MANAGING ACCESS CONTROL ISSUES IN THE CHOOSE YOUR OWN DEVICE ENVIRONMENT

by

Khalid Ali ALMARHABI[*]

Department of Computer Science, College of Computing in Al-Qunfudah, Umm Al-Qura University, Makkah, Saudi Arabia

Original scientific paper
https://doi.org/10.2298/TSCI22S1445A

Enterprise mobility is taking the business to another level. Organizations are nowadays managing to adopt varying enterprise mobility that helps run the transactions conducted in a bigger and better way. Despite their huge assistance, most enterprise mobilities are causing mayhem to most organizations that have integrated them as the sole strategy to keep things running. They are becoming inevitable and unstoppable trends that pose new security risks and challenges in controlling and managing corporate data and networks. If not well monitored, they can unwontedly lead to disclosing vital information, disruption of services, legal implications, financial issues, loss of productivity, and modify access policies. One such largely implemented enterprise mobility is choose your own device. The intention of this paper is to propose a new framework that would help in managing the access control issues in the environment of choose your own device. The main aim of the proposed architecture is to reduce restrictions and enforce access control policies in choose your own device and the cloud.

Keywords*: choose your own device, access control, security, policy*

Introduction

Any person investigating enterprise mobility will run into terms such as COBO, COPE, BYOD, and CYOD, among others. Each letter in these acronyms has a distinctive meaning. For instance, COBO stands for Company Owned/Business Only and CYOD represents Choose Your Own Device [1]. However, beyond these word representations, there is little agreement on what they mean and the kind of purposes they carry out for any organization. For CYOD, it refers to a business trend and phenomenon designed to allow employees to select preferred devices from a company-approved range of options [2]. The application of CYOD varies by its various advantages and disadvantages it offers. Some of the advantages realized by the application of CYOD include; they help in reducing risks and upgrading security. A report by Norris highlights the importance of CYOD reduces risk and security by up to $3200 per employee per year [3]. In addition, the cost of employee turnover can sometimes be as much as 2.5 times the salary of an employee, depending on the role. It increases productivity. 0ver 65% of enterprise employees believe they are more productive when they are permitted to select their own work devices. In addition, over 76% of workers believe using a single

[*] Author’s e-mail: kamarhabi@uqu.edu.sa

mobile device of their preference aids them in balancing their professional and personal lives [4]. Lastly, CYOD offers the latest technology and improves morale at the workplace.

Just like any other policy, CYOD also has several disadvantages within the workplace, and every organization has varying needs as far as resources, costs, and security are concerned [5]. One of the most crucial challenges after deploying CYOD is meeting the costs and demands required in integrating the policy [6]. After selecting CYOD, the organization would be required to meet up with the hardware, staff support, data, and other device-related services. Even with negotiated discounts, managing to meet up with total added costs would weigh up huge costs, considering that the number of headcounts would affect the charges to be incurred [7]. Another disadvantage is support. The organization would be required to introduce or upgrade a new support team that would support the IT integration and facilitates frequent changes and updates to all programs required in those CYOD devices [8]. Employees may also feel restricted from their specific preferred devices. This is because they have to choose from the specific devices chosen by the organization. Other disadvantages relate to less defined responsibility for hardware repair and slower deployment than CYOD.

The CYOD presents a better management method for counteracting issues presented by cyber threats. Any organization using CYOD policy manages to secure its information in a better way due to the company-owned devices. Some of the ways CYOD manages to solve cyber issues are displayed in tab. 1.

Table 1. Cyber Issues counteracted by the application of CYOD

Cyber issue/threat	Counteracted issue using CYOD
Deliberate software attack/compromise to intellectual property	CYOD enables the organization to control the device and protect it from attack
Deliberate acts of trespass or espionage	CYOD allows the company to outfit devices with essential applications that mitigate security measures before giving the devices to employees
Technical software failures or errors	CYOD policy allows IT, experts, to narrow the upgrade list instead of having to upgrade multiple operating systems as in CYOD
Act of human error or failure	CYOD policy can be centrally monitored, therefore minimizing human errors and also allowing quicker recovery in the cases of human failure

Access control refers to a method of guaranteeing that users of a certain product on the internet or in the workplace are who they say to be and that they have the full right to access the company’s data [9]. In accordance with this definition, organizations greatly consider the kind of enterprise mobility to deploy into their organization, considering that they would permit employees to access information using various devices. CYOD counteracts the issues of access control using various techniques, tab. 2.

