IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

A Defended and Adequate Mutual Verification with Key Concession Architecture in Wireless Network

N. Praveen Kumar

Asst. Prof, CSE, Dadi Institute of Engineering and Technology, Visakhapatnam, India

Abstract: Now a day's mobile networks are rapid development by performing the e-commerce transaction such as online shopping, internet banking and e- payment. So that to provide secure communication, authentication and key agreement is important issue in the mobile networks. Hence, schemes for authentication and key agreement have been studied widely. So that to provide efficient and more secure techniques is necessary. In this paper we are proposed random prime order key agreement protocol proposed for authentication and key agreement. Another technique is used to provide security of transferred data using key x or data transpose technique. By using this technique we provide more security and more efficiency for transferring data.

Keywords: Mutual Authentication Security cryptography Key Aggrement.

I. INTRODUCTION

In a wireless environment using mobile device we can sharing of information can be improved by day by day. So that using mobile device we can perform the online shopping, internet bankingand e- payment. So that by performing those functionalities we can provide secure communication between clients and remote server. By performing secure communication between the client and remote server we can implement the concepts for mutual authentication clients and remote server, key agreement for both. So that by implementing both schemas we studied widely. However in a wireless network does not contain any physical device i.e. wire for provide security of wireless network. So that by providesecure communication of mobile device werequired an efficient schema for secures transformation of data.

By implementing efficient and secure communication in a wireless network each client is required in order to provide flexible and robustness of online transaction. The authentication of the server and the client both are equally important when a client wants to acquire various services from the remote server to protect server's spoofing attack and impersonation attack from the outsiders. Some of schemas also proposed to perform remote mutual authentication of client and remote server. But those techniques are not sufficient for satisfying functionalities of online transaction. So that by implementing session key agreement procedure can satisfy exchange the confidential information in open wireless network. The main contribution this paper is that design of secure and efficient mutual authentication and key agreement schema in client and server environment.

In order provide secure communication of client and server we need build strong mutual authentication and key agreement schema. So that by provide security of transferring information in online we need to implement the cryptography techniques. Now a day's so many cryptography techniques are available in the world. Some of those are contains draw back and also face problem of performance issue. In this paper we are implementing one of cryptography technique for provide securityof transferring information. By implementing this concept it will more efficient and also give more security of transferring information. Before performing encryption and decryption of datathe client andserver will perform the key agreement procedure for generation of shared key. After generating shared key the server will perform the encryption of transferring data and client will perform the decryption process by using that shared key.

The remaining of this paper is organized as follows. Section 2 is to describe the related work. Section 3 is to specify the existing system. Section 4 is to specify the implementation procedure of our propose system. Section 5 is to specify experiment result of our proposed system. Section 6 is to describe the conclusion.

II. RELATED WORK

Recently, several ID-based client authentication schemes [1, 2-4, 5- 8] have been found in literature. However, these are vulnerable to various attacks such as replay attack [6, 7], privileged-insider attack [10], impersonation attack, lost/stolen smartcard attack [11, 12], known session-specific temporary information attack [13], and many logged-in users' attack. In addition, some of these schemes are faces from the problem of users' anonymity, perfect forward security and clock synchronization, Debiao et al. [11] proposed an ID-based client authentication with key agreement scheme on ECC for mobile client-server environments. They claimed that their scheme provides remote mutual authentication and session key agreement with low computation cost and is secure against various attacks.

However, [13] showed that Debiao's scheme cannot withstand the clock synchronization problem, many

logged-in users' attack, known session-specific temporary information attack, impersonation attack, privilege-insider attack, incapable to provide users' anonymity and no provision for changing/updating the leaked private key.

Thus, aforementioned problems inspired us to design an efficient and secure ID-based client authentication with key agreement scheme for mobile client-server environments. By implementing wireless network we can provide less power computation and less memory resources. Yang and chang [14] 10 of impersonation attack and does not provide perfect forward secrecy. Yoon and yoo [15] is proposed concepts of robust key agreement protocol for sharing information inwireless network. This schema also faces the problem of forward secrecy of transferrin information. Later so many mutual authentication schemas are available in the networks. But some of those attacks also face the problem of some of the attack. By implementing bilinear pairing on elliptic curve schema [15,16] is to take the time consuming process for implementation process.

