BYOD environments Security challenges - A Survey

Sanjoy Das
School of Computing Science and Engineering
Galgotias University, India.

Abstract

New mobile technologies are emerging continuously in today's scenario. Like smartphones are used extensively for data communication as well as a processing. BYOD (Bring Your Own Device) is one such technology that has evolved in the business environment. In this environment employees of any organization can bring and use their portable devices like mobile phones, laptops, notebooks to their offices/work places. This helps in sharing, optimizing the utilization of resources. This is a futuristic approach where heterogeneous devices can join hand to work together. Users working in this environment can bring devices of different make and model, which makes it a truly heterogeneous environment. When resources of any organization need to be share among the user of unclassified devices leads to various challenging issues to organizational assets. In this survey, our focus is on security issues and various benefits associated with BYOD. As this field in very new and emerging area of research which may open lots of scope for new researchers to explore this domain for its high acceptability.

Keywords: *BYOD, breached device, mobile device management, risk.*

I. INTRODUCTION

Today's era is of smart communication devices. Now a day's people are migrating from conventional phones to smart phones, which are high speed data processing. Bring Your Own Device (BYOD) is a very new concept. This concept now a day got overwhelming responses in multinational organization for data sharing among employees and others. This facilitates employees to use their communication devices for accessing company resources and use them. Employees want to work with their own tools, and devices with the rise of flexible work hours. So the organizations will have to concede to the employee's demands.

The organizations will have to make a strategy to control the mobile devices which are used by their employees, hence many organizational practices needs to be addressed [6,7,8].

1. How will the devices comply with the organizational policies?
2. How do organizations ensure proper security software on the devices?
3. How do organizations ensure the user is authentic?
4. How will organization tackle lost devices?
5. How do organizations segregate organization and user apps?

Organization needs to be taken care of which includes change in policy and security challenges. In 2009, the concept was first used by Intel who recognized the importance of BYOD and enabled employees to use their own devices [1]. In 2011 IT companies like Unisys and Citrix Systems shared their points about this BYOD trend, and that's when organizations started considering it [2].

A survey conducted by Forrester Foresight's Workforce Employee Survey, Q4 2012 [3] shown in fig.1 shows statistics of the type of devices used by employees in an organization.

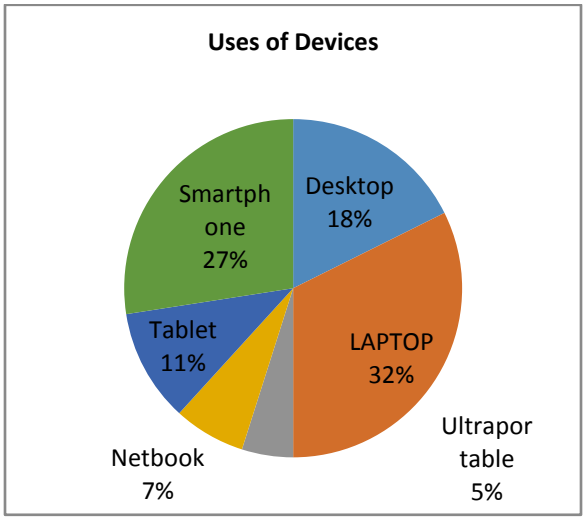

Fig.1 Devices uses in Company [3].

From the Fig.1 it is clear that employees use their own devices like laptops, notebooks, tablets because the data is accessible to them easily, BYOD enhances the functionality of employees [3]. One of the major advantage of this method, it reduces the organization hardware cost drastically, because employees are bring their own devices for work in the organization. This techniques helps in improving employees productivity and efficiency.

Leif – olof wallin from gartner is a world leading IT research and development mentions four important parameters should be considered by organization before they moves to BYOD.

i. Social- Happier employees
ii. Business- effective process management
iii. Financial – lower cost of devices for organization
iv. Risk management- managing the risk of organization.

II. BENEFITS

Now a days users of mobile and latest gadgets increases by leaps and bounds. The companies are having pressure to allow BYOD on their existing network to facilitate their employees and clients with their services and allow them to access their existing resources. There are many benefits of BYOD are mentioned below [R3]

1. Increased satisfaction of employees : Employees are more happier when they use the devices they love, rather than company issued devices.
2. Upto date devices: Upgrading devices for companies can be challenging and costly while the users will be having upto date devices which can be cheaply integrated and used.
3. Save money: Organizations can transfer the device cost to employees, thus saving a lot of money on purchasing and maintenance of the devices.
4. Productivity enhancement: Employees are more comfortable with their own devices hence they can respond faster to the request.
5. Less IT man power: Employees are responsible for maintenance of devices hence IT department can focus on other important jobs.
6. After Hours engagement: Since devices are being carried by employees, they can work from home even after office hours.

