AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Android Framework To Provide Secured Services For Online Banking Using User Profile And Access Matrix

[1]Dr. Pradeep Gurunathan, [2]Ms. J. Santhiya, [3]Ms. B. Kayalvizhi

[1]*Associate Professor, Dept. of Information Technology, A.V.C College of Engineering, Mannampandal*
[2]*Assistant Professor, Dept. of Information Technology, A.V.C College of Engineering, Mannampandal*
[3] *Engineering Scholar, Dept. of Information Technology, A.V.C College of Engineering, Mannampandal*

Address For Correspondence:
Dr. Pradeep Gurunathan, Associate Professor / Dept. of Information Technology, A.V.C College of Engineering, Mannampandal – 609 305, Mayiladuthurai, Nagapattinam Dist., Tamilnadu, India
Mobile: +91 98653 71 172; E-mail: pradeep.g8@gmail.com

ARTICLE INFO

Article history:
Received 26 April 2016
Accepted 21 July 2016
Published 30 July 2016

Keywords:

ABSTRACT

The main objective of this paper is to provide an effective and efficient Android framework for secured banking services using user profile and access matrix. In the past few years, mobile users in India have used 2.5G cellular network to access the Internet using the technologies such as GPRS (General Packet Radio Service), Edge, etc., and the consumers have begun to realize the power of having the Internet access with anywhere in the world. With these technologies, consumers are able to access their mobile phones. The advantage of this approach is to felicitate the users in performing their financial transactions by providing better service through the mobile application. This paper discusses the variety of mobile banking services and its performances. Further, the improvement of financial services for banking through ANDROID application is discussed in this paper.A third party mobile phone user can perform some kind of financial transaction through their mobile phone. But most of the users are interested in performing basic transactions such as querying for account balance and making bill payment.

INTRODUCTION

With the increase in the number of mobile devices, there will be more and more new payment methods. NFC-enabled devices, digital wallets and Beacon as well as PayPal's new wireless payment solution, are steadily reaching the mass market by allowing consumers to buy the products through on-line this transactions. The rapid growth of connected devices/things/products is fueled by several things and the main driving trends are:

- Decreased technology cost (computing, data management, sensors, cloud etc)
- Smartphone adaption (remote control, apps, internet connectivity etc)
- Customer expectations (efficiency, context, intelligent etc).

This offers significant improvement in customer-to-company communication which is vital for marketing research. For instance, the ability to encourage customers to offer feedback on the company's products and service is easy using website popup notices and email reminders. This paper targets the applications that are run on a smartphone device and communicate with remote service providers. The proposed system consists of three devices namely Android-Based Mobile device, Bank Server with local Database and Antimalware providers.

To Cite This Article: Dr. Pradeep Gurunathan, Ms. J. Santhiya, Ms. B. Kayalvizhi., Android Framework To Provide Secured Services For Online Banking Using User Profile And Access Matrix. ***Aust. J. Basic & Appl. Sci.,*** *10(12): 231-236, 2016*

For banks, mobile banking is a brilliant opportunity to simultaneously encourage new customers while paring operational costs. By responding to the innovations in mobile technology, banks are effectively saying they are paying attention to the needs of their customers, while at the same time streamlining a number of processes to meet the fast-paced demands of the 21st century.

Consumers should also be aware that mobile banking poses certain identity theft concerns. While the transmission of data is encrypted across a secure network, hackers are always on the lookout for ways of accessing this information. Due diligence should be employed when relying on mobile banking, including close monitoring of your bank accounts, along with ensuring proper protection in the event that your mobile phone is lost or stolen.

To make maximum benefit of mobile banking, one should have smart phones for the banking operations. Some banks have specific software for specific mobile such as iPhone and Blackberry. People should download different apps based on their Smartphone. Many experts believe that mobile banking is more securing than Internet banking since there may exist few virus or Trojans in the phone. However, it does not mean that they are immune to any kind of threats. As phishing exist for internet banking users, there is "Smashing" for mobile banking users. When a mobile user receives any fake text message requesting for banking details of the customer, the proposed system facilitates with secured questions as a notification to the mobile user.

