Location Based Encryption for Cloud Data Security

Kadam Snehal, Naikodi Ravina, Waykar Rasika, Prof.Jadhav Nitesh

Abstract— **Mobile Android applications often have access to sensitive data and resources on the user device. Misuse of this data by malicious applications may leads to privacy breaches and sensitive data leakage. An example would be a malicious application recording a confidential business conversation. The problem occurs from the fact that Android users do not have control over the application capabilities once the applications have been granted the requested privileges upon installation. In many cases, however, whether an application may get a privilege depends on the specific user context and thus we required a context-based access control mechanism by which privileges can be dynamically granted or revoked to applications based on the specific context of the user. This system proposes such an access control mechanism. The implementation of context differentiates between closely located subareas within the same location. The system modifies the Android operating system so that context-based access control restrictions can be specified and enforced. The several experiments are performed to assess the efficiency of access control mechanism and the accuracy of context detection.**

Index Terms— **Access Controller (AC), Data Encryption Standard (DES), Global Positioning System (GPS), Cellular Triangulation (cell ID).**

I. INTRODUCTION

Security has always been an integral part of human life. People are concern about their confidential data. 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 belief physical security more. Those are inside (part of) particular geographical area are 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.)We are developing banking application using Location Based Encryption. As compare to current banking application which are location-independent, we are developing banking application which is location dependent. It means in Cryptography Cipher-text can only be decrypted at a certain location i.e. location-dependent approach. If an attempt to decrypt data at another location, the decryption process fails and reveals no information about the plaintext[2]. This is important in real time application, example in military base application, Cinema Theater. But our system is flexible enough to provide access to customer to his/her account from any location. Our system also provide solution to physical attack using virtualization, in which customer is allowed to perform fake transaction for his/her physical security purpose.

II. LITERATURE SURVEY

1]Title: On location models for ubiquitous computing.

Authors: Christian Becker Frank Du rr

Common problems regarding information processing in ubiquitous computing are based on the location of physical objects. No matter whether it is the next printer, next restaurant, or a friend is searched for, a notion of distances between objects is required. A search for all objects in a specific geographic area requires the possibility to define spatial ranges and spatial inclusion of locations. In this paper, they discuss general properties of symbolic and geometric coordinates. Based on that, they present an overview of existing location models allowing for position, range, and nearest neighbor queries. The location models are classified according to their suitability with respect to the query processing and the involved modeling effort along with other requirements. Besides an overview of existing location models and techniques, the classification of location models with respect to application requirements can assist developers in their design decisions.

2]Title: Securing Sensor Networks with Location-Based Keys.

Authors: Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang.

Wireless sensor networks are often deployed in unattended and hostile environments, leaving individual sensors vulnerable to security compromise. This paper proposes the novel notion of location-based keys for designing compromise-tolerant security mechanisms for sensor networks. Based on location based keys, they develop a node-to-node authentication scheme, which is not only able to localize the impact of compromised nodes within their vicinity, but also to facilitate the establishment of pairwise keys between neighboring nodes. Compared with previous proposals, their scheme has perfect resilience against node compromise, low storage overhead, and good network scalability. They also demonstrate the use of location-based keys in combating a few notorious attacks against sensor network routing protocols.

3]Title: TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones.

Authors: William Enck, Peter Gilbert, Byung-Gon Chun.

Todays smartphone operating systems frequently fail to provide users with adequate control over and visibility into how third-party applications use their private data. They

address these shortcomings with TaintDroid, an efficient, system-wide dynamic taint tracking and analysis system capable of simultaneously tracking multiple sources of sensitive data. TaintDroid provides realtime analysis by leveraging Androids virtualized execution environment. Taint-Droid incurs only 1430 popular third-party Android applications, they found 68 instances of potential misuse of users private information across 20 applications. Monitoring confidential data with TaintDroid provides informed use of third-party applications for phone users and valuable input for smartphone security service firms seeking to identify misbehaving applications.

4]Title*:* Location Based Services using Android Mobile Operating System.
Authors: Amit Kushwaha1, Vineet Kushwaha.
The objective for every location based information system is: To assist with the exact information, at right place in real time with personalized setup and location sensitiveness. In this era they are dealing with palmtops and iPhones, which are going to replace the bulky desktops even for computational purposes. They have vast number of applications and usage where a person sitting in a roadside cafe needs to get relevant data and information. Such requirements can only be catered with the help of LBS. These applications include security related jobs, general survey regarding traffic patterns, decision based on vehicular information for validity of registration and license numbers etc. A very appealing application includes surveillance where instant information is needed to decide if the people being monitored are any real threat or an erroneous target. They have been able to create a number of different applications where they provide the user with information regarding a place he or she wants to visit. But these applications are limited to desktops only. Need to send them on mobile devices. They ensure that a person when visiting places need not carry the travel guides with him. All the information must be available in mobile device and also in user customized format.

