International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

ROBE- Encryption Protocol for Communication

Neethu Prem
Student, Dept. of Information Technology,
Government Engineering College Thiruvananthapuram,
Kerala, India

Albin John
Student, Dept. of Computer Science,
College of Engineering Vadakara
Kerala, India

***Abstract* - The emergence of Mobile Cloud Computing (MCC) has created a situation where both the data storage and the data processing transpire outside of the mobile device. For storage and sharing of data we use a variety of mobile applications. Unfortunately, the way we store and share such personal data are often unencrypted and insecure. So in this paper, we introduce a secure way to store and share such data using a lightweight, fast, computationally efficient, easy to use protocol suitable for resource constrained devices. ROBE protocol is based on stream cipher and it uses an External Cloud Server for management of cryptographic tokens. We use a strong algorithm with less complexity to secure data. The security of cryptographic tokens is ensured at various levels using Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA) and deceit methods. In ROBE, all data are shared securely between mobile and the server with mutual identity verification. Also various attacks are computationally in-feasible for our protocol.**

Key Words: Cloud Computing, Mobile Devices, Encryption, Decryption, Security Protocol

1.INTRODUCTION

Advanced technologies, availability of smartphones and innovative applications significantly improved the life style of human beings. All of us are using mobile devices for multiple use such as for communication, to share and store personal information etc. But in most cases they are unsecured and can be easily retrieved by others. Because of that companies and organizations denied the employees to store data in their mobile device. So it is important to store or share such data in mobile devices securely.

Here we are focusing on mobile cloud computing, which provides a secure transmission of data. Mobile devices can be used for online transactions, education and health care services etc. To save battery and overcome resource limitations Mobile Device can offload computation intensive tasks to the cloud. Security is a major concern in MCC especially for mobile applications that send unencrypted personal information over insecure wireless medium to the cloud. To protect user data against external internal attacks within cloud environment data encryption is required.

Encryption or decryption algorithms provide security to the user's personal information. Encryption converts plain textdata into a code called cipher text. Decryption algorithm inverts cipher text to plaintext. In this paper we discuss about lightweight, fast encryption and decryption of files in Mobile Devices. Three basic approaches for this purpose are

- A mobile centric approach performs encryption or decryption operations are performed within the Mobile Devices. Standard encryptions are not efficient for the resource constrained MDs due to its high computational complexity. Using S-box optimization and reduction of the number of rounds can help to improve performance but more light weight encryption or decryption algorithm is required [2].
- Secondly mobile devices can offload files to the external server or cloud. Resource limitations can be overcome and large files can be handled effectively in a short time frame by offloading tasks. Some of the major security concerns associated with offloading files are using a trusted third party, secured channel, mobile VPN, file splitting and multipath TCP. Researchers have proposed several solutions to overcome such security concerns [4].
- Encrypting the important parts of a file in mobile device and offloading remaining tasks to cloud is an intermediate approach.

In this paper we propose a protocol referred as ROBE which is used to encrypt and decrypt file within mobile devices in a mobile cloud environment. Our objective is to secure personal information stored in the Mobile Devices (image, pdf, doc) the size of which falls in the range 5- 10MB. The ROBE protocol is based on symmetric key algorithm. To generate token or cryptographically secure pseudo random number (CSPRN) an external cloud server is used. Stream cipher is less computation intensive than block cipher and it can be easily handled by existing Mobile Devices [1]. Due to this advantageous featuresstream cipher is chosen as the basis of our protocol. The design considerations of our protocol are as follows

- Every mobile device requires a light weight encryption protocol which is able to handle small sized files found on Mobile Devices.
- The encryption or decryption algorithm must be performed within an acceptable time frame.
- The control of encryption or decryption operation must rely with the users. This is necessary to establishuser's confidence on the system.
- All PT operations must be performed locally on the Mobile Devices itself and the computations onExternal Server should be in such a way that doesn't affect protocol security [3].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

- Most importantly the protocol must be cryptographically secure.

