An Approach for a Password Encryption Using Dual Server

Palak Jain[A], Nikunj Varma[A], Pratik Tated[A], Prasann Saran[A], Suja.S.Panicker[B]

[A] *B.E Computer Science student, Maharashtra Institute of Technology (MIT), affiliated to Savitribai Phule Pune University, Kothrud, Pune, 411038, Maharashtra, India.*

[B] *Professor in Computer Science department, Maharashtra Institute of Technology (MIT),affiliated to Savitribai Phule Pune University, Kothrud ,Pune, 411038 , Maharashtra, India.*

***Abstract*— Password-Encryption is where a client and a server, who share a password, authenticate each other and meanwhile establish a cryptographic key by exchange of messages. In this paper, we consider a scenario where two servers cooperate to authenticate a client. Current solutions for dual-server Password-Encryption are either symmetric in the sense that two peer servers equally contribute to the authentication or asymmetric in the sense that one server authenticates the client with the help of another server. This paper presents a symmetric solution for dual-server Password Encryption, where the client can establish different cryptographic keys with the two servers, respectively. Our protocol runs in parallel and is more efficient than existing symmetric two-server protocol, and even more efficient than existing asymmetric two-server protocols in terms of parallel computation.**

***Keywords*: Diffie-Hellman Algorithm (DHA), Diffie-Hellman Key Exchange, Public Key (PK), Private Key, SSL, TLS, SSH, PKI, IETF, Elgamal, symmetric cryptography**

I. INTRODUCTION

Here, we have presented a password authenticated two server key exchange system based on Diffie-Hellman [1, 2, 3, 4, 7, 8 , 9, 10, 13, 14] and Elgamal algorithms [5, 6, 7 , 8, 9, 10, 11, 12] to provide a higher level of security to different web applications and other fields. Our system utilizes 2 database servers storing the encrypted passwords, an application server which is responsible to provide different services between the database server and the client. Providing multi-server database gives us a higher level of security against brute force attacks. Even if one of the servers is compromised the intruder does not get the access to the user credentials.

II. RELATED WORK

A. Diffie-Hellman Algorithm [1, **2, 3, 4, 7, 8, 9, 10, 13, 14***]:*
In 1976, Whitfield Diffie& Martin Hellman invented Diffie-Hellman Algorithm [1**, 2, 3, 4, 7, 8, 9, 10, 13, 14**] which was published in "New Direction in Cryptography". This Algorithm is widely used by various protocols such as:

- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
- Secure Shell (SSH)
- Internet Protocol Security (IPSec)
- Public Key Infrastructure (PKI)

This Diffie Hellman Algorithm (DHA) [1, 2, 3, 4, 7, 8, 9, 10, 13, 14] permits two users to exchange a symmetric secret key through an insecure communication medium (wired or wireless channel) and without hiding any prior secrets. In DHA, two parties create a symmetric session key to exchange data without storing the key to use in future [1].
The idea of public key cryptography was born as a result of two major challenges. The first of these was the problem of key distribution: if two people who have never met before are to communicate using digital systems as a medium, using conventional cryptography would mean that they must somehow agree on a common key that will be known to themselves and no one else. The other problem was the issue of signatures: this is a method of providing the recipient of a purely digital electronic message with a way of demonstrating to other people that it had come from a particular person, serving as a signature comparable to a written one on a letter [2]. The DHA basically uses idea when two users who don't know each other want to create a secure connection between them. DHA key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming [3]. And, when two users need a symmetric key to communicate. They both require to choose two numbers, first number is a large prime no., and the second number is a random number. The numbers chosen need not be confidential. These numbers can be sent through the Network; & they can be public. Modifying the security of DHA means improving the security of the protocols that use DHA. Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection. User A generates a private key X_A, calculate Y_A, and send this to user B. User B sends the acknowledged by generating a private value X_B calculating Y_B, and sending Y_B to user A. Both users can then calculate the key. The public values q and α ahead of time would need to be known. Alternatively, user A could pick values for q and α and include those in the first message[3]. DHA is illustrated in Figure 1.

ISSN: 2278 – 7798

B. Elgamal Algorithm [5, 6, 7, 8, 9, 10, 11, 12]:

Elgamal is an asymmetric key algorithm developed by Taher Elgamal in the year 1984. It is based on Diffie Hellman key exchange algorithm [1, 2, 3, 7, 8, 9, 10] and works over finite fields. Taher Elgamal first described the Elgamal Cryptosystem in an article published in the proceedings of the CRYPTO '84, a conference on the advances of cryptology. The proposed algorithm belongs to the family of public key cryptographic algorithms[6]. The Elgamal algorithm is a public-key cryptosystem based on the discrete logarithm problem. It consists of both the encryption and signature algorithms. A fundamental aspect of this system is that the knowledge of the private part makes the decryption easy. If the private key is unknown, it is virtually impossible to decrypt the message in acceptable time [5]. Elgamal encryption [6, 7, 8, 9, 10] consists of three components: the key generator, the encryption algorithm, and the decryption algorithm. [5]Key Generation: The basic requirement for a cryptographic system is at least one key for symmetric algorithms and two keys for asymmetric algorithms. With Elgamal, only the receiver needs to create a key in advance and publish it.

