Multi-Layer Access Control for Bring Your Own Device Environment

Morufu Olalere[1]
Cyber Security Science Department
Federal University of Technology Minna
Minna, Nigeria
lerejide@futminna.edu.ng

Mohd Taufik Abdullah[2], Ramlan Mahmod[2], Azizol Abdullah[2]
[1,2]Information Security research Group
Faculty of Computer and information Technology
Universiti Putra Malaysia
Selangor, Malaysia
taufik, ramlan, azizol[@upm.edu.my]

***Abstract*— As a result of several attractive features (portability and access to voice and data services) of mobile devices, People started going to their work place with their mobile devices and connect to their enterprise network to do their official daily job. This has given rise to a policy called Bring Your Own Devices (BYOD). BYOD policy has come with a lot of benefits for both the employees and enterprise. For instance, employer gains access to employee anytime thereby increase productivity of the enterprise. BYOD faces a lot of challenges such as security challenge. To determine who access enterprise resources and how the resources are been access, poses a serious security concerned as both the knowledge and ownership means of authentication in traditional network are not sufficient for BYOD environment. An unauthorized access to enterprise sensitive information through lost mobile device of employee's, solder surfing password attack and password guessing attack can lead to data leakage. Also, unmonitored employee mobile device when connected to enterprise resources can inadvertently cause malicious application attack on the enterprise network. To address these security issues, this study is proposing a framework for multi-layer access control that will not only authenticate legitimate user of mobile device at point of login to enterprise resource, but also control and monitor the behavior of legitimate mobile device user when connected to the enterprise resources. The multi-layer access control consist of two-factor authentication layer framework and mobile device access monitoring layer. The two-factor authentication framework will combine both the knowledge based and biometrics based authentication technique to form unobtrusive authentication technique for mobile device in BYOD environment. The second layer monitors the behavior of mobile device when connected to enterprise resource. For proper decision in an uncertainty environment like BYOD, Trust-fuzzy algorithm will be developed to form fuzzy inference engine for decision making. The system will be simulated using Matlab. It is expected that the algorithm that relies on trust and fuzzy logic concept will be effective in terms of running-time and throughput.**

Keywords—component; formatting; style; styling; insert (key words)

I. INTRODUCTION

Modern computing has undergone several notable transitions since its birth in the 1960s, with progress from mainframe computing to minicomputers and then to client-server driven personal computing (PC). The PC era led the information technology (IT) world to internet computing. Mobile computing has supplanted internet computing because of the proliferation of cloud-based applications and mobile devices (such as smartphones, laptops, palmtops and tablets). People are able experience high-quality computing at their palms through cloud-based applications and mobile devices. Workers bring their personal mobile devices to their workplaces. Mobile devices such as smartphones and tablets combine portability and voice and data services to open up a wide variety of potential mobile applications, "anytime and anywhere"[1]. People have started to bring their mobile devices to their workplaces and connecting to their company networks to perform their jobs and connect to various social network platforms such as Facebook and BlackBerry Messenger (BBM).

Using personal mobile devices for work has given rise to a trend called "Bring Your Own Devices" or BYOD [2]-[4]. BYOD programs and policies empower people to choose the best device to get their work done, including personally owned consumer smartphones, tablets and laptops [5]. BYOD is an enterprise IT policy that encourages employees to use their own devices to access sensitive corporate data at work through the enterprise IT infrastructure [6]. Ref. [7] defined BYOD as the use of employee-owned devices to access enterprise content and the enterprise network. A BYOD policy not only allows employees access to enterprise data when at the workplace but also allows them to access enterprise data outside the enterprise environment. When employees' access enterprise resources without being control, there will be room for a lot of information security breaches such as data leakage that can lead to data theft. More so, employee mobile device can be infected with malware, due to the interaction with the cloud based applications. Many mobile devices users rely on security measure offer by mobile device manufacturer. Security measures such are four digits password for