Generation and distribution of a Cryptographic token or CSPRN(C) is a major challenge of stream cipher. To save resources of the Mobile Devices this task is offloaded to external server or cloud in ROBE protocol. The cloud can also be used to share encrypted files with multiple recipients. We propose two level CSPRN modification to address the security of CSPRN(C). Initially C is modified to C" by the external server (i.e., C C") prior to its transmission to Mobile Devices. This is to ensure the security of C against the vulnerabilities of unreliable wireless media. We should also ensure that the intended recipients are only able to decrypt the file. To accomplish this another modification is performed on C in Mobile Devices to generate C'. To encrypt a file C' is used and the recipients having the key only can perform decryption. To generate C' we investigate two randomized and a deterministic approach.

The basic requirement of all cryptographic algorithms is the secrecy of the key. To retrieve it adversaries may impose various attacks. Since C' is used for encryption process, its generation procedure is vital to ensure protocol security. In the proposed algorithms C' is generated by using a key (k). We show that it is infeasible for an adversary to generate C' through a brute force attack using an unknown k, it is computationally infeasible for an adversary to generate c' through a brute force attack.

2.EXISTING SYSTEM

Mobile cloud computing (MCC) is an emerging research area focusing on supplementing the storage and computational requirement of mobile devices (MD) by utilizing the cloud infrastructure. By interacting with cloud, mobile device can deliver various services to the user, such as healthcare, mobile commerce and online education. Users can upload and store data (photos, medical records) from their mobile device to the cloud and can share them with others.

Based on recent smartphone trends, SP (service providers) such as Facebook and Twitter, are offering their applications to more mobile Internet application users. This has caused traffic overload problems for some network companies that require

network maintenance, creating an imbalance between profit and investment. Excessive traffic requires network companies to secure MO (mobile operators) availability, mobile network bandwidth, and minimize information processing by users.

Cloud can perform complex computations efficiently while ability of mobile devices to perform such computations is limited so that many problems occur due to the differences between these two. So there are some limitations in implementing cloud computing for smartphones. These issues include limited resources, related to network, related to security of mobile users and clouds. Most of mobile devices have almost same functionalities like a desktop computer. So mobile devices also have to face a number of problems related to security and privacy. There are many efforts to overcome the problems but these also has to face a lot of challenges. The security issues include device security, privacy of the mobile users and securing data on cloud etc. There are so many security threats like viruses, hacking, Trojans in mobile devices etc.

3.1. Basic ROBE Architecture

ROBE is an encryption protocol for secure data communication between two MDs and is based on stream cipher. Key generation and XORing are two fundamental operations of stream cipher. These are independent operation which can be performed separately. This is the key idea of ROBE [1]. The key generation operation can be performed in an ES or cloud and the XORing operation is performed in the mobile device to generate the cipher text.

Clients, external server and the communication media are the three main components of protocol. A smartphone, tablet or a pc interested in performing the encryption or decryption operation is a client. To offload the computationally intensive task from resource constraint mobile device an external server is used in MCC. In ROBE an external server is used to generate CSPRN. According to the requirement of application and the workload the ES can be configured. Through wireless communication media such as Wi-Fi, 3G, 4G, UMTS, LTE the communication between ES and MD is take place.

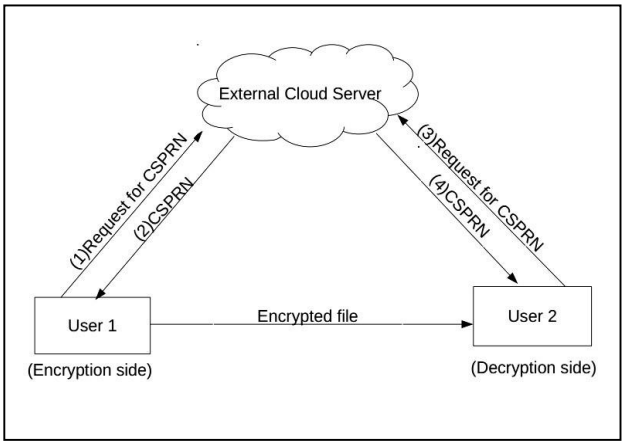

Fig -1: Basic architecture of proposed protocol

Fig. 1 shows the basic architecture of ROBE protocol. Here we consider a user, needs to share a file in her mobile device to another user. Here we do it with the assumption both the users are registered with ES. Here ROBE uses a pre-shared key (S_k) between ES and MD for secure communication. The sender first select an intended file for encryption. Then sends a request to the ES with user-id *(uid)*, file name (f_n), and CSPRN size *(sz)*. A user-defined password or IMEI number of mobile device can be the *uid*. For unique identification of a file which is originating from an MD we use <*uid*, f_n>.

