A SURVEY ON BRING YOUR OWN TECHNOLOGY [BYOT]: APPLICATIONS & SECURITY

[1]Ajaykumar Mishra, [2]Kuntesh Jani
[1,2]Government Engineering College, Sector 28, Gandhinagar
Email: [1]ajaymishra8491@gmail.com , [2]kunteshjani@gecg28.ac.in

Abstract- BYOT (Bring Your Own Technology) , also known as BYOD (Bring Your Own Device) is a business policy to allow employees to bring their own devices at their work. The same device is used in and out of the corporate office and during outside use, it may be connected to insecure internet and critical corporate data become public when device is lost. This can be a big threat to the office as well as business strategies and future policies are derived from this data. This paper discusses about several issues on BYOT and provides solution on loss of device.

Keywords- BYOT, BYOD, Mobile Security, BYOD strategies, Mobile Device Management Technology, Enterprise Security

I. INTRODUCTION

Bring your own technology (BYOT) is a new trend and new emerging technology in business work. It is a business policy that adopted by management where they allow the use of personally owned devices like smart phones, i-pads, tablets etc. at the work place for accessing mails and databases and corporate data etc.[1].

The technology knowledge of information today is well leveraged with all the technologies like smart phones, tablets and internet etc. That has to be made them available to the entire world 24*7. This availability and flexibility people are demanding in their work life also, so that they can do their tasks anywhere and anytime.

It is the new emerging technology that allows the employee in the organization to bring their own devices in the organization and get access the information shared in the organization for that work.

Many organizations are adopting the BYOD strategy subsequently, as they recognize that employees have grown up more familiar and flexible with mobile

devices and used these devices as the key means of connecting, interacting with others, and increasingly using their mobile devices for work-related purposes[2]. Eighty-eight per cent of IT directors involved in a recent survey (300 were involved) believe that employee morale is improved with an organization's BYOD policy [3].

Advantages of BYOT:

1. Employees have the freedom of choosing the type of device they want to use, because employees can use their own choice of device in the workplace and he/she is flexible to use.
2. Reduces the cost of on-going end-user management i.e. the maintenance and keep the devices and applications are no more the responsibility of the organization. Therefore the organization doesn't need to look after the hardware and software as this is done by the employees themselves.[1]
3. BYOT can increase the engagement of the employees in the workplace and also after office hours.
4. Employees can access the corporate data outside of the organization or workplace, so that they can 'work from home' at their ease'.

5. Reduces the training time thereby increasing the productivity and efficiency of the employees [1].

Disadvantages of BYOT:

1. Data Leakage.
2. Most of the people evaluate to company's network through wi-fi connection which is unencrypted.

3. The antivirus and malware which are dangerous for the user and the system as well.
4. The second risk that comes to mind is the stolen devices.
5. BYOD has resulted in data breaches. [7] For example, if an employee uses a smartphone to access the company network and then loses that phone; untrusted parties could retrieve any unsecured data on the phone. Another type of security breach occurs when an employee leaves the company, they do not have to give back the device, so company applications and other data may still be present on their device.[4]
6. Loss of control & visibility: Organizations have less visibility of the security environment for BYOT compared to a traditional networked environment.

II. LITERATURE REVIEW

Abstract of literature:

Managing organizations' networks has become increasingly complex with the "Bring Your Own Techonolgy" or BYOD phenomenon. BYOD is no longer an option for most organizations; rather it's the standard for business in the digital era. It is important to have well-defined policies for what's supported and accessed in organizations. This research study highlights findings from an organizational survey conducted in the upper Midwest region about organizational strategies in coping with BYOD. Recommendations are made to benefit other organizations in adopting strategies for BYOD.[2]

B.Y.O.D. (Bring Your Own Device) or according to some B.Y.O.T. (Bring your own technology) is a recent trend that has been observed where employees bring personally-owned mobile devices to their workplace to access company resources such as email, file servers , databases as well as their personal data. The concept of 'Bring your Own Device' is gaining momentum at the workplace. Most of the companies in India and abroad have applied this policy in their work environment by the end of 2012. Using personal devices at work is beneficial in some ways like more productivity, flexibility, freedom and choice etc. Besides it this policy has some risks as well like the prime issue of data security. It is found in the literature reviews that the organization who embraces BYOD policy found their employees happier, productive and collaborative. Hence the study was done with the primary objective of finding the views of respondents from different sectors and industries for the same. It also depicts the different threats that can be observed and also concludes whether application of this policy will be lucrative for the different type of organizations.[1]

BYOD (Bring Your Own Device) is a business policy to allow employees to bring their own devices at their work. The same device is used in and out of the corporate office and during outside use, it may be connected to insecure internet and critical corporate data become public. This can be a big threat to the office as well as business strategies and future policies are derived from this data. In this paper an approach is explained to guard against this type of threat and to secure the corporate data even outside the corporate premises.[5]

Problem identified

There is a way to it by distributing and managing Virtual Private Network (VPN) solutions for all the mobile devices where employee can access the. Company's network through Wi-Fi connection which is unencrypted [1].

According to Ted Schadler, Sr. Vice President of Forrester Research, "The total cost of BYOD is higher than not supporting BYOD." [1] Because the cost of the implement BYOD policy security.