III. EXISTING SYSTEM

During secure communication, authentication should be performed to protect users and a secret session key should be established for confidentiality. As the development of cryptography, schemes for authentication and key agreement develop accordingly. Early schemes are based on passwords. The first password authentication scheme to authenticate a remote user over an insecure channel was proposed by Lamport. Introducing public key cryptography into cryptography, Diffie and Hellman proposed the first key agreement scheme. Many authentication and key agreement schemes based on traditional public key cryptography were constructed. Since Diffie and Hellman's scheme lacks authentication and it is vulnerable to Man-in-the middle attack, then authentication with key agreement is necessary and attractive in practical implementation. Despite the vulnerability and laciness' of authentication, Diffie and Hellman's key agreement scheme is the foundation for other schemes and most of key agreement schemes use Diffie and Hellman's technique. Since the introduction of identity based cryptography by Shamir, many identity-base cryptosystems were presented in application. It is not until Boneh and Franklin proposed an identity-base encryption scheme with bilinear pairings on elliptic curves that identity-base cryptography develops rapidly. Various identity-based authentication and key agreement schemes are constructed and made into application. Some authentication schemes can be found in .However, these schemes do not provide mutual authentication and key exchange between the client and the server, which is required in mobile client-server environment.

IV. PROPOSED SYSTEM

The proposed system contains mainly two concepts for the authentication, key agreement and security of transferring data. By implementing those concepts we can perform mutual authentication of users and key agreement in both users. After completion of key agreement the sender will encrypt the transferred message using key xor data transpose technique. After encrypting the sender will send the cipher message to receiver. The receiver will receive the cipher message and decrypt the cipher message we get the plain text message. The process of mutual authentication and key agreement as follows.

Random prime order key agreement protocol:

1. The sender will generate private key randomly.
2. Calculate public key using this formula pub=g private % P.
3. After calculating public key the sender randomly choose SR and SV values.
4. Calculate Sa value by performing following steps.

i. C=(message.hashCode)%200000;
ii. C=C%200000;
iii. C3=C-(privatekey*SR);
iv. Sk=Gcd(C3)
v. Int k1=Inverse(sk,p-1);
vi. V=c3*k1;
vii. Sa=V%P;

5. Calculate SA by performing following steps.

SA = for(inti=1;i<=Sa;i++)
i. temp=(temp*SR)%P;

6. Send public key,SR and SA to Receiver.
7. The receiver also perform the step 1 to 5.
8. After that we can calculate RB value using following steps.

RB = for(inti=1;i<=VB;i++)
temp=(temp*SR)%P;

9. The Receiver will send RB value to Sender.
10. The sender will receive the RB value and calculate SA1 and acknowledgment.
11. After calculating the sender will send to receiver.
12. The receiver will retrieve the both values and perform the authentication status.
13. After that the sender will generate key by using following equation.

Key= for(inti=1;i<=RV;i++)
temp=(temp*RB)%P;

14. The receiver will generate key by using following equation.

Key= for(inti=1;i<=CA1;i++)
temp=(temp*RB)%P;

After generating shared key the sender will perform the encryption process as follows.
Key xor data transpose technique :

I) Encryption process:

1. The transferring message can be converted into 32 X 32 matrix format.
2. After generating matrix format we transpose into rows and columns.
3. After transpose matrix that data can be converted into Ascii values.
4. The transpose data and key can be xor again convert into binary format.
5. After that binary data can be converted into ascii format and that data can be sended to receiver.

DOI 10.17148/IJARCCE.2016.5237

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

II) Decryption Process:

The receiver will retrieve cipher format data and performing following steps.

1. The receiver will retrieve cipher format data and generate matrix format using that data.
2. After convert matrix format we can reverse those ascii values and again form matrix format.
3. Taken the ascii format data and xor with key get the xor valued data.
4. Take the xor value and convert into character.

V. EXPERIMENTATION AND RESULTS

In this section we can describe experiment result of our proposed system. The implementation of our proposed system can done by using java language

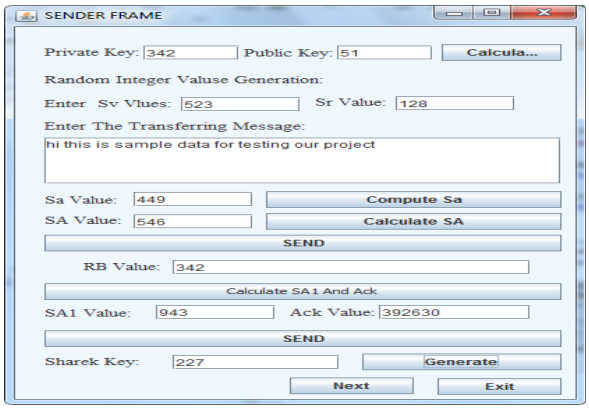

Figure 1

The above diagram specifies generation of shared key. In this screen the sender will generate shared value and acknowledgment by using specified by proposed system. After generating those values the sender will sent to verifier. The verifier will perform the verification process we can get shared key.

