Data Sharing using Key Policy based Authentication & CHAP

Neeru Yadav, Prof. Anurag Jain

Abstract— Data Sharing between number of users whether in distributed systems or in cloud environment needs security from various attacks. Attribute based data sharing is also an efficient technique which provides Cipher text policy attribute-based encryption from the prevention from key escrow problem and user revocation [1]. Although the technique is efficient but further enhancements is needed for the security against various attacks and for the improvement of efficiency. Here in this paper an efficient technique is implemented which is based on Two factor authentication and provides security from various attacks with less computational time and cost.

Index Terms— CP-ABE, OTPK, TRNG, Data Sharing, Key Escrow, Proxy Encryption.

1 INTRODUCTION

Before a long time we were providing authentication with the physical appearance of person and by their signature manually, but now a day's different techniques were implemented. One of them is Data Sharing. Data Sharing is very important protocol by which we can exchange our data by online. So with the help of this technique we can prevent different attack so the solution is implemented a new scheme or new protocol which is more efficient and more secure and preventing from different attacks which can be used in a variety of applications especially in E-commerce. This technique allows an efficient signing between two parties such that the chances of attacks reduce. The technique is based on trusted third party so that the chances of eavesdropping are less. The technique is based on one time where after signing contract between parties the key destroys [1].

Attribute Based Data Sharing

Since various techniques are implemented for the sharing of data in wired and wireless network and hence is the security from various attacks. Attribute based data sharing is based on the conceptual framework of providing encryption using Attributes that are generated by the client.

The figure 1 shows the basic architecture of the data sharing system where a client generates a unique attribute for each of the data be shared among others. This client then encrypts the data using the generated attribute and forms a tupple and sends to the Data Storing Center. Here KGC is used as key generation centers which re-encrypts the data and provides key pairs. The Ciphertext policy attribute based encryption provided here prevents escrow problem and also provides proxy encryption [1].

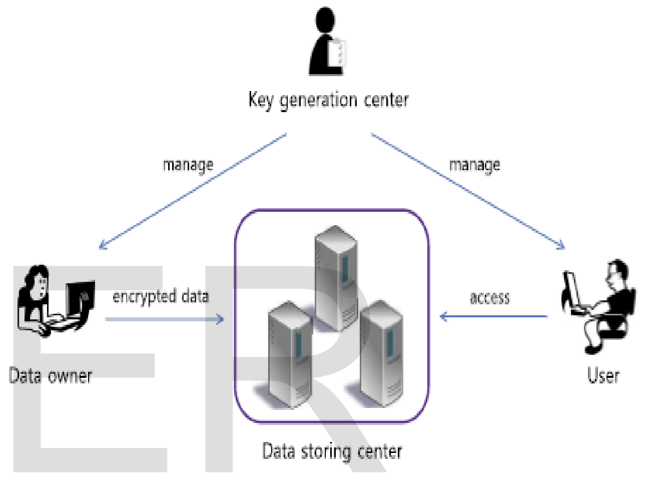

Figure 1. Existing Attribute based Data Sharing [1]

Data Sharing using OTPK

In daily life there are various electronic transaction techniques by which we can perform quick transactions from one party to other. There are various security techniques implemented by which we can perform a secure communication of data from one party to other. But whenever we transferred data or information from one party to other security play a important role in this transactions because many attacker can attack or destroy our transactions or data. So to overcome this problem a newly implemented security technique is used for authentication that is known as One Time Private Key (OTPK). One time private key is key which is used for very short time by the sender and receiver ,when the sender and receiver gets authenticate or performing encryption or decryption the key is destroyed and we can never be use this key for further communication.

One time private key is also a new technique for data shared among a number of users. Here in this technique Client when shared any data needs to be authenticated on the local server and generates a session key on the basis of which data is encrypted and shared among users. But the key generates here is one time and after communication or after a certain time stamp the generated key destroys.

The figure 2 shows the secrete data sharing technique that can be used in the OTPK technique. The technique provides efficient security from various attacks as well as prevents escrow problem and authentication.

