ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A Digital Location Based File Locker using Android Application

Surabhi Juneja, Swapnali Kendre, Parinita Chate

Student, Dept. of Computer Science, BVPCOE, Savitribai Phule Pune University, Pune, India

Student, Dept. of Computer Science, BVPCOEL, Savitribai Phule Pune University, Pune, India

Associate Professor, Dept. of Computer Science, BVPCOEL, Savitribai Phule Pune University, Pune, India

ABSTRACT: In today's world, use of mobile devices have increased the transmission of data and communication among people around the globe very rapid, simple, effortless and accessible. The biggest problem arising in communication is the security of data. To overcome this problem, many techniques are used. Data encryption is one of them. In this paper, we have discussed about the location and time based data encryption. This is one of the most innovative technique. In this technique, data can be encrypted and decrypted using time and location of targeted region. For the implementation of our proposed work, we have used smart phones via which target latitude and longitude are used to send the data. Sender sends the data to receiver using location, latitude, longitude, time and date as parameters. To provide security to the file, user sets a password or in other words called as key. This key data is send to the receiver for the decryption securely through a message. We have used Advance Encryption Standard (AES) algorithm which is known to all the attacks and is very reliable. Using this symmetric key, receiver downloads the file if he/she is present at the targeted location within that time constraint and on the decided date. For secure data transmission, different algorithms are used such as, AES (Advance Encryption Standard) as mentioned above, Discrete Centralization algorithm for real time accuracy in location, SHA-1 i.e. Secure Hashing for passwords.

KEYWORDS:AES, Encryption and Decryption, Discrete Centralization, SHA-1.

I. INTRODUCTION

Our idea is providing a mechanism where we are providing security to the data which is location based. The data which is stored on the server (cloud), is secure due to encryption being applied to that. In cryptography identity component is important, we can specify use- name, address, e-mail id, mobile number as identity, but we can also give place (i.e. Physical presence at a particular location) as identity. This place can be used in encryption. Nowadays, the use of wireless technology goes on increasing as an increase in the wireless applications. To provide a higher layer of security to such application, different data encryption algorithms are used. But traditional data encryption algorithms are location independent. In our proposed work, we are creating an application, which is location based means, we have introduced a new concept for secure communication.

In this paper, we are providing a mechanism which is based on Android systems that allows smartphone users to communicate securely and transfer their information at different contexts. The authenticated receiver will only be able to download the file if he/she is present at the target location as set by the sender also within a specific time constraint and at that particular date as configured by the sender. Otherwise, the file will not be able to download. We are using AES algorithm, for the encryption and decryption process, as it is resistant to all known attacks. The key that is generated will be a combination pack of location (latitude &longitude), time, date, password as set by the sender. Here, in our proposed work, the key size used is 128 so, the number of rounds as per AES algorithm will be 10.

The terms location-based encryption or geo-encryption are used to refer to any method of encryption in which the encrypted information, called cipher text, can be decrypted only at a specified location. If, someone attempts to decrypt the data at another location, the decryption process fails and reveals no details about the original plaintext information.

DOI: 10.15680/IJIRCCE.2017. 0504227

The device performing the decryption determines its location using some type of location sensor such as a GPSreceiver. Location-based encryption can be used to ensure that data cannot be decrypted outside a particular facility - for example, the headquarters of a government agency or corporation or an individual's office or home. Alternatively, it may be used to confine access to a broad geographic region. Time as well as space constraints can be placed on the decryption location

According to our discussion, this approach can meet the, authentication, simplicity, confidentiality and practicability of security issues. Therefore, the proposed approach can meet the demand for personal and industrial data security.