Risk that comes when device has been lost or stolen, then the most difficult situation faced is of changing the email and password.[1]

In addition, 45 percent of devices were reported to be stolen or lost. [2].

Organizations need to purchase an MDM (Mobile Device Management) system to monitor mobile devices, in addition to providing training programs for employees regarding BYOD. MDM software is used to secure, monitor, manage and support the mobile devices deployed in enterprises. [5]

To Secure the BYOD there are three major ways like Organization should be implement the MDM software to protect the BYOD ,Secondly to use some kind of the utility to secure the data and outside of the organization. An utility may have web browser like appearance and all the business tools must be assessed within this utility. For e.g.; Virtual Machine [5] . And third way that is to use some proprietary encryption algorithm instead of Standard algorithm which is to be used in utility. [6].

The devices must be protected with well strong and complex password. Hence an organisation should look for a management solution that means real time visibility of usage and also give alarm when the employee is about to cross the edge of limit.[1]

The key issues are security, fragmented software and according to the study the companies which have to provide implementation to this policy are Accenture, AirWatch, Alcatel-Lucent, Apple, ARM, Asus, Atmel, Authentec, Barclays, Cisco, Citrix, Dropbox , Enterproidz, Fiberlink, Good Technology, Google, HP, HTC, IBM, Ikea, Intel, Intuit,Juniper Networks,LG, Mformation, Microsoft, MobileIron, Motorola,Nokia, OKLabs, PwC,Red Bend,RIM,Samsung, SAP, Sony, SOTI, Sybase, Symantec, Tangoe, Taptera,T-Mobile, Verizon,Vmware,Vodafone, Wavelink, Zenprise .[1]

III. EXISTING METHODS AND DRAWBACKS – A COMPARATIVE STUDY

NAC technology inspects whether or not a user PC (terminal) complied with security policy before it accesses an internal network, and thus controls network access according to the state of the terminal being abnormal. However, BYOD environment has a special security requirement, which is to protect corporate data by isolating users of abnormal behaviors in addition to ensuring the use of diverse personal devices and work continuity. Therefore, NAC solution alone is not sufficient in handling security issues occurring in BYOD environment.

MDM provides a comprehensively protective function for a variety of channels subject to data leaks, such as operating apps, camera, recorder and Wi-Fi, and, at the same time, a function to administer control on company-wide monitoring and user environment through the central management console. There are problems in the access control based on MDM system that provides a function to directly control personal devices in BYOD environment. MDM is an application. Therefore, access control and monitoring of other applications are difficult. In addition, system-level network layer access and behavioral analysis for network data are impossible. Above all, it is difficult to distribute and spread this method because individual users are reluctant about MDM agent installation on their personal devices in demanding their privacy protection. At the same time, as a result of continuous version management on diverse terminals, the related costs increase.

To improve on these weaknesses, an access control method based on a link between NAC and MDM is proposed as of late. This method

provides effective network blocking function through limited terminal information collection. However, it still has such limitations as lack of a real-time terminal device status check function and security issues concerning terminals not installed with MDM agent.

The first component of any virtualization system is the hypervisor: the software that allows the host machine to run virtual machines. There are a variety of hypervisors available addressing a range of applications from server to desktop environments. It demands more investment and makes organization architecture more complex. Context Awareness based Dynamic Access Control is comprised of a collection system, a detection system and a control system. This system collects context information of a device under agentless mode. It is to collect context information through network analysis following user authentication when the users' terminal devices try to access a corporate network. The collected context information is analyzed by the detection system, and thus abnormal and malicious behaviors are detected. But this requires continuous monitoring applying a large system payload and trade off.

IV. CONCLUSION

Even though there are currently a number of BYOD security solutions in the market, these solutions are either vulnerable to a large number of security threats or require modifications of the underlying mobile device OS.

V. REFERENCES

1. Ms.NiharikaSingh,B.Y.O.D. Genie Is Out Of the Bottle – "Devil Or Angel",Journal of Business Management & Social Sciences Research,(Dec-2012).

2. Marzie Astani, Kathy Ready, Mussie Tessema, "BYOD Issues And Strategies In Organization",(2013).

3. Reisinger, Don. "BYOD Taking the Enterprise" by Storm. http://www.CIOInsight.com.

4. Wiech, Dean. "The Benefits and Risks Of BYOD". Manufacturing Business Technology.

5. Mr. Vishal Gupta, Deepak Sangroha, LovekeshDhiman,An Approach to Implement Bring Your Own Device(BYOD) Securely, International Journal of Engineering Innovation & Research,(Sep-2012).

6. University of Oregeon Factors for consideration when developing a bring your own device(BYOD),July 2012 7. http://en.wikipedia.org/wiki/Bring_your_own_ device 8. BYOD Bring Your Own Device – an introduction _ Self Service & Zero Level support.html

8. Eun Byol Koh, Joohyung Oh, and Chaete Im , "A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment", International MultiConference of Engineers and Computer Scientists,(March 2014)

9. Dennis Gessner, Joao Girao, Ghassan Karame, Wenting Li," Towards a User-Friendly Security-Enhancing BYOD Solution", NEC Technical Journal,(March 2013)