iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5117

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Location Based Encryption

Maruti Garaje[1], Saurabh Gedekar[2], Anup Gite[3], Vrushabh Gore [4]
[1, 2, 3, 4]*Student, Computer Engineering, Sinhgad Institute of Technology, Lonavala, India*

Abstract: Bank are providing mobile application to their customer. 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. User can perform transaction only if he/she is with in TD region. TD region is area of Toleration Distance (TD) where user can perform transaction. If user go out of TD region then transaction will terminate automatically. We are providing extra security by OTP and secret key.
Keyword: Encryption, secret key, toleration distance.

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.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 with in TD region. TD region is area of Toleration Distance (TD) where user can perform transaction. If user go out of TD region then transaction will terminate automatically.

In our system user register himself/ herself in our application. He/she 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 specify range in meters. After generation TD region successfully user can view account details and User can perform money transaction operation. 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, password send on email is encrypted by secret bit

A. Objective

1) The main goal of location encryption is to protect the user bank account by malicious user.
2) To avoid the shoulder surfing .
3) Make the bank application location dependent .

B. Problem Statement

Now day all banking operations are done online. Most of bank provide their bank application. People uses there mobile to do this operation. These application are location independent. Hacker or malicious user could access the user bank account easily.

II. LITERATURE SURVEY

A target latitude/longitude coordinate is determined firstly. The coordinate is incorporated 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 difficult 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 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.

Common queries 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 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

©IJRASET: All Rights are Reserved

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.

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, 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. 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 .

Today's smartphone operating systems frequently fail to provide users with adequate control over and visibility into how third-party applications use their private data. We 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 Android's virtualized execution environment. TaintDroid incurs only 14% performance overhead on a CPU-bound micro-benchmark and imposes negligible overhead on interactive third-party applications. Using TaintDroid to monitor the behavior of30 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.

The motivation 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 we are dealing with palmtops and iPhones, which are going to replace the bulky desktops even for computational purposes. We have vast number of applications and usage where a person sitting in a roadside café needs to get relevant data and information. Such needs 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. 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. All the information must be available in his mobile device and also in user customized format .

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

A. Architecture

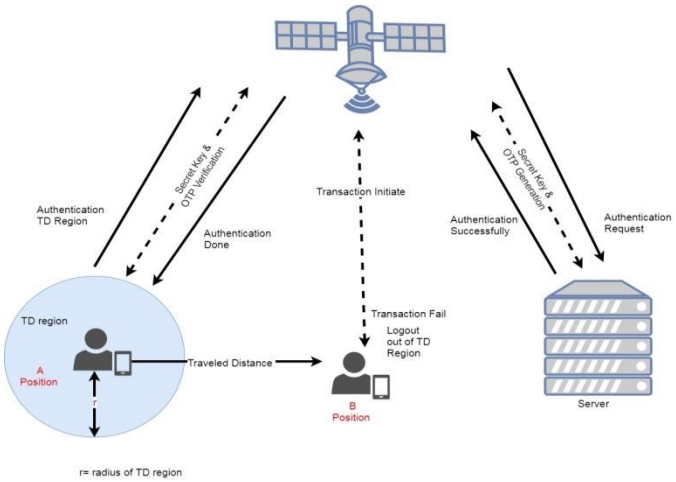


Fig.1 Architecture of transaction process

©IJRASET: All Rights are Reserved

B. Mathematical Model

Let 'S' be the system
Where
S= {I, O, P}
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 contain 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**.**

C. Outcomes

Using this system user can able to do the secure transaction from mobile with the help of Geography location and anti-spoof GPS. In case of physical attack, our system creates a virtual environment with extra key bit in password.

