IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

# Advanced Protocol in Cloud Computing

Ms.K.Sindhu[1], Mr.K.Phaneendra2

1.Student of MCA department, Lakireddy Bali Reddy College of Engineering, Mylavaram, Krishna distict, AP.

2.Asst.proffessor, MCA department, Lakireddy Bali Reddy College of Engineering, Mylavaram, Krishna distict,AP.

## ABSTRACT

The enormous development of mobile phones has star produced new type of security defects. The show based consent in android gadgets is one of the strong security dangers among all .We propose shroud convention based encryption. We utilize outside apache server for creating CSPRN and furthermore we make utilization of the session id which will be exceptionally useful in following client sessions and it will be troublesome for the programmers to split the document. For numerous client enlistments we characterize another method for two dimensional graphical verifications utilizing one-time secret word with the session ID to monitor clients. With this, the client can safely handset messages.

**Keywords:** Mobile Computing, Encryption, Authentication, CSPRN, Graphical Authentication, Transmission

## I.INTRODUCTION

Rapid increase in mobile parallels exposing various threats on ABI research the raise in percentage of unique threat is 261% but here we protect our mobiles with password, picture password, pin etc., all these pass code system will be visible to others while you are unlocking it and on the other hand their comes the bio -metric way fingerprint, eye scanner, heart beat scanner, face recognition etc [1]. which is appreciably secured but at some emergency case the device may not be in a position to handle while it may not be possible for access which shows its limitation so in this paper the cryptographic way of securing information is proceeded which brings algorithms into picture to makes the mobile more strong against to get compromise its security on a special note this paper mainly focus on hybrid process through which the data is being secured not only at the storage point but also while pushing the data or at

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

the time ease of access between mobile to mobile or mobile to cloud [2].

The few guidelines for the mobile computing security are

**Encryption-**The encryption of sensitive data must be done at its origin and the data must be stored in the encrypted format and key for decryption must be provided only after proper authentication of the user.

**External Identification-** The mobile devices must be properly labeled with the username and his contact number so that the device can be easily returned to the owner in case if it is lost.

**Storing Limited Data-** The sensitive information must be stored less in local. The users can make use of the proper cloud storage or external storage servers with high security and authentication [3].

**Lost Device Locator-** The mobile device which has secured information has to be tracked from a remote location. There are several third-party applications such as Android Device Manager from Google and icloud from apple which can locate the device, lock and erase them with the network connectivity.

**Passwords and Timeout-** The user has to set a proper password and a timeout if it's left unlocked.

**Trusted Sources**- There are various sources available for application download but the users have to rely only on trusted sources such as Google Play, Apple iTunes store which can reduce the risk of malware to a significant amount

**Updates**- Hackers are creating several new methods for getting sensitive user information and defensive software are running battle for superiority, so the frequent updates of all applications will help the users to keep his data secured.

**Public Networks-** Users have to avoid connecting to the public networks where there is a very limited security for the connected devices and it's easier to theft the sensitive user information

Now the availability of high-speed networks has made accessing the cloud resources easier and it also helps the user to connect with their resource from a remote location. The user can also download a huge range of files from the internet and

It increases the security threats as well. More ransom ware which decrypts all the data and requests the user to send bitcoins for the provision of the decryption key in order to avoid such threats the user has to limit the number of download from the internet.

## II.RELATED WORK

Now a day's mobile devices have replaced by computers and laptop. Mobile phone were used not only for communication but also used for email, chatting, music, playing the games. In mobile phone limited storages space are

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

available so when new file added firstly remove odd files. If we need extra space use of memory card but it is not secure way to store data on memory card. So one of the solution is to store data on cloud. Cloud computing providing anywhere and anytime access to the unlimited access to store data [4].

According to Muhammad Shiraz et al, this paper discusses the cloud computing, mobile cloud computing and explains the different techniques to mobile phone based on resources available within the cloud. The objective is to highlight issues in developing, and implementing mobile applications within MCC domain. One more solution provided to maintain the data securely on clouds through token generation algorithm for secure cloud storage service. In this scheme data stores in cloud encrypted block data from and perform token checking algorithm on this encrypted blocks and verify the data in case of modifications of files before storing to cloud. This approach provided two way verification of file blocks which result ensure that data will not be modified. Mainly security is used term surround the characteristics of integrity, authentication, privacy, and Availability. Now a days we depend on the send information over the network; risk of secure transmission over the networks has also increased. For the secure transmission that term are important for data transmission [5].