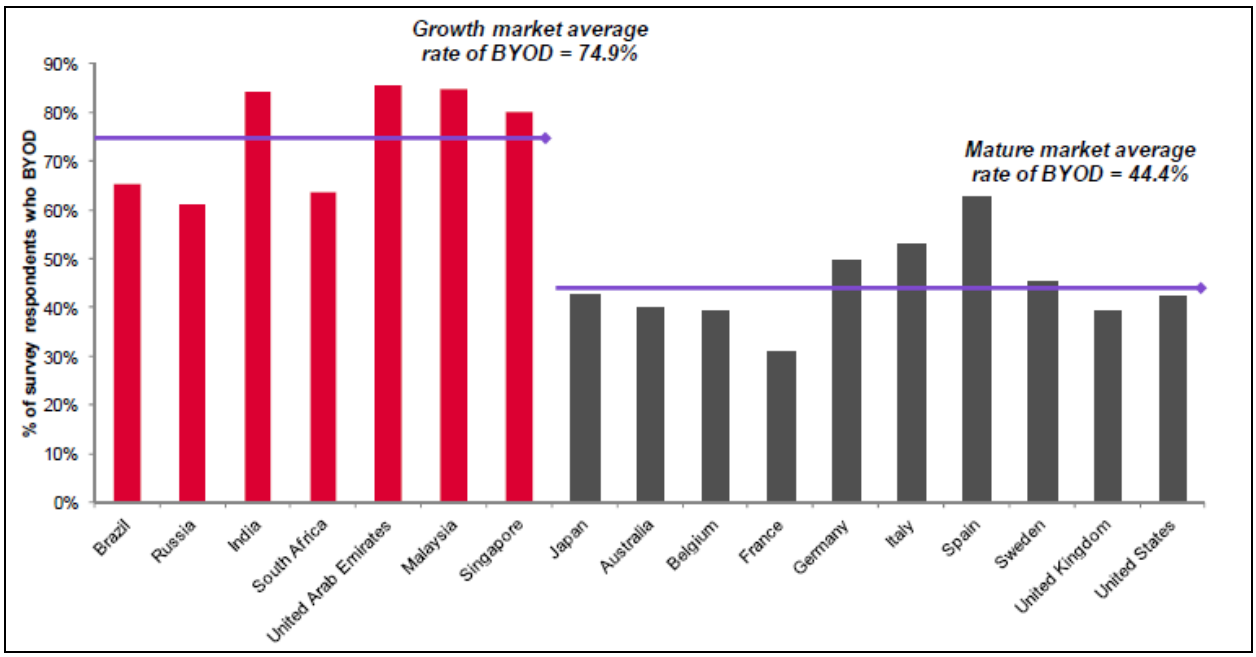

Figure 1 Level of BYOD deployment in both emerging economies and developed economies (Ovum, 2012).

authentication and too weak antivirus are common protection offer by most mobile device manufacture

Meanwhile, the security mechanisms offered by most popular mobile operating system offer only limited protection to the threats posed by malicious applications that may be inadvertently installed by the users and therefore they do not meet the security standards required in corporate environments [8]. To address this problem, this research is proposing a framework for multi-layer access control that aims at addressing the problem of data leakage that may occur as a result of unauthorized access to the enterprise resources and the problem of malware infection that may occur as a result of unmonitored interaction of mobile device with the cloud when connected to the enterprise resources.

II. BYOD DEPLOYMENT LEVEL

Although BYOD began to surface in 2003, it really took off in 2011[3]. Growing pressures to enable and support the use of Smartphone tablets and other personal devices in the workplace means that ignoring the need to put in place some form of BYOD policy is no longer an option for today's businesses[9]. Ref. [10] carries out survey that determines whether BYOD is growing only in United States or a large enterprise reveals that BYOD is a global phenomenon. Cisco carries out this survey across eight countries in three region (Latin America, Asia, and Europe) including both enterprises (1000 or more employees) and midsize Companies (500-999 employees).

A survey of three thousand seven hundred and ninety six consumers conducted by [11] in seventeen countries in both emerging economies and developed economies (figure 1) reveals that seventy five percent of users in countries with emerging high-growth economies such as Malaysia, Singapore, Brazil, India and Russia use their own mobile devices at work, while forty four percent of workers in countries with developed economies like US, UK, Sweden, Italy and Japan use their own mobile devices at work. Ref. [12] predicts that by 2018 seventy percent of mobile users will conduct all their work on personal smart devices. These surveys reports show that BYOD policy has come to stay in both emerging economies and developed countries.