Table 2. Issues of access control

Issue of access control	Mitigation ways deployed by CYOD
Outdated equipment	CYOD enables the organization to choose the kind of devices that would be simpler to run. Therefore, the organization can manage to remotely and centrally update devices
Lack of integration with other devices or system	The organization can advocate for devices that have similar systems that would help make it easy to integrate with other devices
Incorrect setup	CYOD can allow the organization to navigate setup issues even without having to access the device from the employee physically

The organization can face a hard time trying to protect information from being accessed by unauthorized individuals; on occasions when employees have to choose the devices to work with from the company-approved range of options, the issues of access control possess even greater concerns [10]. In conjunction, this paper aims to introduce a new architecture framework to help in managing the issues countered in access control of CYOD. The objective of the proposed framework is to present better managerial and enforce better access control policies in the cloud and CYOD. In order to achieve this objective, the paper starts by presenting related work that analyses similar articles discussing the same concept. The second section would be the proposed framework, then proceed to have the implementation and testing section, and lastly, provide a conclusion analyzing the overall topic.

Related work

Iovan and Ivanus [11] propose that all companies with growing ambitions need to have a formal and well-elaborated mobile strategy, if any of these fails, the organization could lose the economic recovery. They contribute to the research dynamics by offering an article that supports alternative security measures. A similar concept is proposed by Kokolakis *et al*., [12] who claim that the achievement of an organization depends on the implementation of its strategy. Currently, most organizations are considering the option of CYOD, however, the shortcoming it presents causes most organizations to shift to CYOD. This attributes to the rapid proliferation of mobile devices that makes its mobility security to be weak in regard to security management [13]. Overall, Iovan and Ivanus [11], Kokalakis *et al*., [12], and Zambrano and Rafael [13] contribute to the literature by presenting different ideologies through which information can be secured.

Similarly, Ratchford *et al*. [14] conducted a review that answered the security issues and considerations associated with enterprise mobility. Their conclusion was that most threats were registered from the IT domain marking up to 86%, 51% concerned the management domain, 45% concerned the user domain, and 19% were caused by the mobile device domain. The concepts discovered are very similar to the revelation of how cyber threats have greatly affected online credibility. Akram and Markantonakis [15] presented an article that evaluated the security and trust challenges presented by mobile devices in various domains. They argue that the trust and security that would be required to prevent access to the information in enterprise mobility include; secure decommissioning, closely managing and monitoring the provision of applications to users, and utilize a trusted execution environment [16]. Generally, Ratchford *et al*., [14], Akram and Markantonakis [15], and Raj [16] present literature reviews that are purposely in-depth on responding to security issues associated with enterprise mobility. They form many concepts of security mitigation that are similar to current demand for securty integrations.

A formal and well-elaborated mobile strategy needs to achieve security services that include non-repudiation, data integrity, data confidentiality, access control, and proper authentication [17]. However, the execution of these security services requires policies and procedures. Some of the procedures require to be simple by availing a fair amount of security, temporal, outline on separation of duties that would help in reducing the possibility of the issues associated with issues of access control, be easy to maintain by facilitating easy access to examining and modifying and having the least privileges by having the least permission for users to gain access to information that is not meant for them [18]. In addition, to provide solutions that address the access control issue in CYOD, there are four requirements necessary to drive the development solutions, as listed below.

Check CYOD essential apps

It is very crucial to ensure the security of CYOD devices is met. The devices that employees prefer to choose must me*et* all the requirements of the organization in order to avoid threats that may damage or allow access to confidential information of the organization. The organization can consider installing some apps with antivirus detectors and only allow the company-approved range of devices to install apps for work [19]. They can be designed as inbuilt applications in order to prevent employees from removing them from the devices. The selected inbuilt apps can be as well designed to educate employees on how their personal data are managed and how the legislation is deployed to protect the data of both the company and employees.

Enforce access control policy

Any organization intending to implement an access control system is required to consider three abstractions, they include, access control mechanisms, models, and policies. Access control policies are regarded as high-level requirements that outline how access is managed and the personnel that can access data under what circumstances [20]. The enforcement of access control policies occurs through a mechanism that translates a user's access request, mostly regarding the structure that a system provides. Majorly, the enforcement policy associated with CYOD devices that meet the minimum requirements of security, the authorization phase, and the authentication phase. Mandatory Access Control is one of the best mechanisms to enforce the implementation of access control policy [9].