III. RESULTS

When two sides exchange a secret value than result will be as follows. Here X_A and X_B are private, hence they have only following ingredients to work with: q, a, Y_A, and Y_B. Thus, the adversary is forced to take a discrete logarithm to determine the key. For example, to determine the private key of user B, an adversary must compute X_B = d log a, q (Y_B). The adversary can then calculate the key K in the same manner as user B calculates it. The security of the Diffie-Hellman key exchange [1, 2, 3, 7, 8, 9, 10, 13, 14] lies in the fact that, while it is relatively easy to calculate exponentials modulo q prime, it is very difficult to calculate discrete logarithms.

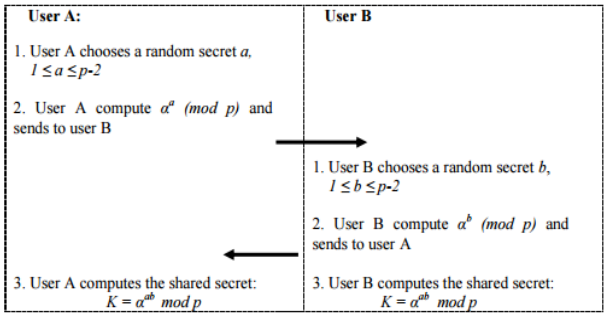

Fig 1: Demonstration of DHA [4]

This presents the following limitations:
1. There is no identity of the parties involved in the exchange.
2. It is easily susceptible to man-in-the-middle attacks. A third party C, can exchange keys with both A and B, and can listen to the communication between A and B.
3. The algorithm is computationally intensive. Each multiplication varies as the square of n, which must be very large. The number of multiplications required by the exponentiation increases with increasing values of the exponent, x or y in this case.
4. The computational nature of the algorithm could be used in a denial-of-service attack very easily.
5. The algorithm cannot be used to encrypt messages.

IV. PROPOSED WORK

Password-authenticated key exchange is where a client and a server, who share a password, authenticate eachother and meanwhile establish a cryptographic key by exchange of messages. Current solutions for two-server PAKE are either symmetric in the sense that two peer servers equally contribute to the authentication or asymmetric in the sense that one server authenticates the client with the help of another server. We are going to present a symmetric solution for two-server PAKE, where the client can establish different cryptographic keys with the two servers, respectively [8].

V. SYSTEM ARCHITECHTURE

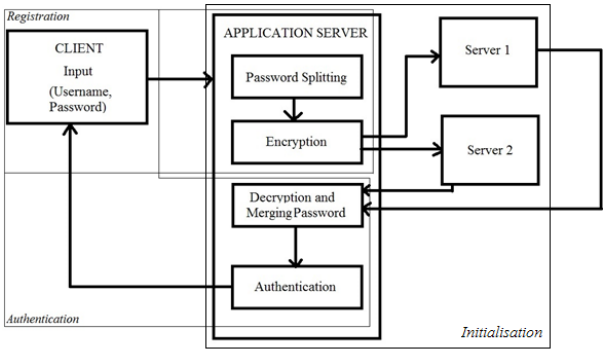

Fig 2: System Architecture

As shown in the above figure, our system comprises of a client machine, an application server which is responsible for the Diffie-Hellman[1, 2, 3, 4, 7, 8, 9,10, 13, 14] and the Elgamal protocols and 2 database servers which are responsible for storing the usernames and the respective encrypted passwords.(Note : Unencrypted passwords are not stored.) Our system is based on 3 different stages:

1. **Initialization.**
2. **Registration.**
3. **Authentication**.

In the initialization phase the 2 database servers interact with the application server to exchange keys and authenticate themselves for further communication.In the Registration phase the client enters his/hers data to register with the authentication system. Here the password to be saved by the user is taken and is spliced into 2 halves (as no. of database servers = 2) by the application server, then these 2 halves are encrypted using the elgamal encryption scheme and then stored into the 2 database servers. In the authentication phase the user enters the username and the password to login to the system, the application system then gets the decrypted halves form the respective database servers which are then merged together and compared with the password entered by the user at the time of authentication.

