IIOAB JOURNAL

ARTICLE

# SECURING INTERNET BANKING USING MULTIPLE ATTRIBUTES SCHEME AND OTP

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

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

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

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

ISSN 0976-3104

## ABSTRACT

*In the latest cryptographic trends, attributes play important role in increasing security level. In online banking, users are relocated to the banking domain with secure medium. In this paper attributes are used as measure components to form secrete key. Attributes of website data, trusted authority & user attributes from banking domain are considered as parameters to form key. Based on these attributes, one time password is generated. After one time password verification, same key will be formed which will be matched with the newly formed key by one time password. In this approach, key will be generated temporarily and it will be matched with newly formed key by one time password method. This multiple approaches will increase the security level to make online transaction safely.*

**KEY WORDS**
*Merchant System; Trusted System; Bank System; Secure System; Randomized Selection; Encrypted data; User*

Received: 30 Aug 2016
Accepted: 9 Sept 2016
Published: 5 Oct 2016

## INTRODUCTION

In the recent networking approaches, network security is prioritized thing which can't be avoided. Even its level is important. Through cryptographic approaches are applied to increase the level in the network security, unauthorized user act as the level breaker. Hence, we need to improve the security level in online transaction. When the term money transaction comes, it shows data sensitivity and its importance. Online banking transactions show extreme need to improve its secure mechanism in current and in future point of view. In previous system of online banking one time password (OTP) scheme has been used as an authentication mechanism in dynamic structure where it overcame the server database compromising problem at one time by adding the breakpoints in hash chain of OTP [1]. It has used the computational calculations of Deffie Hellman problem so as to prove the security against attacks in insecure network [2].OTP actually carried out in numbering format and changed its state in every 30-40 seconds to another format. Hence it has dynamic feature of using over the traditional network [3]. To make it more effective in privacy we are further adding flavor of OTP in attribute based encryption in which multiple attributes will be taken in considerations so that we can possibly achieve highly secure transaction with reduced complexity [4].

## MATERIALS AND METHODS

After the traditional digital signature system in cryptography, new systems has stepped out and proposed with new and innovative techniques. Some alternative way is made to signature scheme called as identity based encryption (IBE) [5]. In this particular concept keys are generated based on users credentials after the authentication. Person transferring the messages over the network doesn't needs to know the public key of receiver [2]. Receiver just has to authenticate himself as to get so as to access to message. Online Email system is the first demonstration example given which was based on identity based encryption technique [6].

### Attribute Based Encryption

In this era, attributes are considered as measure factor to make encrypted form [7,8]. Attributes are considered as user attributes. User attributes are considered as set of user component details like user name, date of birth, city and so on. User attributes are uniquely applied where their values are predefined with respect to attribute value [4].

***Corresponding Author**
Email:
surasal@bvucoep.edu.in
Tel.: +918793000079

Attribute set = $A_1 = \{a1_1, a1_2, a1_3, a1_4, \ldots, a1_n\}$= {'Name' ,'Surname' ,'City' ,'Date of Birth',……,'Country'}
Attribute set = $A_2 = \{a2_1, a2_2, a2_3, \ldots, a2_n\}$= {'Time of registration' , 'place of registration' ,……,'agent'}

These attributes are used to form a secrete key [10]. After applying logarithmic approach and probability, main attribute set is formed which is combination of these attributes. Further cryptographic algorithm is applied and secrete key is generated. Attribute based encryption is technique is widely used technique in the online security approach. Even cloud services are made more secured by applying multiple security approaches using attributes [9].

### Cipher text Policy

In networking users able to access the data only if a user proves themselves with set of credentials or attributes to authority. Cipher text policy provides the confidentiality of data over the compromised server and provides security against the collision attack [7]. This method is closer to KP-ABE (Key Policy) access control [10] in which cipher text has been dealt with set of attributes. Unlike this, CP-ABE (cipher text policy) has used the user's secret key with number of attributes. Before decrypting data any message has to pass through an attribute based access structure. Suppose we have different users with attributes set {S1, S2,...., S$_n$}.
The combination gives

$A \subseteq 2^{\{S1,S2,S2,..Sn\}}$ If $\forall \alpha, \beta$
Where, $\alpha \in A, \alpha \in \beta \; then \; \beta \in A$

In this structure access structure is non empty subset structure of {S1, S2,...., S$_n$} in which if all sets appeared inside A are said to an authorized set where as the sets outside the A are not authorized sets [7]. Hence the roles of different parties are given by all attributes and that are associated with the keys in cipher text policy attribute based encryption. On the other hand when we are using CP-ABE, there are four fundamental steps to use it for secure data transmission [10]. First is the setup to generate the public parameter and creating secret master key. Second is the encryption where message, public parameter and cipher policy access structure is used. Key generation is the next step which takes master secret key and attributes sets which provides private key of user in output. Last step of decryption has been done using cipher text having access policy, master key, public parameter and decrypts the message.

