ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Cryptographically Securing the Data Tansfer to Cloud from Mobile Devices Using Csprn Generation

[1] Sharanya G, [2] Bhargavi KN, [3] Sushma G, [4] Rashmi, [5] Arpitha Vasudev
[1][2][3][4][5] UG Student, CSE dept, SSEC

Abstract: *-* **The way we store and share data has been revolutionized with the help of mobile device and its applications. It is now becoming warehouse to store personal information of the user. The data stored here are mostly in encrypted format, resulting in security threats. In this paper, we propose a protocol called CLOAK which is computationally efficient and light in weight for the mobile devices. CLOAK is based on stream cipher that generates and distributes cryptographically secure pseudo-random numbers (CSPRN) with the help of external devices. Here we use the concept of symmetric key cryptography to enhance the security of the protocol. There are three versions of protocol referred as d-CLOAK, s-CLOAK, r-CLOAK, and these protocols differ on the basis of key selection procedure. To secure data at its origin a core encryption/decryption of a CLOAK is performed within the mobile devices. Here deception method is used ensure the security of CSPRN.Using mutual identity verification all messages are exchanged securely between mobile and the server in a CLOAK. We use Android smartphones to evaluate CLOAK, and for generating CSPRN we use Amazon web services.**

Key Words- **Mobile devices, mobile cloud computing,stream cipher, encryption, decryption, security, cloud computing.**

I. INTRODUCTION

1.Mobile cloud computing MCC is an emerging research area focusing on improving the storage and computational requirements of MD by utilizing the cloud infrastructure. 2.by interacting with cloud MD can provide various services to the users such as health care, mobile commerce, online education. User can store data from their MD to the cloud and can share them with others. 3.since mobile applications sends unencrypted personal information over insecure wireless median to the cloud, hence security is a major concern in MCC.Data encryption is also required for protecting user's data against external and internal attacks within the cloud environment.4.To provide security to user's personal information encryption/decryption algorithms are commonlyused. 5.Encryptionis a process of converting plain text [PT] data into appropriate code called ciphertext [CT] 7. Description algorithm is used for inverting the CT to original PT. In this paper, we focused on encryption and decryption of files for the MD.There are three basic approach for the same.

- The encryption/decryption operations can be performed. within the MD which we refer as mobile centric approach.
- Secondly the MD can offload files and perform the computation intensive encryption/decryption task to the cloud or an external server ES. By offloading the task MD can overcome its resource limitations and can efficiently handle large files in a short time frame.
- An intermediate approach is to share the computation by encrypting the important parts of a file in the mobile devices and offloading the remaining tasks to the cloud.

In this paper, we propose a protocol for encrypting/decrypting files with in the MDs in a mobile cloud environment referred as CLOAK. Our aim is to secure personal information stored in MD of the size in the range 5-10 MBs. The CLOAK protocol based on stream cipher. The advantage of using this stream cipher as a basis of our protocol is that it is less computation intensive compared to block cipher and can easily be handle by existing MDs.

One of the major challenges of a stream cipher is theGeneration and distribution of the key-stream or CSPRN (C).In CLOAK, we offload this task to an external server (ES),In the cloud to save resources of the MDs. In addition, thecloud can be used for sharing the encrypted files with multiplerecipients. To address the security of the CSPRN (C),we propose two level CSPRN modification. Firstly, the C is modified to C'' by the ES before transmitting it to the

MD. This ensures the security of C against the vulnerabilities of unreliable wireless media. we perform another modification on C in the MD to generate C'. The C' is used for the encrypting and can only be decrypted by the recipients having the key.We investigate two randomized s-CLOAK and r-CLOAK and adeterministic approach d-CLOAK for generating C.
Finally, we evaluate the performance of a CLOAK on five different androids based smart phones and use Amazon web services for CSPRN and study the complexity of the algorithm (i.e.time, space, processing power by varying the file size.

