Location Based Authentication For E-Banking

Rohit Joshi
Department of Information Technology
MET's IOE Bhujbal Knowledge City, Nashik, Maharashtra,India

Prince Gupta
Department of Information Technology
MET's IOE Bhujbal Knowledge City, Nashik, Maharashtra,India

Mahendra Hinde
Department of Information Technology
MET's IOE Bhujbal Knowledge City, Nashik, Maharashtra,India

Abstract- This paper reviews techniques that use location as an authentication factor, and make recommendations how location can be used for enhancing the security of banking using smartphone applications which require robust client authentication, and lastly how a secret key using algorithms will ensure in securing fund transaction. Authentication is one of the three main processes Authentication, Authorization , Accounting.

Keywords – Dataprivacy,authentication,mobile,authorization,location.

I. INTRODUCTION

The smart phones are becoming a major part in everybody's daily life. And all kinds of activities, including banking or financial mCommerce transactions (e.g. online shopping), nowadays are performing online via Smartphone applications whilst at the move. Approximately 50% of all Smartphone owners in the U.S. are using their Smartphone for banking transactions during the first quarter of 2011. There is an increase of nearly 100% compared to the year before now . However, many of the techniques used to authenticate the authorized client towards the remote authenticator (i.e. the bank is offering a financial services) in these mCommerce applications still based upon classic (i.e. static) authentication factors like passwords, biometrics, or tokens,etc. The fact is that the client while on the move, whilst using these mCommerce applications is not considered or used to enhance the authentication security. Reliable client authentication and the data protection are still major concerns for mCommerce application providers because a classical authentication factors are open for hackers. As a result, mCommerce application providers restrict access, on average, to 30% of possible services to their clients via the Smartphone applications.

Any financial institutions engaging in any form of Internet banking using smart phones necessarily have effective and reliable methods for authenticating customers. An effective authentication system is required for compliance with requirements for safeguarding customer information, for preventing money laundering and terrorist financing, and to reduce fraud, for inhibiting identity theft, and promote the legal enforceability of all electronic agreements and transactions. The risks of doing businesses with unauthorized or incorrectly an identified persons in an Internet banking environment have result in financial loss and also reputation damage through fraud, disclosure of customers information, corruption of data, or an unenforceable agreements. There are variety of technologies and methodology financial institution can use to authenticate customers. This project reviews techniques that use location as authentication factor, and makes recommendation that how location can be use to enhance the security of a banking using smart phone application requiring robust client authentication and lastly how secret key using an AES algorithm ensure securing fund transaction. This shall encourage financial or ecommerce application providers to offer more services via Smartphone application to their clients.

II. TERMS AND DEFINITION

Authentication is the act conforming the truth of an attribute of a single piece of data or entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually conforming that identity of a person by validating their identity document and verifying the validity of website with a digital certificate, tracing the age of the artifact by carbon dat-

ing or ensuring that product is what is packaging and labeling claim to be. In other words, authentication often involve verifying the validity of at last one form of identification

Authorization or **authorisation** is the function of specifying access rights to resources related to the information security and computer security in general. More formally, "to authorize" is to define an access policy. For example, human resources staff is normally authorize to access employee records and this policy is usually formalized as an access control rules in the computer system. During the operation, a system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved or disapproved . Resources include individual files or item's data, computer programs, computer devices and functionality provided by computer applications. Examples of consumers are computer users, computer programs and other devices on the computer.

The **International Mobile Station Equipments Identity** or **IMEI** is a number, usually unique, to identify 3GPP (i.e., GSM, UMTS and LTE) and iDEN mobile phones, and also some satellite phones. It is an usually found printed inside the battery compartment of the phones, but can also be displayed on-screen on most of the phones by entering ***#06#**on the display, or alongside other system information in the settings menu on Smartphone operating systems.The IMEI number is use by a GSM network to identify valid devices and therefore can be used for stopping a stolen phone from accessing that network. For example, if a mobile phone is stolen, the owner can call his network provider and instruct them to "blacklist" the phone using its IMEI number. This renders the phone useless on that network and sometime other networks too, whether or not the phone's SIM is changed. The IMEI is only used for identifying the device and has no permanent or semi-permanent relation to the subscriber. Instead, the subscriber is identified by transmission of anIMSI number, which is stored on a SIM card that can (in theory) be transferred to any handset. However, many network and security features are enabled by knowing the current device being used by a subscriber.

