RESEARCH ARTICLE OPEN ACCESS

Accountable Obliviously Transfer With Access Control

Mrs.K.Aruna [1], Ms.S.Durgadevi [2]
M.E [1], B.Tech [2]
Department of Information Technology
AVC College of Engineering, Mannampandal
Mayiladuthurai, Nagapattinam
Tamil Nadu - India

ABSTRACT

The accountable obliviously transfer with access control is cryptography used in encryption and decryption technique. An authorized user can access the protected records without the database provider knowing his personal information and choices. It prevents to allow an authorized user to the database record. The database record can be used in RSA algorithm. Encryption system is the encrypted data authorized user allows the database record. The database record does not allow unauthorized user. To the best of our knowledge, the first AC-OT scheme where timely revocation and overuse detection. Each user can access their database within the standard bounds. Timer set in cryptosystem used in authorized user, one or more times. Key management can be used in server side.

Keywords:- Obliviously, Accountable, Encryption And Decryption, Authorized RSA Algorithm.

I. INTRODUCTION

Secure the sensitive data access Permission to the authorized user. The authorized user can be access database record. The authorized user has time limit and amount of accessing data. It does not allow unauthorized user. The user can be registering the user details about the database record. The details are the database record name, password, secret key for the encryption and decryption process. The user enters the correct value for the verification process. After the verification the encryption to the secure and sensitive data for stored into database record. The encryption process using the RSA algorithm. The encryption data is modified and readable data. The decryption data is unreadable and it can be converted to readable format. Security model is monitoring the login process using RSA algorithm. The user can register the number of time access to the encryption data. It detects to the unauthorized user access the sensitive data. It is highly protect to the user data.

1) Encryption technique for secure and sensitive data.
2) Decryption technique for readable data.
3) RSA algorithm can be used in process.
4) Timer set in the Server side.

Timer set is only used in authorized user, one or more times. Key management can be used in server side. To secure and sensitive data in encryption and decryption technique.

II. RSA ALGORITHM

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secures public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (e,n), the algorithm is as follows:

1. Represent the message as an integer between 0 and (n-1). Large messages can be broken up

into a number of blocks. Each block would then be represented by an integer in the same range.

2. Encrypt the message by raising it to the *e*th power modulo *n*. The result is a cipher text message C.
3. To decrypt cipher text message C, raise it to another power *d* modulo *n*

The encryption key (*e*, *n*) is made public. The decryption key (*d*, *n*) is kept private by the user.

Keys (PK):

The Keys algorithm takes to the public key *PK*, and private key. Authorized user's analysis input. It outputs the private key of the authorized user.

Encrypt:

The Encrypt algorithm takes the public key *PK*, the learn to access policy. The algorithm outputs cipher text (*CT)* such that only a authorized user with satisfying the access policy.

Decrypt:

The Decrypt algorithm decrypts the data and cipher text authorized user learns and allow to the policy

III. PROPOSED SYSTEM

In this paper, they greatly worked to their process in order to find the encryption and decryption access data in the system. The file should be initially encrypted using the cryptography RSA algorithm. The encrypted data is stored in the server. The data can be accessed through the key management by decrypting of the data. A timer set only authorized user access to the data.

2.1) first one encrypted data in secure and sensitive data access to authorized user. Authorized user in limit and amount of sensitive data.

2.2) A encrypted data is register to the database record. The user can be register to the analysis to the correct value for encryption technique.

2.3) Key management can be used in the process, (secret-public key).The algorithm is input secret-public key and output public key. The membership public key is access to the encrypted data.

2.4) The decrypted data in readable data. Decrypt process collected to the authentication information. The open to file analysis to the database record in decrypt file.

2.5) The unauthorized user to learn and record does not record database. Only authorized user access to the database record.

IV. IMPLEMENTATION

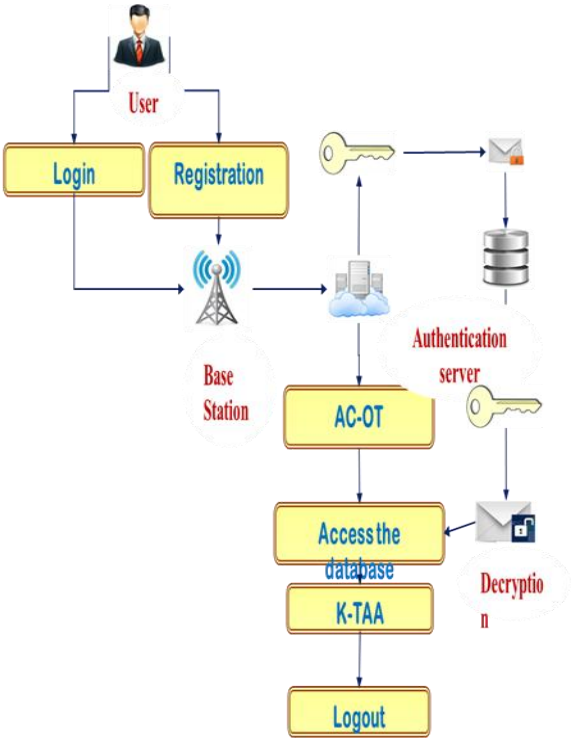
In ACC-OT, it includes some modules. It was described below as follows:

(a)Enrollment

The users can be registering the user details into the data base. Thus the details contain the name, password, secret key for the encryption and decryption process. The user can be entering the correct value for the verification process.