To provide the flexibility of users, an interface has been developed a graphics concepts in mind, associated through a browser interface, the GUIs at the top level has been categorized as follows

1. Administrative user interface design
2. The operational and generic user interface design

The administrative user interface concentrates on the consistence information that is practically, part of the organizational activities and which need proper authentication for the data collection. The interface helps the administration which all the transactional status like data deletion, data insertion and data updating along with executive data search capabilities.

The operational and generic user interface helps the user upon the system in transaction through the existing data and required services. The operational user interface also helps the ordinary users in managing their own information in a customized manner as per the assisted flexibilities.

One way to roll out a mobile-based service, for instance mobile banking, mobile payments or mobile e-Invoicing, is to build the front-end application this would be typically be an app in the Apple Store or Android Market) and the bank-side "mobile application server" separately. The front-end application can then communicate with the Bank's systems using web services: sending and receiving data through the API, over the internet and the mobile network. A Bank can decide to "lock down" access to their API to their own developed applications. Access can also be provided to clients or third parties, either on a subscription basis (accessing current accounts and moving money) or open to the public (such as news stories, offers, public statistics). Files would still exist within the Bank's environment, hidden behind the web services API. For example a mobile payment initiated by a user could probably become a UK Faster Payment transaction, a SWIFT MT101, or even be embedded within an SEPA XML file over the inter-bank space. In this case, web services are an enabler that can allow a bank to bridge their "file" world with a myriad of custom-made applications, without causing too much chaos onto the existing architecture.

Related Work:

Improving access to financial services, such as savings, deposits, insurance and remittances, is vital to reducing poverty. Savings can help poor people to invest in productive assets like livestock, a loan may help to expand business activities, and insurance can provide income for a family if a bread winner becomes sick.

Ali AlSoufi and Hayat Ali discussed an extended Technology Adoption Model (TAM) to incorporate the role of factors in influencing customer's perception towards M-banking adoption. In addition, the results of measuring this model empirically were presented to measure the factors' impact on M-banking adoption in of Bahrain. Mobile banking usefulness has to be continuing improved in order to match the user interfaces of elderly, retailers and others leading the curve with mobile technology. Attention should be given to the risks which that could affect day-to-day transactions performed through mobile devices. Thus, it should be eliminated or reduced in order to enhance customers trust in the banking services being offered. To motivate customers to adopt this technology, the bank should try to increase the level of service expansion periodically as it should offer versatility in its offerings. Technical infrastructure of mobile banking services should be sophisticated and developed in order to ensure reliable and timely offering of services to customers. New functionalities a bank should bush it up to continue improve customers overall mobile experience and allow them to access most critical information.

Hisham Sarhanet al., discussed the applications that are run on a smart phone device and communicate with remote service providers. Any remote information will be stored in the mobile devicestorage, andthe application transfers the information during the transaction to the remote service provider.Keeping suchdata private is asecuritykey purpose forboth user and serviceprovider. The proposed system consists of three parties, Android-Based Mobile device, Bank Server with localDatabase and its own cloud that can analyze SW applicationsand communicate with antimalware providers, and Bankprovided SD Card.

Munish Sabharwal and Prof. Anoop Swarup discussed Mobile banking with SMS is conducted through SMS codes sent to a particular number as directed by your bank. You will receive the response in the form of a text message on your mobile phone screen within a few seconds. For example to get details of your HDFC bank account you will use codes like HDFCBAL, HDFCTXN, HDFCSTM, HDFCSTP < 6 digit cheque number etc. for balance enquiry, last transaction details, account statement, stop cheque payment etc. respectively. It works in this manner that the message sent by you travels from your mobile phone to the SMS Centre of the Cellular Service Provider, and from there it travels to the Bank's systems. The information is retrieved and sent back to your mobile phone via the SMS Centre, all in a matter of a few seconds. With 3G telephony entering the Indian market this 2011 and also the smart-phones and tablets running on open source OS like Android becoming cheaper and their number increasing each day. Itseems more people use new and innovative banking applications from banks in form of special programs called Rich Clients downloaded to the mobile device and installed, it embeds the Banking option on your device menu. Mobile banking solution empowers retail and corporate banking customers with access to banking services offering both mobile commerce (m-commerce) and mobile payments within the DNA of mobile banking, with built-in support for merchant initiated payments and reversals, in addition to customer-initiated payments. Leveraging recent technological advances in the mobility space, the mobile banking solution empowers banks with the means to innovate by easily deploying new services, with improved time to market.

