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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Location Based Management for Mobile Phones (Android) To Provide Secured Transactions

Jyoti Kshirsagar[1], Juhi Deshpande[2], Poorva Chougule[3]

Professor, Department of Computer, JSPM's RSCOE, Tathawade ,Pune, Maharashtra, India[1]

UG Student, Department of Computer, JSPM's RSCOE, Tathawade, Pune, Maharashtra, India[2]

UG Student, Department of Computer, JSPM's RSCOE, Tathawade, Pune, Maharashtra, India[3]

ABSTRACT: Today in wireless communication users transmit their location using beacon. For online banking transactions, users need to have GPS enabled devices. Banks use GPS for transactions which are location independent. They provide mobile application to their customer. The system is developing banking application using Location Based Encryption. As compare to current banking application which are location independent, the system developing banking application which is location dependent. User can perform transaction only if user is within TD region. TD region is area of Toleration Distance (TD) where user can perform transaction. If user goes out of TD region then transaction will terminate automatically. The system is providing extra security by OTP and secret key.

KEYWORDS: Location Privacy, Mobile Networks, One Time Password, Toleration Distance, Secret key, GPS.

I. INTRODUCTION

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.

The system is developing banking application using Location Based Encryption. As compare to current banking application which are location-independent, the system developing banking application which is location dependent. It means User can perform transaction only if user is within TD region. TD region is area of Toleration Distance (TD) where user can perform transaction. If user goes out of TD region then transaction will terminate automatically.

In this system user register them in this application. User provide the personal details like name, mobile number, email id , secret bit, etc. then system will send the encrypted password to email. Encrypted password means "Secret bit" is added into the password, this is done to protect password from visualization. After entering correct user name and password user will login to system and get the secret key on registered email id. If user entered key is correct then OTP will receive on mobile by SMS. If entered OTP is correct then generate TD region. This TD region specifies range in meters. After generation TD region successfully user can view account details and User can perform money transaction operation.

This system is flexible enough to provide access to customer to his/her bank account from any location. This system also provides solution to physical attack using virtualization, password send on email is encrypted by secret bit.

II. PROBLEM STATEMENT

In banking, applications of mobile phones are location independent. Hacker or malicious user could access the user bank account easily. This system is providing applications that are location dependent.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

III. EXISTING SYSTEM

The existing system is having many problems such as security problems, more human involvement which is a time consuming process with many manual calculations. Existing system causes damage to the machines and the process for signature verification is time consuming for customers as well as the banks. The major problem in online banking system is unauthorized user access with fake passwords. The hackers are trying to hack the user accounts and are performing different unauthorized transactions.