D. Feature and Application

Secure Online Money Transaction. Banking application

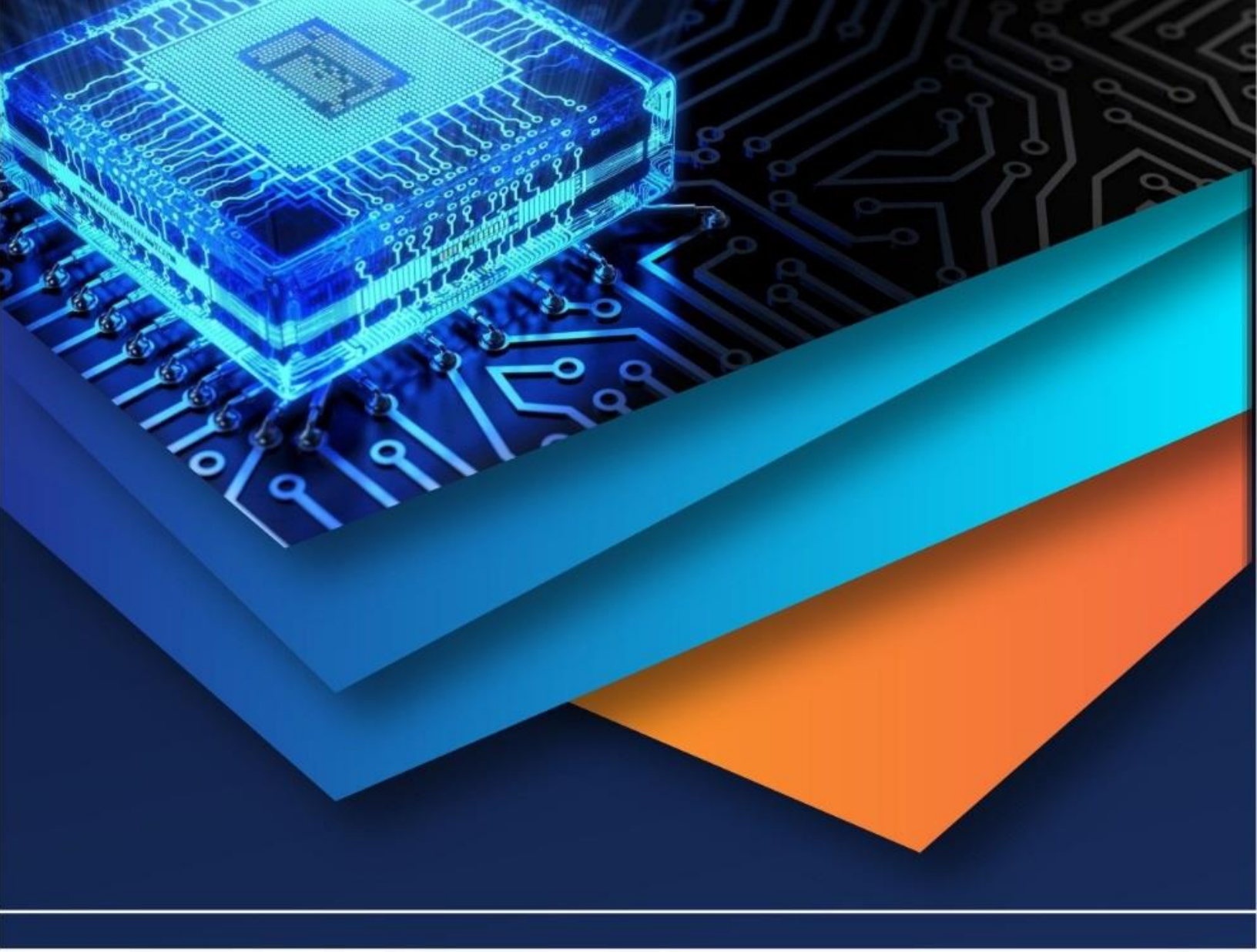
III. CONCLUSION AND FUTURE SCOPE

In this paper, we have studied how We are developed 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 with in TD region. TD region is area of Toleration Distance (TD) where user can perform transaction. If user go 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] Becker, C. and F. Durr, 2005. On Location Models for Ubiquitous Computing. Personal and Ubiquitous Computing, 9 (1): 20-31, Jan. 2005
[2] Gruteser, M. and X. Liu, 2004. Protecting Privacy in Continuous Location-Tracking Applications. IEEE Security & Privacy Magazine, 2 (2): 28-34, March-April 2004.
[3] 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.Krishna and M. N.
[4] Ye Yuan, Xiang Lian, , Lei Chen, Yongjiao Sun, Guoren Wang"Achieving Perfect Location Privacy in Wireless Devices Using Anonymization "2016.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)