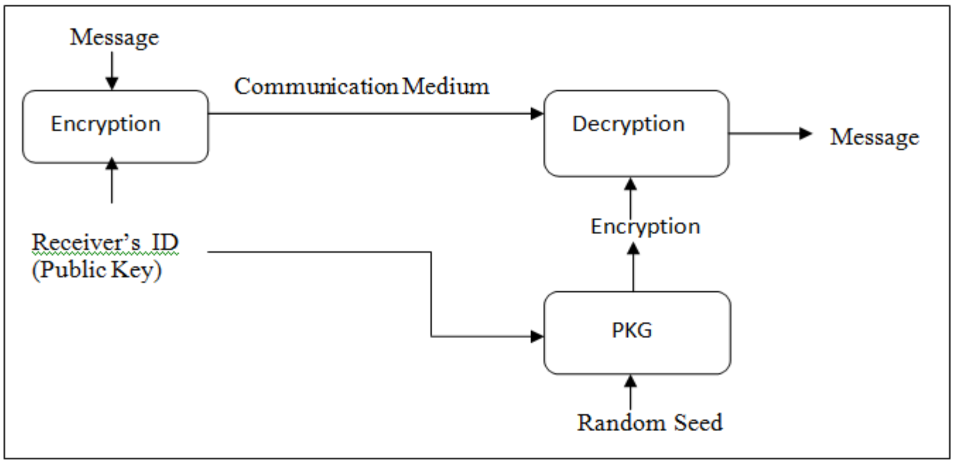

**Fig. 1:** Identity Based Encryption [4]

## RESULTS

User uses secure online banking to do online transactions [11]. User visits merchant's website directly or indirectly and connects to the banking domain to complete online financial transaction [12]. In this paper, three main components of the system are considered. Each system has its own policy. This policy is applied when particular request is generated. All systems are installed at different locations which are unknown to the users and merchants.

### Policy M-S (Merchant System)

Policy M-S (Merchant's Policy) has its own components like attributes and data validation. Merchant makes request to the trusted authority and bank domain simultaneously. These requests carry current data attributes and co ordination request. Attributes are carried towards bank domain are current data attributes including hosting site name, day, date, month, time in hour, minute and second. Request carried towards trusted authority is coordination request which means to poke the trusted authority to contribute its attributes in encryption technique. Current data attributes are considered as a secrete data which changes according to transactions done by the user. This is the new term added to the existing approach. Here current data attribute set is considered as D$_A$.

$D_A$ = { 'Hostname','Day','Date','Month','Time1:Hours','Time2:Minutes','Time3:Seconds'}.
$D_A = \{D_1,D_2,D_3,D_4,D_5,D_6,D_7\}$

Above attributes are considered as attribute set of current attribute set which is generated by the registered merchant at the time of transaction [7]. These attributes are delivered to the bank domain.

## Policy T-S (Trusted System)

After receiving request from merchant, trusted authority sends its own attribute set to the bank domain to form main attribute set [12]. Trusted Authority Attribute (TAA) is formed from the policy T-S. This policy checks for merchant and user validity. Also it applies random logic while generating TAA. Trusted authority acts as third party trusted authority [12]. While doing official registration of trusted authority with bank, some secrete attributes set is shared between bank domain and trusted authority. While delivering attributes to the bank domain for encryption, random selection is done. These randomly selected attributes are delivered which are identified by Policy B-S of the bank domain.

