International Journal of Research in Engineering, Science and Management
Volume-2, Issue-5, May-2019
www.ijresm.com | ISSN (Online): 2581-5792

GeoMob - A Geo Location based Browser for Secured Mobile Banking

A. H. Srinivasa Rao[1], C. S. Deepashree[2], Dhanashree Pawaskar[3], K. Divya[4], L. Drakshayini[5]
[1]*Associate Professor, Dept. of Computer Science and Engg., Dr. Ambedkar Inst. of Tech., Bangalore, India*
[2,3,4,5]*Student, Dept. of Computer Science and Engg., Dr. Ambedkar Inst. of Tech., Bangalore, India*

***Abstract*: With banks reaching its users via mobile banking, it is becoming one of the essential feature that is demanded by almost every smartphone user. Mobile banking via a mobile browser is similar to internet banking. Browsing-based threats for smartphones are just the same as those for personal computers, elevating the need to focus on mobile security. Among the several authentication schemes, geolocation authentication is gaining importance as it is found most suitable for mobile devices. In this paper, GeoMoB, a dedicated secure mobile browser for mobile banking that makes use of multifactor authentication is designed and developed. GeoMoB features a geolocation based authentication scheme which ensures security of mobile transactions based on the user location. In addition to the existing two factor authentication scheme using user ID, password and OTP, the mobile number and geolocation is used to authenticate the user. The geolocation intimates the banks location from where the transaction is going to be performed thus helping banks to ensure secure transactions. The geolocation of the user is acquired through the network provider and hence the need for using GSM is eliminated. The multifactor authentication used in GeoMoB ensures security while performing mobile transaction and prevents users from various attacks.**

***Keywords*: Mobile banking, Geolocation, Authentication, Mobile browser, Multi factor authentication**

1. Introduction

Smartphones offer several ways to access a services which may include mobile apps, mobile browsers and even as widgets. It comes to the decision of the business to choose how to reach their customers. Though mobile apps are being commonly used among the users, mobile browsers find their own importance. Mobile browsers are the ones that enable the user to view websites on their hand-held devices whereas mobile apps or applications are the ones that are to be downloaded on the user's mobile phone in such a way that once downloaded it may be used any time. Though mobile applications are the easiest way in accessing a service, mobile browsers are preferred in accessing various services as they have certain advantages when compared to the mobile applications. A mobile browser called a minibrowser, microbrowser or wireless Internet browser (WIB), is a web browser designed for mobile phone and tablets. They are specially designed so as to display web content for small screens. Mobile browser software must be small and efficient to accommodate the low memory capacity. Some common mobile browsers are Google Chrome, iris, Mozilla Firefox, kindle, Apple Safari, Opera, Internet Explorer, Maxthon, Blackberry, UC browser, etc.

According to current statistics, it can be observed that the trend of mobile internet is growing tremendously over desktop internet. Since 2013, more tablets and smart phones were sold than PC's., bringing in the need for mobile browsers. Now a days, world is tending towards mobile dominated web. One out of every ten costumers are coming to a site using their mobile devices. More people in Africa have a mobile phone than access to electricity. Mobile browsers make the various websites instantly available unlike mobile applications that need to be downloaded for accessing services. The mobile web browsers are capable of rendering websites in a common fashion whereas in case of apps, the operating system has to be considered. The advantages that mobile browsers are that there is no need for frequent updates and makes the websites instantly available. The mobile banking scenario has several threats associated with it. All time connectivity to the internet in the mobile devices have paved way to several attacks including man in the middle attack, phishing attacks etc. making security an important factor to be considered when providing services to the user.

When the business decides offer their services through mobile browsers, there comes the need for choosing the appropriate browser. Several public and private sector banks have launched mobile applications to satisfy the customer demands. But the drawback with such applications is that the frequent updates and the all-time connectivity has posed several threats. Hence accessing mobile banking services through mobile browsers is much more significant. Several mobile browsers have been evolved since the advent of mobiles, yet they are faced with several shortcomings. In the initial days when the mobile browsers were into the smart phones, rendering the websites on the handheld devices was one of the major issues. But today the challenge is in terms of preventing from various attacks. Though web browsers are provided with sophisticated features in terms of security, mobile browsers are yet to cope up with such changes. The issues in the existing mobile browser have led to the need for development of a secure mobile browser for mobile banking based transactions.