Yang Shulin, proposed the combination of Web Services and mobile devices, which will promote the development of mobile applications. Volley framework Google 2013 proposed the advantages of convenient use and network request faster, but it does not support Web Services. Extension of Volley, to support the Web Services, which can facilitate the Web Services application development, but also can improve the access performance of Web Services. On the basis of analysis and research of the Volley, Ksoap2 and Java Web Services, through the implementation of the HttpStack interface and the expansion of Json Object Request to realize support for Web Services. The scheme uses JSON format to transfer data, support SSL/TLS protocol requests, custom parameter, sets or gets the request header. This scheme is good compatibility, easy to use, suitable for application on Android platform.

Kishor Wagh and Dr. Ravindra Thool analyzed the performance of Mobile Host with Hospitaland Blood bank Search web service. Deployed web services are based on REST architecture styleusing corresponding URL and provide access to detailed information related to the particularservice. For performing controlled web service architecture, preferred jfuzzy lite rather that jfuzzy logic because of some advantages that jfuzzy lite has. Comparatively Size of jfuzzy lite is very small than jfuzzy logic. The experiments testing a GET request for getting hospital or blood bank information and POSTto add information of hospital or blood bank in database. From analysis, it is observed that Mobile Host for Android can handle a more number ofconnections as compared to the previous researchers result.The approach truly paved scope for the client-server and distributed mobile information networks.

Proposed Framework:

The proposal targets the applications that are run on a smart phone device and communicate with remote service providers. For example, when a smart phone user needs to check his / her bank account or make some transactions remotely. Such applications exchange secret data that might be used for authenticating the smart phone users with the service provider in case of remote access or other business logic between them. Any remote in the mobile device storage and the application transfer the information during the transaction to the remote service provider. Keeping such data private security key is used for both user and service provider.

Today most of the financial transactions flowing between Banks, Financial Institutions, Corporates, Government agencies, Insurance companies and Securities counter parties are based on files. Today, most financial flows are optimized around bulk transactions, cut-off times, and traceability from a file level to batch and single level instructions.

The proposed system consists of three parties' namely Android-Based Mobile device, Bank Server with local Database and its own cloud that can analyze Software applications can communicate with anti-malware providers, and Bank provided SD Card. The following scenario summarizes the process:

A. Browser-based Mobile Banking:

Mobile Banking offers various functionalities for consumer and corporate banking leveraging GPRS or WAP-based transmission. Indicative lists of features are

- Account management and requests
- Bill payments, Local payments and transfers
- Transaction approvals for corporatecustomers
- Merchant payments and reversals for POS,
- Telephonic or internet-based purchase
- Transactions

Support for administrative tasks like secured e-mails to relationship manager, approvals, password change, data synchronization and self-auditable Mobile banking solution that empowers retail and corporate banking customers with access to banking services through SMS (Short Message Service) and GPRS/WAP (Wireless Application Protocol)Enabled handsets, leveraging a single platform. It offers both mobile commerce and mobile payments within the DNA of mobile banking, with built-in support for merchant-initiated payments and reversals, in addition to customer-initiated payments and reversals. Leveraging recent technological advances in the mobility space, the mobile banking solution empowers banks with the means to innovate by easily deploying new services with improved time to market.

B. Mobile Banking /SMS Banking:

It is a term used for performing balance checks, account transactions, payments etc.via a mobile device such as a mobile phone. Mobile banking today is most often performed via SMS (Short Message Service) or the Mobile Internet.

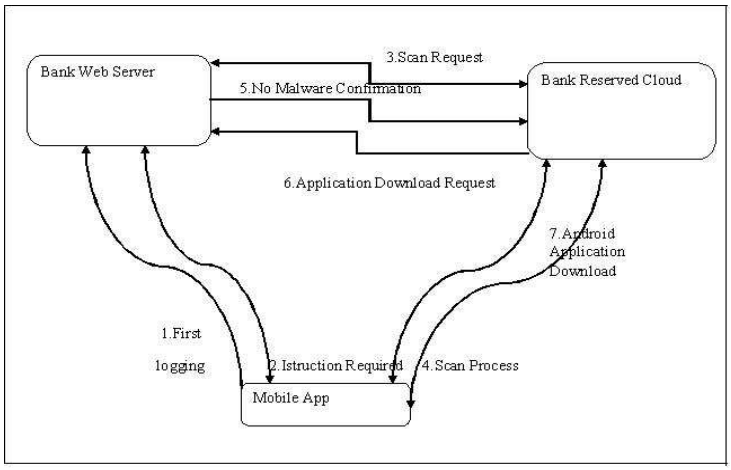

Fig. 1: Dataflow diagramfor application downloading from the browser

The proposed system consists of various modules and operations such as Regional cash, user profile and application form, Company details, Contact information, corporate accounts, Service required, corporate administrator details, User nomination details, Authorized account, Authorization matrix and Clientdeclaration.