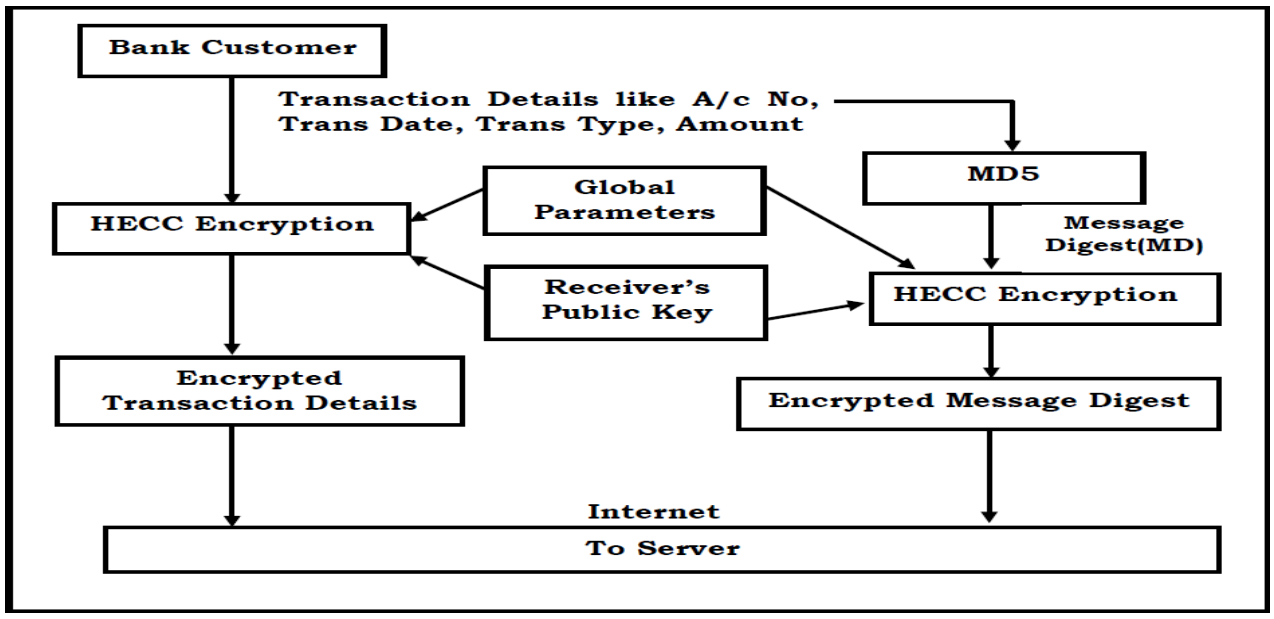

Fig.1. Existing System

Disadvantages of Existing System:

- User have to wait in line in offline banking
- Existing banking applications are location independent

IV. RELATED WORK

A. LDEA: Data Encryption Algorithm Based on Location of Mobile Users

A target latitude/longitude coordinate is determined firstly. The coordinate comprises with a random key for data encryption. When the coordinate of GPS receiver and target is matched then the receiver can decrypt the ciphertext data. However, current GPS receiver is inaccuracy and inconsistent. It is difficult to match the location of user and the target coordinate. A toleration distance (TD) is also implemented in LDEA [1] to enhance 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 implemented for experimental study. The results show that the ciphertext can only be decrypted under the restriction of TD. It illustrates that LDEA is effective and practical for data transmission in mobile environment.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

B. On location models for ubiquitous computing

Common queries regarding information processing in ubiquitous computing [2] 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 certain geographic area requires the possibility to define spatial ranges and spatial inclusion of locations. In this paper, we discuss 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. 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 approaches, the classification of location models with respect to application requirements can assist developers in their design decisions.

C. Securing Sensor Networks with Location-Based Keys

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. Node-to node authentication scheme is developed using location-based key. This helps to localize the impact of other nodes in their vicinity as well as to facilitate the establishment of pair wise keys within nearby nodes. Compared with previous proposals, our scheme has perfect resilience against node compromise, low storage overhead, and good network scalability. We also demonstrate the use of location-based keys in combating a few notorious attacks against sensor network routing protocols

D. Location Based Services using Android Mobile Operating System

Location based system should assist the user with correct information, at correct place having real time personalized setup and sensitivity of location. In this era we are dealing with palmtops and iPhones, which are going to replace the bulky desktops even for computational purposes. We have number of applications where a person sitting anywhere can access information. Such needs can only be catered with the help of LBS. These applications include jobs for security purpose, survey about traffic patterns, etc. A very attractive application includes surveillance where quick response is needed to decide if the people being supervised are any real threat or an inaccurate target. We have been able to create a number of different applications where we provide the user with information regarding a place he or she wants to visit. But these applications are limited to desktops only. We need to import them on mobile devices. We must ensure that a person when visiting places need not carry the travel guides with him. The information generated must be in the user's mobile device and also in customized format

E. Location Based Services using Android

In earlier days, mobiles were used just for voice communication. But today, they are now one of the many features of mobile devices. There are many other aspects that have been added recently to the devices. Two such new features are web browser and GPS. These services are implemented by the manufacturers but they cannot be implemented by the users. As manufacturers have the proprietary rights, they can access the mobile hardware directly which was restricted for the users. The release of Android based open source operating system user has the rights to access the mobile hardware. The user can also design customized applications for using Web browser and GPS services. Location based services and geo-services are now available for the user.

F. Context Sensitive Access Control

We investigate the practical feasibility of using context information for controlling access to services. Based solely on situational context, we show that users can be transparently provided anonymous access to services and that service providers can still impose various security levels. Thereto, we propose context-sensitive verification methods that allow checking the user's claimed authenticity in various ways and to various degrees. More precisely, 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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

G. Supporting Location-Based Conditions in Access Control Policies

We present an approach to LBAC aimed at integrating location-based conditions along with a generic access control model, so that a request or can be granted or denied access by checking her location as well as her credentials.

