Password Based Client-Server-User Authenticated Key Agreement Mechanism for Cloud System

Arif Mohammad Abdul, Sudarson Jena, Balraju M

Abstract: ***The authentication is an essential concern in the cloud environment to restrict the unauthorized users to retrieve the files from cloud server. Moreover, authentication mechanisms are used to prevent illegal access of resources over insecure channel. Thus proposed work provides the strong and efficient authentication process in cloud computing environment by chebyshev polynomial based chaotic maps Diffie Hellman property. The proposed authentication mechanism does not disclose the identity of the user to CSP. Moreover proposed authentication mechanism enables mutual authentication, Identity management, and session-key agreement. The Proposed mechanism of security analysis includes the enabling mutual authentication and key agreement, restricting the impersonation attack, man in the middle attack and replay attack.***

Keywords : Cloud, authentication, session key and attacks

I. INTRODUCTION

Nowadays, cloud becomes an essential technology for upcoming organizations and users that provide various services on demand in a flexible and elastic way without owned the resources. Any person can access the cloud from any point, which leads to the privacy issue. To overcome the confidentiality problem users encrypt the outsourced files but threats are continuously showing interest on others data, there is a need of trusted authentication mechanism which halts the illegal or unauthorized users into the cloud. Earlier, remote authentication mechanism proposed by Lamport [1], this scheme based on verifier table which compromises with stolen verifier attack also difficult to maintain a dictionary table on a remote system. Das et al.[2] proposed a system which does not require maintaining a verifier table, this scheme generate dynamic remote password which resist replay, stolen verifier, insider and guessing attack. Awasthi and Lal [3] points Das et al. work is unsafe against impersonate attack. To overcome the issue of impersonate attack Liou et al.[4] proposed a dynamic identification remote authentication method but Shih [5] proved their scheme fail to gain mutual authentication, Again sood et al.[6] demonstrate and proved that Liou et al.[4] scheme susceptible. Jung gil cho et al.[7] proved that Sood et al[6] proposed method is compromised to database attack.

Kumari et al. [8] points Chang et al.[9] method that compromise to user impersonates, insider and password guessing attack. Moreover, kumar et al. shows the flaws in changing the password phase that fails in session key agreement for communications. Later, they come up with another enhanced key agreement authentication technique and claimed that their mechanism is efficient and trusted.

Recently, Kaul Awasthi et al. [10] demonstrated the Kumari et al.[8] method is threatened, intruder can acquire mutual session key for furthered communication and also obtain the secure key of the user-server. Qi-Chen et al.[11] proposed key exchange authentication between sender and receiver method for wireless network but fail to achieve authentication when user is in offline and also fail to gain user anonymity , local password verification.

The aim of the paper is to design the end to end authenticate key agreement protocol for cloud environment, and it explained in the following section.

II. PASSWORD BASED AUTHENTICATED KEY AGREEMENT

We consider the system with three entities such as client, user and Cloud server. Client consists of n number of files and wants to securely store inside the cloud server. They are $'n'$ number of users, and wishes to view and download the data from the cloud server. The server must give the access to only valid users. In order to get secure communication between these three entities they must be authenticate one another in a following ways:

1. The client must uploads the files to valid cloud server i.e., mutual authentication must be done between client and cloud server
2. The cloud server must give the access to the valid users i.e., mutual authentication must be done between cloud server and users

In order to achieve the goal paper proposes a password-based authentication and key agreement mechanism for cloud architecture consist of client-server-user entities. The authentication and key settlement is computed by the "Discrete Logarithmic problem" property of Chebyshev polynomial based Chaotic Maps.

Any entity participating in communication in this environment must contains the user identity (ID_i) and also it select the one private key K_i and compute the public

Revised Manuscript Received on July 22, 2019.

