IIOAB JOURNAL

ARTICLE

ENHANCING PRIVACY AND SECURITY THROUGH MEDIATOR USING DCP-ABE WITH OTP

Varsha S Rasal[1*], Suraj U Rasal [2], Shraddha T Shelar [3]

[1]*Dept of Computer Science & Engineering, Nehru College of Engineering and Research Center, Thrissur, INDIA*

[2]*Dept of Computer Engineering, Bharati Vidyapeeth University College of Engineering Pune, INDIA*

[3]*Dept of Information Technology, D Y Patil College of Engineering Akurdi, Pune, INDIA*

ABSTRACT

In the previous 394Technology has given a wonder full gift to man which is called as Internet. Traditional internet techniques were based upon the centralized structure which is now extended to a complex network of decentralized smart devices. This shift requires a strict authentication which ensures that system's resources are obtained by legal user. In this proposed paper, an OTP concept is added to the existing DCP-ABE-M scheme which will add another layer of security to the current system. OTP (One Time Password) is a time dependent unique sequence of character code or password which is valid only for a single login session up to a specific time. The proposed system will complete the login session if and only if the user passes the primary and secondary check in test conducted by the system. Since the OTP code is transferred only to the registered phone number, the owner of the account will be only able to login successfully. This scheme focuses more on password authentication and login session. Existing approaches had used only user attributes and GID for secret key generation but in our approach secret key is a combination of data attributes, user attributes and One Time Password (OTP). The most effective feature of this system is, it performs three factor authentications. So even if the attacker gets the user attribute and static secret key, attacker will not be able to cross the login session without OTP which will be sending only to the registered phone number of account owner. Hence the proposed system is more reliable and secure than existing system.

KEY WORDS
Mediator, OTP; Three factor authentication; Time dependent login session; Data attributes; User attributes; Mediator; static key

Published: 30Oct 2016

***Corresponding Author**
Email:
varshasurajrasal@gmail.com
Tel.: +918793000079

INTRODUCTION

All recent approaches are utilizing one of the most conventional and simplest authentication schemes over the insecure network, which is known as Password Authentication scheme. The identity of the connection originator can be validated by using the password authentication schemes which is based upon two-way hand shaking procedure. Since this scheme is vulnerable to playback attack, error attack, modification attack and trial attack, it can't provide high security. Hence numbers of researchers are focusing on new password authentication schemes which will provide highly secure network environment for legal users.
The traditional password authentication based systems had provided a user identity (ID) and a unique password to each user for his authentification purpose during login process or when user wants to access remote server. The remote server maintains a password table which stores user ID and corresponding password. If and only if the user entered details matches with the password table details then only the server access permission will be granted. But this system have few drawbacks 1) it is vulnerable to stolen-verifier attack, 2) system load will be high when number of users were huge, 3) it is difficult to maintain a long password table when more number of users register in a same server.

In order to solve the problems related to password table a new scheme is proposed by A. Evans [1] in which the passwords are hashed or encrypted and then stored in password table. There are two types of hash function 1) computable hash function, 2) uncomputable hash function. The another new approach introduced a scheme which gives proof of erasure which is based upon uncomputable hash function. But still [1] is not secure because the passwords may get leaked or modified, if the intruder break the server. For solving this problem J.K. Jan and Y.Y. Chan [2] had proposed a new system in which the server doesn't require the verification of password table for a long time.

Later Lamport's method of one time password using one way hash function is further extended by Haller and Yeh [3] [4]. In 2002, two stolen-verifier attack on SAS and OSPA protocol is proposed by Chen and Ku [5] in terms of time computation and utilization of storage space. Some existing schemes had used smart cards for password authentication [6][7][8][9]. Here the existing [10] had given the smart card based schemes on secure one way hash function which had solved the problems such as 1) it doesn't require password table, 2) computational and communication cost is very low, 3) reply attack is prevented. But the major disadvantage of this scheme is, it can't achieve mutual authentication. These problems can be solved by using [11] which is given by I.En Liao and Cheng-Chi Lee. These techniques are further extended to [12] in order to improve the security level. Then further OTP concept had used in multi-authentication factor process. Multi-authentication process uses three factors for authentication. They are 1) Something you know, 2) Something you are, 3) Something you have. Here we have combined the concept of one time password with DCP-ABE-M in order to provide highly secure system.

