Taylor & Francis
Taylor & Francis Group

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

Evaluation of security framework for BYOD device in cloud environment

Jimshith V. T & V. Mary Amala Bai

To cite this article: Jimshith V. T & V. Mary Amala Bai (2024) Evaluation of security framework for BYOD device in cloud environment, Automatika, 65:3, 803-814, DOI: 10.1080/00051144.2024.2310458

To link to this article: https://doi.org/10.1080/00051144.2024.2310458

Published online: 26 Feb 2024.

AUTOMATIKA
2024, VOL. 65, NO. 3, 803–814
https://doi.org/10.1080/00051144.2024.2310458

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Evaluation of security framework for BYOD device in cloud environment

Jimshith V. T[a] and V. Mary Amala Bai[b]

[a]Department of Computer Applications, Noorul Islam Centre for Higher Education, Kumaracoil, India; [b]Department of Information Technology, Noorul Islam Centre for Higher Education, Kumaracoil, India

ABSTRACT
The widespread practice of Bring your own device (BYOD) to work significantly raises cybersecurity risks. All organization's employees and employers will greatly benefit from this trend. The growth of spyware, malware and other dubious downloads on individual devices has compelled the government to review its data security guidelines. Without user knowledge, hazardous apps are downloaded to personal devices. Both people and governments could suffer tragic consequences as a result of this. In this situation, BYODs are problematic since they can alter policies without permission and release private information. The main goal of the research was to detect fraudulent communications coming from BYOD environments. A network monitoring and managing information configuration settings of mobile devices in the network is established by providing policies and authenticating endpoint devices in the BYOD network using a mix of NAC and MDM. This framework deals with Security Manager (SaaS) as the second module is briefly described. The study's early results were positive and suggested that the framework would lessen access control-related issues.

ARTICLE HISTORY
Received 8 September 2023
Accepted 22 January 2024

KEYWORDS
Bring your own device (BYOD); privacy and security; security manager (saas); data security; NAC and MDM

1. Introduction

Employees utilize personal devices like smartphones and tablets for work-related tasks under the "BYOD" policy, which is a standard business practice. By 2021, it's predicted that 11 billion people will use personal mobile devices at work. Employee-owned devices in the BYOD environment have access to company data, creating a variety of unique risk profiles that need additional investigation [1].

Mobile devices can be utilized for both personal and business reasons due to their versatility and widespread availability. All industries use BYOD, with the healthcare sector being one of the main drivers of its adoption [2]. The business prefers to permit employees to access company information and network resources using personal devices solely for work or personal purposes [3].

The business's data keeps expanding due to the phenomenon known as "BYOD". Employees want to work from "any device, anywhere" and integrate personal and professional activities whenever they choose. It is a by-product of using computers [4]. A study discovered that 97% of participants in a different survey utilized their gadgets for work-related tasks [5]. Due to its many advantages, BYOD usage has recently grown in popularity. This trend enhances employee satisfaction, productivity, work ownership, flexibility, and mobility [6].

When employees continue utilizing the government network without the necessary official approval, this is referred to as "shadow IT." Additionally, since governments are unable to regulate employee access during working hours, the adoption of BYOD in the workplace increases security vulnerabilities, particularly the possibility of cyber-attacks [7]. BYOD devices are unmanaged and may be more vulnerable, lack a basic security defense system, and include malicious material. Once BYOD is implemented, these become company-trusted devices, and insiders are more dangerous because they are responsible for 63% of digital mishaps [8].

Network Access Control (NAC) gives visibility control the ability to enforce access control policies on devices linked to corporate networks, monitor and examine configured network devices, and notify network administrators about policy violations [9]. It has been discovered that malware, keyloggers, and other cyberattacks increase unauthorized users' access to company networks, potentially resulting in data theft or corporate espionage [10].

A networking solution called NAC is made up of a collection of protocols that establish and carry out a policy for securing devices' first access to network resources.