II.IMPLEMENTATION

In this section, we discuss the implementational details of theproposed protocol. We begin by introducing a generaloverview for the generation of CSPRN and the basic overviewof the proposed CLOAK protocol. Then introduce thesecurity issues of CLOAK.

A. BASIC CLOAK ARCHITECTURE:

CLOAK is a light-weight, stream cipher based encryptionprotocol for secure data communication between two MDs.The two fundamental operations of a stream cipher are keygeneration and XORing. In CLOAK, the key generation operation can be performed in an ES/cloud and the XORing operation isperformed in the MD to generate the CT.

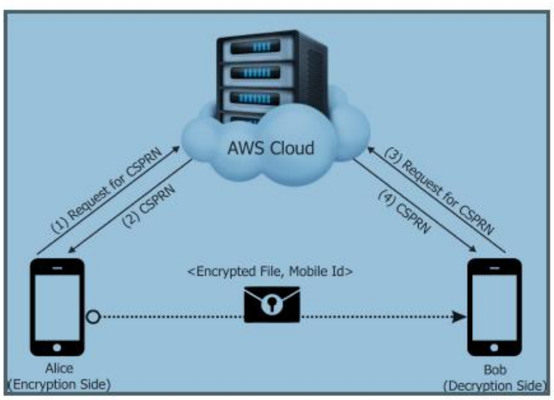


FIGURE 1. Basic architecture of proposed protocol.

There are three main components of the protocol they are clients, the external server (ES) and the communication media (CM), A client can be a smartphone, tablet or a PC that is interested in performing the encryption/decryption operation. In MCC for offloading thecomputationally intensive tasks from resource constrained MD an ES is used. In CLOAK, for generating theCSPRN we use ES. The ES can be specifically configured accordingto the requirement of an application and the workload. Thecommunications between MD and cloud ES can take placevia any wireless communication media such as Wi-fi 3G,4G, UMTS, LTE. The commonly used notations in CLOAK protocol is shown in table-1 In CLOAK, XORing is the only operation performed in the MD. For encryption, the PT is XORed with the CSPRNto generate the CT and in decryption, the CT is again XORedwith the same CSPRN to retrieve the original PT. In our protocol,to handle the memory limitations of the MD, we performchunk-wise XORing operation by gradually reading thefile and CSPRN in chunks of equal sizes. Generally XORingis a simple operation with less computation and memory requirement, which can be easily implemented in MD. moreover, by offloading the CSPRN generation task to the ES, the MD can save resources. So, the CLOAK protocol is mobile centric and it does not need to exchange data in a PT format.

Notation	Description
MD	Mobile Devices
ES	External Server
PT	Plaintext
CT	Ciphertext
CM	Comunuication Media
C, C', C''	Cryptographically Secure Pseudo-random number (CSPRN), Key-stream
PRN	Pseudo-random number
OTP	One Time Password
OOB	Out-of-band Channel
fn	File Name
cs	CSPRN Size
un	User Name
uid	Unique User ID
s	Seed
k	Key
S_k	Pre-shared key between MD and ES
T_k	Token
T_s	Time Stamp

Table 1

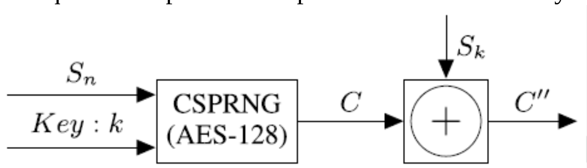
B. PSEUDO RANDOM NUMBER GENERATION

Pseudo-random number (PRN) is a stream of random orpseudo-random characters, used for generating the ciphertextin a stream cipher. It is a set of values or elements that arestatistically random but is derived from a known startingpoint, called seed and typically the elements are repeated aftera fixed interval [50]. The PRN is generated using a deterministicprocess and is reproducible. Since the generator can reproduce the sequence for a special seed value, it is called ``pseudo" random and thus the PRNs are not entirely random. In addition to cryptography, PRN is also used for simulations electronic games etc.

