Cyber Times International Journal of Technology & Management

Vol. 10 Issue 2, April 2017 – September 2017

TABLE OF CONTENTS

CYBER SECURITY: A BOON TO SUCCESS DIGITAL INDIA

Rohini P. Lokare
Assistant Professor,
Department of computer Science, TMV-Solapur,
rohinilokare@gmail.com

Jyoti Maske
Assistant Professor,
Department of Law, TMV-Solapur,
jyoti_maske11@rediffmail.com

ABSTRACT

India, with unique features of big geographical area, varied culture and linguistic diversity is a developing nation. For a country with large population and scarce resources like India, computer technology comes as a great tool of social transformation. Today it is recognized as an effective tool for catalyzing the economic activity in efficient governance and in developing human resource. The government of India has introduced and taken steps to make India as digital India. It is a vision to transform India into a digitally empowered society and knowledge economy. It is a step ahead to strive towards excellence in all spheres and to strive nation constantly rises to higher level and to make compatible with other members of the world community. In spite of the merits of Digital India it is inevitable that there are some challenges which might be proved great hurdles in the successful working of the system. In this perspective, cyber security becomes boon to curb and control obstacles in the functioning of Digital technology. In the present paper researcher aims to focus on the cyber security which will ensure the working of digital technology and also attempts to give suggestion on the application of cyber security with special reference to Mobile Banking, a key programme for cashless economy to empower Digital India.

KEYWORDS: *Computer Technology, Cyber Security, Digital India, Mobile Banking.*

I. INTRODUCTION

The present world's scenario is the symbol of arena of computer technology. It is recognized as an effective tool for catalyzing the economic activity in efficient governance of every country. India as a member of world's community is rapidly moving towards digital transformation. The innovations in technology help to achieve full-fledged and faster development in all dimensions of human life. "A life without technology is a life without oxygen."

India is little aware with digital technology in post-independence period but after a long gap, recently the Government of India started programme of digital India since 1st July 2015 [1]. This programme is comprehensive in nature that it can be applied to every affair of the government, private or public sector. We have proved excellence in technology and achieved world's third biggest position in tech startup hub and the world's largest souring destination for IT industry [2].

It is essential to take into consideration the probable hurdles/obstacles in the working of digital technology. Cyber security is an innovation in the digital world to curb and control obstacles in the functioning of digital technology. Cyber security plays an important role in arena of Mobile Banking, E-Banking, E-governance, E-commerce-Learning, Defense etc. Mobile Banking proves a need in current scenario. It helps to create cashless environment with the surplus benefit of saving of time and energy without the barrier of location. In spite of its benefits, there are certain cyber-attacks which hurdles the smooth functioning of mobile banking. But cyber security is answer to these kinds of attacks. It is with a view to make a planned effort to wake up and make capable India for the digital war [3].

II. CYBER SECURITY AND ITS UTILITY

Cyber security is the body of technologies, processes and practices designed to protect network, computers, programs and data from attack, damage or unauthorized access. It is a protective measure to curb cyber terrorism, cyber warfare and cyber espionage. It covers the different major areas like Application security, Information Security, Disaster recovery, Network Security etc.

- Application security covers measures or counter-measures that taken during the SDLC to protect applications from threats which come through the flaws in SDLC. The security techniques used for application security are input validation, user/role authentication and Authorization, session management, parameter manipulation, exception management, Auditing and logging etc.

- Information security is concerns to information protection, unauthorized access restriction, identity theft, privacy protection etc. which will be controlled by Identification, Authentication and authorization of user and cryptography etc.

- Disaster recovery planning is helpful for risk assessment, establishing priorities, recovery strategy designing in case of disaster.

- Network security consists of activities for protecting the usability, reliability, integrity and safety of network and its effect which will controls the threat from entering or spreading on network. Network security can be maintained with Anti-Virus, Anti-spyware, firewall, intrusion prevention system etc. [4]

Among all these applications, application security and network security are widely used for the smooth and efficient working of mobile banking.

III. CYBER SECURITY VIS A VIS MOBILE BANKING IN DIGITAL INDIA

The government of India proposed the program of digital India with unique nine pillars i.e. Broadband highway, Universal Access to Mobile Connectivity, Public Internet Access programme, E-Governance, E-Kranti, Information for All, Electronic Manufacturing and IT for job. The fifth pillar attributes with E-Kranti. It deals with delivery of services in the electronic form to citizens through with integrated and interoperable system with different mode. It is with a vision to transform “E-Governance for Transforming Governance” [5].

Mobile banking is a prime technology of E-Kranti. In India mobile banking was started since 2002 with the functioning of SMS Banking [6]. Today India is the second largest mobile phone market globally with more than one billions mobile subscriptions, Smartphone users account for

approximately 240 million subscriptions, which is expected to grow to 520 million by 2020[7]. The Digital India aims to provide wider incentives for the working of mobile banking. Mobile Banking provides multiple services in banking sectors such as account balance inquiry, credit/debit alerts, bill payments alert, transaction history, fund transfer, minimum balance alert etc. Mobile Banking is helpful to complete banking transactions by way of crediting and debiting transactions with Smartphone. It is a very good measure to cashless environment to make digital India successful. It is recent new approach by ICT (Information and Communication Technology) for financial services.