Logical Design And Implementation:

Mobile Banking allows you to review transactions, transfer funds, pay bills and check account balances via mobile device. M-Banking also offers enhanced security with SMS transaction notifications; eventually, mobile phones may even replace automated teller machines (ATMs) and credit cards. The proposedsystemconsistsofvariousmodulesand operations such as:

1.1 Application Form And User Profile:

It consists of sign up and signs in modules in which the user can register their details for the first time and sign –in for transaction process.

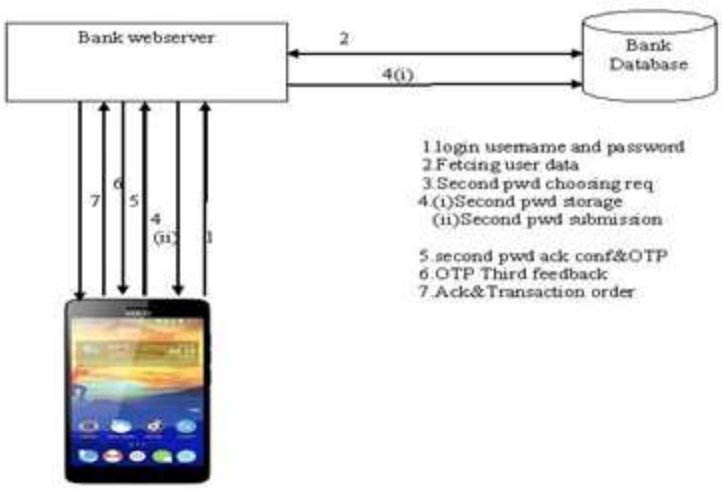

Fig. 2: Login to Bank Web server

1.2 Company Details:

This module mainly focused on corporate sector, company details are asked which includes Company name, Business registration number, Business Address, Nature of Business, Company Website, etc.,

1.3 Contact Information:

Contact information is of two types namely Primary contact information and Secondary contact information. Both primary and secondary contact information includes Name, E-mail, Telephone number, Mobile number and Fax number.

1.4 Corporate Accounts:

A corporate account refers to an account that specializes in offering services for companies and off-shore businesses. Its differentiation from personal and investment bank accounts lies on the fact that it provides services targeted directly to businesses. In this scenario, the user has to specify the primary Billing account which is used for billing and charges (if any). The charges varies from resident and non- resident.

Fig. 3: Corporate Account

1.5 Service Required:

The user has to select their required service from the offered service. The service that are offered by the bank includes,

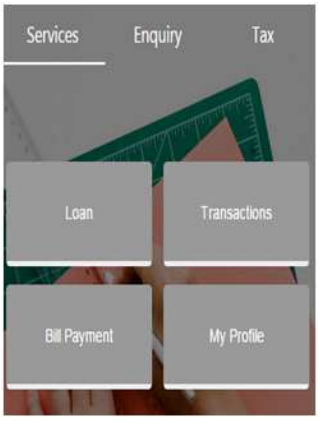

Fig. 4: Services

- ***My Profile:***

This displays the account details such as current savings, transaction details and Online Payment details of the user.

- ***Loan:***

Without using a loan calculator, it is extremely difficult to get an accurate calculation, not to mention time-consuming. Hence, in this app the user has to enter their Loan Amount, Rate of Interest and the duration (Months). It calculates and displays the total amount to be paid by the user. The formula used to calculate the Loan amount to be paid by the user is:

r = Interest Rate/1200
r1 = power(r+1, Loan Period)
Total Payment = Monthly payment * Loan Period.
Monthly Payment = ((r+(r/(r1-1))) * Loan Amount.