III. BENEFITS OF BYOD POLICY

When employees have the flexibility to choose the best device for their office work, they become more mobile and productive. The business benefits by having access to its employees anytime, anyplace, blurring the work-leisure divide, and it may save costs by having employees purchase their preferred device rather than providing devices out of the corporate budget [13]. Ref. [7] and [14] identify some valuable benefits of BYOD. These benefits are management flexibility, cost saving, maximized employee contentment and simplified IT infrastructure. BYOD also provides a high level of convenience to employees. There are published whitepapers about BYOD from corporate organizations and information security experts that discuss the benefits of BYOD. More details about the benefits of BYOD can be found in ([1], [5], [7], [15]-[21]). However, if both the organizations and their employees are to reap the benefits of BYOD, then they must also worry about the challenges of BYOD policy.

IV. CHALLENGES OF BYOD POLICY

While businesses are mainly concerned with maintaining security, employees are worried about preserving the

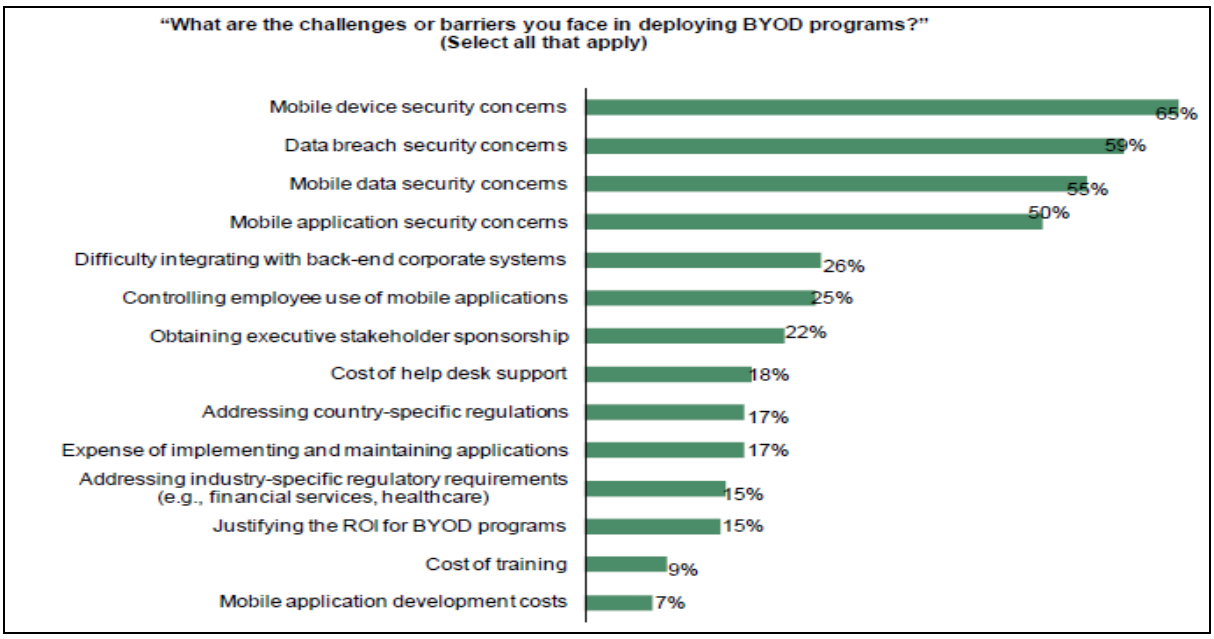

Figure 2 BYOD challenges with security concerns at the top (Forrester, 2012).

convenience they need in order to work from their mobile devices, as well as the privacy they expect regarding the personal information on the device [14]. One of the biggest challenges for organizations is that corporate data are being delivered to devices that are not managed by the IT department. This has security implications for data leakage, data theft and regulatory compliance [21]. Ref. [22] notes that the real BYOD challenge is security and that the real security challenge is not actually about the devices, it is about controlling access from the devices to the corporate data. Ref. [23] claims that loss or theft of mobile devices is the biggest risk that a business could face by implementing BYOD because it leads to loss of data to an unknown user. A survey of 202 respondents (Figure 2) by [24] with an understanding of the impact of the BYOD program on their business unit or organization reveals that security concerns are among the top challenges to implementing BYOD programs.