There so many others benefits of deployment of such system in organization. When system is open for employees to interact with their own devices leads to several security threats for overall organization. There are many security issues arises in the system. So, overall controls become decentralized.

III. SECURITY CHALLENGES

The portability of BYOD is a great challenge as the devices can be lost as well as stolen. In this, heterogeneous working environment communication devices make it more challenging to integrate due to various security issues. The device security is not that significant as the device belongs to the user rather than the organization. Privacy of employee is a challenge as the device contains individual credentials and data.

The biggest BYOD deployment concerns for any organization are

i. Information security
ii. Device security
iii. Device support
iv. Lack of standards
v. Loss of device
vi. Ownership of device
vii. Malicious attacks on mobile devices
viii. Ability to create enterprise applications.
ix. End user experience.

Many mobile devices are always on, so they are vulnerable to security attacks via different communication channels. Some human factors also come into picture. Employee can store and share confidential data with third party or competitors. If these vital information disclosed or hacked may cause significant financial and other losses to the organizations. Sometimes this may be havoc for any organization.

IV. BYOD POSSIBLE ATTACKS

Here we have mentioned few potential attacks of BYOD environment [9].

i. Lost or stolen mobile devices
ii. Eavesdropping
iii. SQL injection
iv. Advanced Persistent Threat (APT)
v. Data privacy for company and client
vi. Social engineering
vii. Malware
viii. Secure socket layer attack
ix. Man-in-the mobile

V. EXISTING SOLUTIONS FOR MANAGING BYOD

The MDM (Mobile Device Management) tool [5,6] helps organizations can centrally monitor control and manage the BYOD portable devices. The MDM tool can lock the devices, the tool can enforce policies, it can encrypt data and also it can wipe the data from remote if the device is lost. Various device groups can be made by MDM which can classify the files and devices. If required it can uninstall applications.

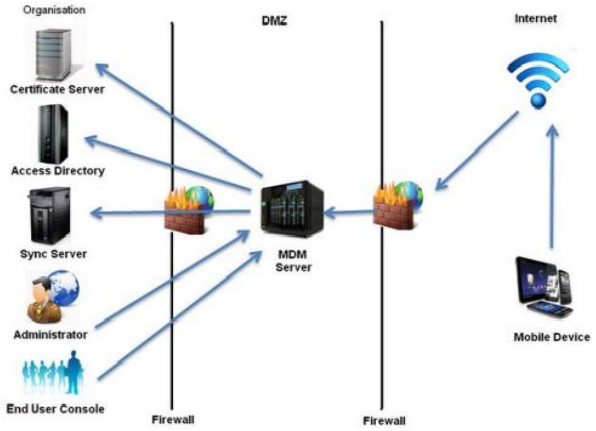

Fig.2. A MDM Architecture [6]

The mobile devices like android, blackberry, apple etc. are connected to the network via an encrypted tunnel/channel. In DMZ, MDM is placed to authenticate various devices. This can also perform other tasks like access, backup and synchronization. A portal / frontend can be provided on MDM which will facilitate password changing etc. for the users.

At present there are many MDM tools available in the market from different vendors. Some of the tools [4] are as follows

i. Airwatch
ii. Mobileiron
iii. Citrix
iv. SAP
v. Symantec
vi. IBM

VI. CONCLUSION

There are various surveys and articles which address the security challenges of BYOD. This comprehensive survey will definetly help new reserchers to explore this area, it also gives clear presentation of all the current challenges faced by various organizations while deploying BYOD.

In this survey we tried to cover the recent security threats and some existing solutions for BYOD environment.

REFERENCES

[1] http://www.govinfosecurity.com/webinars/mobile-learnfrom-intels-ciso-on-securing-employee-owned-devices-w-264. [accessed on 1st February 2016].
[2] http://en.wikipedia.org/wiki/Bring_your_own_device#cite_note-6. [accessed on March 2015].
[3] https://www.forrester.com/Forrsights+Workforce+Employee+Survey+Q2+2012/-/E-SUS1251[accessed on March 2015].
[4] http://www.appstechnews.com/news/2013/may/29/gartner-who-are-leading-mdm-players-2013.[accessed on February 2015].
[5] Bring your own device Security and risk considerations for your mobile device program, http://www.ey.com/Publication/vwLUAssets/EYBring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf .[accessed on April 2015].
[6] Prashant Kumar Gajar et al., "BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES", Volume 4, No. 4, , pp.62-70, April 2013.
[7] http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html [accessed on March 2015].]
[8] Kathleen Downer, Maumita Bhattacharya, "BYOD Security: A New Business Challenge", IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)-2015,Chengdu,19-21 Dec. 2015, pp.1128-1133.
[9] M.M. Singh et al., "SECURITY ATTACKS TAXONOMY ON BRING YOUR OWN DEVICES (BYOD)MODEL", International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 4, No.5,October 2014,pp.1-17.