ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 4, April 2019

Location Based Encryption for Banking Application

Shruti modak, Mrunali dhere , Ketaki pawar ,Prof. Raghunath Kawale

BE Student, Department of Information Technology, PDEA's Engineering College, Pune, India
BE Student, Department of Information Technology, PDEA's Engineering College, Pune, India
BE Student, Department of Information Technology, PDEA's Engineering College, Pune, India
Associate Professor, Department of Information Technology, PDEA's Engineering College, Pune , India

ABSTRACT: Bank is providing mobile application to their customer. We square measure developing banking application victimization Location primarily based cryptography. As compare to current banking application which is location independent, we are developing banking application which is location dependent. User can perform transaction provided that 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 square measure providing extra security by OTP and secret key.

KEYWORDS: GPS, Mobile Interaction, Smartphone

I. INTRODUCTION

Today in wireless communication users transmit their location using beacon. 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 another to human security concerns. We are developing banking application using Location primarily based encryption. As compare to current banking application which is location-independent, we are developing banking application which is location dependent. It means User can perform transaction providing 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.

II. LITERATURE SURVEY

1) LDEA: 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 incorporated with a random key for data encryption. The receiver can only decrypt the cipher text 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 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.

2) On location models for ubiquitous computing

AUTHORS: Christian Becker Æ Frank Du¨ rr

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 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 modelling 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.

3. 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, 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

4. Taint Droid: An Information-Flow Tracking System for Real-time Privacy
Monitoring on Smartphones

AUTHORS: William Enck, Peter Gilbert, Byung-Gon Chun

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 Taint Droid, an efficient, system-wide dynamic taint tracking and analysis system capable of simultaneously tracking multiple sources of sensitive data. Taint Droid provides real-time analysis by leveraging Android’s virtualized execution environment. Taint Droid incurs only 14% performance overhead on a CPU-bound micro-benchmark and imposes negligible overhead on interactive third-party applications. 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 Taint Droid provides informed use of third-party applications for phone users and valuable input for smartphone security service firms seeking to identify misbehaving applications.

5. Location Based Services using Android Mobile Operating System
AUTHORS: Amit Kushwaha1, Vineet Kushwaha

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

III.RELATED WORK

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 that "Secret bit" is accessorial into the word, this is done to protect password from visualization. As compare to current banking application which are location-independent. 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. Bank are providing mobile application to their customer. This TD region specifies range in meters. After generation TD region successfully user can view account details and User can perform money transaction operation. Our system also provides solution to physical attack using virtualization, password send on email is encrypted by secret bit.

IV. APPLICATIONS

Detect frauds at crowded areas such as

- Secure online money transaction
- Banking application

V. EXISTING SYSTEM

A target latitude/longitude coordinate is determined firstly. A toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver .The Target coordinate and TD (toleration distance) is provided by the sender to generate the LDEA key, there is randomly key generator which issues a session key, called Rekey Which is then Exclusive-Oared with LDEA key to generate the final key for encrypting the plain text. There is no restriction over the use of encryption algorithm DES, AES or Triple DES etc. can be used to encrypt the plaintext by the given final key, TD and R-KEY is transmitted to the receiver via asymmetric encryption algorithm. As soon as the receiver gets the access of TD and R-KEY, the LDEA key can be generated (at the receiver end) by exclusive OR R-KEY with LDEA key. If the acquired coordinates is matched with the target coordinate within the range of TD, the cipher text can be decrypted back to the original plain text, otherwise nonsense and indiscriminate result is displayed. The target coordinate is either determined by the sender or receiver. It must be communicated between the other party/parties via very secure communication.

VI. PROPOSE SYSYTEM

In our system user register him/ her 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 additional into the positive identification, 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 secret is correct then OTP will receive on mobile by SMS. 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

- **We perform a detailed security analysis and performance evaluation of the proposed data**
- Required less time
- Increase Efficiency
- Improve the accuracy

VII. SOFTWARE RESOURCES

There has to be required packages, software's etc to interact with system.

Operating system	:	Windows 7 and above.
Coding Language	:	Java 1.8

Tool Kit	:	Android 2.3 and above
IDE	:	Android Studio

VIII. Hardware Resources

There should be required devices to interact with software.