However, in stream ciphers, we mostly use cryptographicallysecure pseudo-random numbers (CSPRNs). TheCSPRNs are unpredictable i.e., it is computationally infeasible to compute thesubsequent bits for some given output bits of the key sstream.

Another way of defining CSPRN is that, fora given `n' consecutive bits of a key stream, no polynomialtime algorithm can predict the next or preceding bits ofthe key stream. There is various method for generation ofCSPRN, such as Middle Square Method Linear Congruential generator etc.

In our implementation, we use the Advanced Encryption Standard (AES) for generating CSPRN. AES is a secure and widely used symmetric-key based cryptographic algorithm, published by National Institute of Standards and Technology (NIST) in 2001. The encryption algorithm of AES requires two parameters: plaintext and a secret key.



Cryptographically Pseudo random number generator.

C. SECURITY ISSUES OF CLOAK

The security of CLOAK depends upon the security of its components (i.e., MD, ES and the communication channels). In the following, we analyze the security of these componentsin detail. The main aim here is to explore the vulnerabilities and to Highlight the security concerns of the CLOAK protocol.

1) Security of MD:Ensuring the security of the MD isthe duty of OS and researchers have proposedvarious mechanism to overcome the security challenges of the same. In CLOAK, we assume that the
XORING and the read/write operation on the PT/CTcan be performed securely within the MD. This is thebasic assumption of any encryption algorithm, i.e., the device on which the cipher is performed should besecure.

2) Security of ES:In MCC, the use of an ES or cloud isincreasing to overcome the resource limitations of the MDs.It is performed by offloading the computationintensive operations to the ES. Providing security ofa shared platform against internal and external attacks is a challenging task and is currently a major researchissue for the Cloud Service Providers (CSPs). In ourcase, security of the CSPRN generator against modification or deletion of code/data is the responsibilityof the CSPs. However, the protocol must ensure thatthe data obtained from a compromised ES (leaked ormodified data) has no effect on the security of theprotocol.

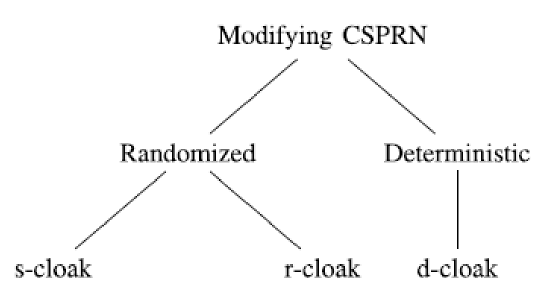
3) Security of CM:One of the basic requirement of a stream cipher is to protect both the CT and CSPRN(Key-stream) from therival. This is the mostchallenging task for the CLOAK protocol since thecommunications between MDs and ES can take placeover an unreliable wireless medium in the MCC environment. Thus, the CLOAK protocol must ensure thatthe adversary retrieves no information about the PT, from CSPRN and/or CT. Thus, in the CLOAK protocol, the main security challengeis to protect the CSPRN and CT pair from the adversary.Note that, the CSPRN and CT can be compromised in oneof the following ways: (a) by fetching the CSPRN from ESand CT from the CM or (b) by compromising the two communicationchannels used for exchanging data between theES and MDs,

III.SECURING CLOAK

In this section, we try to address the above security challenges
in detail. We begin our discussion with the deception technique,
here we investigate techniques for altering theoriginal CSPRN within the mobile devicesfor producing CT. Furthermore, to handle other security attacks, as discussed above, we modify the basic CLOAKprotocol by securing the message communication betweenthe CLOAK entities.