***** Correspondence Author

Arif Mohammad Abdul*, Computer Science & Engineering, Jawaharlal Nehru technological University, Hyderabad, India. Assistant Professor, GITAM Deemed to be University, Hyderabad India. arif.software@gmail.com

Sudarson Jena Computer Science Engineering & Applications, Sambalpur University Institute of Information & Technology, Burla Sambalpur, Orissa, INDIA.

Balraju M, Computer Science & Engineering, Jawaharlal Nehru Technological University Hyderabad, Swami Vivekananda Institute of Technology, Secunderabad, INDIA

information $\left(x,\ T_{K_i}(x)\right)$, using the below equation of Chebyshev polynomial.

$$T_n(x) = 2x * T_{n-1}(x) - T_{n-2}(x) * (\text{mod } N) \quad \ldots\ldots\ldots\ldots (3), \quad n \geq 2$$

During registration phase all the communicating entities must agree on the value of x, the password and hash function through secure channel.

The authentication is an essential concern of the cloud computing architecture to restrict the unauthorized users to retrieve the files from CSP. Thus proposed work provides the strong and efficient authentication process in cloud computing environment by chebyshev polynomial based chaotic maps Diffie Hellman property. The proposed authentication mechanism does not disclose the identity of the user to CSP. Moreover proposed authentication mechanism enables Identity management, mutual authentication and session-key agreement. The proposed mechanism is based on following assumptions:

1. All the users need to be agree on the key during the registration phase by assuming that the all the users and CSP are honest.
2. The user needs to be verify itself with CSP during the login phase by mutual authentication to retrieve the files
3. It is assumed that the after registration phase CSP and user are trusted mutually each other.

A. *Mutual authentication between User-Client-Cloud service provider*

Whenever user want to access the files form the CSP, he must authenticated itself with the CSP with the help of client. The authentication process is explained as follows:

1. All the three parties must be agree on the hash function and password agreed between them and the value of $'x'$
2. Client select a large prime number K_{cl} and computes the value of public information chaotic maps based Diffie Hellman problem as $\left(x, T_{K_{cl}}(x)\right)$, and this value is public.
3. Then client and CSP agree on a long secrete key as follows

a. CSP select a large prime number k_c and compute the value of $\left(x, T_{k_c}(x)\right)$

b. CSP sends the value of $T_{k_c}(x)$ to client, and at the same time Client sends the value of $T_{K_{cl}}(x)$ to the CSP

c. Now both compute the long secrete key as follows
$x_{c,cl} = T_{k_c}(T_{K_{cl}}(x)) = T_{k_{cl}}(T_{K_c}(x))$

4. Whenever user want to access the data, he select the large prime number K_u and computes the value of $T_{k_u}(x)$ and then compute the value of $T_{k_u}(T_{K_{cl}}(x))$ and sends the value to the CSP in the following format
$M_{U-csp} = \{T_{k_u}(x), ID_u, ID_c, H_u\}$, where
$H_u = \left(ID_u \,||\, ID_c \,||\, T_{k_u}(x) \,||\, pw_u\right)$
5. CSP, after receiving the message $\left(M_{U-csp}\right)$ from the user it computes the value of $x_{cs,u}$ as follows
$x_{cs,u} = T_{k_{cs}}(T_{K_u}(x))$

   And then construct the message
$M_{csp-cl} = \{M_{U-csp}, T_{k_{cs}}(x), ID_{cs'}, H_{cs}\}$, where
$H_{cs} = H\left(ID_u \,||\, ID_{cs} \,||\, T_{K_{cs}}(x) \,||\, x_{c,cl}\right)$
Then CSP sends the M_{csp-cl} message to Client
6. Client, After getting the information from the CSP, Client construct the M_{cl-csp} as follows:
$x_{cl,\ u} = T_{k_{cl}}(T_{K_u}(x))$