A. Related works

Shivangi Gupta et. al. [1] concentrates on the diverse estimation procedures and the apparatuses that are utilized for web advancement. This paper likewise connotes the different real and true issues and difficulties that ought to be taken under thought while growing expansive web applications. The work done in [2] analyses the means of accessing sensitive and non-sensitive data from websites though web browsers. It emphasis on the protocols that are used for accessing such information from the web browsers. The work in [3] elaborates on one of the most common type of attacks man in the browser attack. This paper proposes a secure communication protocol between human and bank servers for preventing man in the browser attacks. The work in [4] proposed a new web browser, OP web browser that was able to improve browser security by combining operating system design principles with formal methods. It ensures security in three levels which include developing novel and flexible security policies that allows the user to include plugin into the system, adapting formal methods to prove that the address bar displayed within our browser user interface always shows the correct address for the current web page and implementing a browser-level information-flow tracking system to enable post-mortem analysis of browser-based attacks. Though this browser was able to overcome many of the attacks, it had a limitation of the dependency on the OS for its development. Mobile browsers, though has comparatively lesser security features when compared to the desktop browsers, several schemes have been proposed to ensure security. Among the various aspects of security, authentication is the prime factor that is considered for accessing services. Authentication is the means of validating the user to access a particular service. Several authentication mechanisms have been proposed to ensure secure access. In the work of Patel, Vishal M., et al. [5], continuous authentication scheme is proposed in which the user is monitored continuously once the initial access to the mobile device is done. Such kind of authentication schemes consume large amount of memory as the user activity has to be monitored till the end of service access. Several other authentication schemes which include fingerprint based authentication for mobile devices as in authentication based on human movement usage and location patterns make use of learning algorithms to identify users and prevent users from various attacks like brute-force, social engineering etc., Authentication based on the user behaviour like the typing pattern was analysed in which served as a means of securing a mobile device in cases of mobile theft. The typing behaviour of the valid user is observed and is compared with the typing behaviour of the fake user based on which the user is authenticated. Multi factor authentication schemes for mobile devices have been evolving with the increase of performing financial transactions in the mobile devices. The multifactor authentication scheme which makes the use of touch dynamics biometrics along with the usage of a personal identification number (PIN)-based authentication identified impersonation attempts.

The study of the existing system paved way for the transpiring the idea of the proposed GeoMoB which is a dedicated browser for performing mobile banking based transactions. Rather than possessing several mobile applications for various bank accounts, the GeoMoB creates a unified interface to access several bank accounts in a single browser. By using GeoMoB the user may also be able to secure his transactions from the alarming phishing attacks and the multifactor authentication validates the user before performing transactions.

B. Mobile banking

Mobile banking allows the customer of an institution to conduct banking activities such as receiving account alerts, checking balances or making payment through a smartphone or a tablet. There are several challenges for building a dedicated browser to access mobile banking features:

- *Handset operability:* It is one of biggest for banks to make a mobile banking solution that can work on different types of mobile phone devices. Some devices support Java ME, some WAP browser, SIM Application Toolkit and some support only SMS.
- *Security:* Security of financial transactions and transmission of financial information are most complicated challenges in front of banks. They can increase security by using authentication of device before allowing for transactions, authentication of user ID and password of costumer, encryption of data transferred and stored in device, security of application and offering physical security of device. OTP generation is a good measure adopted by banks to increase security.
- *Reliability and Scalability:* With the increasing demand of mobile banking the banks has to assure its best service that is able to work quickly and secure all the 24x7 time.
- Personalization: Application has to support different preferred languages, date/time format, amount format, alerts and default transactions.

