describe the two main categories of K-CI attacks that can be classified into all the most well-known comment systems, including MQV and HMQV. It show that some of the defined attacks can be partly avoided (or not completely eliminated) by the combined use of digital signature and timestamps; however, there is still a category of K-CI threats in which there is no obvious solution[4].We expect that there are many families of authenticated key exchange (AKE) protocol attacks that are outside the scope of the current definition of security definitions. In an effort to bring this attack to the analytical center we extend the AKE security system to give greater power to our opponent. We provide a standard framework for protecting AKE security, which we call robust AKE security, in which existing security definitions appear as framework instances. Here it has been introduce NAXOS, AKE's new protocol, and prove that it is safe in this regard. Itillustrate the importance of this principle by demonstrating that the AKE secure protocol may be at risk if placed in unprotected signing systems by the disclosure of the privacy risk app. lied to the signature generation[5].The rapid growth of using cloud-based services in recent years is an undeniable fact as it has increased efficiency in finding shared pools of interactive computer resources. However, there are serious concerns regarding the reliability of these emerging technologies and it is expected that concerns about cloud security become a very important and challenging issue for the IT industry. Ideally, a hybrid encryption model is introduced in this paper to ensure data security in cloud computing environments based on concepts of index classification, time-consuming processes, and attributes. In line with this, the information is separated into four main rings according to their attributes. In addition, a hybrid ring was developed to provide secure connection between the rings through a dual encryption process. This is about source features and destination rings. Protected rings facilitate the rewriting process according to four key parameters: time-based, unauthorized authorization, user withdrawal, and data owner request. In addition, the performance, safety, and vulnerability of the proposed model were evaluated by a simulation analysis to determine the strength of this rewrite model compared to the current models. The results of the analysis indicate that the model met the stated requirements of this study to strengthen the reliability and efficiency of data protection in cloud computing environments [7]. Network traffic protection has always been a requirement for any network the application uses an insecure communication channel. The reason is to provide protection for data transmitted to the network against unauthorized disclosure and modification of messages between communication organizations. The cryptographic key exchange protocol the first one that can establish secure communications. The first exchange agreement is the first presented by Diffie-Hellman. The purpose of the Diffie-Hellman agreement is to give you two powers groups to exchange a session key that can be used for the following message encryption. However, Diffie-Hellman himself does not confirm the connection organizations. In this paper, we learn about the Diffie-Hellman Key exchange protocol. Next define a valid key exchange protocol with the One-pass key exchange protocol, that is variant of the Diffie-Hellman protocol [12]. In cryptography, exchanging keys is a way of sending a key between the sender and the recipient. The key exchange topics are how they refer the message so that no one can understand the message except the sender and the recipient. The process is one of the most basic cryptographic public keys used to create a secret key between each other over a security channel. The protocol itself is compressed to rotate keys for example: we make the key together instead of sharing data while the exchange is key. We use an algorithm for exchanging information through a public channel to create the secret of an interaction between two circles that can be used for private communication. Diffie-Hellman is suitable for use in data communication and has been used frequently for archiving or archiving for a long time [17]. In a cryptographic protocol having a key exchange is the first problem. Designed to improve people, people try to hide information from other people so that their building can be named. This is thought to be the original and subtle form of decryption, but it is only part of the concept. Another component is the rate of reproducing the original message in its encrypted structure. Cryptography is like a normal message but no one will understand the message. At that time most of the cryptosystems were private symmetric key cryptosystems. In this case two clients Alice and Bob choose a key, which is their private key and then use the key in the private key cryptosystem to transmit personal information to the public channel. We are investigating public key cryptography relating to the Diffie-Hellman key Exchange Protocol, which is the very first concept behind public key cryptography. In the Diffie-Hellman key protocol, two anonymous clients can set up a private but controversial key for their symmetric key system. Diffie-Hellman (1976) main protocol was the first effective way to create a shared secret over an insecure communication channel. In modern cryptography, we think the key is only private. If there are multiple keys, then the hardest cryptosystem opponent. It will create a general protocol for the exchange of keys in groups. We choose the key that is the automorphism group in the highest group of the automorphism group [13].

3. PROPOSED METHODOLOGY

Secure text transfer Application is used to provide a platform to share the data in secure way. This system helps the user to encrypt their text and send it to the other users. It will also help users to decrypt the encrypted text received by other users.

- Key Generation

This is a Web Application to generate private and public key of each users. User has to register by giving all required details.

Introduction: Web Application to generate private and public key of each users. User has to register by giving all required details. Input Data: Username, First name and

Second name. Process: All the input data will be collected and stored in the database. Output Data: Private key and public key will be generated. Private key will be generated only once after registration.