   $x_{cl,\ csp} = T_{k_{cl}}(T_{K_{cs}}(x))$

   It validate the two hash values with the help of $x_{c,cl}$ and password
H_{cs} is validated with the help of $x_{c,cl}$ and
H_u is validated with the help of password
Then it construct the two hash values and message M_{cl-csp} as follows
$H_{cs} = H\left(T_{K_u}(x) \,||\, x_{c,cl}\right)$
$H_{cs} = H\left(T_{K_{cs}}(x) \,||\, pw_u\right)$
$M_{cl-csp} = \{ID_{cl}, H_{cs}, H_{cs}\}$
It sends the M_{cl-csp} value to CSP
7. CSP, After getting the information from the client, CSP construct the M_{csp-u} as follows:

   It calculates the value of $H\left(T_{K_u}(x) \,||\, x_{c,cl}\right)$ and validate the H_{cs}
Then CSP computes the session key
$Session\ Key = T_{k_{cs}}(T_{K_u}(x))$
And computes the hash value
$H_{cu} = H(session\ key \,||\, ID_{cs} \,||\, ID_u \,||\, H_{cs})$
And construct the message
$M_{csp-u} = \{ID_{cs}, H_{cu}, H_{cs}\}$
8. User, After getting the information from the CSP, validate the information and compute the session key
It computes the value of $T_{K_{cs}}(x) \,||\, pw_u$ and validate the H_{cs}
And compute the session key

   $Session\ Key = T_{k_u}(T_{K_{cs}}(x))$
And then compute $H(session\ key \,||\, ID_{cs} \,||\, ID_u \,||\, H_{cs})$ and validate the H_{cu}.

Thus the proposed mechanism authenticate the user, who wants to access the files from the cloud server, and also enable the secure communication among them by assigning the session key between them.

III. PERFORMANCE ANALYSIS

Proposed algorithm performance is evaluated with respect to the computational overhead and the security, and it is explained as follows:

A. *Computational Overhead analysis*

Computational overhead of the discreet logarithmic problem of chaotic maps based chebyshev polynomial is evaluated with processor Intel-core I5, 8 GB RAM and one TB hard disk and compared it with the modular arithmetic of RSA and scalar multiplication of ECC computational overhead in an identical environment. During performance paper considered the different prime numbers up to maximum size of 1024 bits for time complexity computation of each key agreement algorithm. The results are clearly indicated that the time complexity of chaotic maps computation is less compared to the ECC and RSA. We analyses the time complexity, as it is negatively impact on other network performance metrics in terms of end to end delay, consumption of energy and memory. As we designed the authenticated key agreement protocol based on chaotic MAPS discreet logarithmic property, thus the proposed mechanism less overhead in comparison with RSA & ECC, as it is free from modular exponential computation and scalar multiplication on an elliptic-curve, it is shown in figure 1. Session key computed on reactive manner and no clue is stored inside the network, thus the proposed mechanism resist from modification and stolen verification attacks.