II. Related work

In [1] this paper, we have proposed EPLQ, an efficient privacy preserving spatial range query solution for smart phones, which preserves the privacy of user location, and achieves confidentiality of LBS data. With the pervasiveness of smart phones, location based services (LBS) have received considerable attention and become more popular and vital recently. However, the use of LBS also poses a potential threat to user's location privacy. In this paper, aiming at spatial range query, a popular LBS providing information about POIs (Points Of Interest) within a given distance, we present an efficient and privacy-preserving location based query solution, called EPLQ.[2] In our method we use the user's location and geographical position and we will add a security layer to the existing security measures. Our solution is more appropriate for banks, big companies, institutions and examples like this. The only thing we need is an Anti-Spoof and accurate GPS that company can afford to buy. Also implementing the location-dependent data encryption algorithm (LDEA), on the cloud and the user's computer (which is connected to the GPS) is required.Our idea is providing a mechanism where we providing the security for cloud data which is the location based. The user transaction data is stored on the cloud which is secured by applying the encryption on that. Security has always been an integral part of human life. People have been looking for physical and financial security. With the advancement of human knowledge and getting into the new era the need of information security were added to human security concerns. Data is encrypted only when person is having private key can decrypt it. In cryptography identity component is important, we can specify name, address, id as identity, but we can also give place (i.e. Physical presence at a particular location) as identity. This place can be used in encryption. We trust physical security more. Those are inside (part of) particular geographical area is approved for data decryption otherwise not allowed. Another use of Location Based Cryptography is access control. (Ex-accessing printer in a room but cannot access outside of room.). In [3] In this paper we have presented a location based query solution that employs two protocols that enables a user to privately determine and acquire location data. The first step is for a user to privately determine his/her location using oblivious transfer on a public grid. The second step involves a private information retrieval interaction that retrieves the record with high communication efficiency. In the first stage, the user privately determines his/her location within a public grid, using oblivious transfer. This data contains both the ID and associated symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR , to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage. Our protocol thus provides protection for both the user and the server.

III. Proposed algorithm

A. *Design Considerations:*

In this section, we describe the design of our application in detail.

- **Terminology and Attacker Model:** Whenever it comes to location coordinates, it refers to the longitude, latitude pairs associated with real-world locations. GPS returns the pair of coordinates and is used to associate data with a location. Location data or location information refers to such data associated with a location. In this paper, users store their data on the servers to obtain the service. In our attacker model, we assume that the attacker wants to access the encrypted data and tries more than 1000 times of iterations to crack the data and obtain the key to decrypt the data for example, for our proposed work we have applied Brute Force attack to our system. This attacker could be an employee of the company running the service or an outsider that compromises the servers. We assume that the attacker does not perform any attacks on the consistency or integrity of data on the servers, but aims only to learn users' location as well as his information.

- **Basic Design:** The description of our proposed work and basic design of our application is given below:

  - As listed in our requirements, the server is storing three queries i.e. about the user information, location information, and file information. User's information such as (user's id, file name, location name, address, mobile no, e- mail address, and password). Similarly, location data (location id, location-name, latitude, longitude) and regarding the file information(id(primary-key),UseA(uploader_id),UserB(receiver_id), file name, file data, date selected when to download the file, time offset, latitude offset, longitude offset) all this data is stored with the server in the database.
    - The basic architectural diagram is shown below:

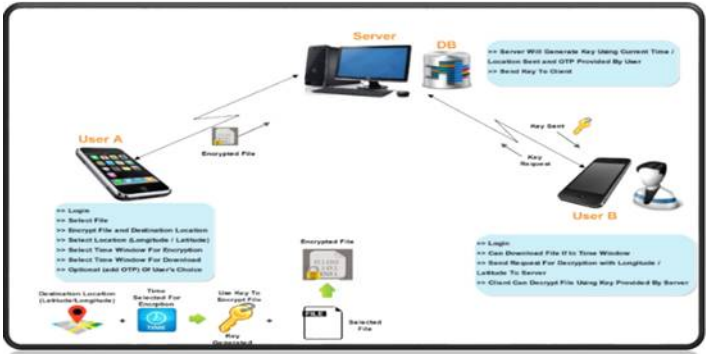
Server
DB
>> Server Will Generate Key Using Current Time / Location Sent and OTP Provided By User
>> Send Key To Client
User A
Encrypted File
Key Sent
Key Request
User B
>> Login
>> Select File
>> Encrypt File and Destination Location
>> Select Location (Longitude / Latitude)
>> Select Time Window For Encryption
>> Select Time Window For Download
>> Optional (add OTP) Of User's Choice
Encrypted File
>> Login
>> Can Download File If In Time Window
>> Send Request For Decryption with Longitude / Latitude To Server
>> Client Can Decrypt File Using Key Provided By Server
Destination Location (Latitude/Longitude)
Time Selected For Encryption
Use Key To Encrypt File
Key Generated
Selected File

Figure01: Basic Architectural diagram.