The following are the common attacks targeted on Mobile Browsers

- *Proxy Trojans:* Keyloggers are the most primitive form of proxy Trojans, followed by browser-session recorders which capture more data, and lastly MitBs are the most sophisticated type.
- *Man-in- the-middle:* SSL/PKI etc. may offer protection in a man-in- the-middle attack, but offers no protection in a man- in- the-browser attack.
- *Boy-in- the-browser:* Malware is used to change the client's computer network routing to perform a classic man-in- the- middle attack.
- *Clickjacking:* Clickjacking tricks a web browser user into clicking on something different from what the

user perceives, by means of malicious code in the webpage.

2. Geo location authentication

Two factor authentication schemes has gained immense importance after the launch of mobile banking. Two factor authentication schemes verifies the user based on what he knows and what he possess. The popular two factor authentication scheme used for mobile banking scenario works based on the username and password which the user knows and the One Time Password (OTP) which the user receives through his mobile phone, which the user possess. Though the existing OTP based authentication mechanism is found to be effective, the problem with this kind of authentication scheme is with loss of the device (i.e. what the user possess). To enrich the authentication capabilities, GeoLocation based authentication has been evolved. Geo Location authenticates the user based on the location of the user (i.e. where he is). Geolocation is a term used to infer the geographical location of the user, based on available information. GeoLocation can authenticate users based on cookies, IP address, MAC address etc., In case of authenticating the users based on the IP address, host system's IP address is segregated from a packet header, identifying the owner of the IP address range associated with the target system. It works by looking up an IP address on a WHOIS service and thus retrieving the user's physical address. The IP address location data include information such as country, region, city, postal/zip code, latitude, longitude and time zone.

GeoLocation which generally denotes the latitude and longitude of a particular region has augmented its proficiency by identifying several other parameters apart from the geographical information. It possible to obtain several other parameters such as domain name, connection speed, ISP, proxies etc., based on the data which the IP address makes use of to determine the location of the user. GeoLocation authentication has been used for several application ranging from fraud detection to mobile voting. Comprehending the potentials of geolocation based authentication, this paper presents GeoMoB, a secured browser for mobile banking which verifies the authenticity of the user by making use of the geolocation.

A. Proposed system: Geomob

A browser with more features is more dangerous for online banking, features like cookies, add-ons, plugins, bookmarks, save history, JavaScript enabled, etc. further add to vulnerabilities. The browser which is used for making transactions, is usually used for surfing whole web so there are large changes of attacking malwares. Hence the proposed GeoMoB is designed in such a way that it is dedicated for using only mobile banking. GeoMoB provides an integrated interface to access several bank websites where the user possess accounts as well as assures secure authentication mechanisms to validate the user.

1) Features of GeoMoB

- A mobile browser is designed, which is exclusive for bank transactions and cannot surf any other sites.
- The browser contains only four options namely previous, next, refresh and history to avoid vulnerabilities.
- The previous option goes to the previous bank site;the next option goes to the next bank site;the refresh option reloads the current bank site and the history option consists of two button such as to view history and to clear history.

2) GeoLocation authentication in GeoMoB

As discussed in Section IV, to obtain the geolocation of the user, several parameters can be conidered. The proposed GeoMoB browser considers IP address of the mobile device as it is easy to obtain and accuracy of the result obtained may be accurate. GeoMoB makes use of GeoLocation database which contains information regarding country, region, city, latitude, longitude, zipcode and time zone and is capable of supporting IPv4 and IPv6 address formats making it compatible for updates. GeoMoB authenticates its user as follows:

- *Step 1:* GeoMoB obtaines the IP address of the user.
- *Step 2:* Based on the IP address of the user, the location of the user is obtained from the database.
- *Step 3:* The location of the user is obtained using the service provider to confirm that the IP address has not been modified to surpass the geolocation authentication.
- *Step 4:* If the user's current location matches with the GeoMoB's database, then the browser homepage is displayed else the GeoMoB shuts down abruptly.

B. Workflow of Geomob

- The user has to initially register with GeoMoB by listing the banks in which the user possess account. Apart from this a set of valid locations from which the user will be performing the transactions is also to be given to the user.
- If the user has the need to perform bank transactions in newer locations, a security question and answer is to be chosen by the user.
- This registration details are maintained in the local database of the browser and does not require connectivity to the internet.
- When the browser is opened, mobile number is given as input and the system acquires the location as illustrated above.
- If the location detected match with the location at the time of generation, an OTP is generated. If OTP matches, then the homepage are shown else a warning message is sent.
- In case of new location, the user has to choose among the security questions the one which the user has chosen and its corresponding answer. If it matches

then OTP is generated else a warning message is sent.