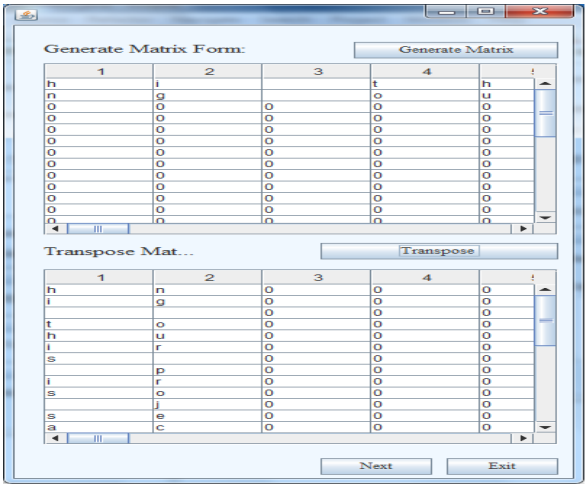

Figure 2

The above diagram specifies generation matrix format data. In this screen the sender will get transferring message and generate matrix format. After generating matrix format the sender will transpose that matrix and again form the transpose matrix

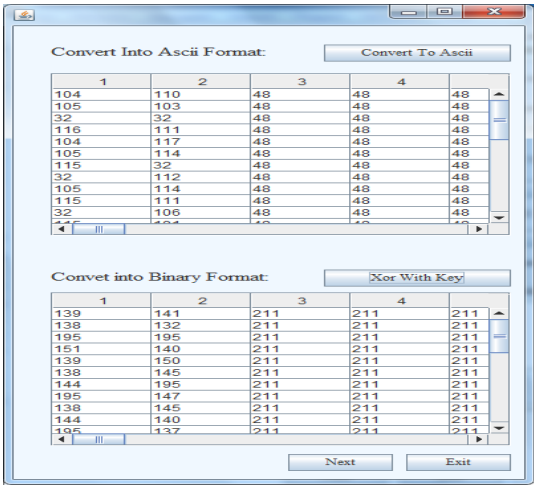

Figure 3

The above diagram specifies converting transpose matrix into ascii formatted data. The sender will retrieve the transpose matrix and convert into those characters into ascii values. After converting we can xor with shared key.

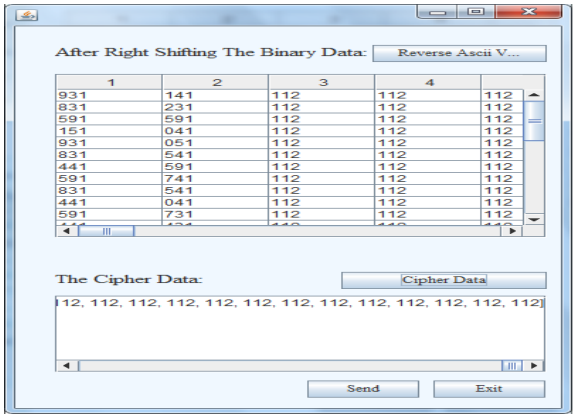

Figure 4

The above diagram specifies generation of cipher format data. The sender will retrieve the xor values and reverse those values. After that those values sent to verifier.

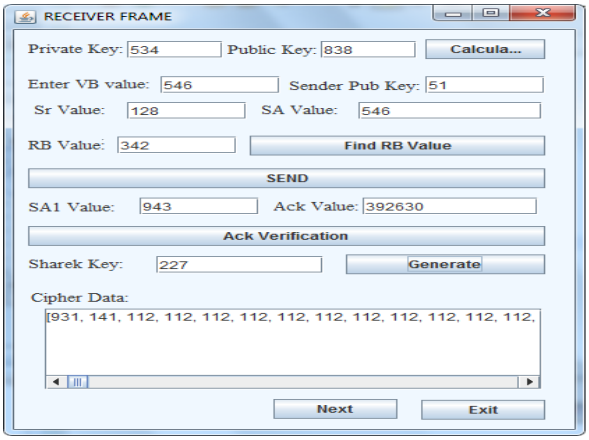

Figure 5

The above diagram specifies the generation of shared key and retrieves the cipher data. The verifier will retrieve the shared value andacknowledgement verifies the

DOI 10.17148/IJARCCE.2016.5237

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

authentication status. After that the verifier will generate shared key and also retrieve the cipher format data.

