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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Location Based Security for Online Transaction

Dipak Auti[1], Krishna Landage[2], Swapnil Chavan[3]

Student, Dept. of Computer Engineering, P K Technical Campus Pune, India[1]

Student, Dept. of Computer Engineering, P K Technical Campus Pune, India[2]

Student, Dept. of Computer Engineering, P K Technical Campus Pune, India[3]

ABSTRACT: We are developing banking application using Location Based Encryption. As compare to current banking application which is location-independent, we are developing banking application which is location dependent. It means in Cryptography Cipher-text can only be decrypted at a specified 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. Our system is flexible enough to provide access to customer to his/her bank 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.

KEYWORDS: Global Positioning System, Context Provider, Access Controller, Encryption, Cellular triangulation.

I. INTRODUCTION

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 this paper, we propose a context-based access control (CBAC) mechanism for Android systems that allows smartphone users to set configuration policies over their applications' usage of device resources and services at different contexts. Through the CBAC mechanism, users can, for example, set restricted privileges for device applications when using the device at work, and device applications may re-gain their original privileges when the device is used at home. This change in device privileges is automatically applied as soon as the user device matches a predefined context of a user-defined policy. The user can also specify a default set of policies to be applied when the user is located in a non-previously defined location.

Our aim is to Design and Implementation secure access to critical and confidential information in banks using location based cryptography and Geo-Encryption algorithm, anti-spoof GPS.

II. RELATED WORK

In [1] author had explained the Data Encryption Algorithm Based on Location of User Mobile. Thus the results show that the cipher text can only be decrypted under the restriction of TD. It illustrates that LDEA is effective and practical for data transmission in mobile environment. In [2] author had explained On location models for ubiquitous computing. this discuss the general properties of symbolic and geometric coordinates. Based on that, we present an overview of existing location models allowing for position, range, and nearest neighbor queries. In [3] author explained the Securing Sensor Networks with Location-Based Keys .This is proposes the novel notion of location-based keys for

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

designing compromise-tolerant security mechanisms for sensor networks. Based on location based keys, we 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. In [4] author explained Taint Droid: An Information-Flow Tracking System for Real time Privacy Monitoring on Smartphones, In this paper using Taint Droid to monitor the behavior of 30 popular third-party Android applications, we found 68 instances of potential misuse of users private information across 20 applications. Monitoring sensitive 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. In [5] author is explained on Location Based Services using Android Mobile Operating System .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. They need to import them on mobile devices. They must ensure that a person when visiting places need not carry the travel guides with him. All the information must be available in his mobile device and also in user customized format. In [6] author had explained on Location Based Services using Android. After the release of android based open source mobile phone a user can access the hardware directly and design customized native applications to develop Web and GPS enabled services and can program the other hardware components like camera etc. In this paper they will discuss the facilities available in android platform for implementing LBS services (geoservices).In [7] author had explained on Context Sensitive Access Control. This is conventional information management approaches are used to compare historic contextual (service usage) data of an individual user or group. The result is a relatively strong, less intrusive and more flexible access control process that mimics our natural way of authentication and authorization in the physical world. In [8] author had explained on Supporting Location-Based Conditions in Access Control Policies. They present an approach to LBAC aimed at integrating location based conditions along with a generic access control model, so that a requester can be granted or denied access by checking his/ her location as well as her credentials. In [9] author had explained on The Data Encryption Standard: Past and Future .The Data Encryption Standard (DES) is the first, and to the present date, only, publicly available cryptographic algorithm that has been endorsed by the US. Government. This deals with the past and future of the DES. It discusses the forces leading to the development of the standard during the early 1970s, the controversy regarding the proposed standard during the mid-I970s, the growing acceptance and use of the standard in the 1980s,and some recent developments that could affect the future of the standard. In [10] author had explained on Pipeline Algorithms of RSA Data Encryption and Data Compression. The first pipeline shows that encryption fails to map large amount of redundancy for the input file into a favorable form for its later compression. The second pipeline, however, offers a good potential to improve the compressed output for further compression by another compression algorithm.

