A SURVEY OF MOBILE SECURITY IN BYOD (BRING YOUR OWN DEVICE) & THE CLOUD

Akanksha Sharma[1], A.K. Sharma[2]

[1]*Research Associate, Faculty of Engineering and Technology, MITS University Laxmangarh Dist (Sikar), Rajasthan, INDIA,* ***akanksha.sharma183@gmail.com***
[2]*Head of the Department, Faculty of Engineering and Technology, MITS University Laxmangarh Dist (Sikar), Rajasthan, INDIA,* ***aksharma.et@mitsuniversity.ac.in***

Abstract

The growing adoption of Bring Your device amongst corporation is heading towards the greater need for technologies. A movement to BYOD (Bring Your Own Device) with additional resources on the cloud seems inevitable. However the trend towards mobility in enterprises there is a notable requirement for BYOD users to re-examine their point of view toward the security of their own mobile devices and the resources they utilize on cloud. This paper outlines re- examining business users to use their own mobile devices at their business organizations. The paper also outlines the result of a survey of business users towards resources stored on the cloud. At last the recommendations are made regarding the best practice in aiding the user's conception of security risk in BYOD and the cloud.

Index Terms: *Cloud; Bring Your Own Device (BYOD), Mobile Devices, Security.*

---------- *** ----------

1. INTRODUCTION

Recent years have seen a tremendous growth in BYOD (Bring Your Own Device)[1] policies amongst enterprises and as many such enterprises are currently struggle with prospective security risks accessing company personal data on personal mobile devices. The lack of ownership and corporate control of these devices can make the security of the crucial data that is accessed and stored on these mobile devices make a significant challenge for corporate IT Departments.A recent survey has been conducted by Aruba Networks Inc. (ARUN) of 3000 employees around the world in which study revealed 66% of American respondent claimed that they fears of data loss compared to the 45% of Europeans and 40% of middle easterners who felt the same. The BYOD trend will push the organization into adopting cloud based services for mobile devices particularly in the small size and medium size business (SMB's) market where the IT staff is less and budget to adequately to deal with it. The cloud provides the most cost effective and least resource environment to secure data in the era of BYOD and "work from anywhere" and at "any place" computing. The demand for BYOD is a trend that entrepreneurs can't afford to ignore any longer; the risk of these mobile devices has lead to the

Widespread development of mobile devices from a wide range of leading companies including blackberry, Apple etc. and many others[2][3]. These platforms allow business to implement security features such as control over installed application, remote wiping, mandatory encryption and password protection of the device and provide method for securely accessing entrepreneur's data. For example many of these platforms provide a secure container for accessing corporate data that the corporation can control, while keeping all corporate data separate from personal data. The survey was carried out to establish the behaviors of the respondent to security when accessing their own mobile devices using their BYOD style purpose.

2. BACKGROUND

The recent trend towards the data storage on the cloud is increasing at exponential rate. This trend is growing up fast among the current generation.

The OWSAP[4] groups have defined the top ten security risks for 2013 as-:

- *Injection attacks-:* flaws such as SQL, OS injection occurs when an unauthorized data is received by an

interpreter as part of command .the attackers hostile data can automatically trick the interpreter to make an executing unintended commands or grants permission to accessing data without proper identification.

- *Broken authentication and session management-:* it allows attackers to exploit data security and implementation flaws to assume other user identities, compromises passwords, keys and session tokens.
- *Cross site scripting (XSS)-:* XSS allows attackers to execute scripts in the victim's browsers which can hi- jack user sessions, deface websites and redirect access the users to malicious websites.
- *Insecure direct object references-:*direct object references can take place when a developer try to exposes a reference to an internal implementation object such as file, directory and a database key, without accessing any security check attackers can manipulate these references to access unauthorized data.
- *Security mis-configuration-*: security should be pre defined, implemented and maintained and provide secure connections for web applications, database server and web server.
- *Sensitive data exposure-*: third party users can modify data and lead to security breaches. Sensitive data needs extra protection and encryption techniques when accessing in the browser.
- *Missing function level access control-:* Each application needs to perform access control check on the server when each function is accessed.
- *Cross site request forgery-:* cross site request forgery also known as a one click attack or session riding. It s type of malicious exploit of a website where unauthorized commands are transmitted from a user that website trusts and exploits the trust of a user has for a particular website.
- *Using component with known vulnerabilities-:* components (libraries, frameworks and software modules) always allowed running on full privileges .if a component is exploited by a attack that facilitate serious data loss. Applications using components with known vulnerabilities may challenge application lines and enable a range of possible attacks and impacts.
- *Un-validated redirects and forwards-:*web application often redirects and forward users to other pages and websites and use untrusted data to establish the destination pages .Without proper validation, attackers can redirect victims to phishing or malware sites or use forward to access unauthorized pages.