MATERIALS AND METHODS

IBE

The first Identity Based Encryption (IBE) scheme was introduced by Boneh and Franklin in 2001. As IBE doesn't require public key infrastructure, this scheme can be taken as an exciting alternative to public key encryption. That is the sender requires only latter identity instead of certificates and public keys of the receiver for sending messages to other side. Later Adi Shamir extended this concept IBE [13] where the user can use any string as his public key. For example: Alice and Bob are two persons who want to communicate with each other through mail. Alice sends an encrypted message to bob at bob@company.com. She encrypts her message by utilizing the public key string bob@company.com. Public key certificate of bob is not required by Alice, So Alice doesn't generate public key certificate of bob. Bob receives a message in an encrypted form. In order to decrypt the mail he contacts a third party, which we call private key generator(PKG).Bob introduces himself to the PKG. PKG generates a private key for bob which can decrypt the received mail. The PKG contains only bob's private key.

ABE

The main drawback of existing IBE scheme is, multicasting is not supported by this scheme. In order to solve this problem Sahai and Waters proposed a new scheme Fuzzy Identity Based Encryption or Attribute Based Encryption (ABE) [14] which allows multicasting. Here a set of descriptive attributes of user are utilized to provide his identity. In this scheme user is able to decrypt data if and only if the user holding attributes matches with the cipher text attribute. There are two types of ABE:
KP-ABE: In this approach, set of attributes will be attached with cipher text, while an access structure is integrated with in the secret keys.

CP-ABE: In this scheme, secret keys are attached with a set of attributes, while access structure embedded in the cipher text [15].

MABE

The existing approaches which use single authority can easily generate and share secret keys because single authority knows all the attributes of the user. But the main disadvantage of the existing schemes is, dependency on the central authority. That is the entire system get effected when the central system get failed. M. Chase introduced a new scheme Multi-authority Attribute Based Encryption (MABE) [16] in which central authority is not required for managing the entire system. Since there is no communication between the authorities, each authority work independently and follows his own procedure. In this approach two main authorities were introduced, Central Authority (CA) and Multiple Attribute Authorities (MAA). In these authorities, Central Authority is considered as main authority under which other allocated authorities are created according to assigning random attributes. Central authority is only responsible for MAA allocation or initial setup. These authorities are created according to requirement of the user communication setup. In MABE either its own policies will be applied or Cipher Policies will be applied. In both of these cases, attributes will be allocated randomly. The user can decrypt the cipher text if and only if he has all the required attributes which satisfies access policy. Secret keys are used for decryption, these keys corresponds to the attribute of a user. The key generation depends upon all the multiple authority. So when the user require secret key the system combine all the secret keys and generates the decryption key. For example: authority 1 and authority 2 both have some attributes of same cipher text. Let Alice have all the attributes of authority 1 and Bob has all the attributes of authority 2, it is not possible to decrypt the data even if we combine their keys. The cipher text can be decrypted only if the user holds all the attributes. The drawback of this system is dependency on multiple authorities and initializing authority.

DCP-ABE

Jinguang han, willy susilo had introduced a scheme called Decentralized Cipher Policy ABE (DCP-ABE) [17] which removes all kind of dependency. That is, here multiple independent authorities are organized in a decentralized environment which doesn't require a system for its initialization. It obtains secret keys for user from multiple authorities without knowing them the users global ID and attributes. Since the user sensitive attribute gives user identity, it protects the privacy of user sensitive attribute. Multiple authorities together generate a secret key by using user information. But the only disadvantage of this system is, if any authority gets failed then it will be difficult to get the secret key [18] [19].