H. 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 paper 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.

I. Pipeline Algorithms of RSA Data Encryption and Data Compression

Various pipeline algorithms [7] of data compression and encryption are designed to assess the impact of encryption on 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. The pipeline algorithm also identifies the different performances between dictionary data compression and statistical compression algorithms. In addition; the compression prior to encryption improves the efficiency of encryption and lead to the possible development of a multifunctional algorithm which could operate as both compression and encryption

V. PROPOSED SYSTEM

In our system user register them in our application. They provide the personal details like name, mobile number, email id, secret bit, etc. then system will send the encrypted password to email. Encrypted password means “Secret bit” is added into the password, this is done to protect password from visualization. After entering correct user name and password user will login to system and get the secret key on registered email id. If user entered key is correct then OTP will receive on mobile by SMS.

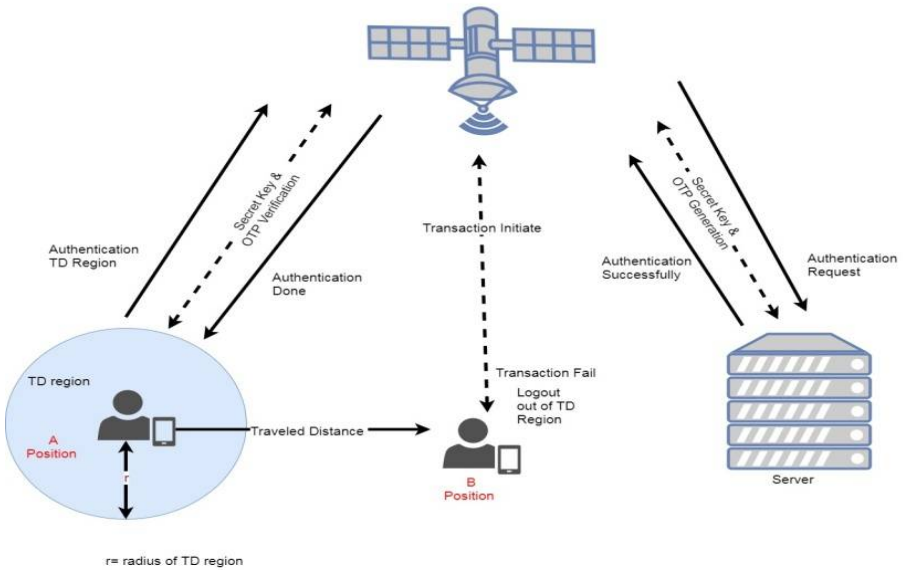

Fig.2. Proposed system

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

If entered OTP is correct then generate TD region. This TD region specifies range in meters. After generation TD region successfully user can view account details and User can perform money transaction operation.

Advantages of proposed system:

- Location dependent
- Access account from any location
- Provide extra security by secret key and OTP

VI. MODULES

User:

- User registers themselves into system then login into application.
- Enter Secret Key receive from email. If key is correct then OTP will receive on mobile by SMS
- Enter OTP receive on mobile. If OTP is correct then generate TD region
- Enter TD region range in meters to generate TD region
- After generation TD region successfully user view account details
- Users perform money transaction operation.

Server:

- After user successfully register into system, system send “encrypted password” to email. Encrypted password means “Secret bit” is added into the password, this secret bit is provided by user at the time of registration. (all these operations are perform to secure the password)
- After successfully login, system will generate “secret key” and send to the registered email id
- If user enters correct secret key then system will generate OTP and send it to the registered mobile number.
- “Haversine” Distance calculation algorithm is used to calculate TD region. It utilizes user current location.[3]
- If user is within TD region then transaction are allowed. If user out of TD region transaction will be terminated.

VII. ALGORITHM

Haversine algorithm to calculate the distance from target point to origin point

R is the radius of earth in meters.

LatO= latitude of origin point
LatT= latitude of target point
Difference in latitude = LatO-LatT

LongO = longitude of origin point
LongT= longitude of target point
Difference in longitude = LongO-LongT

Φ =Difference in latitude in radians
O= LatO in radians.

Λ =Difference in longitude in radians
T= LatT in radians.