On receiving the request, the ES produces the CSPRN using algorithm-1 and returns the CSPRN back to sender.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

Replication or truncation is required for making size of CSPRN (sz) equal to size of Plain Text (PT) say n. The CSPRN can be replicate (|n|/|sz|) times if sz < n. In case sz > n,truncation can be performed to discard the extra bits. Then user1 can encrypt the file using this CSPRN and save it in the MD. Sender sends the <*uid*, f_n> to user2 for sharing encrypted file. For decryption of the sharedfile user2 sends a request to the ES specifying <*uid*, f_n>, for the CSPRN. ES generates CSPRN of size sz by consults its database with <*uid* , f_n> and forward it to user1. Then user 2 decrypt the file using CSPRN[1].

XORing is the only operation performed in ROBE. In encryption to get CT, PT is XORed with the CSPRN as well as for decryption CT is XORed with CSPRN to get PT.

XORing is a simple and easily implemented in MD. It requires less computations and memory space. By offloading the CSPRN generation task to the ES, the MD can save resources. So, the ROBE protocol is mobile centric and it doesnot need to exchange data in PT format

Algorithm-1 CSPRN Generation

```
Function CSPRN_Generate( size: sz)
        s← random_number();
        sn← random_number();
        CSPRN ← NULL;
        n     ← [sz/128];
while n>0 do
        CSPRN ← CSPRN + AES(s,sn);
        sn    ← sn+1;
        n     ← n-1;
return CSPRN;
```

3.2. Pseudo Random Number Generation

For generating cipher text in a stream cipher we use Pseudo-random number (PRN) which have pseudo-random characters. It is a set of values that are statically random but are derived from a known starting point, called seed and typically the elements are repeated after a fixed interval. The generator can reproduce the sequence for a specific seed valueand thus the PRN are not entirely random so it is calledpseudo-random.

Here we use Advanced Encryption Standard (AES) for generating CSPRN. AES is symmetric-key based cryptographic algorithm. The two parameters required for AES are plain text and secret key. Substitution and permutation are the two design principles of AES algorithm .It makes it faster both software and hardware implementation. Inside the substitution box or s-box the main functionality of AES will occur.

In ROBE, we generate CSPRN of size 192 bit using AES 192 bit. Seed /key (s) and sequence number (sn) are used as parameter for AES. The sn and s are integers and which can be chosen randomly. In each itration sn will increment for producing subsequent 192 bit of CSPRN(C). ES needs a sure transmission of CSPRN to MD. for the secured transmission ES XOR C with pre-shared key(S_k). S_k is also generated bythe ES. It will passed to MD at the time of login. At the MD the C" is converted into C using P_k.. The generation of C" is shown in the Fig. 2.

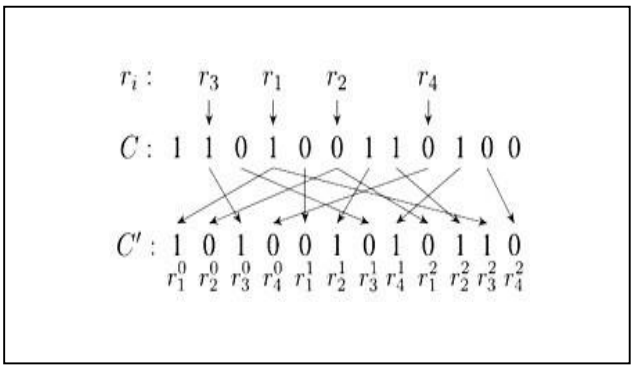

Fig 2. Cryptographically Secure Pseudo Random Number.

4.ROBE SECURITY

For ensuring the security of ROBE the CSPRN (C) is modified into C' in the MD for producing Cipher text (CT). (i.e C ^{k} C' & C' XOR PT CT). Here we also secure the message flow between the users. All these security process willdiscussed in the session.