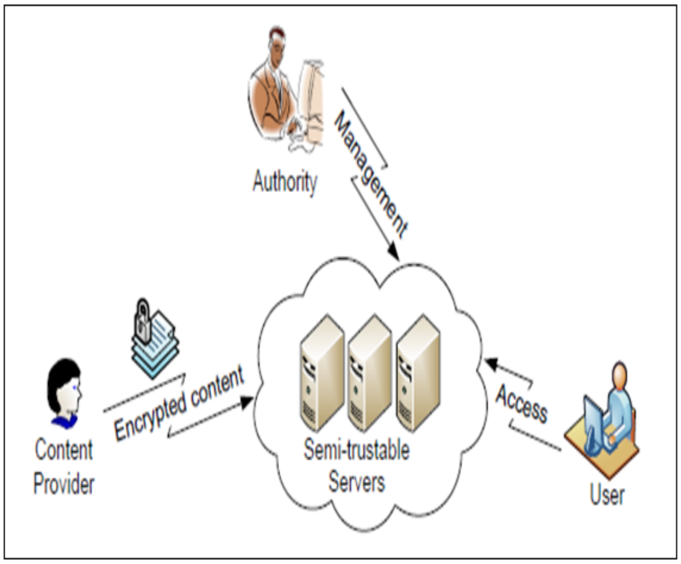

Figure 2. Example of secrete Data Sharing

True Random Number Generator using Image

It is based on the generation of random numbers which can be used a secrete unique number for the generation of keys or encryption. Image based generation of random numbers starts with the scanning of each of the pixel from left to right and top to bottom and convert each of the pixel into gray value and generate bits value and concate every bit value to the next generated bit value and hence form a long string.

2 RELATED WORK

Junbeom Hur has proposed a new and efficient technique of sharing data among multiple users using cipher text policy attribute based encryption [1]. The technique implemented here provides prevention from escrow problem and user revocation per attribute using the concept of proxy encryption. The technique efficiently provides access policies and decision support to access the data. CP-ABE is used for the encryption of data and key generation center is used for the decryption or the generation of keys for the data to be shared. A secure two party computation is used for the resolve of key escrow problem and then proxy re-encryption is used for the solution of user revocation. The technique also provides less communication cost as compared to the other existing techniques of Data Sharing [1].

Amit Sahai Brent Waters proposed and uses the multilinear maps for the encryption of data to shared [2]. Here in this technique first of all the generation of circuits can be done using attribute based encryption. The technique is based on both the combination of ciphertext policy and key policy [2].

Shucheng Yu, Cong Wang uses the concept of attribute revocation for the sharing of data among number of users [3]. Here in this technique cipher text policy attribute encryption is used, where each of the user deals with a set of attributes and the data to be shared can be encrypted using these attributes and data can be decrypted when the access policies generates for the data is matched with the attributes [3]. The technique provides the central authority to revoke the users with the minimal efforts, hence prevents from user revocation and escrow problem [3].

Amit Sahai and Brent Waters uses Fuzzy concept for the encryption of data [4]. Here in this technique an identity is used with a set of descriptive attributes. This technique generates a private key for the identity and encrypt and hence to decrypt the same identity is used and matched and verified if they are equal or not, Here Fuzzy technique is used for the biometric generation of identities which reduces the error tolerance of the technique [4].

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters minimizes the user revocation during the data sharing among users using attribute based encryption [5]. Since the concept of data encryption allows only the other arty to shared the private key. Hence a new technique is implemented for the fine-grained data sharing which is based on key policy based encryption using attributes or identities. The technique uses the concept of hierarchical Identity based encryption in which only the delegation of keys is shared among various users [5].

Alexandra Boldyreva, Vipul Goyal, Virendra Kumar is implemented fort the better and efficient revocation of user using identity based encryption [6]. Since IBE is based on public key based encryption. The technique enables the users to encrypt the data using identity based encryption where the concept of time stamp factor is used and hence the receivers also update their keys a regular interval of time. The technique efficiently improves the concept of key updation by the third party or trusted third party [6].

Pascal Junod, Alexandre Karlov uses the arbitrary access policies for the data to shared and broadcast among users [7]. Here a new and efficient public key cryptographic technique is implemented for the secure attribute based broadcast encryption of data for the complex access policies using various gates. The technique is based on the enhancement of Boneh Gentry waters which removes collusion resistant and also supports complex Boolean access policies [7].

Luan Ibraimi, Milan Petkovic Svetla Nikova, Pieter Hartel, Willem Jonker is based on the mediated cipher text attribute based encryption [8]. Since cipher text attribute based encryption is implemented in which users uses the secrete key and generates attribute for each of the data and encrypt the data using the secrete key. The receiver when used to decrypt the data uses the identity as a secrete key. But here an enhanced mediated technique is used for the enhancement of CP-ABE which enhances the attribute revocations so that the techniques are used for the applications especially in Personal Health records [8].

Rafail Ostrovsky, Amit Sahai, Brent Waters uses the non monotonic access structures for the attribute based encryption [9]. Here an attribute based encryption is used which allows the user's private key that can be used in any access formula for encryption. Since the existing technique is only based on the identity based encryption using mono tonic access structure. Hence a new and efficient technique is implemented using decisional Bilinear Diffie-Hellman access policies. The technique implemented takes less user revocation and more security [9].