These risks are all appropriate to cloud computing environment. Access to these resources in the cloud is frequently provided by the web services interface. Risks that are more generally applicable to cloud connection include broken authentication and session management. The connection control to the cloud is crucial to secure session management. Further this information could be used in a court of law as authentication of security breaches. Organizational risks associated with cloud computing environment are defined as -: vendor lock-in, loss of governance, compliance challenges, cloud service termination/failure, cloud provider acquisition and supply chain failure.

There are many policies on providing information on the risks of utilizing smart-phones for data transfer and cloud access. A comprehensive report outlines the common risks such as: data leakage, improper decommissioning, phishing, surveillance, to name but a few. Number of recommendations to the users of external devices such as the cloud. The references include-:

- Assessment of risks
- Identification of used cases based on risks level
- Selection and identity of security control (before making a live project)

The information outlined here point out the significance that industry and regulatory bodies place on the protection of BYOD and Cloud. However, the remainder of this paper provides a suggestion as to the lack of emphasis placed on security by the average BYOD & Cloud user.

3. NETWORK ENVIROMENT

When taking into account support for the BYOD users functioning from home it is worth analyzing the access to broadband available to them. Within this area there is a comparatively good Always on Digital Subscriber Loop (ADSL) connection to the majority of towns and villages. However, the area is quite rural with many users experiencing little or no broadband support. This can be a significant problem if all the resources are supported on the cloud. A separate survey was carried out to analyze the internet connections available to the learners. Just over 70% of respondents used wireless router to ADSL connection. The remaining 30% used a dongle to connect to the Internet. When questioned as to their broadband package details 76% did not know the details including items such as download/upload speeds and the maximum allowable download before penalties are applied. This is an area for concern as it shows the obvious lack of regard for contracts and regulatory details.

The rates of faults on the connection were quite high with 29% reporting daily downtime. A remarkable 70% stated that their broadband connection went down at least once a month or more often. None of the respondents could provide any reasons as to why this occurred and the vast majority was unconcerned as they felt this was normal. When considering the placement of all learning resources on the cloud it is important that the learner is aware of whether or

not their home network can support working from home. Again the lack of knowledge is quite disconcerting.

4. BYOD SURVEY RESPONDENT

Bring your own device is all the rage because it lets consumers to use the smart phone, laptops and tablets they already own and carries at their business organizations. While there are many management and security challenges, BYOD is gaining acceptance at a growing number of companies. A recent survey has been conducted by Cisco [5] in six countries in which the number of BYOD devices will climb 105 percent between 2013 and 2016, a compound annual growth rate (CAGR) of 27 percent. China will be at peak on all countries by 2016, with 166 million BYOD devices, followed by the United States and India at 108 million and 76 million, respectively. Companies in Brazil, Germany, and the United Kingdom will also experience a noteworthy growth of employee-owned devices in the coming years-:

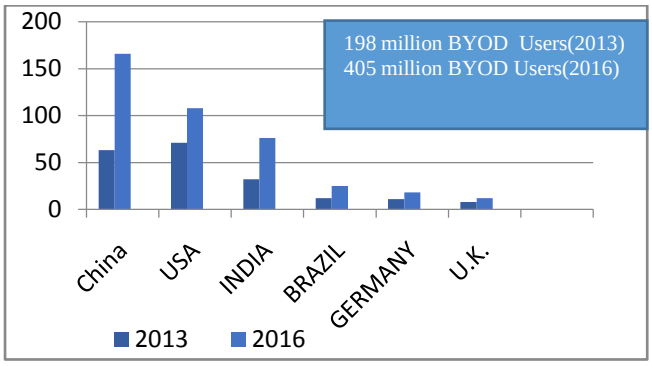

Figure 1- Estimated BYOD in workplaces, by country.

Mobile users who currently use their own device at their workplace are approximately 1.7 BYOD devices. The explosive demands of Smartphone's are gaining demands among the users and became a good choice for BYOD-ers, tablets and PDA is also increasing dramatically. Fifty-six percent of users use their own devices at their business organization. The percentages of users who use their own laptops at their workplace are also high in number, approx 37 percent of users use their own laptops at their work.

