Secure Online Bank Authentication Using Geolocation Based System

Swati Gorde¹, Rajashree Gorde², Ashvini Dhayonde³ & Pradip Waghmare⁴

²¹³⁴ Student, SPCOE, Department Of Computer Engineering, Dumbarwadi, Otur

Abstract: In particular, authentication is the life of every individual essential closest friend. The user authentication security is depend on the strength of the security provided by the system. Today’s attacker, hackers, crackers, and spammers. Authentication authorization and auditing are the most important issues of security on data communication. In this system we proposed a new Geo-location based authentication system to solve this problem of security violation. The new approach is the way used by an information system, to authenticate a user and detect fraud based on their geolocation using geolocation as mechanism of authentication poses multiple issues and challenges including that location is not a suitable authentication factor, there are some privacy issues related to tracking user location and user location information can be forged. However, location and user behavior based security is not going to be a replacement for existing authentication and fraud detection mechanisms. It is implemented to augment current technologies and make security attacks more complex and be a deterrent against internet fraudster. We are providing the authentication according to the location of the client. Using GPS we are going to find out location of the user and according to location of user they will be allow to login into the system. Then also provide security from the textual password attack we are using the sharing algorithm to create share and use it in next step of the authentication during transaction. Our authentication server only needs to store user information and share instead of large password database.

1. Introduction

Today’s banking system has brought core banking for the user’s convenience, which is a set of services, where authentication plays main role. But these days, because of tremendous realization and growth in the field of hacking it is not safe to rely on internet to store all the information. So in order to overcome this problem we are proposing an efficient algorithm for secured bank authentication. The concept of Location Tracking is wide and popular and has profound uses. Marketing combined with technology has become an important aspect for the survival of global business entities. Geolocation is the ability to determine where online visitors are physically located. With geolocation, merchants can use information they already have to non-intrusively determine where their customers are physically located. For such type of an abnormal transactions a higher level of security can be intended. The Location based services is one such application that tends to focus a new medium of information mining and global marketing thus enhancing business prospects. The Location based services (LBS) are the mobile services in which the user location information is used to provide a service. The user location information consists of X-Y coordinates generated by any given positioning technique such as Cell-ID, GPS, etc. According to a report from the research revenues from mobile location based services (LBS) is frequently increasing which shows how important LBS applications are becoming to mobile users. The GPS is the most efficient positioning technique. It was developed mainly to be used in navigation systems. Because of the reduction in the size of the GPS receivers and because of the integration of GPS with some mobiles; GPS became one of the most important service providers in the LBS.

The mobile that is embedded with GPS receiver calculates the exact longitude, latitude and altitude values and those values can be used by LBS for finding the location. GPS also provides information like time for calculating sender and receiver locations based on the information received from the satellites. Using GPS receiver in the mobile device we can even set the navigation path from source to reach a particular destination. Three satellites may be enough for computing the position of mobile devices. There are not many projects that are carried out in the LBS field. This is because this type of application was somehow exclusive for mobile service providers because they use mobile cells information to get the signals from GPS Satellite. It determine the exact location in three dimension i.e longitude, latitude and altitude which then converted to get the exact address.
2. Related Work

In the literature review, we will focus on what work has been published in the area of geolocation and user behavior, what tools have been developed, and what challenges these technologies have. Today's network environment is full of dangerous attacker, hackers, crackers, and spammers. Authentication, authorization, and auditing are the most important issues of security on data communication. In this section, we proposed a new Geo-location based authentication system to solve this problem of security violation. We are providing the authentication according to the location of the client. Using GPS we are going to find out the location of the user and according to the location of user they will be allowed to login into the system. Admin add the location to database by using google map. Then also provide security from the textual password attack we are using the sharing algorithm to create share and use it in next step of the authentication during transaction.

The topics reviewed are:

Geolocation: This section is reviewing geolocation and the developed technologies to determine the location of a device which is connected to internet.

Geolocation tools: This section reviews the tools that have been developed to determine location of internet or mobile user.

Geolocation authentication: This section reviews current approaches of using geolocation as an authentication mechanism. Current fraud trends analyzed by an internet fraud analyser.

User Behavior: This section reviews current work related to the behaviour of user. By generating geographic boundaries on the Internet and providing location of customers, geolocation can be used effectively to detect potential fraud by analyzing the differences based on the user location and other information as user profile i.e. billing address or historical data. Traditionally, geolocation services were based on computer/device IP address. However, geolocation services have developed significantly with the adoption of mobile devices. All these approaches can be used by all types of mobile devices like mobile phones, laptops and even traditional desktop computers. GPS approach requires the device which having a proper GPS hardware. The Wi-Fi Location scheme requires the wireless access point to have additional location appliance hardware. The other approaches do not require additional hardware. The new mobile devices like IPhone or Android use a combination of cellular, Wi-Fi, and GPS to determine your location. If you're not within a clear line of sight to GPS satellites, the device can determine your location using Wi-Fi. If you're not in range of any Wi-Fi, it can determine your location using cellular towers.