- Encryption and Decryption

This is a Stand-Alone Application which has options to encrypt the text file and to decrypt the encrypted text file.
Introduction: Stand Alone Application will contain options to encrypt the text file and to decrypt the encrypted text file. Input Data: File path, Folder path, private key and public key. Process: Encrypts or decrypts the data based on user selection. Output Data: Encrypted(cipher) text or Decrypted (Main) text.
The Diffie-Hellman key switch is complicated and it can be hard to get your head on how it works. It uses enormous numbers and lots of math, something many of us are still scared of because of those high and famous high school lessons. To make things easier to understand, itwill start by defining the Diffie-Hellman key exchange key metaphor. Once you have a great idea of how it works, we will move on to a more technical description of the processes below. The best analogy of the Diffie-Hellman program is to think of two people mixing paint. Let's use standard graphics, and say their names Alice and Bob. They both agree on a random color to start with. Let's say they send a message and decide on yellow as their usual color, as in the diagram below:

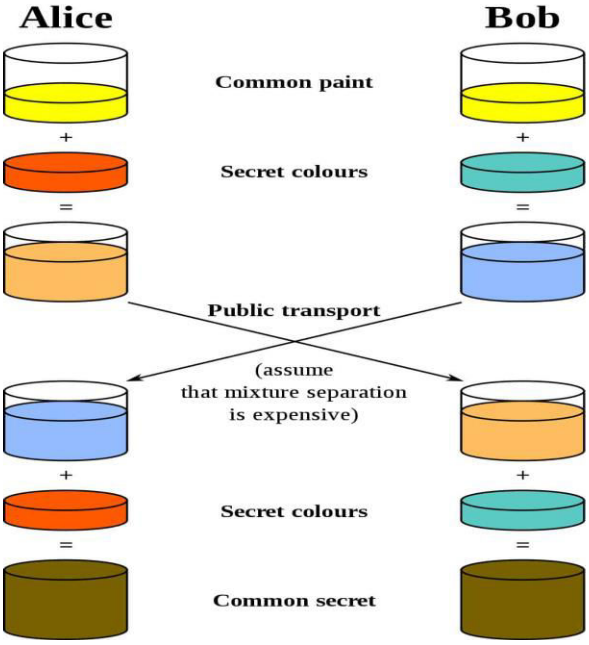
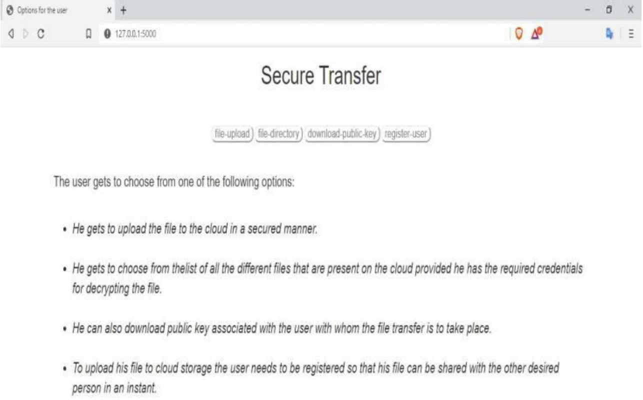


Figure 1 : Process of Encryption and Decryption

Enter their secret color. They do not tell the other party of their choice. Let's say Alice prefers red, while Bob prefers green. The next step is for both Alice and Bob to mix their secret color (red for Alice, blue for Bob) and yellow for which they agree. According to the sketch, Alice ends up in an orangish mix, while Bob's effect is blue. When they had finished mixing, they sent the result to another group. Alice gets blue, while Bob is sent in orange-colored paint. Once they have found the result mixed with a colleague, they then add their secret color to it. Alice takes the blue and adds her secret red paint, while Bob adds her blue and blue to the newly discovered orange mixture. The result? They both come in the same color, which in this case is brown. It may not be the kind of color you would want to paint in your living room, but it's a shared color nonetheless. This shared color is called general secret. The critical part of the Diffie-Hellman exchange of keys is that both sides end up with the same result, without needing to send all the usual secret to the communication channel. Choosing a common color, their secret colors, exchanging mixes and adding their own colors too, gives both parties a way to get to the same common mystery without having to send everything. Once the attacker listens to the exchange, all they can find is the familiar yellow color that starts with Alice and Bob, and the interchangeable mixed colors. Since this is actually done in large numbers instead of paint, these pieces of information are not enough that the attack gets any original secret color, or common secret (technically it is possible to calculate a common secret from this information, but in the safe implementation of the Diffie-Hellman key exchange, it will take less than once and resources to do so). This exchange structure in the Diffie-Hellman key is what makes it so useful. It allows both sides to communicate with potentially dangerous communications and come up with a shared secret that they can use to encrypt their future communications. It doesn't matter if there are hackers listening, since a complete shared secret is not sent over the network.