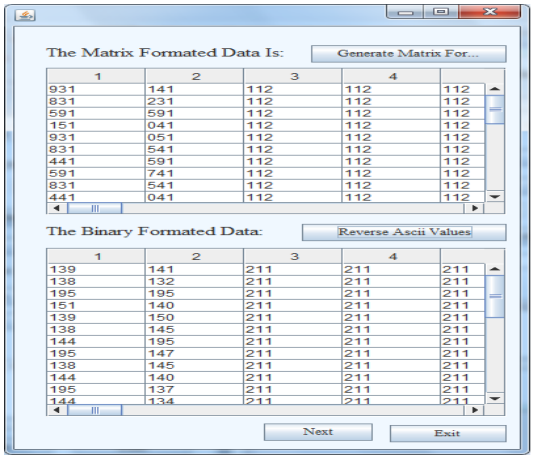

Figure 6

The above diagram specifies generation ascii formatted matrix and reverse those ascii values. The verifier will retrieve the cipher data and generate matrix format. After that those ascii values can be reversed and again generate matrix format.

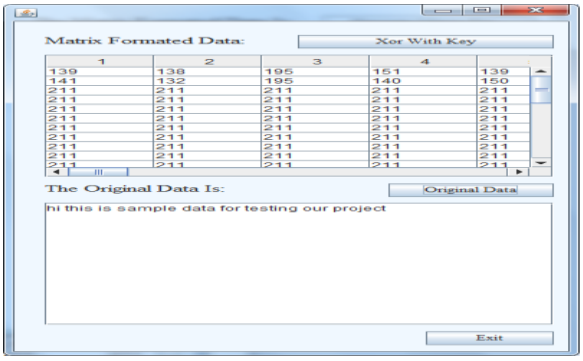

Figure 7

The above diagram specifies the ascii values xor with key and get original plain format data. The verifier will retrieve the reverse ascii values and xor the with key. After that those values can be converted into character, we can get original plain format data.

VI. CONCLUSION

This paper proposes random prime order key protocol and key x or data transpose technique for mobile client server environment. Compared with known our scheme is more efficient and good properties against for various types of attacks. This paper also provides more security of transferring data. So that by implementing those techniques we can improve efficiency given project and also provide more security for transferring data.

REFERENCES

[1] J.H. Yang, C.C. Chang: An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Computers & Security 28, 2011, 138-143.

[2]. E. Yoon, K. Yoo: Robust ID-based remote mutual authentication with key agreement protocol for mobile devices on ECC, In: Proceedings of the International Conference on Computational Science and Engineering, Vancouver, Canada, 2009, pp. 633-640.

[3] T.H. Chen, Y.C. Chen, W.K. Shih: An Advanced ECC ID-Based remote mutual authentication scheme for mobile devices, In: Proceedings of the Symposia and Workshops on Ubiquitous, Autonomic and TrustedComputing, Xian, Shaanxi, China, 2010, pp. 116- 120.

[4]. S.H. Islam, G.P. Biswas: A more efficient and secure ID-based remote mutual authenticationwith key agreement scheme for mobile devices on elliptic curvecryptosystem, The Journal of Systems and Software 84, 2011, 1892-1898.

[5] M.L. Das, A. Saxena, V. P. Gulati: A dynamic ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics 50, 2004, 629-631

[6]. J.S. Chou, Y. Chen, J.Y. Lin: Improvement of Das et al.'s remote user authentication scheme, .

[7]. J.H. Yang, C.C. Chang: An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Computers & Security 28, 2011, 138-143.

[8]. S.H. Islam, G.P. Biswas: A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, The Journal of Systems and Software 84, 2011, 1892-1898.

[9]. T. Goriparthi, M.L. Das, A. Saxena: An improved bilinear pairing based remote user authentication scheme, Computer Standards & Interfaces 31, 2009, 181-185.

[10]. H. Debiao, C. Jianhua, H. Jin: An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security, Information Fusion, 2011, .

[11] Y.Y. Wang, J.Y. Kiu, F.X. Xiao, J. Dan: A more efficient and secure dynamic ID-based remote user