A. MODIFYING CSPRN

The security of a stream cipher depends on the security ofthe key-stream, i.e. CSPRN. Since we consider an unreliable communication medium, we investigate two randomizedapproaches (s-CLOAK and r-CLOAK) and a deterministicapproach (d-CLOAK) for generating modified CSPRN (C). ’



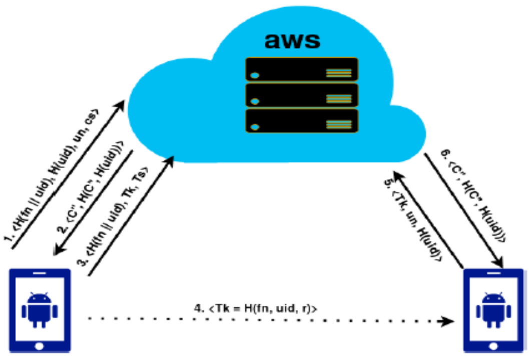
B. SECURING THE MESSAGE FLOW

In MCC, the message exchanges between MD and the ES takes place over insecure CM and is susceptible to varioussecurity threats. In this section, we address the issue

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

bysecuring the messages exchanged in the CLOAK protocol. The goal is to protect all parameters used for fetching the CSPRN from the external ES. We assume that, all users areregistered with the ES with user-name un and unique userid(uid) for accessing its services. We also assume that themobile device and the external ES, use a common one-wayhashed function for protecting their respective messages. The below figure shows the message flow of our protocol.



IV. ATTACK ANALYSIS

The security threats on CLOAK can be imposed in two ways. An attacker may either try to find vulnerabilities in the ES or on CM. In this section, we consider both issues and perform the attack analysis on the CLOAK protocol.

A.KNOWN PLAINTEXT ATTACK AND ALGEBRAIC ATTACK

A known plaintext attack tries to determine the secret key(or key stream in case of a stream cipher) from the knownbits of a plaintext and its corresponding cipher text. Similarly,in an algebraic attack, an attacker tries to recover the secretkey by finding and solving a system of the equation over a limited field. Both attacks try to determine the secret keyusing different procedure. A known plaintext attack is notpossible in CLOAK. This is because, from the known bits ofa PT and CT, the attacker can only determine the correspondingbits of C'. To determine the subsequent bits of C', theattacker needs to know the original CSPRN (C). iif the attacker knows the shared secret key then only the C can be determined. Similarly, an adversary must determine C for a successful algebraic attack. For this, the attacker must perform the algebraic attackon the CSPRN generation procedure, i.e. on AES algorithm in CLOAK. however, the algebraicattack is computationally infeasible on AES-128.

B. IMPERSONATION ATTACK

For this, we consider two cases, i.e. mobile user impersonationand CSPRN impersonation. In CLOAK, user impersonationattack can happen while the mobile is requestingCSPRN from the ES. This can be avoided by verifyingthe authenticity of the user using OTP, as discussed above.Similarly, the same OTP can be used for countering theCSPRN impersonation by an attacker, by hashing the OTPwith the CSPRN.

V.EXPERIMENTAL RESULTS

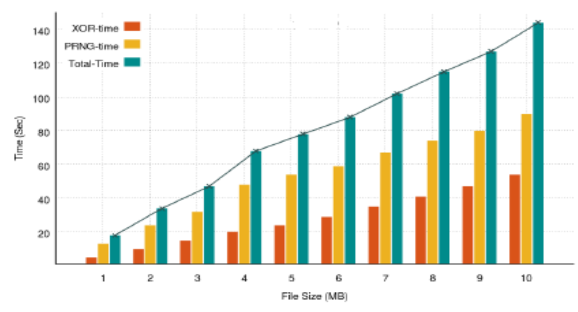
The main factorsaffecting the performance of CLOAK are the time requiredfor downloading CSPRN and the time required to perform the read, write and XOR operations in MD. To evaluate thesefactors, we use two MDs of different configurations, shown intable. We place the CSPRN generator on the AWS cloud. Here we show the total time required for the encryption anddecryption operations and the total time includes the following:

1>CSPRN Time:The time required for sending CSPRNrequest to the external ES, generating CSPRN in the ES,downloading and modifying CSPRN in MD.