## SECURITY REQUIRMENTS

Security requirements are very important in mobile devices and cloud services to protect the information from attacks. Normally, several security services such as availability, authorization, confidentiality, Integrity and Non-repudiation must be applied. The following requirements:

**Availability,** which ensuring that network services are available even in the presence of attacks. Denial of service is the most danger to network availability. Attackers are able to activate attacks which reduce the performance.

**Authorization,** which ensures that only authorized user can be access in providing information to network services. If authentication is not there, then without any difficulty attackers are easily manipulated data into the network.

**Confidentiality** is a fundamental security service. Confidentiality which ensures that to keep privacy of data transmitted among network.

**Integrity**, which ensures that a message cannot be changed or modified by attackers Non-repudiation, which denotes that a node cannot refuse to admit sending a message it has previously sent.

## III.EXISTING SYSTEM

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018

ISSN: 2320-1363

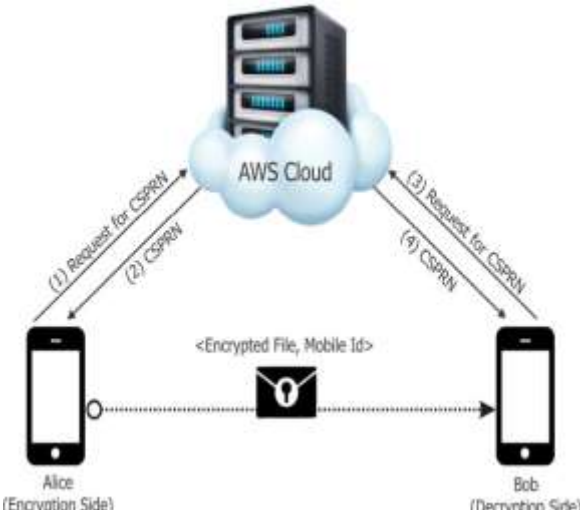



**Fig: 1, Existing System [1]**

The existing system used Amazon Web Service (AWS) cloud and it generated the RID (Random Identification for Device) locally which is sent as a parameter for getting the CSPRN key from Cloud. Most of the mobile devices now use manifestly based permission method which allows the third party application to access the sensitive data. There was just a kind of registration for users and no proper authentications if the intruders get the RID through any third party application then it is easy to get the CSPRN key. The key used here is symmetrical so the same key will be used for decryption purpose. The CSPRN in the cloud is generated through CLOAK Protocol in which the key is generated based on the number of clockwise and anti-clockwise rotations. The CSPRN further generates the symmetric key for encryption and decryption of data

The major concern is that the cost the AWS servers are very much high even tough it is bought on a rental basis and since the locally generated RID is a major flaw in the security of the system and user data

## IV.PROPOSED SYSTEM

For Proper authentication of the user, we use a new way of Graphical Authentication in which each and every pixel in the monitor is considered as the coordinates. The monitor is 2dimensional and we generate a onetime password of 8 digits first 3digit of the OTP points to the X coordinates and other 3 maps to Y coordinates the remaining 2 digits are considered as the dummy for enhanced security [6]. The graphical authentication is more secured since the awareness of this kind of authentication is very much less among the intruders.

The graphical user authentication is alternate to text-based passwords which makes the user easy to remember the password and visual interaction makes them more convenient to work with. The possibility of intruders guessing the password is very less. The authentication server sends the one time password to the user via mail and the user will interact on the screen based on the OTP provided.

The session id keeps track of the user and provides the security post authentication. Both the sender and receiver are allocated with their own unique session id which monitors them throughout the session in

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363

case of any network errors the session id of the user is renewed and all the logs recorded in the previous session is erased. Consider if a hacker is performing an attack and even if he is successful he won't get access to the files since he will be allocated with the separated session id. The session should be monitored, recorded but it has to be deleted once the session gets over.

The entire process occurs in three phases

**Authentication Phase**

In Authentication, the user will get the one time password and the link to authentication monitor is provided along with the one time password the coordinates are provided as a tooltip when the user clicks in the correct location the authentication will be successful and the unique session id is allocated to the user.

