Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

OTP Processing using UABE & DABE with Session Management

Suraj Rasal (Assistant Professor**), Sanya Relan, Karan Saxena**
Dept. of Computer Engineering, Bharati Vidyapeeth University, College of Engineering Pune, Maharashtra, India

Abstract - In existing approach, user details are used in terms of attributes. Based on these user attributes, encrypted keys are generated and used for secure transactions. Secure data and encrypted keys are stored in secure databases. Its security maintenance and transportation is vital challenge in the cryptographic world. In this paper this problem has been decreased by increasing security levels at higher extents. User and data attributes are used to generate encryption key. Encryption key is formed by combining user attribute key and data attribute key. One more level is increased by using session management approach in the system. Generated encryption key is stored for predefined session. When final session time is over, generated key is automatically deleted from temporary database. This encryption key is matched to access main database. So total five levels of security are added, including security user credentials, OTP, session management, key generation by combination of user and data attributes & data attribute check from user which increases encryption levels to make secure online transactions.

Keywords: OTP, ABE, RSA

I. INTRODUCTION

Electronic commerce is the way of conducting the business communications and transactions over networks and computers. It includes buying and selling of goods and services over the web, electronic fund transfer, smart cards, digital cash and all other ways of doing business over digital networks. It also includes all inter-company and intra company functions such as marketing, finance, and manufacturing that enable commerce and use of fax, video conferencing or interaction with the remote computer [5]. A merchant is the person or an organisation that wants to sell goods or services to the cardholder which is authorized holder of payment card such as MasterCard in order to gain profit. The merchant must have a relationship with an acquirer which is a financial institution for accepting user payments on the internet and user authorization [5]. E-Banking is an electronic payment system .It is a simple, convenient and secure method of accessing bank accounts on the internet. Online banking enables the customers of a bank to perform different transactions over the internet. To access the financial institution's facility, customers are provided with the userId and password. A customer with internet access would need to register with the institution for the service and set up password [5]. A third party transaction is a type of business deal in which the dealings between the buyer and seller are managed through an intermediary third party. The idea is to create a connection between the buyer and seller that works to the benefit of all the parties concerned. In all aspects there is need of increasing the level of security. In this paper its existing security policy has been improved by increasing additional level while doing online transaction. User attributes and data attributes are considered to generate encryption key which is temporarily stored and accessed for security purpose.

II. EXISTING SECURITY APPROACHES IN ONLINE TRANSACTION

A. ABE(Attribute Based Encryption)

It is a type of public key encryption that allows users to encrypt and decrypt messages based on their attributes. There are two main types of ABE:

- Key policy
- Cipher text policy

In Key-Policy ABE there is a key with a formula having phi symbol and also a cipher text with a set of properties (attributes).One can decrypt if the attributes satisfies the formula. In cipher text policy ABE the roles are exchanged: a key is associated with a set of attributes and the cipher text with a formula having phi symbol.

One of the biggest problem in using attribute based encryption is that, it is expensive than public key cryptography. Consider a Key-Policy ABE system in which the encryption time will vary with the number of attributes which are assigned to the Cipher Text and key generation time will vary with the size of the chosen formula associated with user's private key. These costs have a great impact on the many applications.

B. OTP(One Time Password)

A one-time password (OTP) offers two-factor authentication using something user know such as a user_id combined with something like a token to generate an OTP. As its name specifies OTPs are only valid for one login session or one

single transaction. They are expired after use. They overcome the disadvantages of the traditional static passwords, the most important of which is that OTPs are not vulnerable to replay attacks. Therefore, if an OTP is stolen, it can only be used one time.

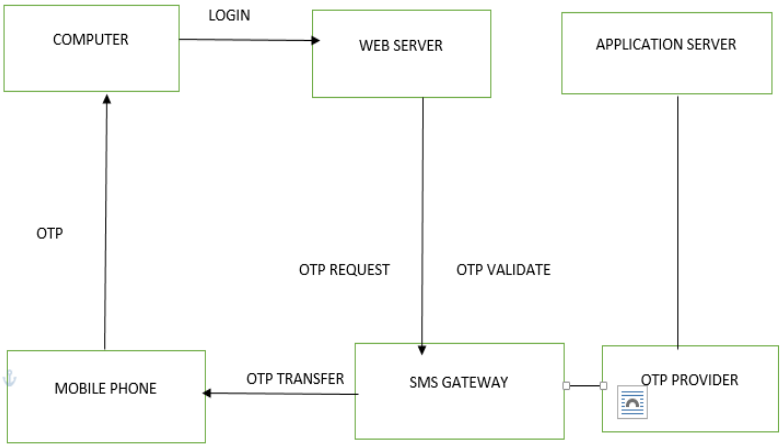

Fig. 1 One Time Password working[6]

OTP solutions are ideal for all companies where a there is a need to access resources such as network, mail, and WebPages, and where they want to access these resources through the Internet or via an intranet [6].

C. Need of secure online transaction

Security is a very important factor while doing online transactions .As web applications are susceptible to a large number of threats such as man in the middle attack, phishing, spoofing and sniffing. In order to overcome such kind of attacks and keep intruder away from accessing the information we need to secure our transaction [5]. In existing approach user attributes are used which is keen to improve security level in terms of attributes. Database security is important factor while doing online net banking which shows need of improved security.

III. RESEARCH METHODOLOGY

In this paper the system concept is consider to avoid phishing attacks. In internet banking phishing is serious issue. In existing approach, while using OTP (one time password) the sensitive secrete data can be leaked. To overcome this problem combination of user and data attributes are used to generate secret encryption key.