III. PROPOSED ALGORITHM

Step 1 : The target coordinate at the centre is acquired from the GPS receiver.
Step 2 : For every TD, a source file is encrypted by using the target coordinate and TD firstly.
2a : For every circle, the tester moves randomly along the curve of the circle and tries to decrypt the data about every minute.
2b : There are totally 10 times of data decryption. The destination file is checked whether the content is the same as the original file. The number of successful decryption is recorded.
Step 3 : Repeat step 2 until finishing the testing of all TDs. The successful rate is computed for every combination of TD and testing distance.
Identify the process P:

P= {location fetch, Encryption, decryption, key value generation}

If the latitude/longitude coordinate is simply used as the key for data encryption, the possible key space is the same as the -
Surface of the Earth =(5.11×10^{8})^{2} km
i.e., 5.11×10^{14} m^{2}.
However, 80% of people live on only 3% of the surface on the Earth.
If TD = 20 meters
Then,

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Probability to break such key = $1/1.22\times10^{10}$ as shown in Eq. (1).
The strength is not strong enough.

$$\frac{1}{5.11\times10^{14}m^2\times0.03/(3.14159\times20^2)m^2}=\frac{1}{1.22\times10^{10}} \quad (1)$$

That is the reason why a random key is incorporated into LDEA algorithm. The final-key is generated from the exclusive-OR of R-key and LDEA-key. The DES algorithm is used in current design of LDEA and the length of final-key is 64 bits.

The probability of breaking the
LDEA = $1/2^{64}$ ($\approx 1/10^{19}$) .

IV. PRESENTATION OF THE MAIN CONTRIBUTION OF THE PAPER /SCOPE OF RESEARCH

Our system uses location based encryption technique for providing security to the banking application. Our system only allows authenticated people for doing transaction. Authentication is based on location based encryption. In case of physical attack, our system creates a virtual environment with extra key in password and allows fake transactions. Our system allows access of account from any location.

V. PROPOSED METHODOLOGY AND DISCUSSION

We are proposing system in which when the user is under attack he/she can login to his /her account by entering the password with extra key, that is identified at server side and hence access will be prohibited. We are using Geo-Encryption algorithm,location based cryptography, positioning tools (Anti-spoof GPS).That means our system provide solution to physical attack using virtualization, in which customer is allowed to perform fake transaction for his/her physical security purpose.

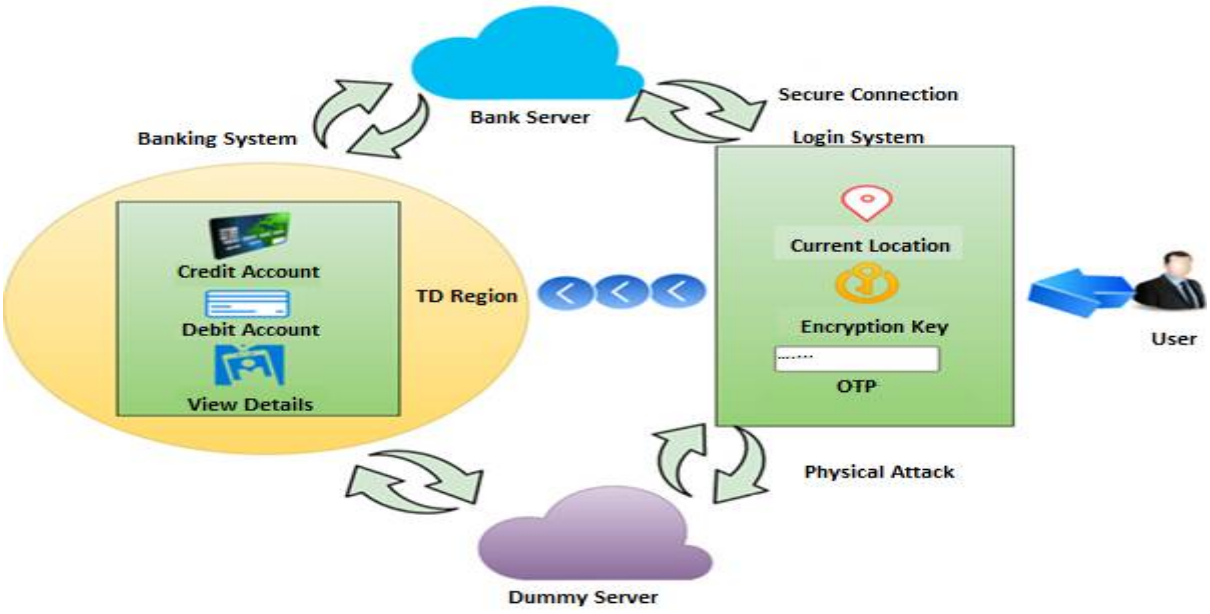

Figure1 : System Architecture

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Using this system one can able to do the secure transaction from mobile with the help of Geo-encryption algorithm and anti-spoof GPS. In case of physical attack, our system creates a virtual environment with extra key in password and allows fake transactions.
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 any place and using any computer through the internet. It is even possible to deploy a platform in a cloud and use it (instead of installing software on a personal computer).