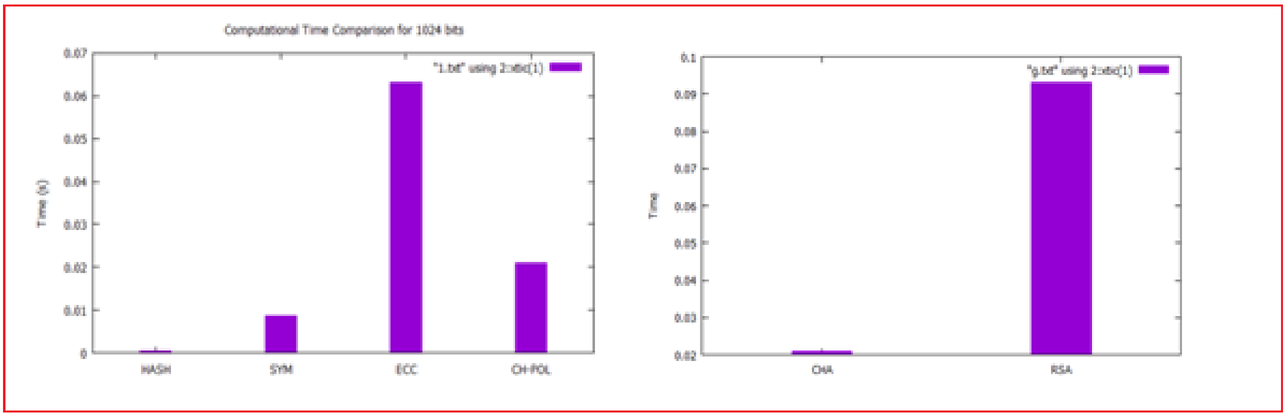

Figure 1:- Time complexity comparison of RSA, ECC and Chaotic Maps

B. *Security Analysis*

The security analysis of proposed mechanism includes the enabling mutual authentication, and key agreement, restricting the impersonation-attack, man-in-the-middle attack and replay-attack. The work achieved the mutual authentication, and key agreement based on the property of Chaotic Maps Based Diffie-Hellman problem and Discrete-Logarithm problem, these properties cannot be disclosed by an opponent in the polynomial time. Consider the opponent consist of entire command to launch misbehaving activities through insecure medium. However, opponent cannot catch the information to calculate the session keys.

IV. CONCLUSION

Authentication mechanisms are used to prevent illegal access of resources over insecure channel in any network environment. Moreover, the authentication is one of the major aspects of the cloud computing architecture to restrict the unauthorized users to retrieve the files from cloud server. The paper design a strong and efficient authentication process in cloud computing environment by Chebyshev polynomial based chaotic maps Diffie Hellman property. The proposed authentication mechanism does not disclose the identity of the user to CSP. Moreover proposed authentication mechanism enables Identity management, mutual authentication, and session-key agreement. The security analysis of proposed mechanism includes the enabling mutual authentication and key agreement, restricting the impersonation, man-in-the-middle, and replay attacks.

REFERENCES

1. Lamport, Leslie. "Password authentication with insecure communication." Communications of the ACM 24.11 (1981): 770-772.
2. Das, Manik Lal, Ashutosh Saxena, and Ved P. Gulati. "A dynamic ID-based remote user authentication scheme." IEEE Transactions on Consumer Electronics 50.2 (2004): 629-631.
3. Awasthi, Amit K. "Comment on a dynamic ID-based remote user authentication scheme." arXiv preprint cs/0410011 (2004).
4. Liou, Y. P., J. Lin, and S. S. Wang. "A new dynamic id-based remote user authentication scheme using smart cards." Proc. of 16th Information Security Conference. 2006.
5. Shih, Hsi-Chang. "Cryptanalysis on two password authentication schemes." Laboratory of cryptography and information security, National Central University, Taiwan (2008).
6. Sood, Sandeep K., Anil K. Sarje, and Kuldip Singh. "An improvement of Liou et al.'s authentication scheme using smart cards." International Journal of Computer Applications 1.8 (2010): 16-23.
7. Shin, Kwang Cheul, and Jung Gil Cho. "An Improvement of Sood, et al.'s Authentication Scheme using Smart Card." International Journal of Security and Its Applications 7.3 (2013): 271-282.
8. Kumari, Saru, Muhammad Khurram Khan, and Xiong Li. "An improved remote user authentication scheme with key agreement." Computers & Electrical Engineering 40.6 (2014): 1997-2012.
9. Chang, Ya-Fen, Wei-Liang Tai, and Hung-Chin Chang. "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update." International Journal of Communication Systems 27.11 (2014): 3430-3440.
10. Kaul, Sonam Devgan, and Amit K. Awasthi. "Security enhancement of an improved remote user authentication scheme with key agreement." Wireless Personal Communications 89.2 (2016): 621-637.
11. Qi, Mingping, and Jianhua Chen. "An efficient two-party authentication key exchange protocol for mobile environment." International Journal of Communication Systems 30.16 (2017): e3341.