4.1. Modifying CSPRN

Security of steam cipher depends on the security of CSPRN. Here we use a randomized approach call r-ROBE. Byusing r-ROBE we convert C into C' at the MD. Then C' is XORed with PT to produce CT.

1) r-ROBE: r-ROBE is a randomized approach for modifying CSPRN. In this we use a set of m-random numbers (r_1,r_2,……,r_m), indicating a bit position in the range of 0……(n-1). To increase the randomness of the system order of random number is important in r-ROBE. And r-ROBEperforms single XOR operation.

In r-ROBE, the first *m-bit* is obtained from the initial position of m random numbers. Then the random numbers are incremented by one to obtain the next *m-bit* of C'. Using this same procedure successive bit can be obtained, as shown in fig 3.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

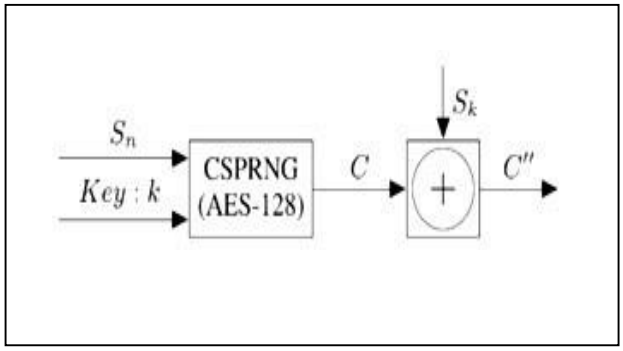

Fig 3. r-ROBE with randomized ke pair:K={ri, 0/1}

The notation r_i^j indicates a shift of j bit from r_i in C. If we change the order of random numbers, the C' change. The relationship of shown C&C' is shown below.

$$C'[jm + i] = C[r^j] = C[(r \pm j) \bmod n], \forall\ i=1.....m,$$

$$J=0.....[n/m]$$

The complexity of the r-ROBE is O(n), as the preprocessing of C to C' requires O(n).the key shared between encryptor and decryptor is (r_1, r_2 r_m).

4.2. Securing The Message flow

Here our goal is to protect all parameters used for fetching the CSPRN from the ES. We assume that all users are registered with the ES with user-name *un* unique user id (*uid*) for accessing its services. We also assume that mobile device and external ES. Use a common one way hashed function for protecting their respective message.

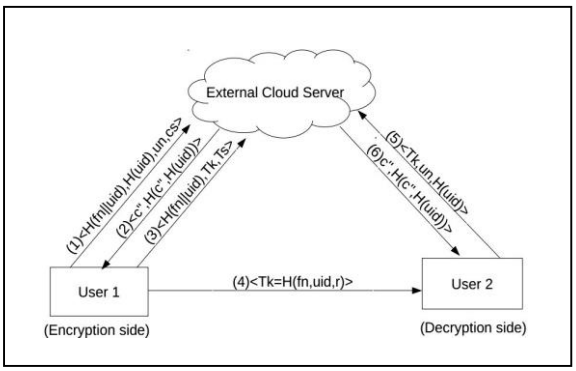

Fig 4. Message flow

Here we have two messages between user1 and the ES respectively. Message 1 includes : un, cz and H(fn || uid), it is the hash value of concatenated file name and user id. Message 2 includes: C'' which is the CSPRN XOR ed with preshared key S_k , and also hash value of C'' and H(uid).

The user1 sends the encrypted file embedded with uid and fn to receiver. Then the user2 sends a request to cloud with uid and fn. After receiving the request the cloud sends C'' to the user2. With the help of S_k user2 converts C'' to C and decrypt CT.

5.RELATED WORKS

Nowadays new challenges and opportunities are introduced in the field of security and privacy. That is related to proliferation of mobile device and maturing of cloud computing technologies. Many works continue to boost the security and privacy of the mobile device storage and processing resources offered by cloud computing. Securityarchitecture and encryption schemes for mobile cloud computing have been proposed by others working to find an effective way to secure data stored on an external server while at the same time limiting the amount of resources such as memory foot print and CPU storage.