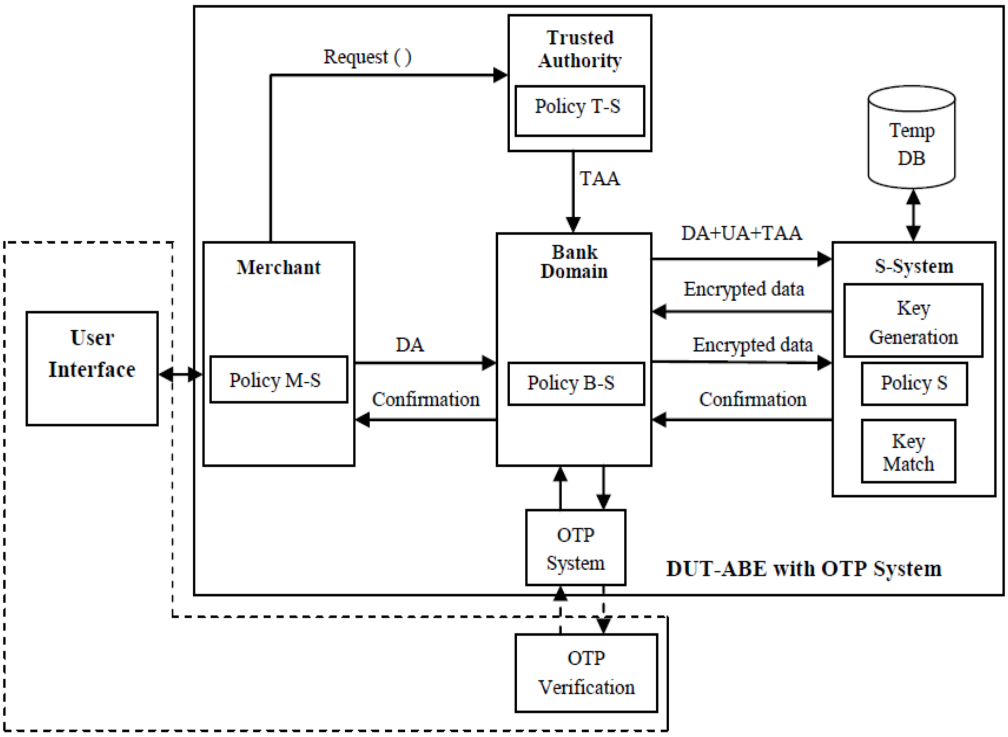

**Fig. 2:** DUT-ABE with OTP System

Trusted attribute set is considered as $T_A$.

$T_A$ = {'Attribute1',' Attribute2',' Attribute3',' Attribute4',' Attribute5',.....,' Attribute N'}
$T_A = \{T_1,T_2,T_3,T_4,....,T_N\}$
$T_{AA} = \{T_2,T_4,T_5,T_9\}$

From this attribute set, some attributes are selected randomly which are delivered to the bank domain. Delivered attribute set is considered as $T_{AA}$.

## Policy B-S (Bank System)

Bank domain already has user attributes which are taken from user details. Policy B-S (Bank's Policy) waits for TAA & DA. After receiving it, it adds User Attribute (UA) set to the received attributes. This policy forms main attribute set from DA, UA &TAA [4][12]. Main attribute set is transferred to the S-System. When user creates bank account, his or her user details are considered as bank or user attributes like name, date of birth, city and so on. Here we have considered user attribute set as $U_A$.

$U_A$ = {'Name ,'Surname' ,'City' ,'Date of Birth',.....,'Country'}
$U_A = \{U_1,U_2,U_3,U_4,.....,U_N\}$

Bank system receives the attribute sets from trusted authority and merchant. Bank system delivers these attribute sets including its own user attribute sets to the S-System

### Policy S (Secure System)

S-System (Secure System) is neither directly connected to any other system except bank domain. Retrieved attribute set is converted into encrypted format. S-System receives all attributes and forms main attribute set considered as $M_A$.

$$M_A = D_A \mathbf{U}\ T_{AA}\ \mathbf{U}\ U_A \qquad (1)$$
$$M_A = \{D_1,D_2,D_3,D_4,.....,D_N,T_1,T_2,T_3,T_4,....,T_N,U1,U_2,U_3,U_4,.....,U_N\} \qquad (2)$$

(1)&(2) shows that $M_A$ is a union set of current data attributes, trusted authority attributes and user attributes [4] [12]. On these attributes, randomized selection method is applied. These Randomized Selection (RS) algorithm is applied on this data where selected components are stored in the array set [13]. As shown in (3), random elements are selected by applying randomized selection algorithm. It is stored in array set. This array set is applied with RSA algorithm to form encrypted format of data as shown in (4) [14]. This data is considered as $E_D$.

$$M_A \xrightarrow{RS} \{D_2,T_3,T_4,\ D_4,\ U1,\ U_4\} \qquad (3)$$
$$M_A \xrightarrow{RSA\text{-}E} E_D \qquad (4)$$

RSA algorithm based application is installed on both sides where RSA-encryption (RSA-E) and decryption(RSA-D) is done [15]. In similar way, normal data is nothing but decrypted data $M_A$. When decryption occurs at both S-System and bank domain, same decryption technique is applied [15].

$$E_D \xrightarrow{RSA\text{-}D} M_A \qquad (5)$$

In (4) and (5), represented data is similar. Decrypted data is in the form of user understandable format which is in the form of combination of text and numbers. Policy B-S delivers this data to the user through one time password for versification purpose. One password is generated through this formatted data which is unique. One time password generated will be received either through email or through SMS(Short Message Service) [1]. It will be based on user's option.