The growth of technology in all spheres carries with it the cyber threat. It adversely effect on the economic growth of nation and thereby wellbeing of its people. The increasing ratio of use of mobile banking also shows the risk factors belonging to it. According to the article published in Indian express dated 17 December 2016 "With the surge in digital transactions and other online payment gateways, mobile frauds are expected to grow to 60 to 60% in India by 2017".[8]

The increased use of mobile banking due to demonetization also becomes a platform for creating threat and fraud in this area [9].

IV. ROLE OF BANK IN MOBILE BANKING

Every bank ensures complete security to its customers for operating mobile banking through various ways as –

- Giving instructions to its consumers.
- Verification of mobile for its compatibility.
- Issuing mPIN to consumers on registered mobile number which is used as authentication for further mobile banking transaction which can be changed later on. [10]

V. RBI GUIDELINES REGARDING SECURITY AND TECHNOLOGY STANDARDS ON MOBILE BANKING

- Mobile Banking IS valid only after compliance of two factor authentication as specified by Reserve Bank of India.
- A higher standard mechanism or mPIN shall be used to authenticate the customer.
- mPIN should not be in clear text format it should be in end to end encrypted form.
- Privacy of mPIN should be maintained by the customer.
- Bank should maintain regular information security audits on mobile banking system to ensure complete security.

The data center of the bank and service provider should have proper network protection mechanism for wired and wireless data network for mobile banking app.[10]

VI. CYBER TERROR IN MOBILE BANKING

The major disadvantage of mobile banking consists of Malware, SIM swap, unsecure network or Wi-Fi, Phishing, Third party apps, Jail broken or rooted devices etc.

MOBILE MALWARE

Mobile Malware is a common type of Cyber-Attack in today's era across the world and India is not an exception to this. India is listed among the top five in the world to be attacked by ransom ware. Some of the common types of mobile malware are Zbot/zeus, SpyEye, Citadel, Torpig, etc. [11]. The mobile malware are used to gain information belongings to financial transactions from mobile, computer or entire

network. Now days a malware includes keyloggers, spayware, ransom ware and botnets with the activities including system destruction, dropping other malcode, stealing data etc. The possibility of malware infection is through SMS, MMS, and Bluetooth, Wi-Fi or infrared. In this kind of attack social engineering method is propagated. An SMS is sent to the user with fake URL to download application containing Trojan app or malicious content with some serious issues like security, security advice etc. from bank.

In the botnet infection, the malware automatically installed on mobile to gain a complete access to the device with content and provide control to botnet. It compromises the mobile device and allows hackers to control the mobile so hacker can send emails, text messages, phone calls, contacts etc. Malware also steals the personal information like photos, audio, videos etc. The transaction authentication numbers like mPIN, OTP, Two factor authentications can be stolen because it is not practically possible for the bank also to upgrade the app with every change in versions of Smartphone Operating System and its security concern.

PREVENTIVE MEASURES TO STOP MOBILE MALWARE ATTACKS

- Use of anti-malware protection will be helpful to prevent against malware attack.
- Updating the banking app regularly is necessary by customer.
- Mobile security solution apps like intrusion detection system should be installed or activated on mobile.
- Unknown application should not be downloaded.

SIM SWAP

In this type of fraud the fraudster manage a new SIM card from mobile service provider for the victims register mobile number. In other words fraudster approaches mobile service provider by creating a fake identity of genuine customer by giving false reasons like losing mobile handset, damage of SIM card, etc… The mobile service provider, after verifying the information given by fraudster, deactivates the old SIM and issue a new SIM card to the fraudster. In this process the Victim will not receive any kind of SMS information or alert message regarding it. With this new card, fraudsters install the mobile banking app and got mPIN on registered number. After verification of mobile number from the app, the fraudster can work with the mobile banking app.

PREVENTIVE MEASURES AGAINST SIM SWAP ATTACK

- The user should be aware about cellphone's network connectivity status. If any alert, SMS notification are not receiving for a long time then make inquiry regarding this.
- Some mobile network operators send an SMS alert regarding SIM swap, while the user can stop this kind of attack by contacting the mobile operator or service provider immediately while he got this king of SMS.
- Both mobile and E-mail ID should be register to the bank account to get alert on email also, in the case of SIM is block.
- To ensure update of bank transaction and its history.

UNSECURED MOBILE NETWORK WI-FI

The public Wi-Fi or open Wi-Fi network is another way of attack on mobile banking. This kind of Wi-Fi hotspots on network doesn't encrypt the information communicated through network. Transactions done through this kind of network or the data communicated with this

network, can be seen whatever is done by the fraudster to hijack the session and logs or the mobile phone of victims can be accessed remotely with new tools like Wi-Fi kill, Droidshep, Androrat, Fing etc. [13]

With the help of these tools the fraudster can open URL's into the browser, can send mobile messages, and monitor phone transactions from the targeted victims mobile. The fraudster without any technical knowledge can work with use of these kinds of tools.