Allison Lewko, Amit Sahai uses the concept of generating very small private keys for the revocation systems [10]. Here in the technique public key based broadcasting of the encryption data is used. The technique is implemented for two issues one for the overhead generated during ciphertext and second to use the concept of attribute based encryption for non-monotonic access policies [10].

S.Jaya Nirmala, S.Mary Saira Bhanu, Ahtesham Akhtar Patel uses and analyze the various techniques implemented for the data sharing in the cloud computing [11]. Here various techniques are implemented for the data sharing such as Private Information retrieval and Secure Data Outsourcing but during the implementation of these techniques Confidentiality and Integrity and Availability are the issues for the data sharing [11].

Kamel Faraoun has proposed a new technique of generating keys from images using chaos based key stream generator [12]. Here in this paper a new way of generating keys using n-ary keys stream generator which is based on the combinatorial method of three chaotic maps. The keys generated using this technique provides scalable and uniform key distribution and non-zero cross correlation and also provides sensitivity. The key generator using chaotic maps are thus used for the image encryption [12].

Jun Peng, Du Zhang and Xiaofeng Liao also proposed a new and efficient technique of Key Generation using Chose maps [13]. Here in this technique a block cipher is used for the image encryption and then 32 bits image block and a secrete key of size 192 bits. The technique includes a generation of chaotic sequence which is then given as an input to function G where a block size of 8*8 is used for the image encryption [13].

3 PROPOSED METHODOLOGY

The proposed methodology implemented here is based on the concept of key attribute based encryption. The technique includes generation of keys using the concept of One time private key and then shared image is used for the generation of keys and then session key generated after authentication is used for the encryption of shared data. The process includes the following steps:

1. User 'U1' wants to share the data in the network to a number of receivers.
2. User sends a request message to the trusted third party, where TTP in response will asks for the user U1 to send the shared password.
3. User 'U1' then sends the password to the TTP where TTP verifies if the user is an authenticated user or not.
4. TTP then generates a random number and send to the respective User.
5. User uses the random number and generates Master Key and send to TTP, where TTP checks and verifies the key.
6. Now the image to be shared between users and TTP is used for the authentication.
7. User 'U1' then chooses the image and using TRNG generates a master key and sends to TTP.
8. TTP again verifies the key generation using TRNG and generates a session key for the users.
9. The encryption and decryption of the shared data is done using the shared session key.

The figure shown below is the proposed architecture of the system. It includes the data sharing system with technique of key based encryption.

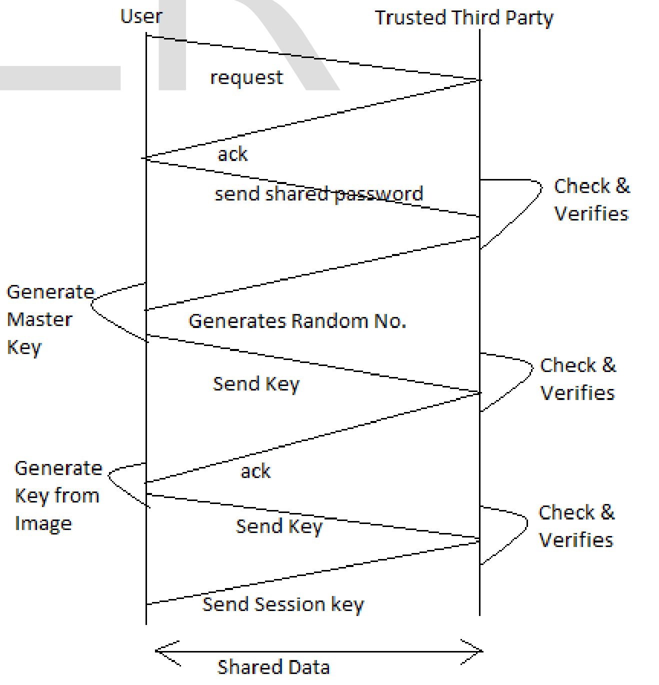

Figure 3. Architecture of Data Sharing System

4 RESULT ANALYSIS

The table shown below is the analysis and comparison of data sharing techniques using ciphertext attribute based encryption and proposed work. The comparison is based on the time for the data to be shared and the communication cost required in bits.

	Communication Cost in bits	
Time in hours	CP-ABE	Proposed Work
10	1000	500
20	1200	738
30	1385	917
40	1586	1038
50	1749	1328
60	1829	1521
70	2538	1826
80	2847	1920
90	3164	2017
100	3522	2237

Table 1. Comparison of Communication Cost in bits

The table shown below is the comparison of total user revocations time required for the data to be shared. The proposed methodology generates and requires less user revocations as compared to CP-ABE.

