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 – Data privacy, 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 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-
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. Moreover, 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 privileges. 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. Hardware Interface
Mobile Device: The external hardware interface will support the mobile devices, such as smart phones. Any device that supports GPS
External Storage: The product will support the transparent connections with an external hard drive 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 the next step in securing banking transactions. The next security 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 number of internet users are increasing rapidly. The number of attacks on current systems is increasing day by day and this system will be helpful in reducing these threats in future.

REFERENCES