V. COMMON THREATS TO BYOD POLICY

Survey carried out by security vendor trustwave revealed that ninety percent of vulnerabilities common in desktop computer were also present in mobile devices, regardless of operating system [3]. Literature shows that data leakage, distributed denial of services, and malware are the most challenging security threat to BYOD [21].

A. Data leakage

Data leakage occurs as a result of access to enterprise data anywhere and anytime by employee. Enterprise has little or no control over corporate data because corporate data are now stored and accessed by personal device of employee. If by mistake, employee loss the device, the enterprise data on the device will be available to the person that posses the device. If the data available in the lost personal device are enterprise confidential data, the data can be made available publicly by the person in the possession of the lost device. The solution that can be employed in this kind of scenario is to wipe the data on the lost device

B. Distributed Denial of service

A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. DDoS can deny regular employees to run computer networked machines or their own personal devices.

C. Malware

Malware is a malicious application that can affect both mobile device and corporate application. Mobile malwares are application with code embedded within them that compromise the security of the device or related data. When a device is compromise by malware, corporate confidential data can be lost and this can lead to background operation (sending text message on behalf of the organization that owns the data) by the attacker. Apart from device compromise by malware, Corporate Application can also be affected by malware application thereby making the application unusable or malfunctioning. Malicious application normally take the form of normal corporate application that have been injected with malicious code. Also malicious application can be encountered when a user visit a compromised site. More detail on how malware affect BYOD can be found in [25].

VI. PROBLEM STATEMENT

When employee is empowered to choose the best device to get their work done, people become more mobile and productive. The business gains from having access to the employee anytime, anyplace, blurring the work-leisure divide, and in addition may actually further save costs by having the

employee purchase the preferred device rather than providing it out of the corporate budget [13]. However, as both the organizations and their employees are reaping the benefits of BYOD, so also they are worry about the challenges of BYOD policy. Ref. [23] claims that loss or theft of mobile devices is the biggest risk that business could face by implementing BYOD, because it leads to loss of data to unknown user. Perhaps, with too restrictive authentication that rely on password or Personal Identity Number (PIN) which surfers from shoulder surfing attack, brute force, and password guessing attacker can gain unauthorized access to enterprise resources through lost mobile device. This unauthorized access leads to a threat called data leakage. To prevent this type of threat, a secure and scalable BYOD strategy is required to manage the risks introduced by employee owned devices as a result of loss of mobile device, stolen or perhaps the employee leave the company [22]. There should be a way in which employee unique identity will be linked with mobile device of the employee, so that when attacker posses employee's mobile device, it will be difficult for the attacker to access enterprise resources through the mobile device.

Apart from the problem of data leakage alighted above, there is also a need for Information Technology(IT) department of any enterprise to monitor or control the way legitimate mobile device user's behave when connected to enterprise resources. Employees' mobile devices are not only use for making phone calls, texting message and for their enterprise, but also use to connect to the available public wireless local area network thereby allowing them to access different cloud based applications services such as social network, online entertainment, online shopping, game applications and all other favorite applications depending on individual. Many of these services do not have required security mechanism to secure consumers mobile devices and some are even sources of malware infection to consumers' mobile devices. Malware infection on employee mobile device can lead to malware infection on the enterprise network if required security measure to prevent this is not in place. Ideally, in a traditional setting where employee's is provided with an enterprise desktop computer, it is very easy to centrally monitor and control the behavior of desktop computer assigned to employee. The BYOD environment is a pervasive environment that requires new access control technique. This new access control technique is lacking in the literature.

