International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

Secured data transmission by LDT Encryption using Android Application with Data monitoring Tool

Aditi Tijage [1], Mayura Ahirrao[2], Madhav Shinde[3], Harshal Wagh[4], Santosh Darade[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 generating key using location-Longitude and Latitude, timing i.e. date and time, whereas we are detecting the tampering of data by using data monitoring tool.*

Key Words: **AES, Encryption, Decryption, Cryptography, Data monitoring tool, SHA, 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. In this system we are introducing Data monitoring tool which is used for detecting of tampering data in the system as data tampering can harm the system processing and can spoil the data. So to avoid this we are using SHA i.e. Secured hash algorithm which can be used to verify the contents in data and monitor the system data and can check the stored hash and current hash. But if we consider that the attacker attacks the system & tries to modify the data in encrypted format, then data monitoring tool will send an alert of change in data to the sender.

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

2. RELATED WORK

2.1 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.

2.2 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.

2.3 Preserving Location Privacy in Geosocial 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.

2.4 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.

3. PROPOSED WORK

Encryption is the process of hiding the data inside data which can be used for security related constraints like maintaining the security for various transactions of data transmit and receive. This encryption technique provides various additional security related features which are mostly required nowadays. In this application we are using this additional security feature to introduce location date and time encryption process, once the encryption process is done it can access the decryption of the data at that particular location data and time which is specified. It gives various additional security layers through which the data remains secure . As highly use of data is increased so there are various issues in data processing as the data can be hack or can damage so to avoid this data monitoring tool i.e. data verification is introduced which in terms can verify the attacks and different users which can damage or hack with the system or the data.

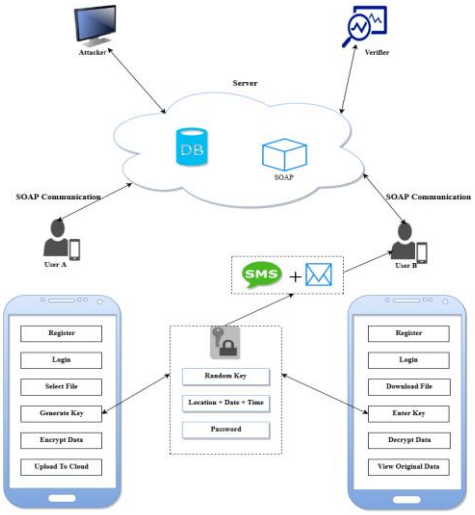


Fig System Architecture

This paper tries to present the data securing and monitoring of data to improve the applicability and efficiency of the data. This application can be used by two users which are sender and receiver to transmit and receive the data securely. The process of sending the data i.e. in message form, is in encrypted format i.e. the data in Cipher text format and this cipher text format which is unreadable format can be decrypted at receiver side at that specified location, date and time to get the original plain text format which is readable form.

3.1 Login and Registration

In this module, registration is the first process user first need to register by providing its personal details like user first name, last name, username, password, address, email id, mobile number, etc. Once the user registers OTP is generated, then by entering that OTP user can login by using that particular user ID and Password which he has given while registration user can Login Into the application.. In this module database is used in the system to store the details of registered user. To create the Database MySQL is used. MySQL is a relational database management system contained in a small C programming library.

3.2 Admin Location Retrieval

In this module, manage location Form is generated which is used to manage the location by using auto location or by manually specifying location. Here GPS is used for specifying latitude and longitude of the location of the user. By using this user can get different location where the file is to be decrypted i.e. it manages all location related tasks. It keeps track of all registered users and can provide the facilities like update, add and delete locations for transactions.

3.3 File Upload and Encryption

In this module, the file is selected from file manager by clicking on "select file" option. Once the file is selected which is to be encrypted sender can select the particular receiver to which the encrypted file is to be send. The sender generates a random key which further can be used for decryption process to decrypt the message. Uploading module contains "Generate key" option which generate the key and let the user select location, date and time where the data can be decrypted. Once the file is selected which is to be upload the particular file can be uploaded on the server. This application uses AES encryption technique which is used for encryption purpose.

AES is an advanced encryption standard algorithm. AES algorithm is symmetric and can be used to provide wide security. This algorithm is faster for encryption and decryption as compared to others. For more security purpose derived keys are used in combination which are called as combined keys. This combined key are made up of AES key and location, date and time parameters. Once the file is uploaded it gets the pop up message or notification "file upload successfully".