A. Diffie-Hellman Algorithm [1, 2, 3, 4, 7, 8, 9, 10, 13, 14*]:*

ISSN: 2278 – 7798

The application server chooses a prime number p, a base number g and a secret number s is randomly selected, then application server ar result is calculated using the function (g^s mod p). A similar process takes place at the server 1 and the server 1 result sr1 is calculated. These 2 results are then exchanged and then secret key application server ska is calculated as (sr1^s mod p) and secret key server1 sks1 is calculated as (ar^s1 mod p1) where s1 is the secret number at server1 and p1 is the prime number at server 1.Now ska and sks1 are compared, if these are equal diffie-hellman algorithm [1, 2, 3, 4, 7, 8, 9, 10] was successful. Similar process is carried out between the application server and server 2.

B. ElGamal Algorithm [5, 6, 7, 8, 9, 10, 11, 12, 13, 14]:

First the server1 creates a public and a private key. It chooses a prime number p, a base number g and a random integer a is selected, after this (g^a mod p) is computed (p, g, g^a) as the public key which is given to the application server for the encryption and the private key. During the encryption procedure the password entered by the user is converted into numeric form m and a random number k is chosen, after this y is computed as (g^k mod p) and o is computed as (m*(g^a) ^k) and the cipher text c = (y, o) is sent to server1 for storing. At the decryption phase server1 computes q as (y^(p-1-a) mod p) and password m is recovered by computing (q*o mod p).this password is then sent to the application server for authentication purposes.

Similar process happens between the application server and server2 during different stages of the system.