Fig. 5: Loan Calculation

- ***Transactions:***

Mobile recharges, bill payments, money transfers and purchases on e-commerce websites dominate the retail transactions that take place on the mobile platform, large-value transactions by corporate clients have resulted in an increase in the amount transacted through the phone. When a user selects the transaction service, then the amount is to be transferred from the user's account and then to whom the amount is to be transferred is mentioned. After that the request is processed by the admin, the amount is transferred.

Fig. 6: Transactions

- ***Bill Payment:***

Instead of customers having to keep up with punched cards or key ring tags, all of their information is stored in the application each time they make a purchase with their mobile device. Most customers and staff find that it's considerably quicker to pay with a mobile device than a credit card. There are various payment services in this app such as Mobile Recharge, DTH Recharge and Electricity bill payment. All these payments are processed by the Admin with respect to the request of the user. The Amount is paid from the Savings account of the user.

Fig. 7: Bill Payment

- ***Enquiry:***

In Enquiry section, the user has to provide their feedback and Query related to the services provided. Admin process the request of the user and provides solution to the request. After selecting their required service, they have to go for the mode of payment by either Local payment or outward telegraphic transfer. If the second mode of payment is chosen then the user has to agree the terms and conditions of foreign currency payment.

1.6 Corporateadministrator details:

This includes two services namely Admin maker and Admin checker which includes Name, E-mail, Designation and Mobile number. The details should be specified in admin checker also in order to validate it. Admin maker details should be the same as the primary contact. Admin checker should be the same as secondary contact. The same details should be specified in admin checker also in order to validate it. Admin maker details should be the same as the primary contact. Admin checker should be the same as secondary contact.

1.7 User Nomination Details:

User nomination details are given which includes name, designation, mobile number, passport number, and role. Role specifies whether the user is super user or role restricted or restricted user. After the specification of role, the user function is provided; it includes Viewer, Data entry and Authorizer. If authorizer is selected then the confidentiality is provided automatically. It results in viewing details in the database and he can either add or delete the records from the table.

1.8 Authorized Accounts / user:

Account number and the user number acts as proxy for the authorization of user. After the verification of the user number and account number the user is able to view his account services such as payroll or payment.

1.9 Authorization matrix:

The authorization matrix will have a set of roles that are required for a corporate user. It is a document with list of roles. Further, it also contains the list of transaction in every role. When a new user joins the organization, he can find out the roles for which access is required based on the FUG (Functional User Group) in the authorization matrix. It may be by a single user, Anyone, Both to authorize or others. In case of joint account both person has to authorize. If othersare selected then remark should be provided. After completing this process next should be given or else the form should be saved.

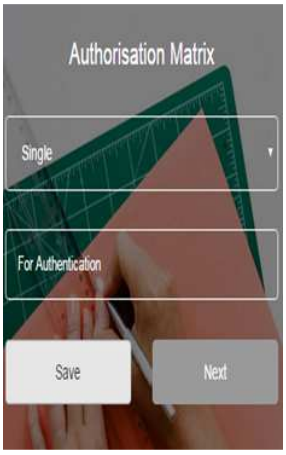

Fig. 8: A Screenshot of Authorization Matrix

1.10 Client declaration:

Client declaration is meant for the confirmation of authorized signatories as per board resolution.

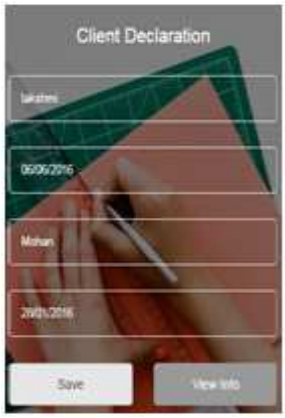

Fig. 9: Client Declaration

1.11 Uploading file:

It outlines the functionality that the process partial files which would be applicable for customer's usage. This enhancement will no longer require customers to re-upload files which have failed the system validation. It allows customers the flexibility of uploading thereby; the system will validate the transactions in the file. Upon uploading, the transactions which may fail in the validation may be sent under the reject repair screen. From the reject repair, customers are able to amend the particular transaction and re-upload it. Name and date is provided to view the transaction of that particular day.

2. Performance Metrics:

When the proposed system is compared with the existing applications, it provides more security to the corporate sector people by providing the type of authorization to their account users and the generation of pdf file at the end of registration by the application and submitting it to the admin, once the pdf file has been

generated it could not be changed by the user. Generation of OTP is the tedious process and it expires within 10 minutes, if expired then the user has to re-login to the account and the OTP has to be generated again.