3.4 File Download and Decryption

Once the file is uploaded at sender side the receiver can login and can get the uploaded file by clicking on downloads. Once he gets the uploaded encrypted file the receiver can download it. Then the file can be downloaded by using download option from the menu form, then it displays list of files to download then the user can select the particular file which is to be decrypted once the file is downloaded it is in encrypted format then to decrypt this file, receiver needs to be present at that particular location, date and time and then the user can decrypt the encrypted file which sender has encrypted and can get the original contents of the file. This is all decryption process which happens at receiver side to decrypt the encrypted file and get the original data which is in encrypted i.e cipher text format. And after successfully processing of decryption process the receiver can get the original message which sender needs to send by maintaining the security constraints.

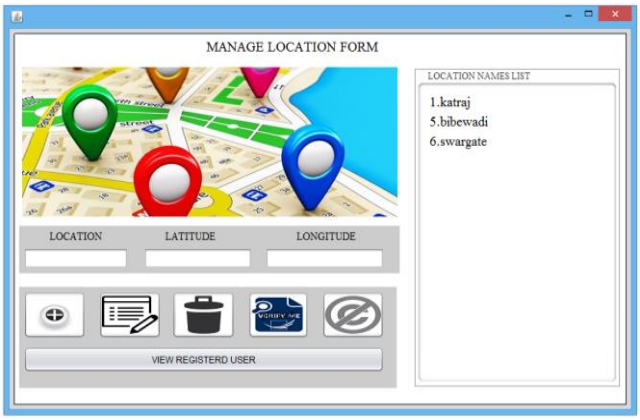
3.5 File Verification

This is used for verification of the data by suing SHA algorithm. Once user uploads the file to cloud server SHA would be applied on the file and stored in the database. It Contains the Verifier module and Attacker Module. The verifier module will continuously monitor on the files and check the stored hash and current hash of the files. The attacker we have designed to that can read files and can make some changes in that file. But if the file contents have been changed then the verifier will compare it with the stored hash if it matches then process will continue else if it doesn't match then it will generate an alert regarding it.

4. IMPLEMENTATION:

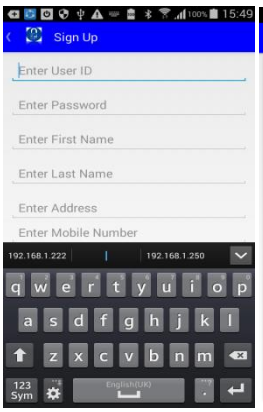
This application is using Android Operating system for implementation as Android is widely used OS nowadays as it provides different tools and libraries which are used for building rich applications. Android is a Linux based OS where application are written in java. Android provides different API's to work with different services such as GPS for location tracking, global timing for standard time specification and also allows communication between two or more devices by peer to peer network.

As 'n' number of users communicating throughout the world with each other through 'n' number of places so wide amount of data is exchanged. Due to this, data is send and received simultaneously so data is not secured. For securing this data we are introducing the android application which is based on location, date and time encryption with data monitoring tool.



(a) Manage Location Form

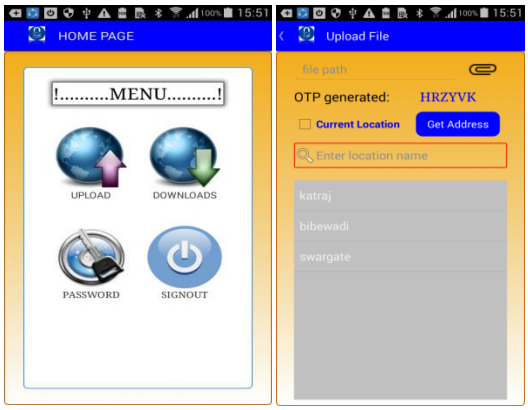
Here Fig(a) is for managing locations and specifying different location for different users manually or automatically. It also helps to keep track of all registered users. Using this one can able to add, update and delete location. It also contains the verifier tool which verifies the transferred file is original one or not.



(b)Sign Up Form

(c) OTP Verification

In fig(b), Sign up form is generated which is used for Registration of new user. User can registers in the app by providing personal details like user id, password, first name, last name, address and email. All these details entered are further checked with database entries when user tries to login with his User ID and password. If match is found then user will get an OTP on his registered mobile number and email ID (refer Fig(c)). After entering the received OTP, then OTP is verified. If the OTP matches, user can able to login and use the application.