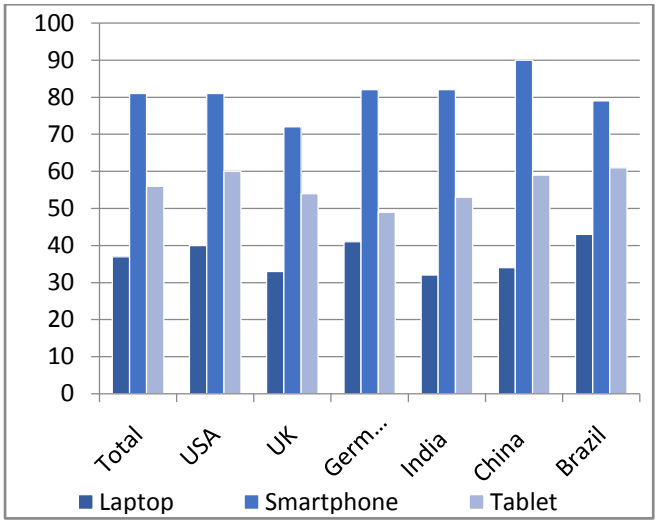

Figure 2-Percentage of BYOD users who bring their devices at their work

A study published by web root, a security firm found that one in three organizations allowed personal cell phones unrestricted access to corporate resources with troubling consequences. One in five companies in the same survey admitted losing business data after personal devices were lost or stolen. In this scenario several frame work based on the state of art mobile technology are emerging and required functions of new generation of mobile networks from initial authentication, managed resource , configurations, sessions, security control and quality of service. Mostly IT organizations restricted employees to BYOD (Bring your own Device) at their work place as it causes threats to small and medium sized businesses as well as large body organizations and government organizations. Because the lack of security applications installed in the employee's devices may lead security breaches, data spoofing, and data theft or stolen as the employees are totally unaware of lack of mobile visibility and lack of control. Network visibility is a major threat to business organizations, an employee doesn't even aware of which network is on their device and doesn't even examine the traffic travelling over it, that may lead to gain access to the third party user from malicious attacks and unauthorized access. Accordingly BYOD is becoming a severe headache to business organizations and entrepreneurs, especially for some methods and activities where mobility can causes threat to new business data and models. Lack of awareness for BYOD protection increasing the risk of malware attacks, less than half of the business employees use mobile protection for their devices and 21% of the business have no plans to implement security features on their devices.

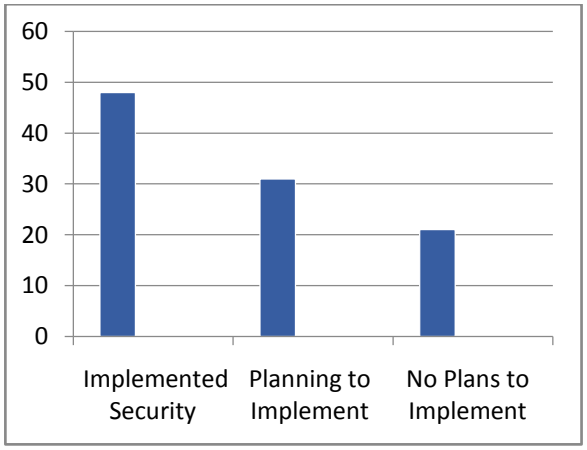

Figure 3-Survey of Mobile protection features Installed

Less than half of Business users (48%) implemented mobile security on their devices , 31% business users planning to implement security features on their mobile devices and 21 % of mobile users have no plans in current to install any applications on their mobile devices or their BYOD cloud environment.

Recently a further survey showed that 68 % of business users use the drop box or sand box for data storage in the cloud environment such as notes, pictures, continuous assessment material and sensitive data. It was also found among the user as that they are not aware about the security features installed on the BYOD cloud storage facilities. The business user's simple believes that the provided security has adequate features to manage the data. Mobile data loss is a major concern among the entrepreneurs most of the BYOD-ers approx 73% admits they are "very concerned" and "extremely concerned". Malware and stolen devices is also a major concern among business users with compliance issues only half of the BYOD-ers is "very concerned" and "extremely concerned". Larger the organization the larger the risk, when an employee attaches a personal Smartphone or tablet to an organizational network or machine, it makes sense to worry about overall security. First, as soon as external devices are attached, malware could migrate from the personal device into the company's machines and over the company's networks. In the other direction, sensitive data is likely to make its way onto the personal devices. This data could include customer information that should be kept private and company information that should be kept proprietary. When that kind of information walks out the door on a daily basis, terrible things can happen, especially if the device is subsequently lost or stolen.

