Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 5, MAY-2018

Achieving Platform Security in Internet Transaction using LDEA

Miss. Shivganga Gavhane[1] ,Mr. Praditya Vishwakarma[2],Mr. Vaibhav Pimparwar[3], Mr. Naveen Kumar[4], Miss.Bhagyashri Ghule[5]

Department of Computer Engineering,
D.Y.Patil Institute Of Engineering Management And Research
shivganga168@gmail.com
praditya vishwakarma@gmail.com
vaibhavpimparwar809@gmail.com
kumarnaveen70584@gmail.com
ghulebs1996@gmail.com

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 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 are providing extra security by OTP and secret key.*

Keywords- Book Location Privacy, Mobile Networks, shoulder surfing, GPS.

I.INTRODUCTION

Security has always been an important 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 within 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 generating 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.

II. LITERATURE SURVEY

1. Location Based Services using Android

Authors: Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta

Initially mobile phones were developed just for spoken language however currently days the situation has modified, spoken language is simply one side of a transportable. There are alternative aspects that ar major focus of interest. 2 such

major factors ar application program and GPS services. each of those functionalities ar already enforced however are solely within the hands of makers not within the hands of users because of proprietary problems, the system doesn't enable the user to access the mobile hardware directly. But now, once the discharge of golem based mostly open supply transportable a user will access the hardware directly and style made-to-order native applications to develop internet and GPS enabled services and might program the opposite hardware elements like camera etc. during this paper we'll discuss the facilities obtainable in golem platform for implementing LBS services (geo-services)

2. Context Sensitive Access Control

Authors: R.J. Hulsebosch†, A.H. Salden, M.S. Bargh, P.W.G. Ebben, J. Reitsma

We investigate the sensible practicableness of victimisation context data for dominant access to services. based mostly exclusively on situational context, we tend to show that users may be transparently provided anonymous access to services which service suppliers will still impose varied security levels. Thereto, we tend to propose context-sensitive verification strategies that permit checking the user's claimed credibility in varied ways that and to numerous degrees. additional exactly, typical data management approaches area unit accustomed compare historic discourse (service usage) information of a private user or cluster. The result's a comparatively robust, less intrusive and additional versatile access management method that mimics our natural method of authentication and authorization within the physical world.

3. **Supporting Location-Based Conditions in Access Control Policies**

AUTHORS: Claudio A. Ardagna, Marco Cremonini, Ernesto Damiani

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.

4. **The Data Encryption Standard: Past and Future**

AUTHORS: milese. smld and dennis **k.** branstad

The Data coding normal (DES) is that the 1st, and to the current date, only, in public on the market cryptologic formula that has been supported by the United States. Government. This paper deals with the past and way forward for the DES. It discusses the forces resulting in the event of the quality throughout the first Nineteen Seventies, the contention relating to the projected normal throughout the mid-I970s, the growing acceptance and use of the quality within the Nineteen Eighties, and a few recent developments that might have an effect on the longer term of the quality.

5. **Pipeline Algorithms of RSA Data Encryption and Data Compression**

AUTHORS: Jiaiimin Jiaiig

Various pipeline algorithms knowledge compression and encoding area unit designed to assess the impact of encoding on data compression. The primary pipeline shows that encoding fails to map great deal of redundancy for the computer file into a favourable kind for its later compression. The second pipeline, however, offers a decent potential to enhance the compressed output for additional compression by another compression algorithmic program. The pipeline algorithmic program conjointly identifies the various performances between lexicon knowledge compression and applied mathematics compression algorithms. In addition; the compression before encoding improves the potency of encoding and cause the potential development of a multifunctional algorithmic program that might operate as each compression and encoding.