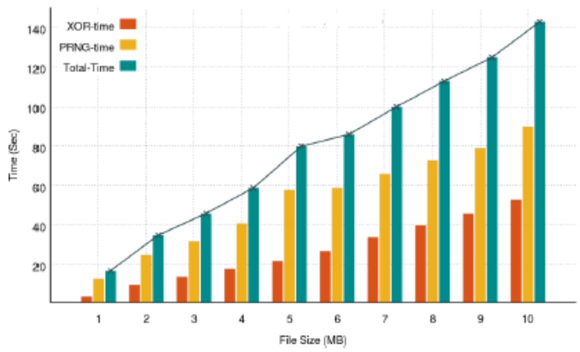
2>XOR Time:Reading the plaintext or ciphertext fromexternal memory, XORing it with CSPRN and writingthe result back to the external memory.

Mobiles	M-1	M-2
Model name	YU Yureka	Xiaomi MI3
OS	Lollipop 5.1	Kitkat 4.4.4
API level	22	19
CPU	Octa-core 1.5 GHz	Quad-core 2.3 GHz
Chipset	Qualcomm Snapdragon 615	Qualcomm Snapdragon 800
RAM	2GB	2GB
GPU	Adreno 405	Adreno 330
Battery	Li-Po 2500 mAh	Li-Ion 3050 mAh

Encryption/Decryption time for r-CLOAK



(a)



(b)

As shown in the above graphs the total time for encryptionand decryption increases with increasing file size and for allcases, the CSPRN time is more compared to XORing time.The CSPRN time depends on various factors, such as thelocation of the ES, the bandwidth of the underlay networksand the workload on the ES. In addition, since the size ofC'is same as the file size, the CSPRN time is also directly proportional to the file size. Our experimental result showsthat the total time varies linearly with increasing file size. To measure the battery performance of ourapplication on the Xiaomi MI3 mobile device havingLi-Ion 3050 mAh battery. We used the ``GSam Battery Monitor" Android applications.To measure the battery consumption,we launched our application and performed the encryptionoperation on two files ranging from 1MB to 5MB. Wenotice a 1% decrease in the battery level, which includesthe power consumed by the screen, Wi-Fi and other backgroundprocesses.

VI. CONCLUSION

In this paper, we presented a light-weight, stream cipher based encryption/decryption protocol for the mobile devices. We can use this protocol for MCC environments Herewe handle the challenges of securing the message communication. Their threevariants of the protocol namely s-CLOAK,r-CLOAK, and d-CLOAK, varying on the modification procedureof CSPRN. The s-CLOAK and r-CLOAK are randomized approaches, while the d-CLOAK is deterministic. We found that CLOAK can resist various security challengeslike known plaintext attack and algebraic attacks and Impersonation attacks. In addition, we studied the security of the messagesexchanged betweenMDand the ES and We have studied the performance of the protocol on two different MDs. Our experimental result shows that theproposed protocol can handle large files in an adequate timeframe.

REFERENCES

[1]. H. T. Dinh, C. Lee, D. Niyato, and P. Wang, 'A survey of mobile cloud computing: architecture, applications, and approaches," Wireless Communication. Mobile Comput., vol. 13, no. 18, pp. 1587_1611, 2013.

[2]. S. Song, B. Y. Choi, and D. Kim, ``Selective encryption and component oriented deduplication for mobile cloud data computing," in Proc. Int.Conf. Comput., Netw. Commun. (ICNC), Feb. 2016, pp. 1_5.

[3] (2015). Pseudo-Random Numbers. (N.D.) Computer Desktop Encyclopedia (1981_2015). [Online]. Available: http://encyclopedia The free dictionary.com/pseudo-random Cnumbers.

[4] D. Barrera, H. G. Kayacik, P. C. van Oorschot, and A. Somayaji, ``A methodology for empirical analysis of permission-based security models and its application to android," in Proc. 17th ACM Conf. Comput. Commun. Secure., 2010, pp. 73_84.