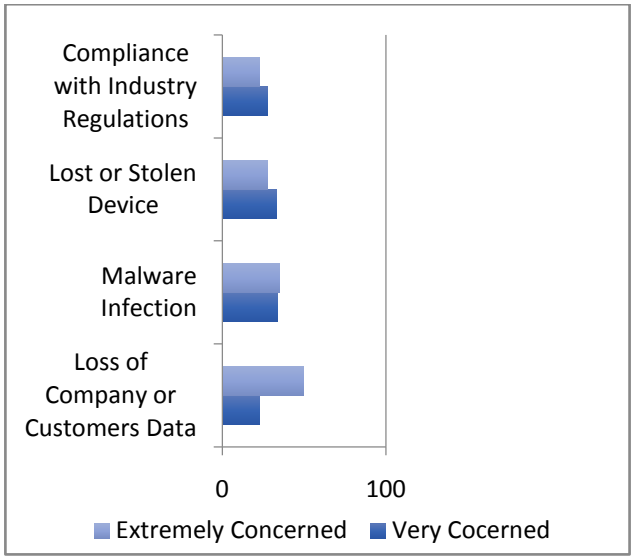

Figure4- loss of mobile data

5. SECURITY POLICY AND PRACTICES

The Acceptable polices for wireless network and cloud environment among the BYOD users share a significant change. However more than half of the users did not know where to locate these policies (e.g. network policies and security policies) and further were unconvinced about where these policies could be positioned. From this survey we can assume that having inflexible security policies in place is of little benefit if the users of the network are not made aware of the location of the policies. It may also be concluded that procedures should be put in place to ensure that the policies are viewed, if not read, by the system users.

6. SECURITY AWARENESS

The brief survey observes the lacks of knowledge system, users as to risks their devices and risks the surroundings of business organizations. In support of general trend of BYOD and cloud resources individuals have little or no information as to the increase of risk through the lack of application of sufficient security [7] features. Pursuant to this it is essential that all BYOD & Cloud system [6] users are educated to risks and methods to alleviate the security risks of such systems. The brief recommendation of list is provided to follow up the security measures adopted by the organizations to provide a safe and secure environment among organizations.

- Security educations programs should be provided to the BYOD users to access the networked resources and cloud resources.
- Restrict sessions from uncommon or suspicious computer configurations.
- Add some extra security features to the BYOD

devices that devices are utilized for the work purpose such as remote wiping.

- All personal devices connecting to the cloud environment must be monitored and logged.
- File encryption techniques must be configured to the device that holds sensitive data.
- Devices which may be utilized to connect to the resources on cloud should not be loaned to others.
- All personal devices should provide a secure channel in which registered device can access the organizations network.
- Ensure the strong assertion of the identity of the user using the device.

ACKNOWLEDGEMNT

I would like to thank my husband Mr Aman Mishra and my Guide prof A.K. Sharma for their kind support and staff of MITS University laxmangarh dist (sikar) Raj for their advice.

REFERENCES

1. Bring your own device "http://en.wikipedia.org/wiki/Bring_your_own_device ".
2. New security perspectives around BYOD" 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications '
3. Mobile security threats "http://focus.forsythe.com/articles/282/5-Mobile-Security-Threats"
4. Anon, "OWASP Top Ten Web Application Security Risks for 2013",Available at: http://owasptop10.googlecode.com/files/OWASP Top 10 -2013.pdf.
5. Jeff Loucks, Richard Medcalf,Lauren Buckalew,Fabio Faria CISCO IBSG "The financial impact of BYOD"2013
6. D. Catteddu and G. Hogben, Editors, "Cloud Computing Security Risk Assessment", European Network and Information Security Agency, November 2009.
7. G. Hogben and M. Dekker, "Smartphones: Information security risk, opportunities and recommendations for users", European Network and Information Security Agency, December 2010.
8. J. Heiser, M. Nicolett, "Assessing the Security Risks of Cloud Computing", Gartner, 3 June 2008.
9. SurveyReport "BYOD Mobile Security Study"WebRootwww.webroot.com/shared/pdf/byod-mobile-security-study.pdf

BIOGRAPHIES

Akanksha Sharma has completed her Mtech from Mody Institute of Technology and Science (Deemed University) Laxmangarh Dist Sikar (Rajasthan) and completed Btech from Rajiv Gandhi Technical University Bhopal (M.P.) ,She has worked with Rajiv Gandhi technical University (RGTU State University)as an assistant Professor from June 2011 to Nov 2011, And has also worked as an assistant professor with Mody Institute of Technology and Science laxmangarh Dist Sikar(raj) from Dec 2011-Dec 2012. She has Currently Pursuing her PhD from MODY institute of Technology and science in the area of Cloud computing under the Guidance of Prof A.K. Sharma , and also working as a research associate in Punjab Engineering College Chandigarh (PEC Deemed University) in the area of Network security of Cloud computing , the project is sponsored by Department of IT (Govt.of INDIA) and also appointed as member of Cyber Security Research Center (CSRC) in Punjab Engineering College Chandigarh (PEC Deemed University) in the Area of BYOD (bring Your Own Device) Cyber Crime and terrorism the project is running by PEC (Deemed University) and Chandigarh Administration and doing research under the guidance of Dr. Divya Bansal

Dr. A.K. Sharma is currently working as a Head of the Department of Faculty of Engineering and Technology at Mody Institute of Technology and Science