B. *Description of the Proposed Algorithm:*

The proposed algorithm is consists of three main steps. The encryption of the file is done using the Destination location(latitude/longitude), time selected, date selected for download the file therefore, all these parameters will together form a combination key which is send to the receiver via mobile message to decrypt the file and download it.

Advance Encryption Standard(AES): The most popular and widely used symmetric key encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is six time faster and stronger than triple DES.AES performs all its computations on bytes. Hence, AES handles the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. It have 128/192/256 bit keys

- Step 1: Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below –
  Byte Substitution (Sub-Bytes):
  The 16 input bytes are substituted by looking up a fixed table given in design. The result is in a matrix of four rows and four columns.

- Step 2:**Shift-rows**:
  Each of the four rows of the matrix is shifted to the left. Cyclically shifts the bytes in each row by a certain offset. Shift is carried out as follows:
  First row is not shifted.
  Second row is shifted one byte to the left.
  Third row is shifted two byte to the left.
  Fourth row is shifted three byte positions to the left.
  The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

- Step 3: **Mix-Columns:**
  This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

- Step 4**Add Roundkey**:
  The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher-text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

- Step 5**Decryption Process**:
  The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order.

IV. IMPLEMENTATION

Implementation based on the pseudo code used as mentioned on above steps of AES algorithm:
Location based encryption is an enhancement to traditional encryption methods that makes use of location of user, time to provide security to data. It limits decryption of information to specified locations and times. Any attempts to access the secure information at an unauthorized location will result in a failure of the decryption process fails. We try to present a discrete location method to improve its applicability and efficiency. The location based encryption can be implemented as an android app. The app is used by two users, the sender and the receiver to transfer data securely between them. The message to be send is encrypted into cipher text by the sender and it is decrypted at the receiver side to get the plain text. Receiver can only decrypt the cipher text when he is at the specified location and at specified time.
The components of the proposed system are:

A. Login and registration
B. Upload file
C. Encrypt and Decrypt file
D. Download file

In this module user first register in to the app by giving their personal details like user-id, username, mobile no, target location, password, e-mail id. User will login to mobile application using username and password. We have used MySQL database.

Sender will login by using user-id and password. After login user will pick file and upload the file after uploading sender enter location, time and date of receiver and sender will put a key and locks the encrypted file.
Same as sender receiver will login and download the file after downloading user enter the OTP and decrypt the file.

V. SCREENSHOTS &RESULTS

The simulation studies involve the deterministic small network topology with 5 nodes as shown in Fig.1. The

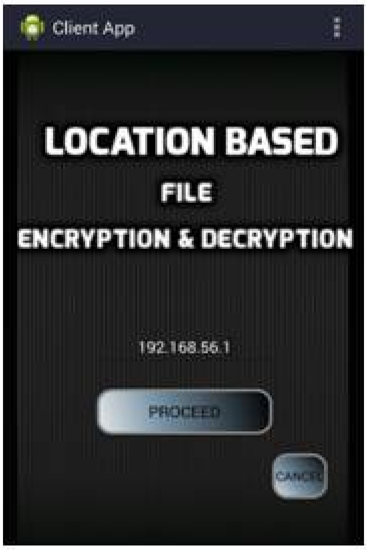

Figure02: Creating private network By using IP address (connecting Client application and server)

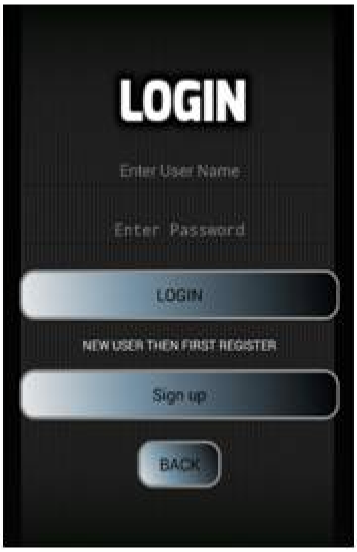

Figure 03: User Signup/Login

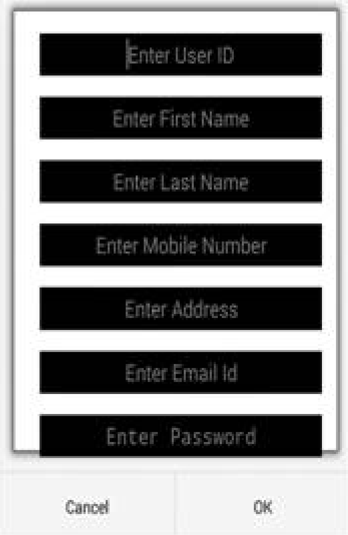

Figure04: Fill the credentials.