In recent year, however, there have been a tremendous efforts in term of research on mobile devices security before workers own mobile devices become tools for workplace. Different platform calls for different security measure. Moreover, most vendors do not design smartphones primarily for businesses but instead for consumers who will utilize their phones as personal devices [26]. The security mechanisms offered by most popular mobile operating system offer only limited protection to the threats posed by malicious applications that may be inadvertently installed by the users and they do not meet the security standards required in corporate environments [8]. Therefore, this study is proposing a framework for multi-layer access control that will not only authenticate legitimate user of mobile device at point of login to enterprise resource, but also control and monitor the behavior of legitimate mobile device user when connected to the enterprise resources. The multi-layer access control aims to address the problem of data leakage that may occur as a result of unauthorized access to the enterprise resources and malware infection that may occur as a result of unmonitored interaction of mobile device with the cloud when connected to the enterprise resources.

VII. SIGNIFICANT OF STUDY

Growing pressures to enable and support the use of smartphones, tablets and other personal devices in the workplace means that ignoring the need to put in place some form of BYOD policy is no longer an option for today's businesses [9]. Cisco survey [10] that determines whether BYOD is growing only in United States or large enterprises reveals that BYOD is a global phenomenon. Ref. [11] survey of 3796 consumers in 17 countries in both emerging economies and developed economies, reveals that seventy five percent of users in countries with emerging high-growth economies such as Malaysia, Singapore, Brazil, India and Russia use their own mobile devices at work, while 40% of workers in countries with developed economies like US, UK, Sweden, Italy and Japan use their own mobile devices at work. Gartner [12] predicts that by 2018 seventy percent of mobile users will conduct all their works on personal smart devices. These surveys reports show that BYOD has come to stay in both emerging economies and developed countries.

With this level of BYOD policy deployment and with future prediction on deployment, the security challenges confronting BYOD need to be addressed. This study is taking a step in addressing security challenges confronting BYOD policy. The need for addressing these challenges makes this study significant.

VIII. OBJECTIVES

The general objective of this study is to propose a framework for multi-layer access control in BYOD environment, thereby offering a potential future applications for better security, implementation, and management of BYOD policy. To achieve this objective, the study will be guided by the following specific objectives:

1. To propose a framework that combines both the biometric and knowledge based technique for remote authentication of mobile device in BYOD environment

2. To formulate a Trust based model that is based on behavior of mobile device with a view/in order to compute trust value of mobile device in BYOD environment

3. To develop Trust-fuzzy algorithm for remote access control of mobile device in BYOD environment.

IX. SCOPE

Literature shows that data leakage, distributed denial of services, and Malware are the most challenging security threat to BYOD policy. Security issue in BYOD environment has been major concerned of academic researchers, though, not

much contributions have been made in addressing these security challenges. In fact, Very little have been done by researcher in addressing the challenges (both security challenges and others) of BYOD.

However, this study is not to address all the challenges confronting BYOD policy. The study is focusing on addressing the problem of access control that is lacking in both the literature and industries, which aim to prevent data leakage and malicious attack on organization resources. It is important to note that the vision of multi-layer access control framework for BYOD is to offer potential future application that will enable IT department of an enterprise to automatically control employees' mobile devices for better security without an infringement on the privacy the employees deserve.

X. Literature Review

Although BYOD began to surface in 2003 it really took off in 2011 [3], most studies on BYOD were executed by consulting firms and offer mostly description of the phenomenon as well as normative advice for executives [27]. There are whitepapers ([7] , [17]) that give details about the deployment of BYOD policy. Some of these whitepapers identified risk associated with BYOD and provided non-technical (more or less like administrative based solutions) solutions to most of these risks. Ref. [3], [16], [20], [21], [22], [28]-[32] present their expertise opinions on BYOD security issues and give their expertise advices on how organization can handle this security challenge administratively.

Ref. [6] identifies a number of issues in a straightforward approach of checking BYOD smart phones periodically in order to prevent security breaches. These issues are: running constantly scanning anti-malware software on smart phones is too costly energy-wise; checking all the smart phones is inconvenient for both the employees and the employer. They propose a carefully planned but otherwise random sampling approach called strategic sampling In order to address the aforementioned problems. Similarly, [33] believes many existing BYOD security practices are costly to implement and intrusive to employees, which to some degree negate BYOD perceived benefits. In order to address this problem, they proposed prioritized defense deployment. A concept and a distributed algorithm both name T-dominance was proposed to capture the temporal-spatial pattern in an enterprise environment. They identified a few desirable properties of prioritized defense deployment, and analytically show that T-dominance satisfied such properties.