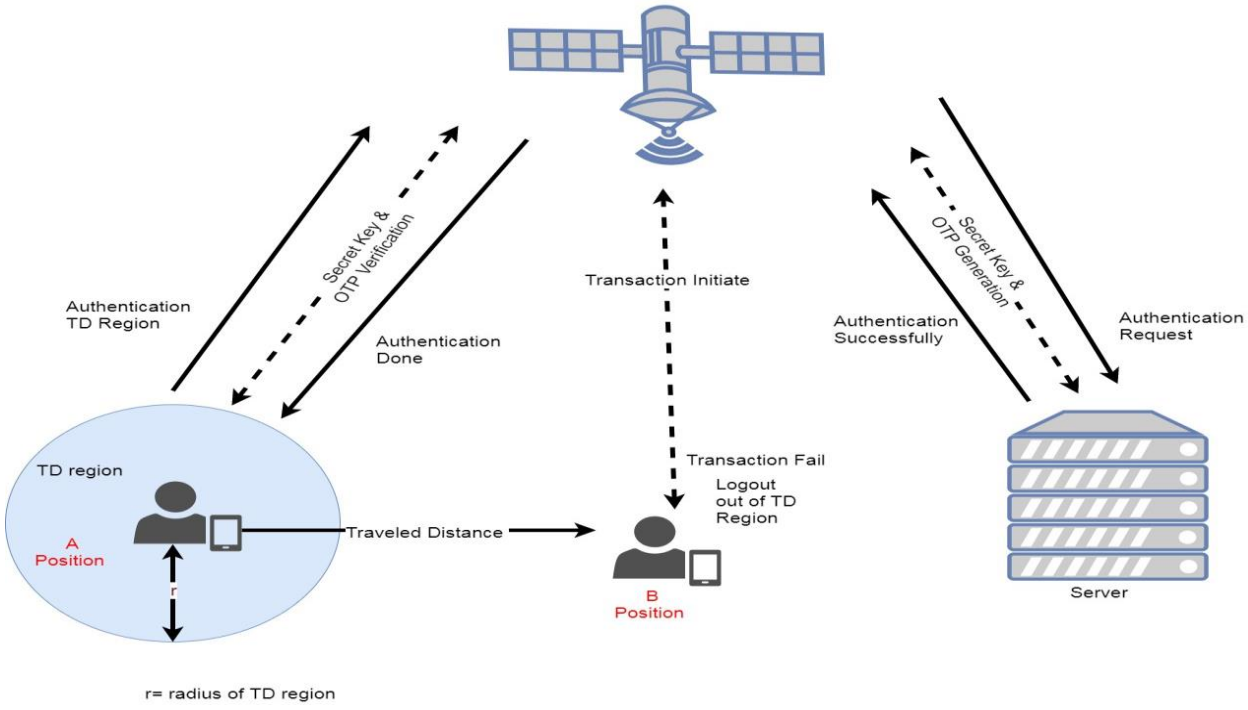
III EXISTING SYSTEM

The existing system has several issues like security issues, additional human involvement that could be a time intense method with several manual calculations. It even includes the machine injury and signature verification method for secured transactions that permits the purchasers and banks to waste their valuable time and resources. the foremost downside in on-line industry is unauthorized user access with pretend passwords. The hackers are attempting to hack the user accounts and square measure activity completely different unauthorized transactions.

IV. PROPOSED SYSTEM

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 specifies range in meters. After generating TD region successfully, user can view account details and user can perform money transaction operation.

V. SYSTEM DESIGN



VI. ADVANTAGES

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

VII. 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.

REFRENCES

[1] Aikawa, M., K. Takaragi, S. Furuya and M. Sasamoto, "A Lightweight Encryption Method Suitable for Copyright Protection." IEEE Trans. on Consumer Electronics, 44 (3): 902-910,1998.

[2] Becker, C. and F. Durr, "On Location Models for Ubiquitous Computing. Personal and Ubiquitous Computing", 9 (1): 20-31, Jan. 2005.

[3] Eagle, N. and A. Pentland," Social Serendipity: Mobilizing Social Software." , IEEE Pervasive Computing, 4 (2), Jan.-March 2005.

[4] Gruteser, M. and X. Liu, "Protecting Privacy in Continuous Location-Tracking Applications", IEEE Security & Privacy Magazine, 2 (2):28-34, March-April 2004.

[5] Jamil,T." The Rijndael Algorithm" IEEEPotentials, 23 (2): 36-38, 2004

[6] Jiang, J. "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, " 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.