The **Global Positioning System** (**GPS**) is a space-based satellite navigation system that provides location and time information in an all weather conditions, anywhere on or near to the Earth where there is unobstructed line of sight to four or more GPS satellites .The system provides critical capabilities to military, civil, and commercial users which are around the world. The United States government has created the system, which maintains it, and makes it freely accessible to anyone with the GPS receiver.

In the cryptography, **encryption** is a process of encoding the messages or information in such a way that only the authorized parties can read it[1]. Encryption does not of itself prevent the interception, but denies the message content to interceptor[2]. In encryption scheme, the message or the information, referred to as plaintext, is encrypted using encryption algorithm, generates cipher text that can only be read if decrypted[3]. For the technical reasons, encryption scheme usually uses a pseudo-random encryption key generated by the algorithm. It is in principle possible to decrypt message without possessing the key, but for well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with a key provided by the originator to recipients, but not to unauthorized interceptors.

A. LITERATURE SURVEY

B. NEED

Today's information systems requires an explicit identification between communicating entities (often the entities are users). Process of entity identification is in general called the authentication. The authentication is defined as affirmation of an identity of certain object in centralized system. Authentication techniques are commonly classified into three groups as [4]

- User has something - techniques uses RFID (Radio Frequency Identification Device), hardware keys, etc.;
- User knows something - this group is based on knowledge of the confidential information, for example password authentication;
- User is someone - biometric techniques that are limited to the human authentication

Nowadays, many projects which discuss using of user's location as a new factor of authentication. The Location based authentication can be useful in many cases. The advantages of location-based authentication are present. The first place of a usage can be found in the hospital sector. A doctor shouldn't handle with patients' privacy information out of the hospital's border. Another example of location-based authentication we can find in the financial branch. If the user (account owner) would like to operate on his account, it should prove his location at the first. If a user is at home or in the bank office, he will get the access. If he is on another position, he won't get the access to his bank account. In general, the location-based authentication techniques can be used also for SSO (Single Sign On) [5], but the techniques proposed in this system principally assumes simply authentication (one identity per user).

Here in this system, we propose a new location-based authentication technique.Our system provides high level security by adding GPS location along with the user credentials i.e. username and password whereas other

systems only provide user credentials i.e. username and password. Our system checks GPS location on timely basis to secure data from unauthorized access and it uses self destructing keys, which expires after some time make this system more secure. Personal data were stored in the private cloud may containing account numbers, passwords, notes, and also other important information that could be used and misused by any competitor. These data are being cached, or copied, and archived by the Cloud Service Providers (CSPs), more often without users' authorization and control.The Self-destructing data mainly aims to protect the user data's privacy. All the data and their copies become destructive or unreadable after any user-specified time, without any user intervention. Morever, the decryption key is being destructed after the user-specified time. In our system, we present SeDas, a system that meets our challenge through a novel integration of cryptographic techniques with a active storage techniques based on T10 OSD standard (i.e. Object-based storage devices standard). According to the statistics, around 80 percent of the population of India uses cell phones and now a days maximum of them use smart phones . It would be very handy if people can carry on their thinking being able to perform banking on their cell phone is not sufficient. The transaction need to be secure our project specifically dealing with securing the online mobile transactions by using the self destructing key which implies in some time and then thereby providing stronger encryption and further using location as a major factor for generating the key.

C. EXISTING SYSTEM

Existing system do not provide high level security.They are only providing user credentials i.e. username and password.Existing systems do not have any GPS location priviledges.They do not secure the data from unauthorized access, and easily cracked by any hackers.They do not have uses self destructing keys.On the other hand,Our system provides high level security by adding GPS location along with user credentials, i.e. username and password. Our system checks GPS location on timely basis to secure the data from unauthorized access, and it uses self destructing keys, which expires after some time making this system more secure.

II. SYSTEM ARCHITECTURE

Smart phones are increasingly used, to perform the Mobile Banking applications whilst on the move. Current techniques are used to remotely authenticate the client to the service provider in an Mobile Banking application which is based on "static" authentication factors like passwords or tokens. The fact that the client is on the move, while using these M-Commerce applications is not considered or used for enhancing the authentication security. This system is concerned with including client's geographical location, is an important authentication factor to enhance security of the M-Commerce applications, especially those requiring robust client authentication. Further more the system secure the Banking Funds transaction online using the Self Destructive Data Crypto system. The SeDas system mainly uses shamir's algorithm to provide a strong security for transfer funds online with a self destruct key mechanism that destroys that key after a specific time interval to avoid misuse of the private data over the server. Location-based authentication is the new direction for the development of authentication techniques. Authentication and authorization are two of the most important security features for mobile transaction systems. We Uses space Time Authentication Technique that uses GPS system for a position determination of the person.

