International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 10 | Oct -2017 www.irjet.net p-ISSN: 2395-0072

A Study of Location and Date-Time Encryption of Cloud using Android Application

Aditi Tijage [1], Mayura Ahirrao[2], Madhav Shinde[3], Harshal Wagh[4], Sangameshwari Maitri[5]

[1,2,3,4]Student, Computer Department, Trinity Academy of Engineering, Pune, Maharashtra, India
[5] Professor, Computer Department, Trinity Academy of Engineering, Pune, Maharashtra, India

---

Abstract - - *In recent years, Cloud Security is became an important issue. Encryption has come up with an important solution to providing privacy and security to the data that transmits through the network. By using encryption algorithm, the data is to be transmitted from sender to receiver through encryption and decryption process which will make the transmission more secure. In this system we are developing an android application for securing cloud data using location, date and time based encryption and also developing key using user password, location-Longitude and Latitude, timing i.e. date and time.*

Key Words: **AES, Encryption, Decryption, Cryptography, Cloud Security**

1. INTRODUCTION

Nowadays as everything is becoming digital and online processed, people are getting more attracted towards it as it in terms is more beneficial and useful which reduces the efforts of human being but it arise problems related to security .This gives rise to many problems like hacking or any other security related issue So Security is the main concern nowadays which is very important. So depending on this we are introducing the project application that is location, date and time based encryption using android through cloud. So here cloud security or data security is the main concept of the application which we need to study further.

So basically cloud computing is a concept which allows the users to online access to computing resources like platforms, hardware components, infrastructure, computing applications etc. and store the data through web services instead of computer system. But there are various securities related threats and vulnerabilities over cloud computing. So to avoid these problems cloud security is very much important.

The term "location, date and time based encryption" means that an encrypted data can only be decrypted on a specified date and time at specified location. We are developing security application for cloud data transmission using location, date and time based encryption. If we try to compare, we find that current security system are location independent. So we are developing application which includes not only the receiver's location but also the date and time of decryption in order to make secure transmission of data over cloud. And if anyone tries to decrypt the data at unspecified location or on unspecified date and time, the decryption process fails and returns nothing or in unreadable format. The android device which is going to perform the decryption will determines its location using location sensor, such as GPS sensor. Also it detects the date and time on which it is going to decrypt so that only the genuine receiver can open the decrypted plain text at specified date and time. Location, date and time based encryption can be used to ensure that data cannot be decrypted outside a particular facility also cannot be decrypted on unspecified date and time.

This system can be useful for the headquarters of a government agency or corporation, military communication, defense services, Cinema Theater, etc.

2. PROPOSED WORK

The proposed work contains overall processing of the application using UML diagrams i.e. Activity Diagram and Use case diagram which shows overall view of the data transmission and how the data is processed, encrypted, decrypted and transmitted from sender to receiver using key generation technique which in case is useful for security related issues and proper enhancement of the data to the particular user without knowing to the third party.

The data transmission at both sender and receiver side contains overall flow of the data transmitting and receiving from cloud server data. In this process, we are studying that firstly the sender and receiver both need to Register and Login to the application through the server once register the particular user can Login and verify the password which is to be given while registering password and if the password doesn't verify it again needs to login for the process. Once the password is verified the sender will login and can be able to select the file which is to be encrypted by using encryption related algorithm i.e. AES through Cryptography Related Techniques. Once the sender selects the file after then key generation takes place at sender side where key is to be generated for further transmission of data to the receiver. Key generation is generating a particular key for encrypting and decrypting the data which is the key constraint of the application. Key generation includes a particular key which is very important to encrypt and decrypt the data without

key the receiver cannot decrypt the data which the sender has send to the receiver. The sender will design the key by using alphabetical, mathematical expression or mixture of it which sender will generate and can send to the receiver through mail or message. With the key the sender also needs to send the location, date and time to the receiver for further decryption process at receiver side .Once the key is generated the encryption of data will take place using cryptography concept i.e. data inside data, the sender will encrypt the original data in particular unencrypted file i.e. a text format file which in case will be a text file but when decrypted will get the original data. Once encryption process is done the encrypted file can be uploaded on the server and can be send to the particular receiver. This was the overall process at sender side encryption.