In GPS there are two techniques are used first is the latitudes and second is longitude to the get the correct position of the user to determine the new key for the encryption this key is made by using the combining of the AES and GPS location with the TD.

Here, Latitude is the measurement of distance in degrees north and south of equator there are 90 degrees of latitude from the equator to each of the poles, north and south. Latitude lines are parallel, that is they are the same distance apart .Equator is 0 degrees, the equator divides the earth into two equal parts . Longitude is defined as the measurement of the distance in degrees east or west of the prime meridian. The Prime Meridian, as do all other lines of longitude, pass through the north and south pole. The Prime meridian divides the earth in two half too. It is also 0 degrees. Longitude Lines give directions East and West of the prime meridian. Longitude lines are not parallel like latitude lines.

Using latitude, longitude to find the exact of the user on the map. So the we need to determine which latitude line and which longitude line meet where user are standing.

In TD is Tolerance distance is used to create a geographical area to the user which is all transaction process will done inside this area this tolerance distance is find out the actual position of user and provide the distance to area. Such as in equation no 2,

$$TD=\text{User current position} + \text{Provided distance} \qquad (2)$$

This Tolerance distance is find out and then this area is provided to the user to complete the transaction for the security purpose . If user can goes out of this area then this process will performed again and new TD is generate and new key is generate to the encryption and decryption.

VI. CONCLUSION AND FUTURE WORK

Data security in the cloud is so important. Users (individuals or companies) are concerned about the access to the information by unauthorized users. Now suppose that data is some critical and confidential information from a bank, or a company and etc. Certainly the necessity of access control in the cloud computing is more than ever and is a very important part of data security in cloud. 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.

Cloud computing is a new approach in the field of information technology and development of computer technologies based on the World Wide Web. One of the most important challenges in this area is the security of cloud computing. On the other hand the security of access to critical and confidential information in banks, institutions and etc is extremely essential. Sometimes even with the enormous costs, it is not fully guaranteed and it is compromised by the attackers. By providing a novel method, we improve the security of data access in cloud computing for a company or any other specific locations using the location-based encryption.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

VII. ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on 'Location Based Security for Online Transaction'.

We are very grateful and would like to thank my guide Dr. S. T. Singh for his advised and continued support without his it would not have been possible for we to complete this paper. We would like to thank all my teacher, friends, classmates for all the thoughtful and mind stimulating discussion we had, which prompted us to think beyond the obvious.

REFERENCES

1. A. Kushwaha and V. Kushwaha, Location based services using android mobile operating system, Int. J. Adv. Eng. Technol., vol. 1, no. 1, pp. 1420,2011.
2. J. Leyden, (Apr. 2013). Your phone may not be spying on you nowbut it soon will be. [Online].
3. L. L. N. Laboratory, Controlled items that are prohibited on llnl proporty(2013).
4. M. Conti, V. T. N. Nguyen, and B. Crispo, Crepe: Context-related policy enforcement for android, in Proc. 13th Int. Conf. Inf. Security, 2011, pp.331345.
5. M. S. Kirkpatrick and E. Bertino, Enforcing spatial constraints for mobile RBAC systems, in Proc. 15th ACM Symp. Access Control Models Technol.,2010, pp. 99108.
6. R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang,Soundcomber: A stealthy and context-aware sound trojan for smartphones,in Proc. 18th Annu. Netw. Distrib. Syst. Security Symp., Feb. 2011, pp.1733.
7. R. Templeman, Z. Rahman, D. J. Crandall, and A. Kapadia, Placeraider: Virtual theft in physical spaces with smartphones, in Proc. 20th Annual Netw.Distrib. Syst. Security Symp. (NDSS), Feb. 2013.
8. S. Kumar, M. A. Qadeer, and A. Gupta, Location based services using android, in Proc. 3rd IEEE Int. Conf. Internet Multimedia Serv. Archit. Appl.pp. 335339.
9. W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A.N. Sheth, Taintdroid: An information-ow tracking system for realtime privacy monitoring on smartphones, in Proc. 9th USENIX Conf. Oper. Syst. Des.Implementation, 2010, pp. 16.

BIOGRAPHY

Dipak Auti, Krishna Landage, Swapnil Chavan are students of the Computer Engineering Department, College of P K Technical Campus, Pune University. We study in the Bachelor of Engineering (BE) degree in 2016-17 from P K Technical campus, Chakan, India.