www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16565-16568

OTP system with third party trusted authority as a mediator

Suraj Rasal [1], Megha Matta [2], Karan Saxena [3]

[1] Assistant Professor,
Dept. of Computer Engineering
Bharati Vidyapeeth University
College of Engineering Pune, India
surasal@bvucoep.edu.in

[2] Dept. of Computer Engineering
Bharati Vidyapeeth University
College of Engineering Pune, India
megha.matta15@gmail.com

[3] Dept. of Computer Engineering
Bharati Vidyapeeth University
College of Engineering Pune, India
karankrsaxena23@gmail.com

***Abstract* - One Time Password is one of the preferable security techniques to do online transaction. If the security level is compared, it shows the need of improvement in its transaction methods and medium. In this paper, two authorities are considered viz. bank domain itself and third party as a trusted authority. Third party authority will have its own secrete key based on its own considered attributes. This key will be combined with user attribute key to form encrypted key. This key will be stored in temp database till session time is available. Here the two new concepts are added as to use third party secrete key and storing this key into temp database for predefined session time only. After these stages only main database can be accessed. It will increase the security level to make secure online transaction.**

I. INTRODUCTION :

OTP (One Time Password) is valid for a short duration of time. It provides two-factor authentication in a way in which we first enter the password to login to our account after which (if authenticated) A onetime password is sent to the registered mobile number or email, which if entered within the period it is valid or the session, the person is authenticated else not. The algorithm for OTP makes use of random id generation i.e. it generates a new id each time a person requests to login which prevents replay attacks because even if the id is captured by an intruder it will no longer be valid since the session would already have been expired [5]. Advantages of Using OTP are, it provides two factor authentications, it is valid for a particular session only, hence expires long before someone tries to catch it, new Random id is generated each time etc. Disadvantages of Using OTP are noted as susceptible to man-in-middle attack, re-entering of the OTP each time the session expires and need to increase security levels [6].

II. EXISTING SECURITY APPROACHES:

A. Attribute based Encryption

It is derived from the traditional public key cryptography (wherein the user text is encrypted using the public key of the receiver which can only be decrypted using private key of receiver) and Identity based encryption (wherein the public key can be any string e.g. email address) Attribute based Encryption is a approach where two or more attributes are used to form the public key using algorithm [2] .This key can then be used for encryption and decryption. These can be generated by a third party who needs to be a trusted party. Let us suppose that head FBI wants to encrypt sensitive memo such that only a person with certain credentials or attributes can access it. It is a Type of identity-based encryption with One public key and Master private key used to make more restricted private keys, here we can use ABE i.e. Attribute Based Encryption. In the previously developed cryptography system we used to encrypt our text based on public key of the receiver which could then be decrypted by him at a later time using his private key. Now, what if the receiver has many attributes associated with him. For example, Alice may be in a group called "internal affairs", she is female, and based in the USA office of her organization. Thus we assign her the attributes "internal affairs", "female" and "USA". If Bob wants to encrypt all the members who belong to internal affairs group, he can use one public key for the entire group. But what if he

DOI: 10.18535/ijecs/v5i5.38

doesn't know the members who belong to this group called "internal affairs ". In that case, we can use Attribute based Encryption. In ABE, a third party is given the responsibility of generating keys for users having certain attributes. This third party has a master secret key (MSK)and public key (PK).Now for each user a key is generated based on this MSK and the attribute of the group for which this key is generated. Generated key is known as secret key (SK) which is provided to the user. Now, when a user wants to encrypt a document they construct a policy for this document. The policy specifies which attributes are required to decrypt this document, for example ("internal affairs" OR ("female" AND "Canada")) [2]. Given the constructed policy and the PK (of the key authority for a system), documents can then be encrypted and distributed to everyone which can only decrypted by users which match the policy assigned to the cipher text i.e. they should know the attributes which are used for generating the policy and the secret key [4].

B. One Time Password Working

Authentication token is a small device used to generate a random value every time it is used. This value can then be used for authentication. These devices include processor, Liquid Crystal Display (LCD) for displaying outputs, battery, keypad (optional), real Time Clock (optional). Also it includes pre-programmed number called SEED which assures that OTP generated each time will be unique.