Secure access control policy

The newly implemented access control policy must aim at reducing the security risks to the logical and physical systems of an organization. The policy should contain measures that outline physical access control, which would enable the organization to secure its hardware, while the logic access control outlines protecting the Software and can also maintain a record of which employees are permitted to access the organization's data at what time. This policy would help in minimizing risks in the devices that employees prefer from physical interference, such as theft and physical damage on the device. This is because the policy would outline consequences or what to be done when an employee causes physical damage or in the case of theft. In addition, the logic access control policy would cover the operating system and ensure all threats in cases of trying to breach organization data or installing intentionally installing malicious threats would be counteracted.

Differentiation between employer's assets and employee's assets

Time and time again, it has been said that confidentiality of information is very vital to any organization. It is very crucial to retain confidentiality matters because of reputational and legal reasons, and it is also important due to future employment may need or depend on it. In our case, the management of access control issues to CYOD offers various confidential information that needs to be mitigated and protected. Some of the confidential information include; employee information, organization information, managerial information, contact or customer information, and professional information. Just like the organization itself, when employees go to the workplace, they expect to be in a space where they are safe and their information will not be manipulated. Therefore, for CYOD, which provides devices to employees, it is important to ensure their information is intact, such that none of the parties can mess with each other. In order to accomplish these, the ultimate best solution is to ensure data is encrypted. Encryption is a way of scrambling data in order to ensure only authorized parties can comprehend the information, tab. 3.

Table 3. Previous approaches comparing to our proposed framework Y – yes, P – partly

Paper citation	Check CYOD essential apps	Enforce access control policy	Differentiation between employers' assets and employee's assets	Secure access control policy
[5]	Y	Y	Y	Y
[6]	Y	P	P	Y
[7]		Y	Y	Y
[8]	Y	Y	P	Y
[9]		Y		
[10]	P	Y		P
[11]	P	P	Y	Y
Overall proposed framework	Y	Y	Y	Y

Based on the literature review, each of the previous studies managed to address a single concern and does not avail of a detailed solution to address managing the issues of access control in CYOD. Therefore, the solutions presented are still insufficient and require further studies.

Proposed framework

As already discussed, access control systems are highly considered for businesses that require added security. This is because access control systems are regarded as a better alternative for generating multiple keys to the building, which are the electronic key system that approves identity before allowing entrance or access to information. Overall, the term access control is contained in the collective terminology cloud security, also referred to as computing security. Computing security is the collection of security measures that are designed to protect cloud-based data, applications, and infrastructure. Computing security is utilized in the cloud environment to protect an organization's data from unauthorized user use or access, hackers, and distributed denial of services.

To attain maximum security in computing security, it is grouped into three main models that include infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). However, in order to mitigate the access control issues in the environment of CYOD, this paper proposes the integration of a newly developed security manager tool called Software as a Service (SaaS). For the development of SaaS, there are several considerations taken into place. The new system has considered several concerns in its framework and tried to make it easier for the addition and application of limited operating requirements and not impact the operations of CYOD and its computing environment. In order to meet the expectations of security, the newly developed framework is designed on a multi-agent system. This is because it is independent Software that operates as a representative of a network user.

With the environment facilitated by CYOD, the newly proposed framework works efficiently because of it self-starts and stops, raggedness, transparency, mobility, and adaptability. The purpose of developing the system is to mainly help in mitigating the access control issues, although it adds other advantages such as reducing costs and minimizing the kind of resources needed when coordinating the operations with other tools. The newly proposed framework can also be divided into three components: the security manager, the policy administrator device or the owner device, and the client CYOD. The illustration of the newly developed system is displayed in fig. 1.