After entering one time password manually by user, information will be delivered back to the Policy B-S. Policy B-S will convert this data into encrypted format and revert it to the S-system through communication channel which is present at other or unknown location to verify entered one time password information. Policy S (Secure) will decrypt the information first. Decrypted data will be checked for data validation and regarding confirmation will be delivered to the Policy B-S. This confirmation will be delivered to the merchant will be further transferred to the user for acknowledgement purpose. After successful delivery of the acknowledgement, all data stored in the temporary database will be deleted automatically. When next time new transaction will occur, new data attributes based data will be used which shows more secured approach in recent cryptographic trend.

## CONCLUSION

In online banking, security techniques applied is important factor. Communication channel is sensitive component of secure online banking. It is not necessary that communication channel is always secured while doing online transactions. In existing security approach, communication channels and security resources are not secure as required. In proposed approach, security provider resources are unknown to the system. Combination of multiple attributes including user, current data and trusted authority makes authentication data more secured. Different policies are applied in different levels to enhance the encryption level. One time password is also additional security method used for user identification. Code travelled through the communication medium is delivered in secured form which is hard enough to decrypt. Attributes are not secured in the existing approaches which are overcome in proposed approach because there is possibility of leaking user details retrieving attributes. Respective attribute data is created for temporary purpose only which shows there is no possibility of data piracy to do next transactions. Each time new attribute based data is generated to complete online transaction. By applying multiple attribute scheme, security in online banking can be enhanced and user details can be securely stored.

### CONFLICT OF INTEREST

There is no conflict of interest.

### ACKNOWLEDGEMENTS

The authors are thankful to Hon'ble Dean and Management

### FINANCIAL DISCLOSURE

None.

IIOAB JOURNAL ISSN: 0976-3104

## REFERENCES

[1] Sediyono E. Santoso K. [2013] Secure login by using one-time password authentication based on md5 hash encrypted sms. In ieee advances in computing, communications and informatics (icacci), 2013 international conference, 1604-1608.

[2] Rasal SU, Tidke B. [2014]. Improving Revocation Scheme to Enhance the Performance in Multi-Authority ABE. International Journal of Computer Applications. 90(18):5-10.

[3] Kim HC, Lee HW, Lee KS, et al. [2008]. A Design of One-Time Password Mechanism Using Public Key Infrastructure.IEEE Networked Computing and Advanced Information Management. NCM '08. Fourth International Conference. 1 (1):18-24.

[4] Rasal S, Relan S, Saxena K. [2016] OTP Processing using UABE & DABE with Session Management. International Journal of Advanced Research in Computer Science and Software Engineering. 6 (5):57-59.

[5] Boneh D, Franklin M. [2001] Identity-based encryption from the weil pairing. In Springer Berlin Heidelberg - annual international cryptology conference. 213-229.

[6] Sahai A, Waters B. [2005] Fuzzy identity-based encryption. In Springer Berlin Heidelberg-Annual International Conference on the Theory and Applications of Cryptographic Techniques. 457-473.

[7] Han J, Susilo W, Mu Y, et al. [2015] Improving privacy and security in decentralized ciphertext-policy attribute-based encryption IEEE transactions on information forensics and security. 10(1):665-678.

[8] Goyal V, Pandey O, Sahai A, et al. [2006] Attribute-based encryption for fine-grained access control of encrypted data. InProceedings of the 13th ACM conference on Computer and communications security. 89-98.

[9] Rasal SU, Gupta K, Mulik VT, et al. [2016] Improving Security in SAP-HANA Cloud by Applying Multiple Encryption Policies. In International Journal of Science Technology & Engineering. 196-200.

[10] Bethencourt J, Sahai A, Waters B. [2007] Ciphertext-policy Attribute-based Encryption. In 2007 ieee symposium on security and privacy. 321-334.

[11] Hiltgen A, Kramp T, Weigold T. [2006] Secure internet banking authentication. IEEE Security & Privacy. 4(2):21-29.

[12] Rasal SU, Mattal M, Saxena K. [2016] OTP system with third party trusted authority as a mediator. International Journal Of Engineering And Computer Science. 5 (5): 16566-16568.

[13] Kumar A, Chandrasekaran S, Chockalingam AB, et al. [2011] Near-Optimal Large-MIMO Detection Using Randomized MCMC and Randomized Search Algorithms. IEEE International Conference on Communications (ICC). 1 (1):1-5.

[14] Muzzi FAG, Chiaramonte RB, Ordonez EDM. [2009] The Hardware-based PKCS#11 Standard using the RSA Algorithm. IEEE Latin America Transactions. 7 (2):160-169.

[15] Zhou X, Tang X. [2011] Research and implementation of RSA algorithm for encryption and decryption. In IEEE Strategic Technology (IFOST), 2011 6th International Forum: 1118-1121.