Web Application provides many options for the user as user can register himself or can download the public key of other users and encrypt the text file. User can also upload the encrypted text on the web through this application



Secure Transfer

The user gets to choose from one of the following options:

- *He gets to upload the file to the cloud in a secured manner.*
- *He gets to choose from thelist of all the different files that are present on the cloud provided he has the required credentials for decrypting the file.*
- *He can also download public key associated with the user with whom the file transfer is to take place.*
- *To upload his file to cloud storage the user needs to be registered so that his file can be shared with the other desired person in an instant.*

Figure 2 : Web Application Home Page

Figure 2 shows the various options for the users like file-upload, file-directory, download-public-key and register user to generate the private and public key one needs to register themselves. As shown in Figure 6.1, to register every user needs to provide general information about themselves such as a username, first name, and last name. All the fields need to be filled accurately otherwise the application will generate an error.

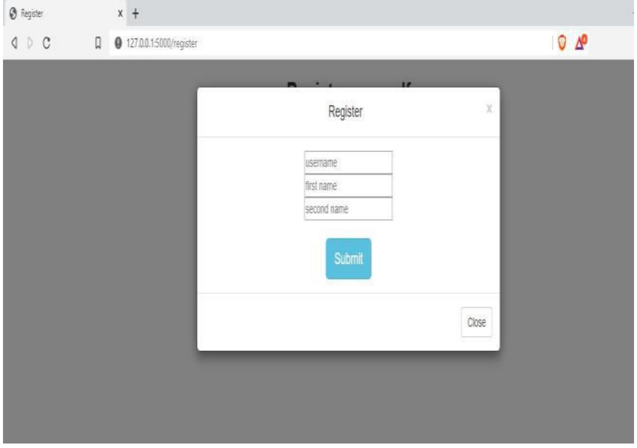
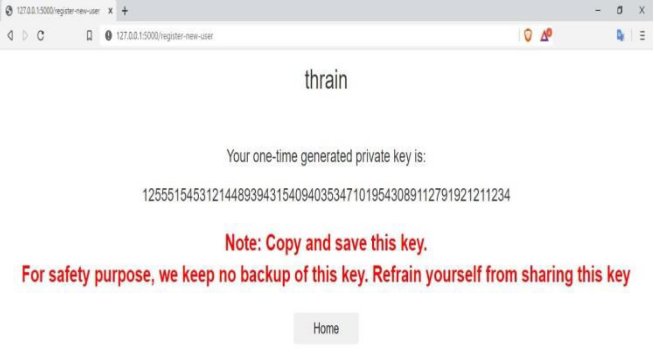


Figure 3: Registration Page

Figure 3 shows the registration page of application. User hasto provide all details in order to get registered.



thrain

Your one-time generated private key is:

1255515453121448939431540940353471019543089112791921211234

Note: Copy and save this key.

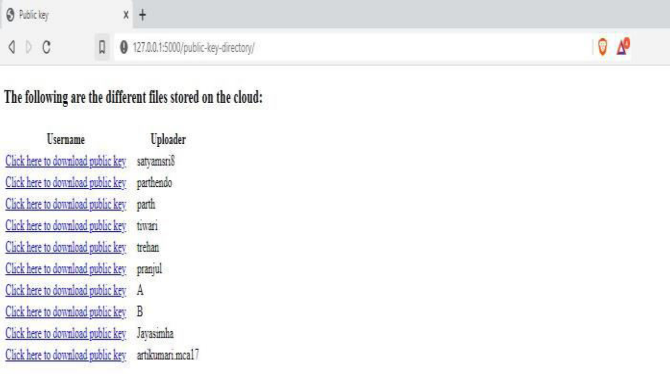
For safety purpose, we keep no backup of this key. Refrain yourself from sharing this key

Figure 4 : Private key generation

Figure 4 shows the user's one-time generated private key. Private key is generated only once when the user register for the first time.

3.1 Public Key List

When the user register himself for the first time one private key and one public key file gets generated. Private key is one-time generated key but public key is generated as file and can be downloaded later also.