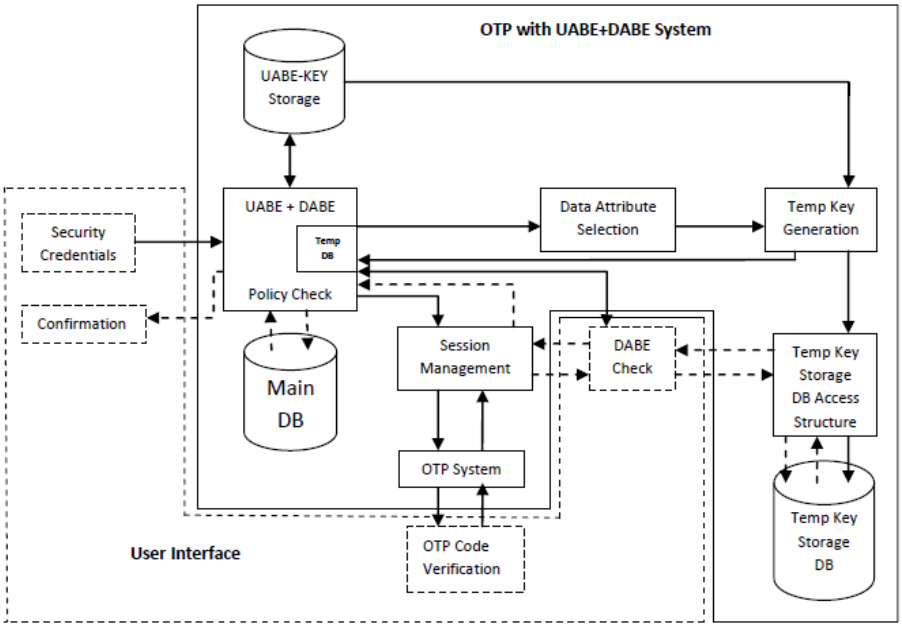

Fig.2 Secure OTP using UABE & DABE

User attributes are stored in the database when user registers on the website. User logins to the website using same user credential details. In this paper both user attribute and data attributes are used to generate encrypted key. User details are stored in terms of encrypted key which is formed by using user attributes. When authorized user logins to the portal, policy check method is initiated. This policy check method is directly connected to the key storage database. After completion of one policy cycle under UABE & DABE with OTP, policy check is initiated again to communicate with main database. RSA algorithm is applied to generate encryption key on user attributes [3]. Its function is considered as R_S. Data attributes set is consider as D_A and user attributes set is considered as U_A.

$$U_A = \{a_1, a_2, a_3, a_4, \ldots, a_n\}$$

$$U_A \xrightarrow{R_S} U_K$$

$$D_A = \{d_1, d_2, d_3, d_4, \ldots, d_n\}$$

$$D_A \xrightarrow{R_S} D_K$$

a_n is user attribute which is based on user details such as name ,mobile number, email id, date of birth etc [1]. Similarly d_n is data attribute such as merchant's URL, name, type of ecommerce website, type of transaction, date, time and type etc [2].

Encryption key is generated by combining user attribute key and data attribute key.

$$E_K = \sum \{U_K + D_K\}$$

Main database access method is available after key verification. Decryption process includes key check policy. User's login session is important thing in actual practice. These login sessions are actual limitation for system process. When user gets logged in the bank domain, session management keeps its acknowledgement and its limitation is set to the particular level. Here logged in time is considered as T_L. Tensile or final time is considered as T_F. Total session time (T_S) required for confirming transaction is ($T_F - T_L$).

$$T_S = T_F - T_L$$

Current processing time is considered as T_C. System checks T_C at each stage of the system. It compares T_C with T_F. Condition to satisfy the process or to proceed is,

$$T_F > T_C$$

E_K (Encryption key) is stored in temp database for T_F time. After T_F time, E_K is deleted from temp key storage database. Policy check method includes temp database. When E_K is generated, same key is stored in this temp database till T_F time. After this time, key is deleted from temp database in policy check. At the last stage of transaction process and while accessing main database, encryption key stored in the temp database of policy check stage which is checked with the encryption key of temp key storage database. In database access structure, user details will be checked based on DABE (Data Attribute Based Encryption). After validation, stored encryption key is retrieved and delivered with respect to session management to access main database. DABE works under database access structure where user is asked to enter credential details based on data for reconfirmation. After accessing main database, confirmation is delivered to user interface segment. While doing back end online transaction, phishing attack can occur. To avoid this phishing attack and to recheck user validation, again user will be asked to enter user credentials based on data attributes. Authorized and session user will be already aware about asked security credentials. Indirectly it will increase one level security and system security process will be more complex.

IV. CONCLUSION

This proposed approach shows new security policy in Attributes Based Encryption (ABE) by combining user and data attributes. Its cryptographic approach is increased by adding session management, temporary encryption key storage, combination of attributes, and reconfirming data attributes. These all concepts are added with existing approaches like One Time Password (OTP) and security user credentials which increase the security level in higher extent. So in this paper there will be five number of encryption levels viz. user credentials, OTP, secure session management, attributes based key generation and data attribute check. It can be applied to enhance and improve security in internet banking.

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] Zhou Lu (Beijing, CN) Huazhang Yu (Beijing, CN) Read more: http://www.patentsencyclopedia.com/app/20140082710#ixzz48Q8v47Aa. (20-03-2014). Patent application title: Method for authenticating an OTP and an instrument there for Read more:http://www.patentsencyclopedia.com/app/20140082710#ixzz48Q8sCRPw.Available: http://www.patentsencyclopedia.com/app/20140082710. Last accessed 12th May 2016.