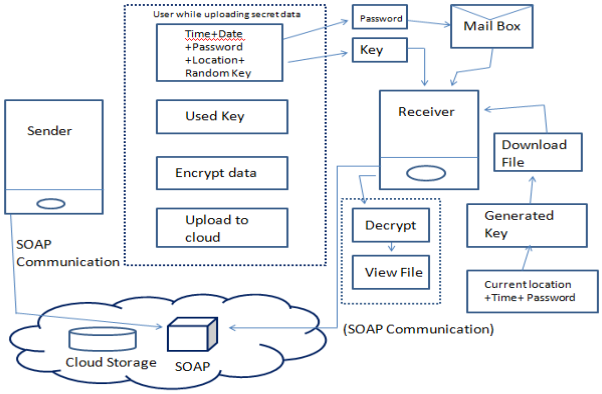

Fig -1: Proposed Model

After encryption process at sender side it includes decryption process at receiver side where receiver too needs to register for transmission process once register the receiver needs to login and verify the password and if the password doesn't verify it again needs to login for the process once verified the receiver logins to the application and can receive the file which sender has send. Once the file is received there are multiple files present where sender selects the particular file which is to decrypted and send by the receiver. After selecting the file , to decrypt the particular file the receiver needs to enter the key which is receive by the receiver from the sender through communication media and the data need to be decrypted at that particular location , date and time given to the receiver by the sender through email or message. After entering the key it will decrypt the file and will get the original data in decrypted format only on that particular date, time and location if the file is not decrypted on that particular date, time and location it will show the unreadable format of data. So the receiver needs to decrypt the data at that particular location date and time by entering the key given by sender Once the key is entered the data will be decrypted at receiver side and the receiver will get the original data in decrypted format which contains the original message send by the sender under the text format file using cryptography technique, key generation technique and AES algorithm.

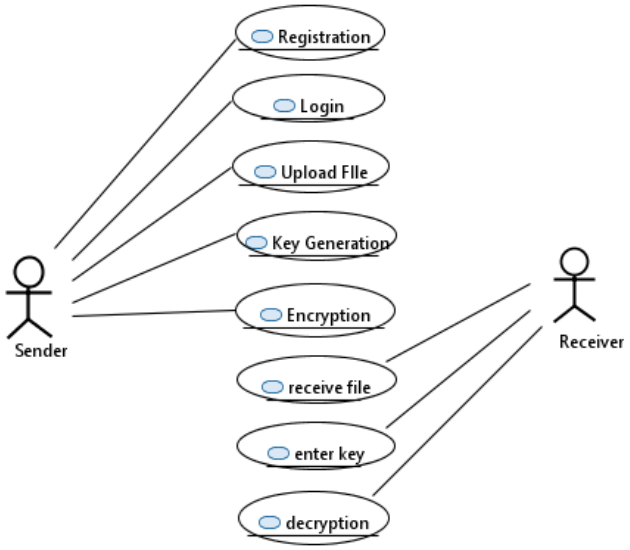

Fig -2: Use Case Diagram

Above Fig -2 contains the Use case diagram which contains all the actions and the tasks performed by the sender and receiver at the time of transmission process. The sender includes the actions like Registering to the application for further process, Login which includes the User ID and password with which sender and receiver can transmit and receive the data through login details, sender will Upload the file which is to be encrypted and send to the receiver for decryption process, Key generation which includes generating key for encryption using AES Algorithm for encrypting and decrypting data through cloud, Encryption which includes encrypting the data in file format i.e. hiding the data inside the data at the particular location date and time . This are the tasks performed at sender side. Receiver side performs the tasks like Receiving the file receive from the sender, Entering the key which the sender has been send to the receiver through email process, Decryption at receiver side at that particular location date and time given by the sender to receiver through email or message send by the sender for decryption process.

3. RELATED WORK

3.1 A Location Based Encryption Technique and Some of Its Applications

This paper [1] helps us to know importance of geo-encryption for data security and gives brief idea of location based encryption technique and its applications where Geo-encryption is a concept for location-based encryption which can be used to establish cryptographic related algorithms and protocols. This paper mainly focuses on data to be

encrypted and decrypted on a specific location to avoid location spoofing and provides strong protection.

Location Based Security for Online Transaction

This paper [2] discusses on cloud security and its challenges briefly. This paper uses location based encryption technique and Geo-Encryption algorithm for providing security to the banking application which only allows authenticated people for doing transactions. It allows the user to access the application at various locations. In this process location is a key constraint for encryption and decryption process through cryptography technique.

3.2 Preserving Location Privacy in Geo social Applications

In this paper[3], LocX is introduce which is a location to index mapping that provides significant location privacy without adding uncertainty into query results. The main purpose is to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server. Due to this it can help the server to correctly evaluate the location queries.

3.3 A Modified Location-Dependent Image Encryption for Mobile Information System

In this paper [4] a cipher Text format of data is developed using Location dependent encryption key where permutation and rotations are used as a primary concept to obtain distorted images. This approach is used for location dependent encryption for mobile information system. Once the target coordinate matches with GPS receiver coordinates then only the client can decrypt the cipher Text.

4. CONCLUSIONS

In this paper we are studying that the system is for developing an android application for securing cloud data using location, date and time based encryption. This application will be beneficial for providing security for transferring the data secretly without knowing to the third party through AES algorithm technique using cryptographic concept.

ACKNOWLEDGEMENT

The authors would like to thank all the reviewers and advisors for their helpful suggestions to improve this paper. We would also like to give special thanks to our Head of Computer Department Prof. S. N. Maitri madam for her valuable guidance and support.

REFERENCES

[1] L. Scott, D. Denning, "A Location Based Encryption Technique and Some of Its Applications", Proceedings of ION NTM 2003..

[2] Dipak Auti1, Krishna Landage, Swapnil Chavan, "Location Based Security for Online Transaction", IJIRCCE.2016.

[3] Krishna P.N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, "Preserving Location Privacy in Geosocial Applications", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 1, JANUARY 2014.

[4] Prasad Reddy P.V.G.D et al., "A Modified Location-Dependent Image Encryption for Mobile Information System", International Journal of Engineering Science and Technology Vol. 2(5), 2010.