5]Title*:* Data Encryption Algorithm Based on Location of Mobile Users.
Authors: Hsien-Chou Liao and Yun-Hsiang Chao.
A target latitude/longitude coordinate is determined firstly. The coordinate is combined with a random key for data encryption. The receiver can only decrypt the ciphertext when the coordinate acquired from GPS receiver is matched with the target coordinate. However, current GPS receiver is inaccuracy and inconsistent. The location of a mobile user is complicated to exactly match with the target coordinate. A toleration distance (TD) is also designed in LDEA to increase its practicality. The security analysis shows that the probability to break LDEA is almost impossible since the length of the random key is adjustable. A prototype is also proposed for experimental study. The results concludes that the ciphertext can only be decrypted under the restriction of TD. It explains that LDEA is effective and practical for data transmission in mobile environment.

III. EXISTING SYSTEM

This technology enables individuals, companies and etc to store their data and information on the cloud and they can access their own data at any time, from anyplace and using any computer through the internet. It is possible to deploy a platform in a cloud and use it (instead of installing software on a personal computer). This technology is either certainly a big advantage or always beside the advantages.

IV. PROPOSED SYSTEM

In this system, first user need to do registration for that he/she needs to enter his/her valid email Id and password. It will generate secret key which would send to user's email id and OTP(on time password) on mobile as a text message in inbox . After that while login user need enter the secrete key and OTP from email account and mobile respectively. then user need to enter TD(Tolerance distance) region (i.e within how much distance user could do his/her transaction that would be beyond 10km).Then user would able to do some activity like credit, debit etc

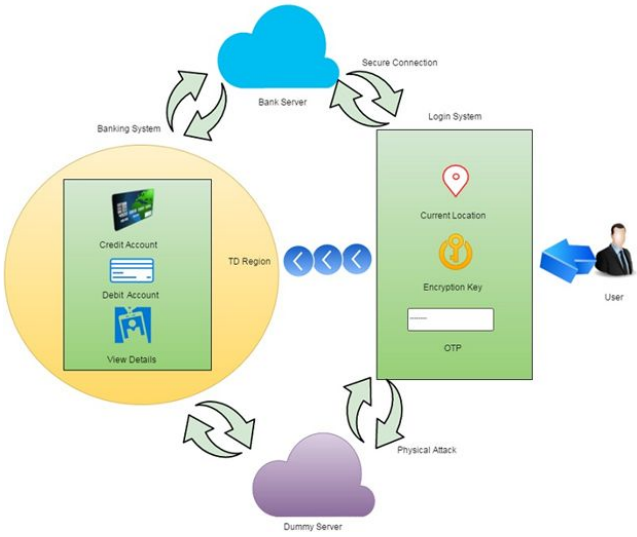

Fig: System architecture

So within define TD region transaction would be secure even if user were not able do to transaction within define TD region then message will pop out i.e no coverage. That means transaction will stop. So even if user's transaction go beyond TD, his/her data will be secure, In this way we are securing data by location based encryption as data will be secure within TD and beyond TD also. System will also give solution to physical attack using virtualisation, allow user to perform fake transaction for his/her security purpose. In this case, if attacker ask user to do transaction forcefully, he/she need to enter valid email id and while entering password required to enter password with one additional digit or alphabet etc. Then transaction would go to dummy server. It will show pop out message i.e transaction successful but actually it will perform fake transaction and user data will be secure.

V. GOALS AND OBJECTIVE

Our aim is to Design & Implement secure access to critical and confidential information in banks using Location Based Data Encryption algorithm (LDEA) .

VI. MATHEMATICAL MODEL

System Description:

- Input: Username, Password, Secret Key, OTP
- Output: Secure Online Transaction.
- Functions : Encryption, Decryption, Location Fetch.
- Mathematical formulation: LDEA Algorithm.
- Success Conditions: Transaction done within Toleration Distance.
- Failure Conditions: Transaction done beyond Toleration Distance.