Ref. [8] describes a security framework for mobile devices that ensures that only applications that comply with the organization security policy are installed on the registered devices. Their framework consists of a security policy manager that mediates access to the application store and an installer application that tells the user which applications can be safely installed. This is done by inferring behavioral models from applications and by validating them against the security policy. One weakness of this framework is that, attack on organization resources through mobile device does not only come through the application on the mobile device. There are different ways in which attack can occur in a pervasive environment like BYOD.

In order to prevent occurrence of data leakage, and malware application attack in BYOD environment, there is need to put in place a mechanism that will monitor/control the way and manner in which mobile devices access enterprise resources. It is in line with this that this study aims to propose a framework for multi-layer access control that will not only authenticate legitimate user of mobile device at point of login to enterprise resource, but also unobtrusively control and monitor the behavior of legitimate mobile device user when connected to the enterprise resources. The authentication layer will base on two-factor authentication technique that combine both the knowledge-based factor and biometrics-base factor techniques of authentications to form a single authentication technique for mobile devices in BYOD environment. While the controlling and monitoring layer relies on the behavior of legitimate user mobile device when connected to enterprise resources.

XI. Research Methodology

BYOD policy is a special pervasive environment that needs special ways of securing it. It a special pervasive environment in the sense that the mobile device users (employees) must unavoidably get access to organization resources to get their daily job done. Unlike other pervasive environment like Grid computing environment where requester can choose from various service providers to get their daily job done. As a result of this specialty, any security measure that will be implemented in BYOD environment must be flexible and free from tampering with the right of the privacy of the employees as well as their convenience. In line with the above issues, this study is proposing a framework for multi-layer access control that combines the concept of two-factor authentication technique, trust concept, and fuzzy logic concept. The two-factor authentication being a separate framework in the multi-layer access control framework will employ both the knowledge-based factor (password) and biometric-based factor (keystroke dynamics) techniques of authentication to form a single remote authentication technique for mobile devices in BYOD environment. Figure 3 shows framework for the two factor authentication.

After successful login by mobile device user, mobile device is then monitored and controlled based on trust value that rely on the behavior of the mobile devices. To determine this trust value, a trust- based model that depend on the behavior of mobile device will be formulated. Trust-based access control has been recognized and used in many areas where dynamism is necessary. These areas include virtual organization, distributed system, network to mention but a