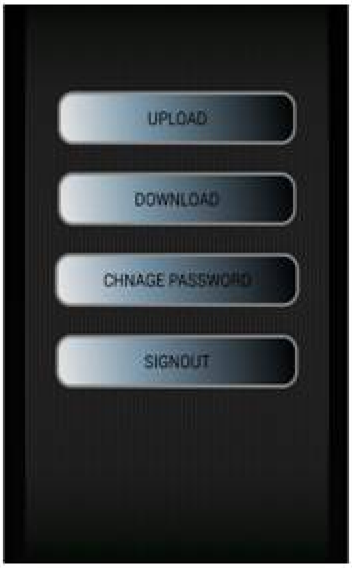

Figure05: Upload the file to send.

VI. CONCLUSION AND FUTURE WORK

In this paper we have presented a location based communication for confidential data to be transferred using Advance Encryption Standard (AES) and discrete centralized algorithms. The first step is for a user to put target location using latitude and longitude. The second step involves that the receiver being present at that target location and download that file. We analysed the performance of our protocol and found it to be both computationally and communication ally efficient. We implemented a software prototype using a desktop machine and a mobile device. The software prototype demonstrates that our protocol is within practical limits.

For the further research, the future scope will involve testing the protocol on many other smart phones. Also, we need to reduce the overhead of the internet connectivity as it needs a very high speed internet supply. Problems may arise for more security and authentication, one solution exists for the case, they can add image based passwords for authentication purpose and also biometrics can play a secure role here. Our work is based on android operating system, can further be expanded to IOS.

.

REFERENCES

1. Lichun Li, Rongxing Lu, *Senior Member, IEEE* and Cheng Huang, “EPLQ: Efficient Privacy-Preserving Location-based Query over Outsourced Encrypted Data”, IEEE INTERNET OF THINGS JOURNAL, VOL. XX, NO. XX, MONTH 2015.
2. Russell Paulet, Md. Golam Kaosar, Xun Yi, and Elisa Bertino, *Fellow, IEEE,”* Privacy-Preserving and Content-Protecting Location Based Queries”, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 5, MAY 2014.
3. Krishna P.N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Fellow, IEEE, Amr El Abbadi, Christopher Kruegel, and Ben Y. Zhao ,“Preserving Location Privacyin Geosocial Applications”,IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 1, JANUARY 2014 159.
4. Swapna B Sasi, Betsy K Abraham, Jinil James, Riya Jose, “Swapna B Sasi, Betsy K Abraham, Jinil James, Riya Jose”, IJCAT – International Journal of Computing and Technology Volume 1, Issue 1, February 2014.
5. Prasad Reddy. P.V.G.D*, K.R.Sudha, P Sanyasi Naidu , “A Modified Location-Dependent Image Encryption for Mobile Information System”, International Journal of Engineering Science and TechnologyVol. 2(5), 2010.

BIOGRAPHY

Surabhi Juneja is a student of Computer Engineering Department in Bharati Vidyapeeth’s College Of Engineering Lavale, Pune, India. Her research interests are Data Mining, Data Security, and Database Management. Currently, working on a project of Data Security and Android Application.

Swapnali Kendre is a student of computer engineering Department in Bharati Vidyapeeth’s College Of Engineering Lavale, Pune, India. Her research interests are Data Mining,Cyber Security & Forensics. Currently, working on a project of Data Security and Android Application.

Parinita Chateis an Associate Professor of Computer Engineering Department in Bharati Vidyapeeth’s College Of Engineering Lavale Pune,India. Her research interests areCloud Computing, Computer Network, and Operating System. Currently, she isan internal guide on variousprojects of Engineering Applications. Also, she has completed her research in Cloud Computing.