PREVENTIVE MEASURES AGAINST UNSECURED WI-FI ATTACK

- Secured Wi-Fi protected with WPA2 and in encrypted form should be used by the customer.
- Use of secured website for communication is necessary. This can be identified by https protocol.
- Log out in a proper way is also helpful for protection.
- WPA2 should be strong and should be regularly updated.
- Use of VPN (Virtual Private Network) helps to encrypt the network traffic.
- Automatic connection to Wi-Fi, Bluetooth and GPS services setting should be off in mobiles to prevent this kind of attack.

The behaviour of user is also responsible for different no. of attacks like downloading third party apps, use of unsecured wireless network, opening links unknowing links, losing mobile devices, working with outside websites or surfing during mobile banking transactions, keeping secrecy in authentication issues, use of rooted or jailbreak devices etc.. To avoid this user should ensure about precautions to combat such frauds.

VII. SUGGESTIONS

The above study shows the need of high level security measures in mobile banking such as;

1) Official app for mobile banking should be strictly regulated without any exemption.
2) Mobile Banking should be connected to Aadhaar so biometric authentication can be added to mobile banking like figure print, face recognition or eye-rise scanning, etc.
3) Online test can be conducted while permitting for mobile banking like RTO conduct while issuing learning Driving license.
4) Awareness campaign by technical expert should be organized. Internet, newspaper, social networking sites etc. can be used for awareness.

"Threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk". The suggested preventive measures are only illustrative and not exhaustive.

VIII. CONCLUSION

Use of technology through mobile banking is need of the present era to survive and promote cashless economy. But due to inefficient security reasons it cannot be avoided. The use of security concerns at both level i.e. customer and banking is necessary to success cashless economy for the growth of E-Kranti which will empower the digital India.

REFERENCES

[1] "Wikipedia", "Digital India" Available At-<https://en.wikipedia.org/wiki/ Digital India>, [Accessed September 2016.]

[2] "IBEF", "IT & ITeS Industry in India Sectorial Report", Available At-<https://www.ibef.org /industry/information-technology-india.aspx> [Accessed March, 2017]

[3] “The New Indian Express”, “Go Digital Drive brought Cyber Security to the fore in India”, Available At- <http://www.newindianexpress.com/business/2016/dec/17/go-digital-drive-brought-cyber-security-to-the-fore-in-india-1550149.html>, [Accessed 17 Dec. 2016]
[4] “The Economic Times”, “Security”, Available At-<http://economictimes.indiatimes.com/definition/cyber-security> [Accessed Mar 29, 2016]
[5] “Ministry of Electronics and Information and Technology” ,“e-Kranti”, Available At- <http://meity.gov.in/content/e-kranti>, [Accessed May 12, 2015]
[6] “DNA”, ”Mobile banking in India does not need a one-size-fits-all-solution”, Available At- , <http://www.dnaindia.com/money/column-mobile-banking-in-india-does-not-need-a-one-size-fits-all-solution-1683740>, [Accessed May 3, 2012]
[7] “New Indian Express”, “[said a joint study by Assocham and Deloitte released in Dec. 2016” Avialable At- <http://www.newindianexpress.com/business/2016/dec/17/go-digital-drive-brought-cyber-security-to-the-fore-in-india-1550149.html>, [Accessed Dec. 2016]
[8] “New Indian Express”,“Warned leading industry body Assocham and global research firm EY in Dec. 2016”, Available At- <http://www.newindianexpress.com/business/2016/dec/17/go-digital-drive-brought-cyber-security-to-the-fore-in-india-1550149.html>, [Accessed Dec. 2016].
[9] “New Indian Express”, “Anand Ramamoorthy,MD, South Asia, Intel Security “, Available At- <http://www.newindian-express.com/business/2016/dec/17/go-digital-drive-brought-cyber-security-to-the-fore-in-india-1550149.html > [Accessed Dec. 2016]
[10] “Reserve Bank Of India”, ,”Master Circular”, Available At- <https://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=8992>, [Accessed Dec. 4, 2014]
[11] “heimdal security”Available At- <https://heimdalsecurity.com/blog/top-financial-malware/>, [Accessed Feb 15, 2017]
[12] “ICICI Bank”, “SIM Swap”, Available At- <https://www.icicibank.com/online-safe-banking/simswap.html>
[13] “GreeksGyan”, “Top 20 Android Hacking Apps”, Available At-<http://www.geeksgyan.com/2015/12/top-20-best-android-hacking-apps.html>, [Accessed 23 Dec. 2015]
[14] Author:-“ Weizhi Meng, Xiapu Luo, StevanFurnell, Jianying Zhou” ,” CRC Press, 25-Nov-2016”, “Protecting Mobile Networks and Devices: Challenges & solution E-book“