**File Upload Phase**

As soon as the Graphical authentication is completed the user is prompted with the panel for file upload and the file will be encrypted based on the CSPRN generated by the external server

**Cloak Protocol**

After the file being uploaded to the server, the cloak protocol starts to encrypt the data using the CSPRN and symmetric key the same key will be used for the decryption purpose the cloak protocol may be either randomized or deterministic

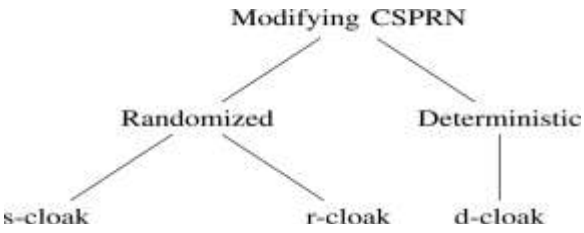
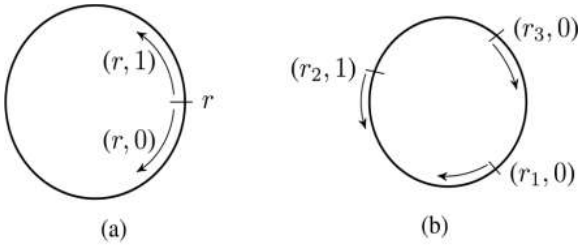



**Fig: 2 Proposed System [1]**

**s-CLOAK:**

There are two random variables are used. One is used to describing the shifts and another one for directions of the rotation. By using factor, it increases the total size of the key pair.

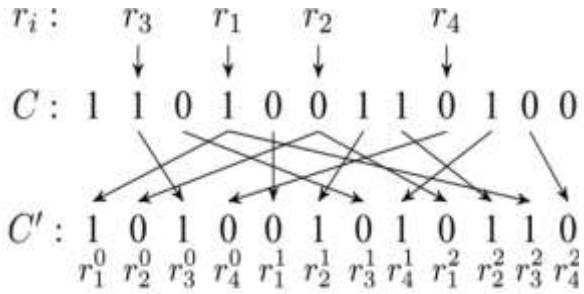



**s-CLOAK with randomized key-pair $k = \{r_l, 0/1\}$.**

**r-CLOAK**

r-CLOAK is randomized cloak used for modifying CSPRN. Using block/chunk-wise both s-CLOAK and r-CLOAK can be implemented. Which is important for memory efficient mobile devices (MDs).

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018 ISSN: 2320-1363




**r-CLOAK with randomized key-pair: $k = \{r_i, 0/1\}$.**

## d-CLOAK

It is the deterministic approach. Where the preset secret key is used for generating modified CSPRN. The encryption process is inverse of the decryption.

## V.CONCLUSION

This is an efficient way for encryption using a cloak Protocol. The CSPRN generation is kept in an eternal server. The session id tracks the user and protects the data transfer from the intruders. The graphical authentication using one-time password is more secured among all the other textual authentication.

## VI.REFERENCES

[1] Amit Banerjee et al.,, CLOAK: A Stream Cipher Based Encryption Protocol for Mobile Cloud Computing, Received July 26, 2017, accepted August 4, 2017, date of publication August 25, 2017, date of current version September 27, 2017.

[2]Pragya Gupta et al., "Mobile Cloud Computing: The Future of Cloud" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue 3, September 2012

[3] Suhas Holla et al., "ANDROID BASED MOBILE APPLICATION DEVELOPMENT and its SECURITY" International Journal of Computer Trends and Technology- volume3Issue3- 2012

[4] Nicolas Lopez; Matias Rodriguez; Catalina Fellegi; Darrell Long; Thomas Schwarz" Even or Odd:Simple Graphical Authentication System "IEEE Latin America TransactionsYear: 2015, Volume: 13, Issue: 3

[5] Marcos Martinez-Diaz; Julian Fierrez; Javier Galballsy " Graphical Password-Based User Authentication With Free-Form Doodles" IEEE Transactions on Human-Machine Systems Year: 2016, Volume: 46, Issue: 4

[6] Karen Renaud; Elin Skjegstand "OlsenDynaHand: Observation-resistant recognition-based web authentication" IEEE Technology and Society Magazine Year: 2007, Volume: 26, Issue: 2