Most commonly, these schemes depend on basic three factors: what you know (secret), what you have (token), and what you are (biometrics). Here, we use SeDas System with the basis of Shamir's Algorithm for Secure Fund Transaction. It describes the architecture of our proposed system protocol including three parts: location registration, authentication and authorization and location verification etc.

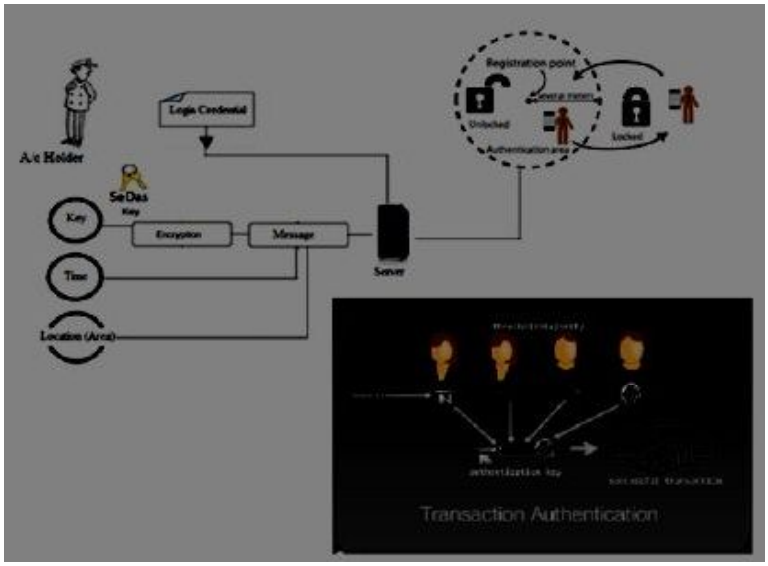

Fig 1: Overall architecture of the system.

IV. INTERFACES

A. Hardwaer Interface

Mobile Device:- The external hardware interface will support the mobile devices, such as smart phones. Any devive that support GPS

External Storages:- The product will support the transparent connections with an external hard drives in order to support automatic archiving capability.

B. Software Interface

Operating System:- The product will work with mainly Android 2.1 and above.

V. CONCLUSION

The system described in this paper which uses location as an authentication factor will be next step in securing banking transactions.The next secutiry level can be achieved by using IMEI no as a factor along with the location. So the online banking is a rapid growing field and the no of internet users are increasing rapidly.Thew number of attacks on current system is increasing day by day and this system will be helpful in reducing those threats in future.

REFERENCES

[1] Dax, J. "Publikationen." To appear in Distributed User Interfaces: Collaboration and Usability. Springer 2014 (2013).

[2] Kuseler, Torben, and Ihsan Alshahib Lami. "Using geographical location as an authentication factor to enhance mCommerce applications on smartphones."*International Journal of Computer Science and Security (IJCSS)* 6.4 (2012): 277-287.

[3] Shamir, Adi. "How to share a secret." *Communications of the ACM* 22.11 (1979): 612-613.

[4] D. Qiu, "Security Analysis of Geoencryption: A Case Study using Loran",Proceeding of ION GNSS 2007.

[5] Denning, D. and Macdoran, P., " Location-based Authentication: Grounding Cyberspace for better Security", Computer Fraud Security, 1996(2), pp.12-16.

[6] Jansen, W. Korolev, V, " A Location-Based Mechanism for Mobile Device Security", in WRI World Congress on Computer Science and Information Engineering, Los Angeles, California USA, pp. 99-104, 2009. http://csrc.nist.gov/publications/articles/articles_2009.html

[7] D. Denning and P. MacDoran, " Location-Based Authentication: Grounding Cyperspace for Better Security." In Computer Fraud and Security Bulletin, Feb. 1996.

[8] I.G.T. Ferreres, B.R. Alvarez, and A.R. Garnacho, " Guaranteeing the authenticity of location information." In IEEE Pervasive Computing, pp. 72-80, 2008. https://scholar.google.co.in/citations?user=ZyAk4EoAAAAJ&hl=en

[9] G. Yan and S. Olariu, " An efficient geographic location-based security mechanism for vehicular adhoc networks." In IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, MASS'09, 2009, pp. 804-809.

[10] Hsieh, Wen-Bin, and Jenq-Shiou Leu. "Design of a time and location based One-Time Password authentication scheme.". *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*. IEEE, 2011.