The following are the different files stored on the cloud:

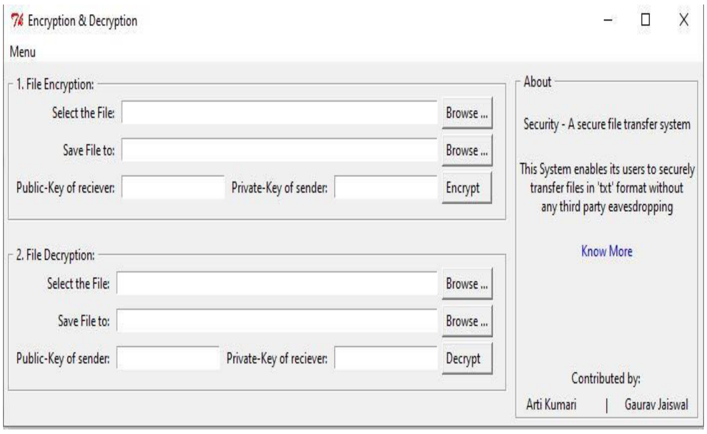
Username	Uploader
Click here to download public key	satyamsri8
Click here to download public key	parthendo
Click here to download public key	parth
Click here to download public key	tiwari
Click here to download public key	trehan
Click here to download public key	pranjul
Click here to download public key	A
Click here to download public key	B
Click here to download public key	Jayasimha
Click here to download public key	artikumari.mca17

Figure 5 : Public key file list

Figure 5 shows the list of public key files for each registered user. Public key of any user can be downloaded by any otheruser and It is used to encrypt the text.

4.ENCRYPTION AND DECRYPTION APPLICATION

This Application is used to encrypt and decrypt the text using proper text file and respective keys of receiver's and senders.



Security - A secure file transfer system

This System enables its users to securely transfer files in 'txt' format without any third party eavesdropping

Contributed by:

Arti Kumari | Gaurav Jaiswal

Figure 6: Encryption and Decryption Application

Figure 6.5 shows the GUI of Encryption and Decryption Application.

5. CONCLUSIONS

The proposed project aims to address the problem of secure file storage on the cloud. This method is a basic implementation of the proposed methodology that can be improvised and customized according to the needs. It proposes to use encryption and Diffie-Hellman to provide double layer of security to the files that are stored on the cloud. Cryptographic techniques and tools play an important role in design network connectivity technology. It is evident from the fact that this world most developed countries like the U.S. are considering cryptographic technologies such as standard storage technology to monitor the security feature of rapid growth commerce, banking, the country's military operations and demand for the day it must be standardized for the whole world to benefit from it. Cryptographic Key Management (CKM) is a fundamental part of cryptographic technology and is considered to be one of the key factors associated with its use. Failure of the methods used to distribute the keys and the usefulness of these methods are very important. That is why Nist (National Institute of Standards and Technology) USA, work to improve the comprehensive management strategies used by the public and private sectors respectively optimizing cryptographic technology to provide scalability throughout cryptographic technology, as well as supporting the management of global cryptographic indicators infrastructure.

REFERENCES

[1] Cheng-Kang Chu et.al, “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.

[2] M. J. Atallah et.al, “Dynamic and Efficient Key Management for Access Hierarchies,” ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.

[3] J. Benaloh et.al, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,” in Proceedings of ACM Workshop on Cloud Computing Security (CCSW ’09). ACM, 2009, pp. 103–114.

[4] K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis and G. Stephanides, Two Types of KeyCompromise Impersonation Attacks against One-Pass Key Establishment Protocols, in 4th International Conference, ICETE 2007, Barcelona, Spain, July 28-31, 2007, Revised Selected Papers, 2009.

[5] B. LaMacchia, K. Lauter and A. Mityagin, Stronger security of authenticated key exchange, in First International Conference, ProvSec 2007, Wollongong, Australia, November 1-2, 2007. Proceedings, 2007

[6] Diffie, W.; Hellman, M. (1976). "New directions in cryptography" (PDF). IEEE Transactions on Information Theory. 22 (6): 644–654. doi:10.1109/TIT.1976.1055638. Archived (PDF) from the original on 2014-11-29.

[7] J. Benaloh et.al, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,” in Proceedings of ACM Workshop on Cloud Computing Security (CCSW ’09). ACM, 2009, pp. 103–114.

[8] Kuhlman, Dave. "A Python Book: Beginning Python, Advanced Python, and Python Exercises", Second edition 23 June 2012.

[9] Padmavathi, B. and S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique.", 2013

[10]] P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm", 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),Chennai, 2016, pp. 1635-1638.

[11] Abhilasha CP and Nataraj KR “Software Implementation of AES Encryption Algorithm”,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, May 2016.

[12] Abhilasha CP and Nataraj KR “Software Implementation of AES Encryption Algorithm”,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, May 2016 .

[13] Siddanth Sarathy, Ketan Pawar, Saurabh Udgirkar and Jehan Joshi “Secured Data Transfer Over Cloud Networks”, International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 4, April 2015, pg.153 – 157.

[14]"How Cloud Computing Works", [Online]. Available: http://computer.howstuffworks.com/cloudcomputing/cloud-computing.htm.

[15] “Hybrid Cryptography on Cloud”, [Online]. Available: https://github.com/Krprashant94/Hybrid-Cryptography-on-Cloud.