(d)Main Form **(e) Selecting File**

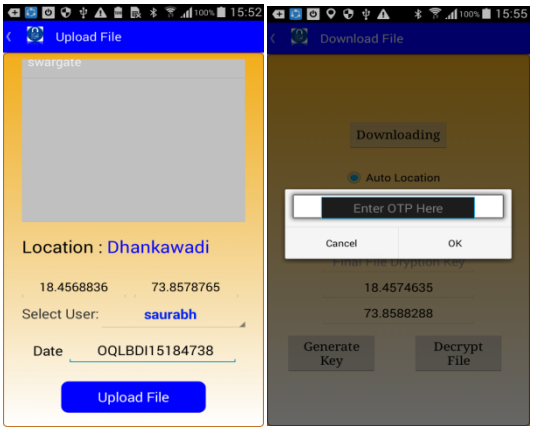
In Fig.(d), after login into the application, main form i.e. Menu page of the application appears which include

1.Uploading – file is uploaded for encryption

2.Downloading – Uploaded encrypted file will decrypt and can be available for download.

3.Password Authentication –It contains password related identification and specification which includes Forgot Password and Password Change.

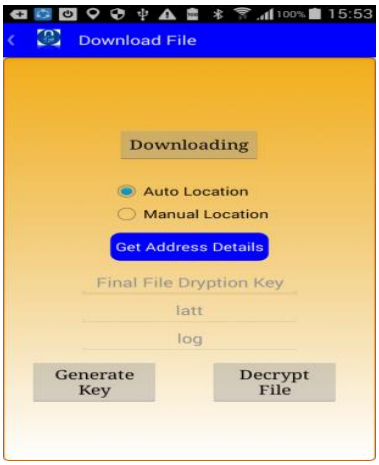
4.Sign Out- It contains signing out once the process is done.



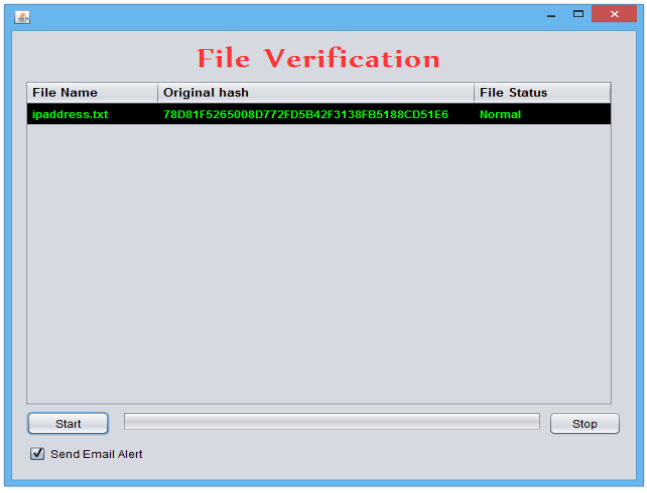
(f) Uploading File **(g) OTP for Downloading**

Here in Fig (f), it contains uploading of the file which is to be encrypted and further then decrypted. It contains location at which file is to be decrypted, OTP through which the file can be uploaded for encryption process and also need to mention the particular date and time where the file is to be decrypted.

Once the file is uploaded the receiver can download the file by using its login credentials which may contain user ID and password, once the receiver logs in he can download the particular file by entering OTP which he can receive at the time of login and once the OTP is entered the user can download the file which is shown in Fig(g). Similarly in Fig(h)it is shown that how the file is downloaded by using auto location, once the Auto Location is selected it can show the latitude and longitude of that particular location where the file is to be decrypted. Once the location is selected we can select the option of decrypt which will show us the decrypted file.



(h) Downloading File



(i) File Verification

Here Fig (i) contains file verification which is used for data monitoring technique, it verifies and check the data entered is tampered or not. It checks all the contents and verifies all the contents are proper. As attackers can attack and damage the file and will try to hack, mess up or

damage the contents of the original file just to avoid this file verification module is used so that to show the attacks and can detect the attacks which can happen and can store the original contents. This process is done by using SHA i.e. Secured Hash Algorithm which maintains the hash record of each content and specifies the attacks and give the resultant Original data.

5. CONCLUSION

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. Santosh Darade Sir for his 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 ImageEncryption for Mobile Information System", International Journal of Engineering Science and Technology Vol. 2(5), 2010.