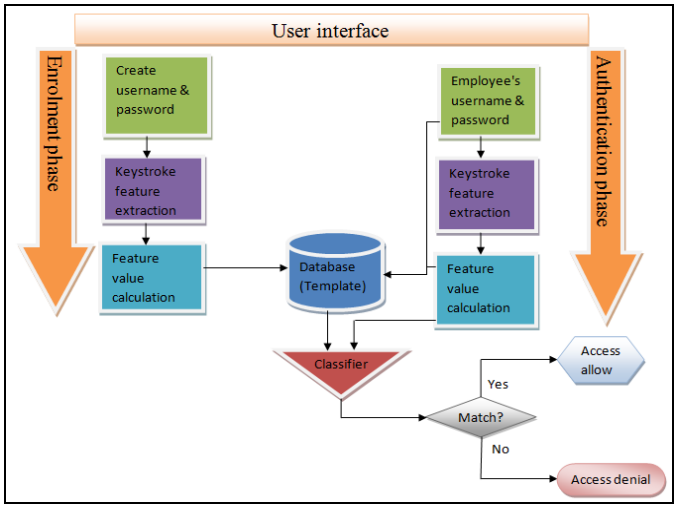

Figure 3 Architecture of two-factor authentication technique

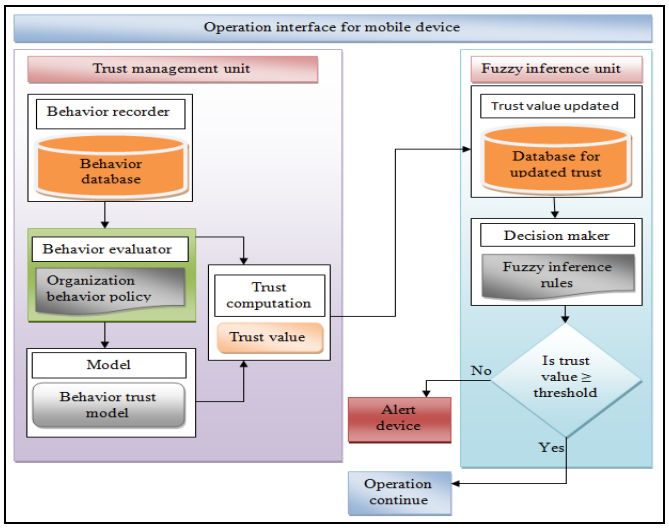

Figure 4 Architectural design of Trust-fuzzy access control

few. In all the areas of applications, trust value or level is always sorted for by formulating trust based access control that suit the area in which trust-based access control is applied. However, in this study, trust-based model that relies on behavior of mobile device will be formulated in order to calculate trust value that will be later used to decide whether a mobile device should remain connected to enterprise resources or otherwise. This trust-based model formulation will lead to trust management system (Figure 4) that automatically calculates and updates trust value of employee's mobile device.

For proper decision making in an uncertainty environment such as BYOD, Fuzzy logic is a great tool for decision making based on rules. The Trust value calculated from Trust based access control model will be used together with fuzzy logic concept to come up with Trust-fuzzy algorithm for access control decision system. Fuzzy inference system based on certain rules will be developed and this will be simulated using Mathlab. Figure 4 shows over all Trust-Fuzzy access control framework.

XII. Expected Results

The overall vision of this study is to offer a framework for multi-layer access control in BYOD environment. The proposed framework consist of authentication layer and monitoring layer. It is expected that the authentication layer provide solution to the problem of unauthorized access that can lead to data leakage. It is also expected that the proposed authentication layer does not affect the privacy that the employee deserve. The second layer of the overall framework has to do with monitoring of mobile devices when connected to enterprise resource. It is expected that this layer addresses the problem of malicious applications that may be inadvertently installed by employee mobile device as a result of improper monitoring, thereby causing attack on enterprise network. It is expected that the overall proposed multi-layer access control framework results to a potential future application that will give room for secure BYOD environment.

References

[1] G. Disterer, and C. Kleiner, " BYOD bring your own device," Procedia Technology, vol. 9, pp. 43-53, 2013. doi:10.1016/j.protcy.2013.12.005

[2] G. Gheorghe, and S. Neuhaus, "Poster: Preserving privacy and accountanbility for personal devices," Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS' 13), Berlin, Germany, pp. 1359-1361. November 2013.

[3] N. Leavitt, "Today's mobile security requires a new approach," IEEE Computer Society, vol. 46, pp. 16-19.

[4] A. Scarfo, "New security perspectives around BYOD," Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, Victoria, BC, pp. 446-451, November 2012.

[5] Citrix®, "Best practices to make BYOD simple and secure," White paper. 2013b Retrieved from http://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf

[6] F. Li, W. Peng, C. Huang, and X. Zou, "Smartphone strategic sampling in defending enterprise network security," IEEE International Conference on Communications, Budapest, Hungary, pp, 2155-2159, June 2013.

[7] Deloitte, " Understanding the bring-your-own-device landscape," A Deloitte research report of 2013. Retrieved from http://www.deloitte.com/assets/Dcom-Guam/Local%20Assets/Documents/Technology,%20

[8] A. Armando, G. Costa, and A. Merlo, "Bring your own device, securely," Proceedings of the 28th Annual ACM Symposium on Applied Computing, Coimbra, Portugal, pp. 1852-1858, March 2013.