RESULTS AND DISCUSSIONS

One of the main challenges in bringing corporate clients to mobile banking services is the two-person approval system that companies have for financial transactions. With banks coming up with better proprietary technology, they have been able to overcome this challenge, allowing for more coordinated transactions among different users from the same company.

By considering these challenges, the proposed Android Application can be used by the Corporate Peoples. The proposed mobile application provides secured Mobile Banking to the users as it uses two way authentications (Primary user detail and Secondary user detail). Mobile banking transactions will overtake internet banking transactions over a period of two years as customers find it a convenient mode of transaction.

Conclusion:

The proposed system theoretically covers most of those requirements and considerations. As it uses AES-256 with two modes of operation, AES-XTS for Decryption, and AES-CBC with variable IV, it achieves a high-level of data encryption. While ECDSA issued for Digital signature purposes which provide lower processing and key sizes. With respect to authentication, more than three levels of authentication are used as it asks for two user chosen passwords (one is known to bank representative andthe othersanonymous) andbank generated OTP (One Time Password). Authentication phases ensure the mutual authentication between user and the APP, then between the APP and bank server. Bank cloud scans the mobile platform to ensure elimination and mitigation of malwares impact. Dynamicity of values, diffusion, and sequence numbers overcome most common attacks such as reply, dictionary, and part force attacks. No keys will be sent via emails. At last, dynamicity of values, levels of authentication, bank authentication involvement and encryption helps against the effort loss.

REFERENCES

Adam Skillen and Mohammad Mannan, 2014. ‘Mobiflage: Deniable Storage Encryption for Mobile Devices’, IEEETRANSACTIONSONDEPENDABLE AND SECURECOMPUTING, 11(3): 1-14.

Ali AlSoufi and Hayat Ali, 2014. ‘Customer’s perception of m-banking adoption in kingdom of Bahrain: an empirical assessment of an extended tam model’, International Journal of Managing Information Technology (IJMIT) 6(1): 46-54.

Amol Bhatnagar, Shekhar Tanwar, and R. Manjula, 2011. ’Secure Multiple Bank Transaction Log’, Inter. Journal of Research in Engineering and Technology (IJRET), 3: 647-650.

Cooper, Santesson, Farrell, Boeyen, Housley, Polk, 2008. ‘InternetX.509 Public Key infrastructure Certificate and Certificate Revocation List (CRL) Profile’RFC 5280, pp: 44-53.

HishamSarhan, Ahmed A. Hafez, Ahmed Safwat, A.A. Hegazy, 2015. ‘Secure Android-based Mobile Banking Scheme’,International Journal of Computer Applications (0975 – 8887) 118(12): 21-26.

Jinseong, Micinski, Jeffrey, Nikhilesh, Foster, Fogel and Millstein, 2012. ‘Dr. Android and Mr. Hide: Fine-grained Permissions in Android Applications’, SPSM‟12, Raleigh, NorthCarolina, USA, pp: 1-14.

Munish Sabharwal and Prof. Anoop Swarup, 2012. ‘Banking by the use of handheld devices & gadgets like Smart-phones, Tablets’, International Journal on Emerging Technologies, 3(2): 61-66.

Narendiran, Rajendran and Albert, 2011. ‘Public key infrastructure for mobile banking security’ International Journal of Research in Engineering and Technology (IJRET), 4: 56-62.

Shabtai, A., Fledel and Elovici, 2010. ‘Securing android- powered mobile devices using selinux’, Ben-Gurion University. IEEE computer and reliability society, pp: 36-44.

Yuksel, Zaim and Aydin, 2014-12. ‘A Comprehensive Analysis of Android Security and Proposed Solutions’ I.J. ComputerNetwork and Information Security, 9(20): 9-20.

Yang Shulin, 2014. ‘Research and implementation of Web Services in Android network communication framework Volley’, 11th International Conference on Service Systems and Service Management (ICSSSM), pp: 1-3.

Kishor Wagh and Dr. Ravindra Thool, 2014. ‘Mobile Web Service Provisioning and Performance evaluation of Mobile Host’, International Journal on Web Service Computing (IJWSC), 5(2): 1-10.