1) Creation of token: This step includes the generation of seed which is done by the Authentication server which is then pre-programmed inside the device or token [6].

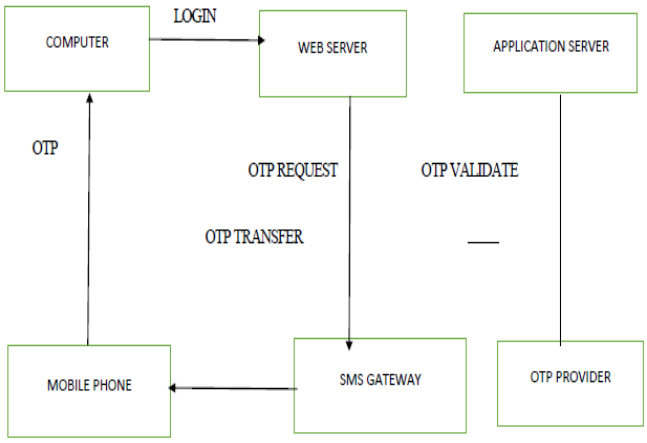

Fig. 1 OTP architecture [6]

2) Use of token: Based on the value of seed which is pre-programmed inside the token a onetime password is generated. These are known as one time because they are used once and discarded These are valid for a short period of time so the user needs to ensure that they are used before the session expires, which if the case requires user to obtain a new OTP which will be completely different from the one generated before Now, to validate the user server obtains the seed from the database and applies the same algorithm which was used to create OTP before which is then matched to the one entered. If a match exists user is authenticated else he needs to log in again [6].

III. RESEARCH METHODOLOGY:

One Time Password is a security technique which is used to identify the user as authorized user. On the basis of OTP the merchant or other registered user is identified to make sensational transactions. So, while making online transaction, it keens to have a high level communication. In this paper two additional levels are added to the security level including assembly of encrypted key using third party trusted authority key and user attribute key. This generated key is stored in the temporary database. After end up with session time, encrypted key is automatically deleted from the database. There are two temporary databases. One database is present in policy check segment. Other temporary data base is present in main OTP-M (One Time Password- Mediator) system. When encryption key is generated, its reflection key is passed towards the temp database of policy check segment. This reflected encryption key is matched with the encryption key stored in temp database of main system.

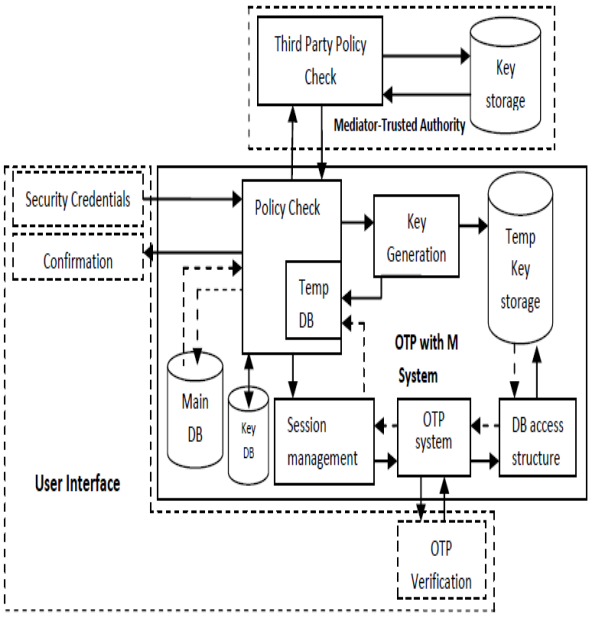

Fig.2 OTP with Mediator as a trusted authority system

A. Mediator Trusted Authority:

Third party trusted authority is considered as mediator. Mediator acts as invisible contributor in encryption key generation. Mediator or trusted authority is interlinked with bank domain. Mediator has its own attributes. Based on its

attribute, mediator key is generated. This key is stored in the key storage segment of the Mediator-trusted authority (M-TA). User is validated after entering user security credentials, main policy check segment contacts to the policy check segment of the M-TA. M-TA policy check segment has some policy methods to check correct request from known domain. According to that it delivers the secrete key to the main OTP with M system. Mediator attributes set is considered as M_A [2]. By using these attributes, mediator key is generated. Here all attributes are considered as data. On that data, RSA algorithm function (R_F) is applied and mediator (M_K) secrete key is generated [3].