$A=\sin(\Phi/2)*\sin(\Phi/2)+\cos(O)*\cos(T)*\sin(\Lambda/2)*\sin(\Lambda/2)$
$B = \min(1,\sqrt{A})$
Distance = 2*R*B

VIII. MATHEMATICAL MODEL

Let ‘S’ be the system where
S= {I, O, P}

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Where,
I = Set of input sensors
O= Set of output applications
P = Set of technical processes
Let 'S' is the system
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- Secure Transaction.
Fma- Haversine -Distance calculation algorithm.
DD- Deterministic Data: Customer information
NDD- Non Deterministic Data: Location of customer
I= {user location, user information}
User location: GPS is used to get users current location
User information: it contains the login id, password, account details.
O= {transaction}
Transaction= if users within TD region and provide correct details then transaction will complete. If user out of TD region or provide incorrect details then transaction will terminate.
P= {UL, secret key, OTP, TD region, }
UL= Fetch User Current Location
Secret key= generate secrete key and send to email
OTP= generate OTP and send to mobile
TD region= generate TD region and perform transaction with in TD region

IX. FUTURE SCOPE

In future propose system will integrate with real time banking application. With some changes propose system could be used in other application for security like ecommerce application.

X. CONCLUSION

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 User can perform transaction only if he/she is within TD region. TD region is area of Toleration Distance (TD) where user can perform transaction. If user goes out of TD region then transaction will terminate automatically. We providing extra security by using the secrete key and OTP. Study show that location could be increase the security of the banking application.

REFERENCES

[1] Liao, H.C., P.C. Lee, Y.H. Chao and C.L. Chen, 2007. "A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security" In: Proc. the 9th International Conference on Advanced Communication Technology (ICACT 2007), 1: 625-628, Feb. 2007.
[2] Becker, C. and F. Durr, 2005. On "Location Models for Ubiquitous Computing. Personal and Ubiquitous Computing", 9 (1): 20-31, Jan. 2005.
[3] Aikawa, M., K. Takaragi, S. Furuya and M. Sasamoto, 1998. "A Lightweight Encryption Method Suitable for Copyright Protection". IEEE Trans. on Consumer Electronics, 44 (3): 902-910.
[4] Eagle, N. and A. Pentland, 2005. Social Serendipity: "Mobilizing Social Software. IEEE Pervasive Computing", 4 (2), Jan.-March 2005.
[5] Gruteser, M. and X. Liu, 2004." Protecting Privacy in Continuous Location-Tracking Applications. IEEE Security & Privacy Magazine", 2 (2): 28-34, March-April 2004.
[6] Jamil, T., 2004. "The Rijndael Algorithm." IEEE Potentials, 23 (2): 36-38.
[7] Jiang, J., 1996. "Pipeline Algorithms of RSA Data Encryption and Data Compression", In: Proc. IEEE International Conference on Communication Technology (ICCT'96), 2:1088-1091, 5-7 May 1996.
[8] Lian, S., J. Sun, Z. Wang and Y. Dai, 2004. "A Fast Video Encryption Scheme Based-on Chaos". In: Proc. the 8th IEEE International Conference on Control, Automation, Robotics, and Vision (ICARCV 2004), 1: 126-131, 6-9 Dec. 2004.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

[9] Zarrin Montazeri; Amir Houmansadr; Hossein Pishro-Nik. "Defining Perfect Location Privacy Using Anonymization" 2016 Annual Conference on Information Science and Systems (CISS) Pages: 204 - 209 IEEE Conference Publications
[10] Marco Gruteser, Dirk Grunwald "Anonymous Usage of Location Based Service Through Spatial and Temporal Cloaking" Published by ACM 2003 Article.
[11] Zarrin Montazeri; Amir Houmansadr; Hossein Pishro-Nik "Achieving Perfect Location Privacy in Markov Models Using Anonymization" IEEE Transactions on Information Forensics and Security
2017 IEEE Journals & Magazines
[12] Gu(Toby) Xu "Location Cloaking for Location Privacy Protection and Location Safety Protection Digital Repository" 2010
[13] Reza S., George T., Carmella T., Jean-Pierre H., Jean-Yves B. "Protecting Location Privacy: Optimal Strategy against Localization Attacks" Published by ACM 2012 Article
[14] Baik H., Markov G., Hui X., Ansaf "A. Preserving Privacy in GPS Traces via Uncertainty Aware Path Cloaking" IEEE Transactions on Mobile Computing 2010 IEEE Journals & Magazines
[15] Hidetoshi K.,Yutaka Y., Tetsuji S. "An Anonymous Communication Technique Using Dummies for Location Based Services" IEEE Conference Publications 2005
[16] Michael Decker "Location Privacy- An Overview" IEEE Conference Publications 2008
[17] Shahriyar A., Janne L., Jason H., Jaliu L., Eran T., Norman S. "Cache: Caching Location Enhanced Content to Improve User Privacy" Published by ACM 2011 Article.