DCP-ABE-M

In [20] this scheme multiple mediators are added in the existing DCP scheme, which stores half part of the secrete key in order to increase the security level. Here, both the authorities, mediators are independent and allocated based upon specific attributes.
Authority generates an encryption key according to user attributes. Mediators are important here to manage key sharing and attribute distribution. Mediators are created according to hierarchy and level of

the authority. Example can be student-faculty-admin. According to that mediators will have access rights and privileges. Each Mediator will be interlinked with specific authority only to validate itself. In this scheme failure of any authority doesn't affect the entire system because each user is handled by some specific authority and mediator not by all the authorities. The advantage of this scheme is it doesn't store any user data and entire key in any part of the system. The secret key will be divided into two and stored in authority and mediator. It provides more internal security but it doesn't provide high security at login page.

OTP

OTP (One Time Password) is defined as one true pairing. That is OTP is a password which is used for authentication and can be used only once before the limited amount of time or before getting expired [21]. Stefan D and Tomaz K have proposed a scheme called one time computable self erasing function [12] which had given one time computable pseudorandom function (PRF). In this scheme, it uses a adversary who is responsible for storing the key K which is generated by a PRF FK (.). This adversary based research is further extended to [22][23][24][25][26]. Some of the existing schemes get effected by the various virus attacks in order to solve this problem few schemes are introduced [12][11]. All these existing methods are combined to provide a single efficient scheme [12] which computes one time computable code.

RESULTS

PROPOSED SYSTEM

Now days, a strong authentication techniques are required for preventing various authentication attacks. In order to reduce the complication networking different authentication techniques are used.
Authentication is defined as a first step of access control in which the authentication server compares the given user credentials with the authenticated user data files which are stored in the database of a local operating system. Authentication and identification are the one of the initial step of access control.

MULTI - FACTOR AUTHENTICATION

Authentification can be done by using three common factors 1) something you know, 2) something you have, 3) something you are.When a system makes the use of more than two authentication factors then it is called as multi-factor authentication. The following figure shows the concept of multi-factor authentication.

Fig.1: Multi-factor authentication

Something you know: User login ID and password is used as a factor in one factor authentication.
Something you have: This factor refers to the items such as hand held tokens, smart cards etc. A token or OTP is generated by using a hand held device (mobile, laptop etc) which displays a secret number on its LED display and the number is synchronized with authentication server.

Fig. 2: One Time Password

In above figure there is an authentication server and a user who holds a temporary OTP or token. Here the token held by user changes in each and every 60 sec under the surveillance of server. The user is able to login if and only if user's current OTP matches with the authentication server OTP.

Something you are: Attributes, biometric methods can be used as the authentication factors

MULTIFACTOR AUTHENTICATION IN DCP-ABE-M-OTP

Existing DCP-ABE schemes are focusing more on the internal process security but proposed system is focusing both on internal and external security in order to increase the reliability of the system. The already existing schemes are based upon 2 factor authentication while the proposed system is utilizing the concept of multi-factor authentication which increases the security level at login page.

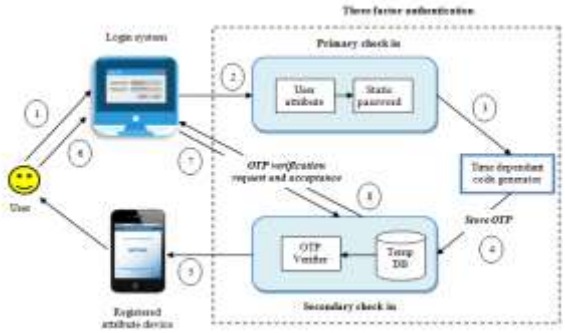

Fig. 3: Three factor authentication processing

Here, the user must go through the primary and secondary check in process for getting logged in into the system. Primary check in contains two factor authentications. Where, first factor is user attributes or biometrical methods and second factor is user name and password.