$$M_A = \{A_1, A_2, A_3, \ldots, A_N\}$$

$$M_A \xrightarrow{R_F} M_K$$

This mediator key is stored in the key storage. This key is retrieved and forwarded after request generated by OTP with M system. Key is retrieved in the policy check segment of the OTP-M system after applying policy check methods. These methods are authorised user validation, RSA function, authority check in, session check, authorised data check in [3]. These policy methods are applied according to type of request is generated. Sam type of policy methods are applied in policy check segment of trusted authority.

B. Key Generation

System has key generation segment in which key is generated using user attribute key and mediator key. User attribute key is generated using user attributes. These processes happen at main system only. Bank domain has authorized user's attributes. Based on these attributes, users attribute key is generated. User attributes set is considered as U_S. Its encryption key is generated after applying RSA function [3]. This RSA function is applied on the data formed by user attributes. Generated key is considered as A_K.

$$U_S \xrightarrow{R_F} A_K$$

Policy check method retrieves keys, user attribute key and mediator key from respective databases. Here user attribute key is retrieved from key database of main system. This key is stored in the database after its creation. Both A_K & M_K are combined to form encryption key K_E [1].

$$K_E = \{A_K + M_K\}$$

This key is stored into main temp data base as well as temp data base of policy check segment. When user will be logged in and validated through security levels including OTP validation, key stored in main temp database will be delivered to check key match. After key matching user validation is done and main database is accessed.

C. Session Management

From user entry till transaction confirmation, session management segment checks for the session. When authorized user logins to the domain, his final session time (F_S) is set to predefined value. For all activities including policy check, key generation, key retrieval & OTP system, session is checked for final session time (F_S). If activities at all segments are not equal to the (F_S), user is considered as unauthorized [3]. Key is deleted after successful transaction from both the temp databases.

CONCLUSION

In cryptographic approach it is necessary to have more number of security levels. In case of online banking system, all sensational data relies on number levels of cryptography applied in the online transaction processing. In this paper security levels are extended by adding combination of two security keys including user attribute key and encrypted key from third party trusted authority. Next thing applied here is session management. In normal way key is formed and permanently stored in the database. In this paper, generated encrypted key is stored and retrieved for particular predefined session time only which increases the security levels by avoiding extra data base requirement to store keys, all time database protection, communication protection etc. Due to this number of methods security level is increased to higher extent compare to previous methods.

REFERENCES

[1] Jinguang Han, Member, IEEE, Willy Susilo, Senior Member, IEEE, Yi Mu, Senior Member, IEEE, Jianying Zhou, and Man Ho Allen Au, Member, IEEE. (MARCH 2015). Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. 10 (3), 665-678.

[2] Shraddha U. Rasal, Bharat Tidke. (March 2014). Improving Revocation Scheme to Enhance the Performance in Multi-Authority ABE.International Journal of Computer Applications (0975 – 8887). 90 (18), 5-10.

[3] William Stallings (November 16, 2005). Cryptography and Network Security: Principles and Practice. 4th ed. -: Prentice Hall. 257-285.

[4] John Bethencourt ,Amit Sahai, Brent Waters. (20-23 May 2007). Ciphertext-Policy Attribute-Based Encryption. 2007 IEEE Symposium on Security and Privacy. 10 (7), 321 - 334.

[5] Andrew S. Tanenbaum,David J. Wetherall (2011). Computer Networks. 5th ed. Prentice Hall Boston: Pearson. 763-863.

[6] ZhouLu(Beijing, CN)Huazhang Yu (Beijing, CN) Read more: http://www.patentsencyclopedia.com/app/20140082710#ixzz48Q8v47 Aa. (20-03-2014). Patent application title: Method for authenticating an OTP and an instrument there for Read more:http://www.patentsencyclopedia.com/app/20140082710#ixzz48Q 8sCRPw.Available: http://www.patentsencyclopedia.com/app/20140082710. Last accessed 12th May 2016.