(b)AAC-OT

After the verification then encrypt the sensitive data and stored into the data base. The encryption process using the RSA algorithm. The original data can be modified into non readable data.



(c) Data retrieve

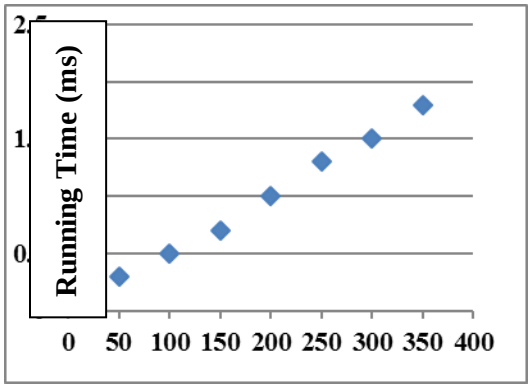
The data decryption method is used to convert the unreadable format into readable format. The decryption process using the RSA algorithm.

(d) Security Model

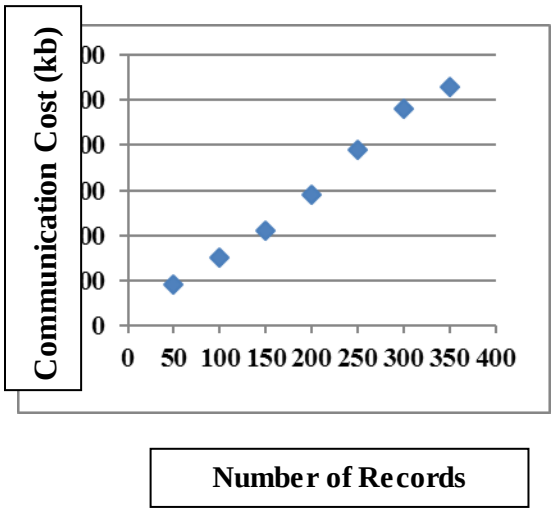
The security modal can monitor the entire login process, and number of time access the data. The user can register the number time to be access the sensitive data to visible. If the users can be try to more then time access the data, that time doesn't allow to access the data. This method is securing the data to access the user. Detect the Unauthorized user access the sensitive data. Compare to the previous method, it is highly protect the user data.\

V. SECURITY ANALYSIS

In ACC-OT, the computation cost and Communication in the trace algorithm. (a) The communication cost of the trace algorithm. (b) The running time consumed by the trace algorithm



(a)



(b)

VI. RELATED WORK

It works on the accountable obliviously transfer with access control. All authorized user access to the database record. Encrypted balance is reduced to the transfer with database. The authorized user authenticate to the server openly. Authorized user's secret satisfies to the database record. Oblivious transfer is adaptive way importance to the application. Encryption allows to the decryption data. AAC-OT used to the hidden access control policies is run and issuer. The system generated to the keys of the user. All database record to the encrypted to the data. The database record can specify and allow for the encrypted record. The secret to the decryption database record granted to the user. Public key and cipher key used in the database record. Database record security is user need to database record. Database record keeps on eye on the overall access frequency. The only information see to the authorized user. It is learn and allows to the unauthorized user. Encryption record is plaintext and the cipher text policy database record. The database record issue and run with authenticated encryption to the user. Authorized user needs and check to the verification record. The user cipher text policy a wants to decrypt record. The process is one state to another state to transmit to current state.

VII. CONCLUSION

AAC-OT In cryptography, encryption is the process of encoding messages or information in such a way that

only authorized user can read it. In an encryption scheme, the intended communication information encrypted using an encryption algorithm, generating cipher ext that can only be read if decrypted. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized user can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

REFERENCES

[1] B. Waters. Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization. *EPrint report*, 290, 2008.

[2] J. Bettencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in *Proc. SP*, May 2007, pp. 321–334.

[3] Y. Zhang *et al.*, "Oblivious transfer with access control: Realizing disjunction without duplication," in *Pairing-Based Cryptography—Pairing* (Lecture Notes in Computer Science), vol. 6487. Berlin, Germany: Springer- Verlag, 2010, pp. 96–115.

[4] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in *Proc. CCS*, 2009, pp. 131–140.

[5] J. Herranz, "Restricted adaptive oblivious transfer," *Theoretical Comput. Sci.*, vol. 412, no. 46, pp. 6498–6506, Oct. 2011.

[6] J. Camenisch, M. Dubovitskaya, R. R. Enderlein, and G. Neven, "Oblivious transfer with hidden access control from attribute-based encryption, "in *Security and Cryptography for Networks* (Lecture

[7] Notes in Computer Science), vol. 7485. Berlin, Germany: Springer-Verlag, 2012, pp. 559–579.

[8] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries, "in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 1666. Berlin, Germany: Springer-Verlag, 1999, pp. 573–590.

[9] M. O. Rabin, "How to exchange secrets with oblivious transfer," Aiken Comput. Lab., Harvard Univ., Cambridge, MA, USA, Tech. Rep. TR-81, May 1981.

[10] D.Chaum,"Security without identification: Transaction systems to make big brother obsolete," *Commun. ACM*, vol. 28, no. 10, pp. 1030–1044, Oct. 1985.