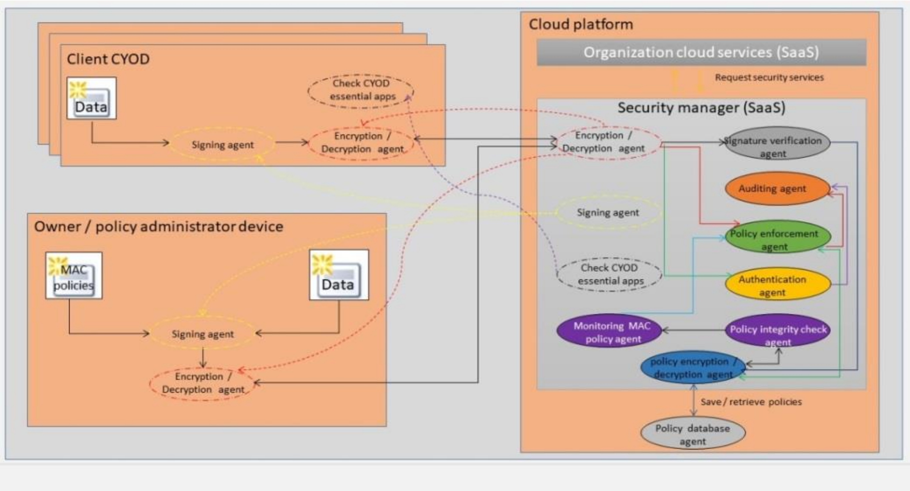

Cloud platform
Organization cloud services (SaaS)
Request security services
Security manager (SaaS)
Client CYOD
Data
Check CYOD essential apps
Signing agent
Encryption / Decryption agent
Encryption / Decryption agent
Signature verification agent
Auditing agent
Signing agent
Policy enforcement agent
Check CYOD essential apps
Authentication agent
Owner / policy administrator device
MAC policies
Data
Signing agent
Encryption / Decryption agent
Monitoring MAC policy agent
Policy integrity check agent
policy encryption / decryption agent
Save / retrieve policies
Policy database agent

Figure 1. The newly proposed framework for CYOD and the computing environment

Policy administrator device/owner

As previously displayed, the policy administrator is on the bottom left of the whole computing environment. This part hosts the person in charge of formulating and setting the policy. It can be any of the organization's owners, the policy administrator, or the Chief Security Officer (CSO). The device that can be utilized in this implementation can be a normal PC or CYOD with a trusted OS, such as Security-Enhanced Linux (SELinux).

The MAC policy

The MAC is an acronym for Mandatory Access Control policy. MAC is a very vital component of computing security because it provides harsh access limits that cannot be trespassed intentionally or unintentionally. It is also effective because it uses a clearance that is possessed by every user of the system. MAC manages to firmly establish if the user can have access to a specific file or deny the user. This design can be implemented using JavaScript Object Notation (JSON) language. MAC further manages to establish four major security classification levels for both objects (resources) and subjects (users), which are unclassified, confidential, secret, and top secret. The operator on the owner part has delegated the responsibilities of determining the use and resource security classification level.

Data

Data associates with all the resources that users or employees what to upload and store in the newly proposed cloud.

Security manager

The security manager serves as the main building block of the suggested structure since, as will be seen below, it has influence over every other component. This framework's application of various agents satisfies at least four requirements: control policy security, independent platform operation, access control policy enforcement, and CYOD device security inspection.

Controller agent

It is the head of all other agents. It is specially equipped with the capability of creating instances from mobile agents and manage to distribute them to other devices by utilizing their IP addresses. This controller agent can also hold the API – Application Programming Interface to liaise with other Software as a service in computing.

Check CYOD essential apps

The check CYOD essential apps are the newly designed programmed application that facilitates the normal functionality of the selected devices. They are implemented and designed on how they would work in the and offer effective communication as they travel between Client CYOD and the security manager in the organization’s software as a service (SaaS). The prior procedures of the signing agent and encryption/decryption agent help in checking the credibility of the client before being trusted to access the essential apps. In cases where the client is not warranted access to the organization’s software, the accessibility to essential apps would not be allowed. The essential apps contain essential information and therefore maximum avoidance of threats must be put in place to protect the confidential information of the organization. In order to achieve the climax of managing the access control issues in the environment of CYOD, the essential apps, in the security manager ensure updated information is always provided for scrutiny. Overall, the security manager provides a summary of what the clients must do in order to use their devices in accordance with the security requirements of the organization.

Authentication agent

Authentication is applied as the basic requirement. This is after the devices have been assessed to comply with the requirements of the security policy. Authentication ensures the user is fully validated for using the account. Authentication agent expects every user to have a personalized and unique identity. In most instances, there are two varying types of authentications that are used to enhance the security of the system.