Let 'S' be the system
Where,
S= {I, O, P }
Where,
I = Set of inputs
O = Set of output applications
P = Set of technical processes
Let 'S' is the system
S ={. . . . . .
S= {s, e, X, Y, Fma, DD, NDD}
s- Initial State: No user login
e- End state: Allow access to authenticated user
X- Input: Login id, password, user's personal info.
Y- Output: Secure Transaction.
LDEA-Location Dependant Encryption algorithm.
DD-Deterministic Data: Customer information
NDD-Non Deterministic Data: Location of customer Identify the Process as P.
P= {Location fetch, Encryption, decryption, key value generation}

VII. ALGORITHM

LDEA Algorithm:

- **Convert latitude/longitude coordinates:**
  1. The coordinates obtained from GPS receiver are multiplied by 10000 to be an integer. Then, integer is divided by a value corresponding to the TD.
  2. In addition, after that one bit is put in front of the integral part of the above result. The bit is zero for east and south sides and one for west and north sides.

- **Combine and hash:**
  1. The conversion results are combined by performing a bitwise exclusive-OR operation.
  2. Then, MD5 hash algorithm is used and generate a 128-bit digest for the combined result.
  3. Then, digest is split into two 64-bit values, called LDEA-keys.

- **Generate final-key:**
  1. A session key (R-key) is obtained randomly with the same length of LDEA-key.
  2. LDEA -keys are exclusive-OR with the R-key separately to create the final-keys.
  3. These two final-keys are used as the secret key[2].

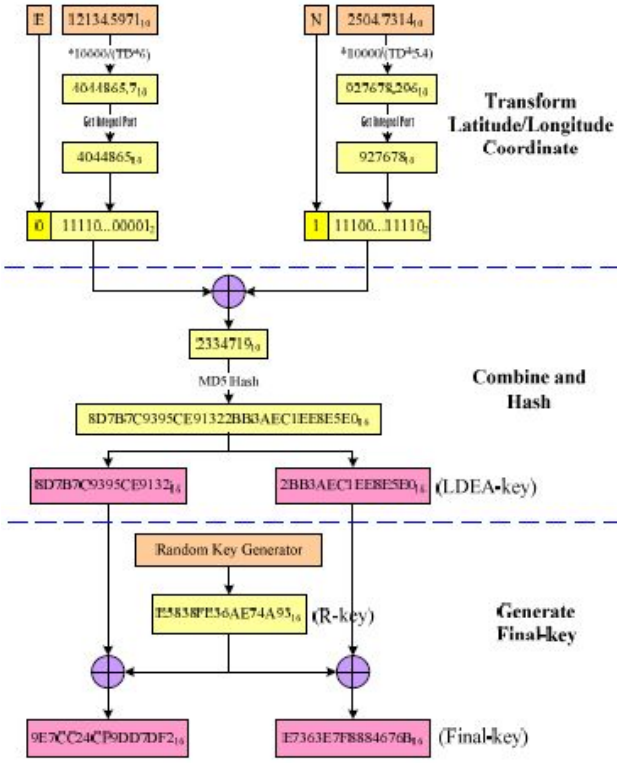

Fig: Algorithm

VIII. APPLICATIONS

1. Secure Online Money Transaction.
2. Online shopping.
3. Ticket booking.

IX. CONCLUSION

In our approach we use the user's location and geographical position and we will add a security standard to the existing security system. Our solution is more appropriate for banks, big companies, institutions and examples like this. The only thing we require is an Anti-Spoof and accurate GPS that companies 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. Location based encryption and LDEA Algorithm were reviewed. Finally a new security level was added to the existing security measures using location-based encryption.

REFERENCES

[1] Bilal Shebaro, Oyindamola Oluwatimi, and Elisa Bertino, "Context-Based Access Control Systems for Mobile Devices", April 2015.
[2] Hsien-Chou Liao and Yun-Hsiang Chao," LDEA : Data Encryption Algorithm Basedon Location of Mobile Users", 2 April 2016.
[3] R.J. Hulsebosch, A.H. Salden, M.S. Bargh, P.W.G. Ebben, J. Reitsma,: "Context Sensitive Access Control For Mobile Devices", April 2015.
[4] Amit Kushwaha1, VineetKushwaha, "Location Based Services using Android Mobile Operating System", 2011.

[5] Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta, "Location Based Services using Android", March 2009.
[6] Christian Becker Frank Du rr,"On location models for ubiquitous computing",2002.
[7] Yanchao Zhang,Wei Liu,Wenjing Lou and Yuguang Fang "TaintDroid: Securing Sensor Networks with Location-Based Keys",2005
[8] William Enck, Peter Gilbert, Byung-Gon Chun, "An Information-Flow Tracking"
[9] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, "A study of android application security," in Proc. 20th USENIX Conf. Security, 2011.
[10] M. Moyer and M. Abamad, "Generalized role-based access control," in Proc. 21st Int. Conf. Distrib. Comput. Syst., 2001.