VI. SNAPSHOTS:

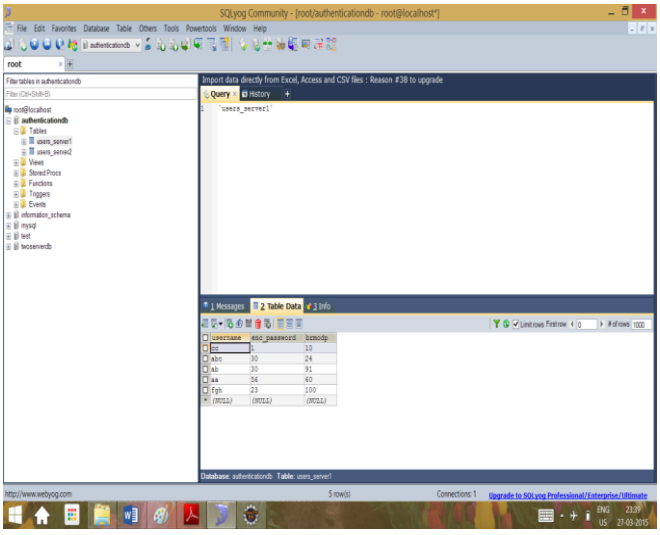

Fig 3: Database 1

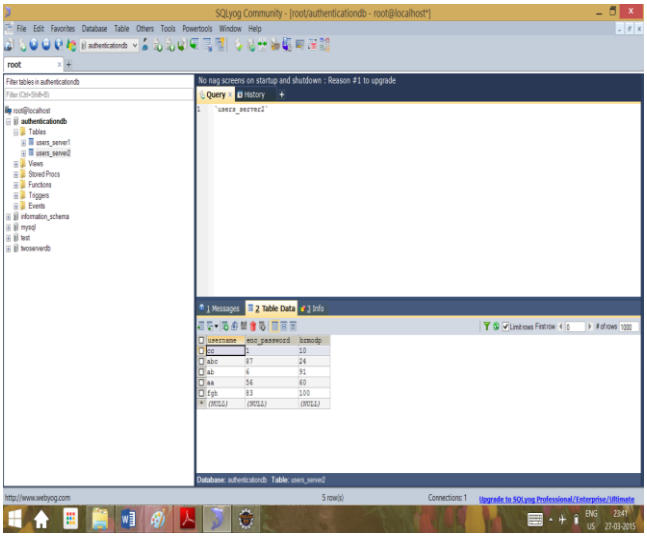

Fig 4: Database 2

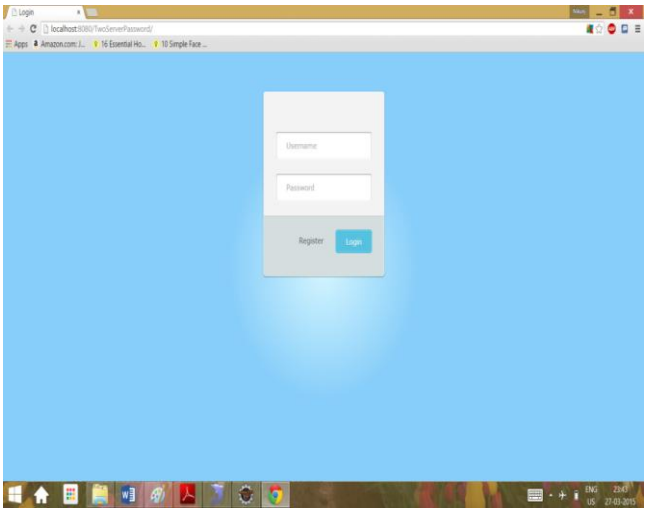

Fig 5: UI 1

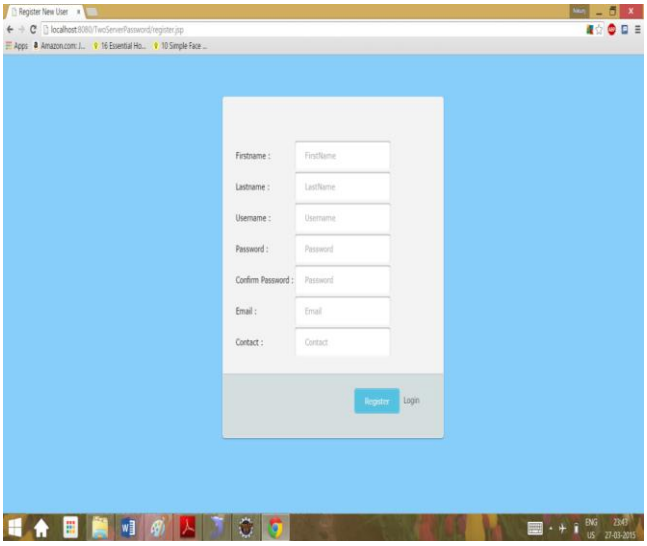

Fig 6: UI 2

ISSN: 2278 – 7798

VII. CONCLUSION

This system eliminated the risk of passwords being disclosed by introducing two servers. This has overcome the drawback of single server. Thus, the system is as efficient as a single server in terms of processing time. Elgamal algorithm used both public and private key, hence, it is asymmetric encryption algorithm. The algorithm gives a different cipher text each time encryption is performed. Our protocol is efficient in terms of computation complexity and communication rounds. We are providing better security by introducing the concept of One-Time-Password in a two-server system. This work can be extended by introducing multiple servers but caution should be taken for the increase in communication rounds, in a multi-server system.

VIII. ACKNOWLEDGEMENT

We would like to take this opportunity to express our profound gratitude and deep regard to Professor Suja.S.Panicker for her exemplary guidance and valuable feedback.

IX. REFERENCES

[1] Preeti, Bandana Sharma "Review Paper on Security in Diffie-Hellman Algorithm", Volume 4, Issue 3, March 2014.

[2] Rohini, Er.Meenakshi Sharma "Enhancing the Diffie-Hellman Algorithm", Volume 4, Issue 6, June 2014.

[3] K.Suganya, K.Ramya "Performance study on Diffie Hellman Key Exchange Algorithm", Vol 2, Issue III, March 2014.

[4] Malek Jakob Kakish "Security Improvements To The Diffie-Hellman Schemes", July 2011, Volume 8, Issue 1.

[5] Ankush Sharma, Jyoti Attri, Aarti Devi , Pratibha Sharma "Implementation & Analysis of RSA & ElGamal Algorithm".

[6] AnnapoornaShetty , Shravya Shetty K , Krithika K "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm ", Vol.2, Special Issue 5, October 2014.

[7] Xun Yi, San Ling, and Huaxiong Wang, "Efficient Two-Server Password-Only Authenticated Key Exchange", IEEE

[8] "Password Based Two Server Authentication System", Journal of Theoretical and Applied Information Technology 15 May 2012. Vol. 39 No.2

[9] Jonathan Katz, Philip MacKenziey, GelarehTabanz amd Virgil Gligorx,"Two-Server Password-Only Authenticated Key Exchange"

[10] M. Abdalla and D. Pointcheval, "Simple Password-Based Encrypted Key Exchange Protocols," Proc. Int'l Conf. Topics in Cryptology (CT-RSA), pp. 191-208, 2005.

[11] S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password- Based Protocol Secure against Dictionary Attack," Proc. IEEE Symp. Research in Security and Privacy, pp. 72-84, 1992.

[12] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. (Crypto '01), pp. 213-229, 2001. [6] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," SIAM J. Computing, vol. 32, no. 3, pp. 586-615, 2003.

[13] D. Boneh, "The Decisional Diffie-Hellman Problem," Proc. Third Int'l Algorithmic Number Theory Symp. pp. 241-250, 1998.

[14] V. Boyko, P. Mackenzie, and S. Patel, "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman," Proc. 19th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt '00), pp. 156-171, 2000.

ISSN: 2278 – 7798