Check permission agent

After the authentication agency finalizes the checking, the check permission agent chips in. Check permission is responsible for taking the username presented by the user and proceeding to match the naming in the database. Check permission agent does to in order to ensure security clarification has been attained. The next stage is moving the username to the CYOD device of the user in order to make a preparatory decision on either allowing access or not. This agency executes the ideas of MAC and utilizes the MAC policy associated with the security classification level for the purposes of making access decisions. In addition, this agency is responsible for the improved performance since it helps in minimizing time consumers if the user is not authorized to legitimately access before the request goes through the internet to the cloud side.

Signing and signature verification agents

These two mobile agencies ascertain that the information or signals are sent by a known user and were not in any way modified in the sending process. They manage to accomplish these by producing digital signatures for every JSON policy file and information presented by CYOD or the owner. The digital signatures are verified in the security manager by the signature verification by comparing various decrypted hash values with the generated value of the original data and the initial JSON policy. In the case where values prove to be equal, the message means that it has not been modified.

Decryption and encryption agent

Decryption and encryption agent are agents that corroborate that only permitted agents and users can log in, access, and read or manipulate the stored data. This mobile agent is solely there to make sure the data in transit is secured and kept secret. The agent has the capability to decrypt or encrypt all data and access control policies transmitted between the user device and the security manager on the computing side. The decryption and encryption agent applies an asymmetric algorithm in order to exchange the symmetric key and utilize it for some time.

Policy enforcement agent

Policy enforcement agent is present to enhance the enforcement of access control policy in order to ascertain what users can access the computing environment. Additionally, it promotes the access control mechanism and succors the DAC to avail a better access control mechanism. For policy enforcement agent to support the achievement of confidentiality, it executes the concept of MAC by applying the Bell-LaPadula model.

Policy monitoring and integrity check agents

These two agents are responsible for saving copies from the initial hash value of the MAC policy that had been updated or generated by the owner. The saved copies are to be continuously used in comparing them with other newly produced hash values. Additionally, it ensures there are no modifications done to the MAC policy by a hacker during the processing phases.

Auditing agent

The auditing agent is there to ensure that all failed and successful attempts to access the system have been recorded. It also records all decision taken by policy enforcement agent that denies or grants to accessing the data. The data included in the auditing agent is associates with the decision, resources, time, date, and username. This information aids the owner in performing disaster recovery, conducting regulatory compliance, analyzing, monitoring, and developing the system.

Policy decryption and encryption agent

The agent is designed with the ability to decrypt and encrypt all information that is being retrieved or stored from the access control database. The sole purpose of these is to protect the data in the transfer and storage phases.

Policy database agent

It is designed to channel communication with other crucial databases such as distributed database management systems (DDMMS), database management systems (DBMS), or databases as a service (DBAAS). Additionally, it handles and exchanges data between varying software architecture patterns and styles.

Client CYOD device

The users can decide to apply their own devices after the confirmation that CYOD devices are trusted by achieving the requirements of the security policy. The testing is done by the check security requirements agent, and it travels to clients' CYOD devices when they desire to access the computing environment. After the assessment and the users meet the requirements, other agents then move to other users' devices to perform similar functions. Users can manage to generate and distribute information by suggesting security classification levels, and the policy administrator device approves it.

In the event that the policy administrator needs to generate or modify existing data or policies through the user interface, the user uses a signing agent that manages to add a digital signature to the message, as displayed in fig. 2. After this step, the policies and data are encrypted by the encryption and decryption agent before being transited back to the internet. The kind of verification that occurs is called a signature verification agent. Once it is passed, there is an implementation of the MAC mechanism using the policy enforcement policy agent and there is permitted to all legitimate request access and denial to all illegitimate access.

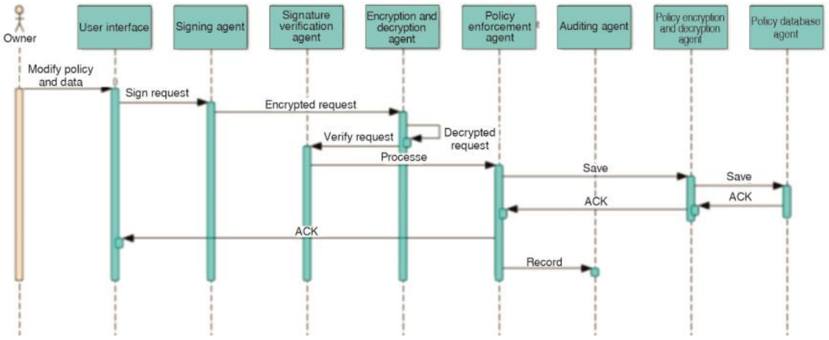


Figure 2. Sequential diagram for generating and modifying data or policies by policy administration