Primary check in:
During the user login period the proposed system checks two factors. First one is user attributes; the system checks whether the entered user attributes are same as the authorized user attributes which are stored in the server database. The second factor is user name and password, the system checks the user name and password and allow the user only if they are valid.
Here U_A indicates current user attributes and S_{UA} gives stored user attributes. F_{AP} , F_{AF} indicates First Factor Authentication passed and failed.
$U_A = \{ U_1, U_2, U_3 \}$
$S_{UA} = \{ U_1, U_2, U_3, U_4, U_5 \}$
If $\forall U_A \in S_{UA} \rightarrow F_{AP}$
$\forall U_A \notin S_{UA} \rightarrow F_{AF}$
$\forall U_A \Delta S_{UA} \rightarrow$ Fake user
In second factor authentication: U_N , U_P indicates User Name and User Password. A_{UN} , A_{UP} specifies Authenticated User Name and Authenticated User Password. S_{AP} and S_{AF} gives Second Factor Authentication passed and failed.
$U_N , U_P = A_{UN} , A_{UP} \rightarrow S_{AP}$
$U_N , U_P = A_{UN} , A_{UP} \rightarrow S_{AF}$

- **Secondary check in**:
It takes place only if the user passes primary check in. After two factor authentication, system will automatically generate a unique OTP (One Time Password) for the particular user which will be valid only for sixty minutes. This level will be completed only if the user entered OTP is same as system generated OTP. Here O_C indicates user entered OTP code and A_C specifies Authorized OTP code. T_{AP} and T_{AF} gives Third Factor Authentication passed and failed.
$O_C = A_C \rightarrow T_{AP}$, $O_{CT} < 60$ sec, $A_{CT} < 60$ sec
$O_C \neq A_C \rightarrow T_{AF}$, $O_{CT} < 60$ sec, $A_{CT} > 60$ sec
Where, OCT and ACT specifies the generated time of user OTP and Authenticated OTP .
The authentication process steps are given below:

1) User enters into the system then system performs primary check in.
2) Primary check in: user attributes, user name, password is verified.
3) After passing primary check in, system generates a unique password for the particular user.
4) System stores the OTP in temporary DB and sends an OTP copy to user hand held device.
5) Second check in: OTP is verified.
6) If OTP matches then login is allowed.

DISCUSSION

ARCHITECTURE

The important segments of the proposed system are 1) Decentralized environment: all members are independent in this system, 2) Multiple authorities: all authorities are independent and are based upon some specific feature, it reduces system load, 3) Multiple mediator: each mediator is based upon some specific feature, 4) Multi-Factor Authentication: It adds 3 layer of security to login page.

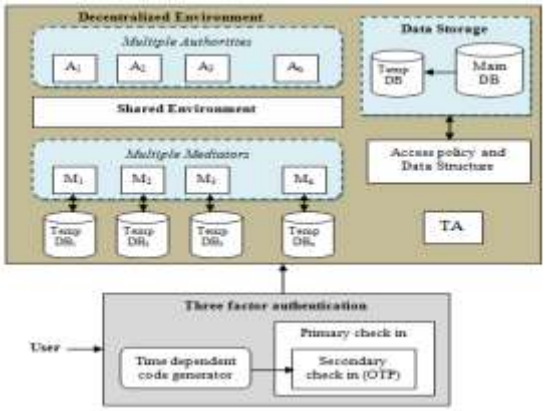

Fig. 4: DCP-ABE system with three factor authentication and multiple mediators

First the proposed system performs multi-factor authentication in order to check the user status. After completing the authentication successfully user will be able to enter into the system. After login, system will provide a unique temporary database for each user, which will be deleted after user logout. System stores all the user information such as time, uploaded file name, file size, file length, user attributes etc which will be used for secret key generation. This information will be stored in 2 different jar file in different location of the DB by giving different directories for each jar file. Here multiple authorities and mediators play an important role, which are based upon specific attribute. The system will allocate specific authority and mediator set to the user based upon user attribute type. For example: if the user is a b tech mechanical student then the system will allocate a student mediator and mechanical authority for that specific user. The specialty of this system is, it is not vulnerable to any attacks or hacking or leakage because it doesn't store any of user information in authority and mediator.

ENCRYPTION

In this proposed scheme, individual session is assigned for each user and all the user information will be stored in a decrypted path of a specific temp data base. When an authorized user tries to upload a data, our system will automatically generates a secret key by using user attribute set UA, data attributes set DA , one time password OC and time at which the OTP is generated OT .