[9] A. Millard, "Ensuring mobility is not at the expense of security," *Computer Fraud & Security, 2013*, pp. 11-13. doi:10.1016/S1361-3723(13)70080-0

[10] Cisco, "BYOD: A global perspective," 2012 survey report. Retrieved from http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf

[11] Ovum, " An emerging market trend in more ways than one," Consumer impact technology. Retrieved from http://www.us.logicalis.com/global/united%20states/whitepapers/logicalisbyodwhitepaperovum.pdf

[12] Gartner, " Gartner says less than 0.01 percent of consumer mobile apps will be considered a financial success by their developers through 2018," 2014 Gartner Newsroom. Retrieved from http://www.gartner.com/newsroom/id/2648515

[13] S. Mahesh, and A. Hooter, "Managing and securing business networks in the smartphone era," Management Faculty Publications. Paper 5. Retrieved from http://scholarworks.uno.edu/mgmt_facpubs/5

[14] Airwatch, " Enabling bring your own devices (BYOD) in the enterprise," Retrieved from http://www.ciosummits.com/media/solution_spotlight/byod-whitepaper.pdf

[15] Citrix®, "Bring your own devices" 2013 Solution brief. Retrieved from http://www.prosysis.com/wp-content/uploads/2013/06/Citrix-BYOD-Solution-Brief.pdf

[16] C. Edwards, "Identity - the new security perimeter," Computer Fraud & Security, *2013*, pp. 18-19. doi:10.1016/S1361-3723(13)70082-4

[17] EY, " Bring your own device: Security and risk considerations for your mobile device program," Insights on governance, risk and compliance. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf.

[18] J. Hayes, "The device divided," *Engineering and Technology, vol. 7*, pp. 76-78, 2012. doi:10.1049/et.2012.0909.

[19] Z. Kerravala, "Bring-your-own-device requires new network strategies," 2012 ZK Research. Retrieved from http://www.xirrus.com/cdn/pdf/zeusk_byod_requires_new_network_strategies

[20] K. W. Miller, J. Voas, and G. F. Hurlburt, " BYOD: Security and privacy considerations," IT Professional,vol. 14, pp. 53- 55. doi:10.1109/MITP.2012.93.

[21] B. Morrow, "BYOD security challenges: Control and protect your most sensitive data," Network Security, 2012, pp. 5-8. doi:10.1016/S1353-4858(12)70111-3.

[22] J. Thielens, "Why API are central to a BYOD security strategy," Network Security, 2013, pp. 5-6. doi:10.1016/S1353-4858(13)70091-6.

[23] K. AlHarthy, and W. Shawkat, "*Implement network security control solution in BYOD environment*," IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, pp. 7-11.

[24] Forrester, "Key strategies to capture and measure the value of consumerization of IT," Cambridge, MA: Forrester Consulting. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf

[25] MTI Technology, "Bring your own device," The future of corporate computing. MTI white paper 2014. Retrieved from https://mti.com/Portals/0/Documents/White%20Paper/MTI_BYOD_WP_UK.pdf.

[26] J. Grover, "Android forensics: Automated data collection and reporting from a mobile device," Rochester Institute of Technology, RIT Scholar Works. Retrieved from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=5389&context=theses.

[27] N. Bjorn, K. Sebastian, O. Kevin, and K. Stefan, "Towards an IT consumerization theory: A theory and practice review," Working papers, ERCIS – European research center for information systems, no 13. 2012. Retrieved from htt://hdl.handle.net/10419/60246.

[28] B. Tokuyoshi, "The security implications of BYOD," Network Security, 2013, pp. 12-13. doi:10.1016/S1353-4858(13)70050-3.

[29] G. Thomson, " BYOD: Enabling the chaos," Network Security, 2012, pp. 5-8. doi:10.1016/S1353-4858(12)70013-2

[30] S. Mansfield-Devine, "Interview: BYOD and the enterprise network," Computer Fraud & Security, *2012*, pp. 14-17. doi:10.1016/S1361-3723(12)70031-3.

[31] S. Denman, "Why multi-layered security is still the best defence," Network Security, 2012, pp. 5-7. doi:10.1016/S1353-4858(12)70043-0.

[32] M. Potts, "The state of information security," Network Security, 2012, pp. 9-11. doi:10.1016/S1353-4858(12)70064-8.

[33] W. Peng, F. Li, K. J. Han, X. Zou, and J. Wu, "T-dominance: Prioritized defense deployment for BYOD security," IEEE Conference on Communication and Network Security (CNS), National Harbor, MD, pp. 37-45, October 2013.