Implementation and testing

The implementation and testing phase of the proposed framework is very crucial for helping verify the validity of the presented solution strategy. The implementation and testing are needed to assess if there is any failure, error, or faulty in the framework. In order to fully assess and understand the implementation and testing process, it is vital to note that there are two core components that can be majorly examined. They consist of the client and the security manager as Software as a Service (SaaS). Numerous agent frameworks, including Jade, Aglets, and Concordia, can be used in the assessment. This study incorporated the utilization of Java and C# in the Microsoft Visual Studio framework for the assessment of client proprietors of CYOD devices. The paper also used actual CYODs running the Windows operating system to install the program and establish a connection to the cloud.

For the security manager, two Software as Services were created using the same environments. The organizational software was one of the pieces of software, and the security manager was the other. The Google cloud platform would be used to deploy the two chosen pieces of software, which would use their storage as a database. The newly proposed framework's structure and functionality were evaluated using the white box and black box tests. By confirming some of the needs that were used in the framework, the testing and validation were effectively completed. There were at least four cases used to test the proposed framework in regard to managing the access control issues in the environment of CYOD to protect the framework from potential attacks as shown in fig. 3:

– Case 1: When both untrusted and trusted individuals utilize untrusted devices.
– Case 2: When trusted persons and trusted devices are used to access unauthorized information.
– Case 3: The process and storage phases are when the access control policy is assaulted.
– Test 10 access control rules using the changed cipher text, the original cipher text, the wrong digital signature, and the correct digital signature during the transfer of phase in Case 4.

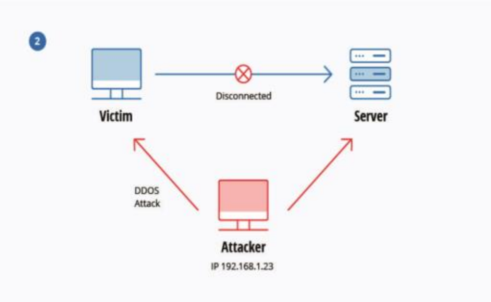
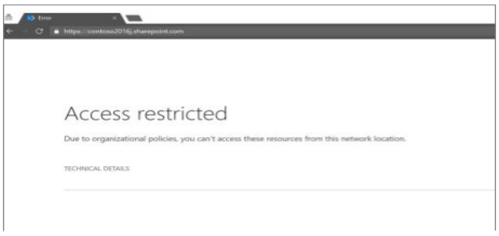


Figure 3. Potential attack that may occur in the cloud and CYOD environment

The system must *check security requirement agent* for Case 1. It was then made capable of spotting an untrusted device that did not adhere to the standards, fig. 4.


Error
https://contoso2016j.sharepoint.com

Access restricted

Due to organizational policies, you can't access these resources from this network location.

TECHNICAL DETAILS

Figure 4. Interface revealing the untrusted CYOD device

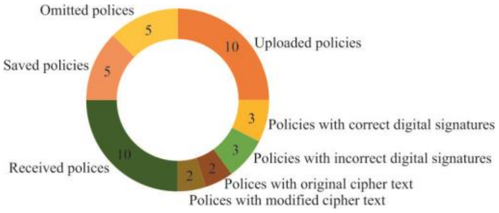


Figure 5. Statistical of attempted upload and threats to CYOD devices

For Case 2, the system detected users were not legitimate due to the resources provided by comparing the MAC security classification level of the user with the classification level of the required resources.

For Case 3, the proposed framework faced numerous attacks that modified the access control policy during the process and storage phases.

Lastly, there were 10 test accesses of the control policy during the transfer phase with different characteristics. Both the decryption and encryption agents and the signature verification agent detected all modified access control policies, as revealed in fig. 5

Conclusion

The paper has introduced a solution that facilitates managing the access control issues in the environment of CYOD. The objectives of the paper were to create solutions for the issues of CYOD while still maintaining its features, such as improved flexibility and mobility. The research managed to create a solution that is based on four major requirements, which include securing the access control policy, working with independent platforms, enforcing the access control policy, and checking the CYOD device security. The paper managed to incorporate all of these four requirements and constructed a proposed framework that is based on the multi-agent system because of it self-start and stops, raggedness, transparency, mobility, and adaptability. While assessing the current recommendations and solutions to issues of access control of CYOD, most of the acquired solutions from the literature work supported specific concerns without consideration of involving a comprehensive evaluation of the effects of these solutions on the CYOD environment or their clients. However, this paper tried to cover the available gap by attempting to reduce most of the barriers and other restrictions and proceed to amplify the mobility and flexibility with an application of the soft implementation of the policy. Following various testing and implementation, the outcomes of the validation revealed outstanding results and positive feedback. The future can manage to fully implement this proposed framework with little to no obstacles to encounter. It would expect that it will manage to offer improved security, mobility, and flexibility when running businesses.