The secret key generating factors are given below.

U_A : { A_1 ,A_2 ,A_3 .....A_n }

D_A: { D_1 ,D_2 ,D_3 .....D_n }

O_C : {OTP, O_C <60 sec or O_C > 60 sec }

O_T : { O_{T1} or O_{TN} }

Here if OTP is generated in first 60 second then it will satisfies (O_C <60 sec) condition or else (O_C > 60 sec) and the OTP generation time will be assigned according to the OTP taken. These four factors are combined for generating the encryption key. A main attribute set M_A is generated by combining the above given factors and by using the elements of M_A secret key or encryption key E_K is formed. By using encryption key the uploaded data is encrypted.

M_A : { $U_A \cup D_A \cup O_C \cup O_T$ }

M_A : { A_1 ,A_2 ,A_3 .....$A_n \cup D_1$,D_2 ,D_3 .....$D_n \cup O_C \cup O_T$ }

E_K = (U_A+D_A+ O_C + O_T) $_K$

E_K = (U_{AK}+D_{AK} + O_{CK} + O_{TK})

Then after generating the secret key, it is divided into two sub keys were one part of the key will be stored in the authority and remaining half key will be stored in the mediator. Here A_K indicates authority key and M_K specifies mediator key.

$E_K \rightarrow A_K + M_K$

DECRYPTION

The decryption is only possible when the user get's the secret key which is combined correctly. Here DK specifies the decryption key which will be provided to the user only if he satisfies the access policy of the system. If DK is equal to EK then only the user will be able to decrypt the data successfully.

DK = AK + MK
AK + MK = (UA+DA+ OC + OT) K
AK + MK = (UAK+DAK + OCK + OTK)
Here (UAK+DAK + OCK + OTK) is a combination of user attribute, data attribute, OTP and OTP generated time. If AK + MK is equal to (UAK+DAK + OCK + OTK) which is equal to encryption key, then only the system will provide secret key to the user.
(UAK+DAK + OCK + OTK) = EK
AK + MK = EK
DK = EK

CONCLUSION

The existing schemes had focused more on internal security than the external security. Since the login of the existing system is based upon the users sensitive attribute which gives users identity, these systems are unable to provide full security and are disable to protect the privacy of the user sensitive attributes. The proposed scheme is focusing on both the internal and external security, for improving external security the concept of multi-factor authentication and for increasing the internal security mediator is added in the existing DCP-ABE scheme. The login process of existing system was based upon only a single factor that is user attribute but in the proposed system three security layers are added in the login page which increases the level of security of the proposed scheme as compared to existing schemes. Since in the existing approach the secret key is made up of user attributes which gives the user identity, any user can get the secret key if he knows the attributes of that specific user. In the proposed system, 4 factors are combined to generate the secret key so that no one can get the secret key by only holding specific user attributes. Hence the proposed system provides more internal and external security than the existing schemes.

CONFLICT OF INTEREST
There is no conflict of interest.

ACKNOWLEDGEMENTS
None

FINANCIAL DISCLOSURE
None.