	CP-ABE		Proposed Work	
Time in hours	Valid User	Revoked User	Valid User	Revoked User
10	28	2	40	1
20	32	25	45	12
30	50	50	67	17
40	53	60	72	24
50	55	100	79	27
60	58	130	83	32
70	60	170	87	38
80	68	200	92	44
90	70	230	95	51
100	75	250	100	62

Table 2. Comparison of Computation Time

The table shown below is the analysis and comparison of data sharing techniques using ciphertext attribute based encryption and proposed work. The comparison is based on the time for the data to be shared and the communication cost required in bits.

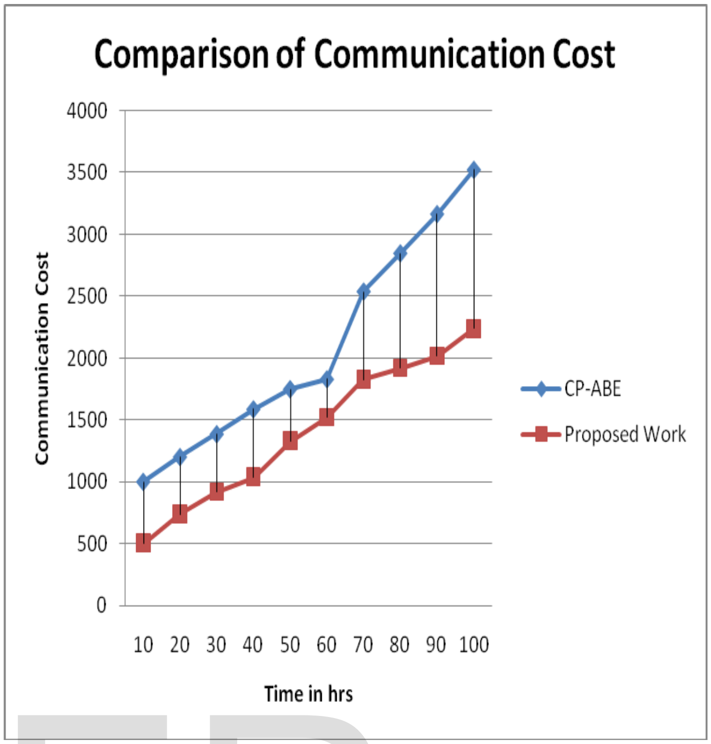

Figure 4. Communication Cost in bits

5 CONCLUSION

Data Sharing using Key based encryption technique is not a feasible technique when compared with the existing cipher text policy Attribute based encryption, but the proposed methodology implemented here based key policy based encryption using Two factor using OTPK and Image based authentication provides efficient security from various attacks and also escrow problem and user revocation is minimal. The result analysis shows the performance of the proposed methodology. The technique implemented for the data sharing takes less computational cost and needs less user revocations as compared to the cipher text attribute based encryption technique.

REFERENCES

[1] Hur, Junbeom. "Improving security and efficiency in attribute-based data sharing", IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, pp. 2271 – 2282, October 2013.

[2] Amit Sahai Brent Waters," Attribute-Based Encryption for Circuits from Multilinear Maps", 2012.

[3] Shucheng Yu, Cong Wang, Kui Ren," Attribute Based Data Sharing with Attribute Revocation", ACM 2010.

[4] Amit Sahai, Brent Waters" Fuzzy identity Based Encryption", Proceedings International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt '05), pp. 457-473, 2005.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted

Data,"Proceedings of ACM Conference on Computer and Communication Security, pp. 89-98, 2006.

[6] Boldyreva, Alexandra, Vipul Goyal, and Virendra Kumar. "Identity-based encryption with efficient revocation." In Proceedings of the 15th ACM conference on Computer and communications security, pp. 417-426. ACM, 2008.

[7] Junod, Pascal, and Alexandre Karlov. "An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies." In Proceedings of the tenth annual ACM workshop on Digital rights management, pp. 13-24. ACM, 2010.

[8] Luan lbraimi, Milan Petkovic, Svetla Nikova, Pieter Hartel, Willem Jonker," Mediated Ciphertext-Policy Atttribute Based Encryption and its Applications", 2008.

[9] Rafail Ostrovsky, Amit Sahai and Brent waters," Attribute-Based Encryption with Non-monotonic Access Structures", 2008.

[10] Allison Lewko, Amit Sahai," Revocation Systems with very Small Private Keys", 2008.

[11] S. Jaya Nirmala, S. Mary Saira Bhanu," A Comparative Study of the secrete sharing algorithms for secure data in the cloud", IJCCSA 2012.

[12] Kamel Faraoun," Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its applications to Image Encryption", IAJIT 2010.

[13] Jun Peng, Du Zhang, Xiaofeng Liao," A Novel Algorithm for block encryption of digital image based on Chaos", 2010.