- To enter into a bank site, click the corresponding bank button.
- The bank home page is opened and now you can surf this website normally.
- Here, the credential login is given as input and then the bank server validates the details.
- The transaction begins and is authenticated; this transaction is confirmed and finally exits.
- The geolocation authentication helps us to provide security with two identities i.e. user's phone number and the geographical position of user so as to verify person's authentication.
- Only if this location matches with the location sent by the user, the transaction can be done.

3. Design

GeoMoB is a dedicated web browser for mobile banking and hence do not possess much features as in a normal mobile browser. The user-interface elements of GeoMob mobile browser include:

1. A back button to move back to previous page.
2. A forward button to move to forward page.
3. A refresh or reload button to reload the current page again.
4. Clear History button so that we can delete all history.
5. The viewport i.e. the visible area in which page loads.

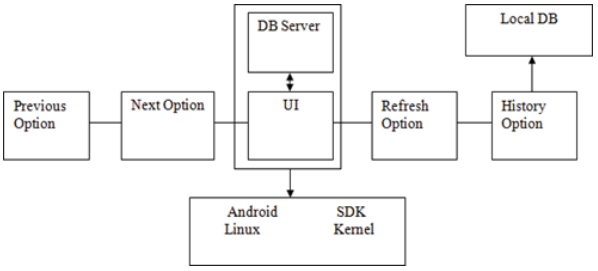

Fig. 1. GeoMoB architecture

The flow diagram of the proposed GeoMoB is illustrated in Fig. 2.

There are total four buttons on this browser namely forward, backward, refresh and clear history button. As the browser is opened, a default website and four browser buttons appears. In addition, various bank buttons also appear. If a bank site is to be opened, then the corresponding option can be chosen and the mobile website of that bank will be loaded on its webview. This browser doesn't contain any search engine, nor URL link, nor any cookies, plug-ins and add-ons. The bank site can be normally surfed as in a browser like Chrome, Firefox, Safari, Opera, etc. One can refresh the page, go back, go forward and view and clear history. Once the clear button is presses, it is not possible to access the previous option as it deletes all history. There is no way that the history can be viewed. Security in the browser is ensured by including some type of authentication which helps us to identify person identity in addition to UserID, password and OTP based two factor authentications.

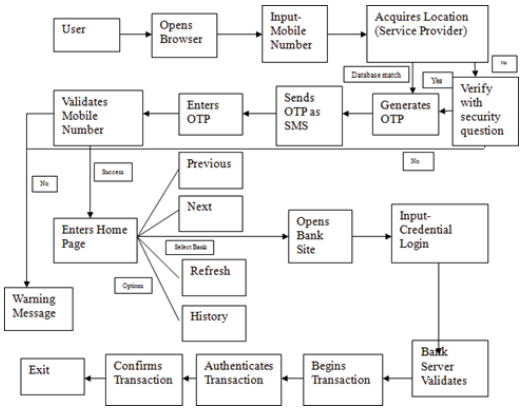

Fig. 2. Flow diagram for proposed GeoMoB

In addition to the existing authentication scheme, geolocation authentication has been used. This will acquire the geographical location whenever the browser is opened through service provider. It is capable of identifying costumer position without activating GPS also. The GeoMoB makes use of the information provided by the Network provider for obtaining the user location and thus ensures additional level of security. This browser has no add-ons or plug-ins. This browser limits by restricting to other websites as it can surf only default website and banks mobile websites. Banks already have taken several measures against some known malware and phishing attacks. As this overall reduces vulnerabilities, man in the browser is less because it appears it in the form of browser helper object/ browser extension/plugins/add-ons. The extra feature to this browser i.e. geolocation authentication helps us to maintain data server of costumers with two identities i.e. costumers phone number and the geographical position of costumers so as to verify person's authentication. Apart from banks multifactor authentication there is also a security authentication in browser. While surfing the banks mobile site on this browser security of your transactions increases as there is no cookies in this browser as cookies can be proved very dangerous as it stores the information about the sites visited and sometimes one has to manually delete this cookie. With the rise of multi factor authentication schemes, the inclusion of geolocation to the existing two factor authentication scenario for mobile banking will assure security to the mobile banking users and prevents the users from several attacks like phishing. As GeoMoB is a dedicated mobile browser to perform banking transactions, attacks including man in the browser attack, proxy trojans, clickjacking etc., can be encumbered