REFERENCES

[1] Jinguang A. Evans Jr., W. Kantrowitz, E. Weiss, [1974] A user authentication scheme not requiring secrecy in the computer, Commun. ACM 17 ,437–442.
[2] JK Jan, Y.Y. Chen, [1998] Paramita wisdom password authentication scheme without verification tables, J. Syst. Softw. 42:45–57.
[3] N. Haller, [1995] The S/KEY one-time password system. RFC Technical Report 1760, February.
[4] T-C Yeh, H-Y. Shen, J-J. Hwang. [2002] A secure one-time password authentication scheme using smart cards, IEICE Trans. Commun. E85-B , 2515–2518.
[5] C.-M. Chen, W.-C. Ku, [2002] Stolen-verifier attack on two new strong-password authentication protocols, IEICE Trans. Commun. E85-B , 2519–2521.
[6] K.-K.R. Choo, Revisit of McCullagh–Barreto, [2005] Two-party id-based authenticated key agreement protocols, Internat J. Network Security 1 (3)P 154–160.
[7] M Kim, CK Koc, [2005] A simple attack on a recently introduced hash-based strong-password authentication scheme, Internat. J Network Security 1 (2): 77–80.
[8] CC Lee. [2005] Two attacks on the Wu–Hsu user identification scheme, Internat. J Network Security 1 (3): 147–148.
[9] H-C. Wu, C.-Y. Liu, S.-F. Chiou, [2005] Cryptanalysis of a secure one-time password authentication scheme with low-communication for mobile communications, Internat. J. Network Security 1 [2), 74–76.
[10] H-Y. Chien, J.-K. Jan, Y.-M. Tseng, [2002] An efficient and practical solution to remote authentication: Smart card, Computers & Security 21: 372–375.
[11] I-En Liao, Cheng-Chi Lee, [2006] A password authentication scheme over insecure networks, Journal of Computer and System Sciences , Elsevier, 72: 727–740.
[12] Stefan Dziembowski, Tomasz Kazana, [2011] One-Time Computable Self-erasing Functions, International Association for Cryptologic Research, pp. 125–143
[13] Adi Shamir, [1998] Identity Based Cryptosystems and Signature schemes, Departments of applied mathematics,.
[14] . Sahai and B Waters, [2005] Fuzzy identity-based encryption, in Advances in Cryptology [Lecture Notes in Computer Science), 3494. Heidelberg, Germany: Springer-Verlag, , pp. 457–473.
[15] J Bethencourt, A Sahai, and B Waters, [2007] Ciphertext-policy attribute based encryption, in Proc. IEEE Symp. SP, May, pp. 321–334.
[16] M. Chase, [2007] Multi-authority attribute based encryption, in Theory of Cryptography [Lecture Notes in Computer Science), vol. 4392. Heidelberg, Germany: Springer-Verlag, , pp. 515–534.
[17] Jinguang han, willy susilo, yi mu, jianying zhou, and man ho allen au, [2015] improving privacy and security in decentralized ciphertext-policy attribute-based encryption ieee transactions on information forensics and security. vol. 10, no. 3 [1), 665-678
[18] Varsha Thanaji Mulik , Shinu A and Suraj Rasal. [2016] A Survey on Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption, International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835, Volume-3, Issue-5.
[19] A. Lewko and B. Waters. [2011] Decentralizing attribute-based encryption, in Advances in Cryptology [Lecture Notes in Computer Science), 6632. Heidelberg, Germany: Springer-Verlag, pp. 568–588.
[20] Suraj Rasal, Megha Matta, Karan Saxena [2016]OTP system with third party trusted authority as a mediator, International Journal Of Engineering And Computer Science,Volume: 05 Issue: 05.
[21] Suraj Rasal and Sanya Relan, [2016] OTP Processing using UABE & DABE with Session Management, International Journal of Advanced Research in Computer Science and Software Engineering, 6(5).
[22] Katz J, Vaikuntanathan, [2009] Signature schemes with bounded leakage resilience, In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, 5912, : 703–720. Springer, Heidelberg .
[23] Standaert, F.-X, Malkin T, Yung, [2009] A unified framework for the analysis of side-channel key recovery attacks, In:

Joux, A. (ed.) EUROCRYPT 2009. LNCS, 5479, 443–461. Springer, Heidelberg.
[24] Dodis Y, Haralambiev K, Lopez-Alt A, Wichs, [2010] Cryptography against continuous memory attacks, In: FOCS.
[25] Faust, S., Kiltz, E., Pietrzak, K., Rothblum, [2010] Leakage-resilient signatures, In: Micciancio, D. (ed.) TCC 2010. LNCS 5978: 343–360. Springer, Heidelberg.
[26] Brakerski Z, Goldwasser, [2010] Circular and leakage resilient public-key encryption under subgroup indistinguishability, In: Rabin, T. (ed.) CRYPTO 2010. LNCS, 6223: 1–20. Springer, Heidelberg.