System	:	Intel I3 Processor.
Hard Disk	:	40 GB.
Monitor	:	15 VGA Colour.
Ram	:	4 GB.
Mobile	:	Android

IX. Scope

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. This protect from unauthorized access. Our system allows access of account from any location

X. SYSTEM ARCHITECTURE

In above architecture 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 intercalary into the countersign, 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 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.

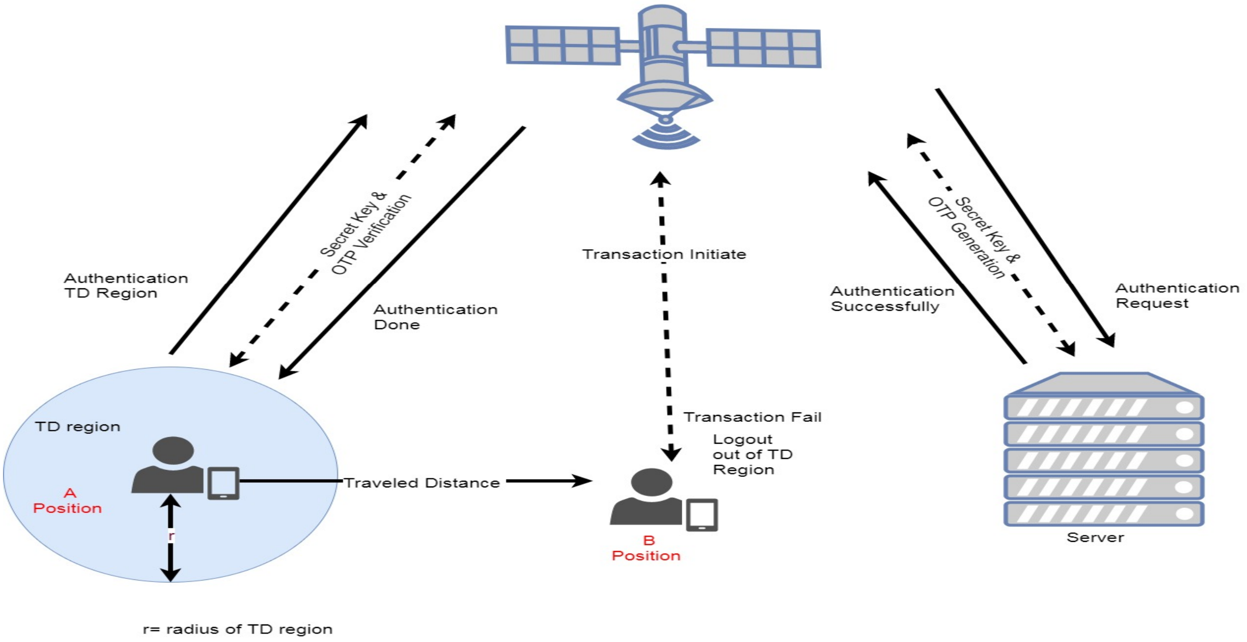

Fig. system architecture

XI.CONCLUSION

It has been realized that the smartphone based mostly car accident detection system is not an easy task to handle. It is really surrounded with many obstacles that prevent the researchers from achieving 100¬curate detection system. The main purpose of the system is to find the nearest emergency points from the accident location this was achieved by using some feature that the GPS receiver and Google maps are providing. Traffic notification is provided by the system to the nearest app users to get the information about the accident place with the help of that they can choose different route to avoid the traffic.

REFERENCES

[1] 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.
[2] Becker, C. and F. Durr, 2005. On Location Models for Ubiquitous Computing. Personal and Ubiquitous Computing, 9 (1): 20-31, Jan. 2005.
[3] Eagle, N. and A. Pentland, 2005. Social Serendipity: Mobilizing Social Software. IEEE Pervasive Computing, 4 (2), Jan.-March 2005.
[4] Gruteser, M. and X. Liu, 2004. Protecting Privacy in Continuous Location-Tracking Applications. IEEE Security & Privacy Magazine, 2 (2): 28-34, March-April 2004.
[5] Jamil, T., 2004. The Rijndael Algorithm. IEEE Potentials, 23 (2): 36-38.
[6] 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.
[7] 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.
[8] 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.