4. Implementation

GeoMob, the secure mobile browser is developed using the Android Studio and Andriod SDK based on the proposed design. The user must register himself with the browser app by choosing the name of the banks with which he has accounts.

Once the user chooses the banks, he will be able to see the name of the banks as icons on the browser. In this way, the user need not enter the URL's of the bank websites ensuring the prevention of Phishing and Man in the browser attacks.

The Fig. 4. shows the home page of GeoMoB. Once the user clicks the GeoMob browser this homepage is displayed. Once The mobile number and the GeoLocation is verified, the homepage of GeoMoB is displayed. Fig. 5. shows the home page with various icons of banks. During the registration process, the user has to list the banks where he possess accounts along with the valid location from where the transactions are going to be performed and the security question with its answer. The list of banks chosen while registration appears as icons and on click of the icon the bank web page can be accessed. The user will be able to provide the username and password to perform the banking transactions.

This multifactor authentication employed in GeoMoB is capable of safeguarding the users from various mobile based attacks.

Fig. 3. Geomob startup page

Fig. 4. GeoMoB page home page

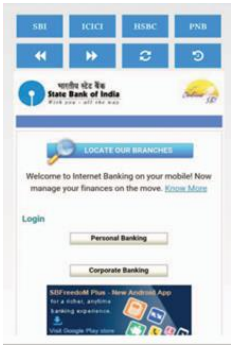

Fig. 5. Accessing bank website through GeoMoB

5. Conclusion

The increasing use of mobile devices has leveraged the demand of the customers to a much greater extent. Service providers choose to offer their services through mobile devices. Though dedicated mobile applications for delivering services are preferred, in terms of security such applications often pose a threat. The frequent updates and the all-time connectivity to the internet in using mobile applications pave way to several attacks. The utilization of mobile browsers is less prone to such attacks as the websites are instantly available unlike mobile apps which require prior installation and updates which are more secured for mobile banking scenario. In this paper, a dedicated browser was developed for banks so as to make secure transactions. The proposed GeoMoB works based on multifactor authentication which makes use of the mobile number, geolocation, userID, password and OTP. The unique feature of the GeoMoB is that it does not use GSM to determine the location. The location is obtained from the network service provider. The browser has a default homepage, whenever a person wants to enter a specific website of a bank it displays the default homepage by verifying the mobile number and the geolocation of customer. Only after verifying the location, the desired bank web site can be accessed. This provides additional security to the financial transactions made in mobile browsers. The application here takes into account the authentication made by geolocation. In future, various other authentication schemes can be combined and a multifactor authentication scheme may be utilized for secure mobile banking.

References

[1] S. Gupta and S. Dhir, "Issues, Challenges and Estimation Process for Secure Web Application Development," *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)*, Ghaziabad, 2016, pp. 219-222.

[2] Ander, Stuart D., et al. "Retrieving both sensitive and non-sensitive content in a secure manner." U.S. Patent No. 9,288,189. 15 Mar. 2016.

[3] Tsuchiya, Takashi, et al. "Secure Communication Protocol Between a Human and a Bank Server for Preventing Man-in-the-Browser Attacks." International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing, 2016.

[4] C. Grier, S. Tang and S. T. King, "Secure Web Browsing with the OP Web Browser," *2008 IEEE Symposium on Security and Privacy (sp 2008)*, Oakland, CA, 2008, pp. 402-416.

[5] V. M. Patel, R. Chellappa, D. Chandra and B. Barbello, "Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges," in *IEEE Signal Processing Magazine*, vol. 33, no. 4, pp. 49-61, July 2016.