5.1. Symmetric and Asymmetric Encryption

There exists much conflict over whether using symmetric or asymmetric encryption schemes are best for data encryption. The resource cost of symmetric encryption allows fast encryption of data. The asymmetric encryption needs more resources to attain same level of security as symmetric encryption. The protocol introduced by Subasree and Sakthivel in [7] use ECC to encrypt data and dual RSA to encrypt the message hash used to ensure integrity. But both these algorithms are asymmetric algorithm, therefore it requires more resources and also it is significantly slow.

Kader et al proposed a New Hybrid Encryption Protocol (NHEP). In hybrid protocols includes both symmetric and asymmetric encryption algorithms. In NEPH protocol, block of data are divided in to half.

The first half is encrypted using AES (symmetric) with ECC (asymmetric), and the second half is encrypted using Blowfish (symmetric), RSA(asymmetric). For both halves, the respective asymmetric encryption is used to encrypt secret key, which is used by symmetric algorithm to encrypt the data. NHEP has a significant edge over other hybrid encryption algorithm.

5.2. FACOR

Flexible Access control with Outsourceable Revocation in Mobile Clouds (FACOR) is a key mechanism to secure out sourced data in mobile clouds. Outsourcing computation is useful tool to allow computational weak clients to deliver time consuming operations to the third parties. Revocation is cryptographic approach to deprive users to access right to out sourced data in mobile cloud computing. Here they consider limited computing capability of mobile devices and manage to outsource the time consuming operations of both encryption and decryption and complicated revocation operation on mobile devices.

In this system there are six polynomial time algorithms. The security of the system is based on q-Decisional Multi-Exponent Bilinear Difie –Hellman Assumption [8]. Therefore the shared key is an asymmetric key, so it is inherently slow and impractical for bulk encryption.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

5.3. Stream Cipher based Encryption Protocol

Our proposed protocol is based on stream cipher based symmetric algorithm. We use AES based algorithm for generating CSPRN (Cryptographically Secured Random Number) in the cloud.

The formation of cipher text is done by simple XORing operation between Plain Text and modified CSPRN. It is quick and efficient process. The cloud sends secured CSPRN to users. The user will encrypt or decrypt the Plain text by using this CSPRN. It consumes very less power and resources for transfer, encryption and decryption of data.

6.CONCLUSION

In this paper, we present a stream cipher based encryption/decryption protocol for mobile devices. We use a MCC environment for implementing the protocol. This paper addresses the challenges of insecure wireless media using CSPRN and securing the message communication.

We use a randomized method called r-ROBE for modifying CSPRN, also we consider the security of the messages exchanged between MD and ES.

REFERENCES

[1] Sandesh Bhatewara, Aman Talreja, Avesh Sapkal, Shalaka Jadhav, “Secure Storage Outsourcing Protocol in Mobile Cloud Computing - a survey paper”, IJESC Volume 62016.

[2] In-Shin Park , Yoon-Deock Lee, Jonpil Jeong, “Improved Identity Management Protocol for Secure Mobile Cloud Computing”, IEEE Conference on System Science 2013.

[3] Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, “Heterogeneity in mobile cloud computing: Taxonomy and open challenges,” *IEEE* Commun.Surveys Tuts., vol. 16, no. 1, pp. 369_392, 1st Quart., 2014

[4] Manmohan Chaturvedi, “Privacy & Security of MobileCloud Computing (MCC)”, IEEE 2011.

[5] Amit Banerjee, Mahamudul Hasan, MD. Auhidur Rahman, Rajesh Chapagain , “CLOAK: A Stream Cipher Based Encryption Protocol for Mobile Cloud Computing”, IEEE Access August 2017.

[6] Sricharan yadavalli, Srinivas upputuri, Dileep kumar, “Mobile Cloud Computing With Safe Security ”, May 2016.

[7] Younghee Park,San Jose State University, Jerry GaoSan ,Jose State University, “A Lightweight Encryptionand Secure Protocol for Smartphone Cloud”, IEEE conference March 2015.

[8] Zhou Shungan1, DU Ruiyingl, Chen Jingt, Shen Jiant, Deng Hua2, Zhang Huanguo,” FACOR: Flexible Access Control with Outsourceable Revocation in Mobile Clouds”, China Communications, April 2016.

[9] E. Fujisaki and T. Okamoto, “Secure integration of asymmetric and symmetric encryption schemes,” Advancesin Cryptology—CRYPTO’99,January 1999.