Number of users of mobile phones were being tracked without their knowledge by installed scanners at secret locations in Bath, UK in order to pinpoint people's whereabouts. The scanners were capturing Bluetooth radio signals transmitted from devices such as mobile phones, laptops and digital cameras. No action perform from users. As they passed the scanners, their devices connected to the scanner and through Bluetooth ID they were registered. The data which is used in a system called Cityware to study how people move around cities. Eamonn O’Neill, Cityware’s director, said: The objective is not to track individuals, whether by Bluetooth or any other means. We are interested in the aggregate behavior of city dwellers as a whole. The notion that any agency would seriously consider Bluetooth scanning as a surveillance technique is ludicrous. This is a good example how a mobile device location can be tracked by using Bluetooth technology which is today incorporated in most mobile devices.

Another more traditional way to detect the location of a computer/mobile device is to use the device IP. Each computer on the Internet has a unique numeric address called IP address. IP is assigned to the computer by the user's Internet service provider, a university or a company, and a database matches such assignments to the location the network has registered. However, a company's addresses it can pool all IPs even it has branch offices worldwide. An ISP like America Online may route its customers' traffic through a single gateway, making AOL users in California appear to come from Virginia. There is a number of free and paid subscription geolocation databases, ranging from country level to city or state level. These databases typically contain IP address data which may be used in firewalls, ad servers, routing, mail systems, web sites, and other automated systems where geolocation may be useful. An alternative to hosting and querying a database is to obtain the country code for a given IP address through a real time transaction from a remote server.

3. Proposed System

We are going to introduce a new approach intended to standardize the solution of how an information system is authenticating a user or detecting fraud by using geolocation information. First, we introduce concepts of how an internet transaction system is architected. The solution intended to detect fraud is using geolocation, transaction monitoring and user behavior to detect
anomalies present in transaction patterns. The solution uses a SAML based authentication to communicate between the systems involved. The fraud detection system is using a historical data mining to detect a falls of transaction is under the user pattern or is anomaly.

A. Internet Transactions:

A transaction processing is a type of computer processing in which the computer responds immediately to user requests. Each request is considered to be a transaction. The example of transaction processing is Automatic teller machines for banks. An end user is, who requests the execution of transactions, such as a customer. Computer is used by the end user. Through web browser interacting with the end user is a web application that is running on the end user machine. The browser displays the web pages rendered by the internet application that is running on a remote server and it is usually using a database. The Browser and server are communicating using TCP/IP and HTTP protocols.

B. Real time fraud/authentication:

Location based services have one important characteristic which is to establish a user context. The user context has the following information:

1. System properties has all the system properties including:
   a. IP - Internet Protocol ID
   b. Device MAC - Unique device ID
2. User information has all the user information
3. Transaction information has information about the transaction the user is performing including:
   a. Time of the transaction
   b. Type of transaction
   c. History of transactions
4. Location information includes:
   a. Current Location
   b. Location History

This figure shows the following steps:
1. The user attempts to reach an Internet application
2. The application generates the authentication request. The request is encoded and embedded into the URL for the Identity Provider.
3. The Internet Application sends a redirect to the user's browser. The redirect URL includes the encoded authentication request that should be submitted to the Identity Provider service. The authentication request includes additional geolocation attributes:
   a. Device IP
   b. Device MAC
   c. Device coordinates, if available
4. The Identity Provider decodes the authentication request and extracts the authentication information. The Identity provider then authenticates the user and assigns a risk score.
5. RTSP performs the following operations:
   a. Retrieve Geolocation information.
6. The Identity Provider encodes the response and returns that information to the user's browser. The Identity Provider provides a mechanism so that the browser can forward that information to the originating Internet Application.
7. Internet Application verifies the response using the Identity Provider's public key. If the response is successfully verified, it redirects the user to the destination URL.
8. The user has been redirected to the destination URL and is logged in to Internet Application.

Location based services:

have grown significantly over the last 5 years fueled by the growth in mobile computing. This trend is likely to continue as the mobile applications are maturing. Location based services can be used for authenticating the end user. Basically, all the technologies are already in place to support this. In this chapter, we are reviewing the issues, trends and challenges related to authenticating the user based on location. This chapter covers the following topics:

a. Location as an authentication factor section is analyzing the suitability of using location as an authentication factor.

b. IP spoofing section is reviewing the internet protocol and looks at how IP can be “spoofed”. This is important for this essay because IP is a traditional method to determining end user location.

c. Privacy section is describing a major concern with using location as part of the authentication. This concern is privacy
4. Conclusion

We proposed an effective technique to provide greater security in the field of core banking and internet banking applications. At the beginning, while creating an account, the bank, location, and signature of the applicant is taken by scanning his/her signature from the application. Now this scanned image is taken as input and is subjected to pre-processing to remove noise and to increase intensity. This pre-processed image is encrypted into two shares by using two out of two scheme. One share is stored in the bank database, another share is printed and given to the applicant. Applicant had to provide his share during every transaction. Then according to the user location tracking using GPS allow user to access system.

5. References