References

[1] Basole, R. C., Enterprise Mobility: Researching a New Paradigm. Information, *Knowledge Systems Management, 7* (2008), 1-2, pp. 1-7

[2] Loh, C. C., *et al*., Enterprise Mobility and Support Outsourcing: A Research Model and Initial Findings, *Information Knowledge Systems Management, 7* (2008), 1-2, pp. 183-210

[3] Norris, B., The Benefits of CYOD and BYOD: 3 Reasons to Consider Employee Choice, Shi.com, 2022

[4] Servos, D., Osborn, S. L., Current Research and Open Problems in Attribute-Based Access Control, *ACM Computing Surveys (CSUR), 49* (2017), 4, pp. 1-45

[5] Hein, D., *BYOD vs. CYOD vs. COPE: What's the Difference?*, Mobility Manag. Solutions Review, 2019

[6] Brodin, M., BYOD vs. CYOD," What is the difference?, *Proceedings*, 9th IADIS International Conference Information Systems, Vilamoura, Portugal , pp. 55-62, 2016

[7] Zambrano, F. R. R., Rafael, G. D. R., Bring Your Own Device (BYOD): a Survey of Threats and Security Management Models, *International Journal of Electronic Business, 14* (2018), 2, pp. 146-170

[8] French, A. M., *et al*., Current Status, Issues, and Future of Bring Your Own Device (BYOD), *Communications of the Association for Information Systems,* 35 (2014), 1, 10

[9] Ouaddah, A., *et al*., Access Control in the Internet of Things: Big Challenges and New Opportunities, *Computer Networks, 112* (2017), Jan., pp. 237-262

[10] Abomhara, M., Koien, G. M., Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, *Journal of Cyber Security and Mobility, 4* (2015), 1, pp. 65-88, 2015

[11] Iovan, S., Ivanus, C., *Bring Your Own Device (BYOD) vs. Choose Your Own Device (CYOD)*, Annals of Constantin Brancusi University of Targu-Jiu. Engineering Series, vol. 4, pp. 112-117, 2018

[12] Kokolakis, S., *et al*., Information Systems in a Changing Economy and Society, *Proceedings*, MCIS2015, pp. 38-511, 2016

[13] Zambrano, F. R. R., Rafael, G. D. R., Bring Your Own Device (BYOD): A Survey of Threats and Security Management Models, *International Journal of Electronic Business, 14* (2018), 2, pp. 146-170

[14] Ratchford, M., *et al*., BYOD Security Issues: A Systematic Literature Review, *Information Security Journal: A Global Perspective, 31* (2022), 3, pp. 253-273

[15] Akram, R. N., Markantonakis, K., Challenges of Security and Trust of Mobile Devices as Digital Avionics Component, *Proceedings*, Integrated Communications Navigation and Surveillance, Herndon, Va., USA, pp. 1C4-1, 2016

[16] Raj, U., Certificate Based Hybrid Authentication for Bring Your Own Device (BYOD) in Wi-Fi Enabled Environment, *Int. Journal of Computer Science and Information Security, 13* (2015), 12, pp. 41-47

[17] Liu, C.-H., *et al*., The Enhancement of Security in Healthcare Information Systems, *Journal of medical systems, 36* (2012), 3, pp. 1673-1688

[18] Zhang, Y., *et al*., Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control, *IEEE Internet of Things Journal, 5* (2018), 3, pp. 2130-2145

[19] Sarkar, K. R., Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures, *Information Security Technical Report, 15* (2010), 3, pp. 112-133

[20] Garba, A. B., *et al*., Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments, *Journal of Information Privacy and Security, 11* (2015), 1, pp. 38-54

Paper submitted: October 8, 2022
Paper revised: November 20, 2022
Paper accepted: November 27, 2022