Major contributions of the research:

(i) This study's objective is to propose a novel architectural framework for reducing BYOD risk.
(ii) Enforcing access control regulations and only permitting authorized user access. MDM protects

CONTACT Jimshith V. T jimshithvt.cit@gmail.com Department of Computer Applications, Noorul Islam Centre for Higher Education, 629180, Kumaracoil, India

company data by encrypting it and limiting access, hence enhancing security.

(iii) The main goal of the research was to detect fraudulent communications coming from BYOD environments.

(iv) A network monitoring and managing information configuration settings of mobile devices in the network is established by providing policies and authenticating endpoint devices in the BYOD network using a mix of NAC and MDM.

The suggested system design is explained in the sections: A quick overview of the concepts and advantages of BYOD is provided in Section I, and the related work involved is covered in Section II. In Section III, the recommended system explains the procedure for securing BYOD devices. The results are provided in section IV, which is then followed by a discussion of the suggested technique. Finally, the article's conclusion is presented in Section V, which also offers research implications for the future.

2. Related work

Organizations require more integrated, methodical processes for controlling threats, maintaining staff devices, and considering the legal ramifications of the BYOD strategy to maximize the benefits for the enterprise [11]. The evaluation would aid in understanding the issues and growing needs of BYOD for organizations and IT professionals [12].

A new framework will be suggested in a separate article, and an experiment will be built to test and assess the findings [13]. In this study, a system for enforcing instantiated policies that are created on-the-fly inside of businesses using reliable BYOD technology is proposed. A role-based access control mechanism is developed using the suggested framework depending on user identity and the present situation [14].

The current BYOD strategy is susceptible to APT (Advanced Persistent Threat) assaults, particularly when spear phishing exploits are used. One of the objectives of this study was to extensively explore the problem of spear phishing to combat APT through it. Security tools like the ACPT (Access Control Policy Tool) are used to examine various security rules to ascertain their functionality and attributes [15]. Numerous firms have adopted BYOD rules, although they are frequently ambiguous and ineffective. A three-tier enhanced policy architecture is suggested to address this drawback and details the rules that must be adhered to by organizations, apps, and devices [16].

Finally, it will suggest selecting a BYOD management solution that works with most mobile platforms [18]. Benefits, risks, and mitigation options for the security flaws present in mobile devices and BYOD programmes in particular are discussed in this study. BYOD programmes are growing in popularity among both large and small enterprises [17].

People, Policy Management, and Technology are the three pillars of the framework. These three pillars will be shown to be essential for securing BYOD installations in businesses. Validating the framework is the final goal [18]. The effectiveness and viability of this model need to be further investigated [19].

Research Gap

- BYOD research is relevant in tackling the above outlined problem by utilizing NAC (Network Access Control) and MDM (Mobile Device Management) technologies to secure the network from unauthorized access.
- A mobile management system, or MDM, monitors mobile device activities and performs compliance checks when a device attempts to connect to the network after being deployed with an agent.

3. Proposed method

The three primary types of cloud services are a software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Novel SaaS-based security manager tools are suggested by available research. This framework can be used by the cloud manager of an enterprise to perform security tests before approving BYOD access to the cloud. The design of this framework must take into account several important factors. First and foremost, it is crucial to make sure the tool can be quickly and readily integrated into a cloud environment or BYOD system. Research recommends limiting operational requirements.

Before making any changes or developments, it provides a precise image of the prevailing system. Without attempting to read the entire code, it uses dependency relationships to find software setup errors and identifies implementation bottlenecks.

The recommender framework is built on a multi-component architecture, where the software runs independently for network users via bridges connecting various brokers. Owner device, security manager, and BYOD client are the three divisions of the framework. The second module of the framework is Security Manager (SaaS). This proposed framework is illustrated in Figure 1. The article outlines each software component's location within the framework.

3.1. Security manager (SaaS)

A key component of the suggested approach is the safety personnel. The main responsibility of a security manager is to supervise the ABAC (Attribute-Based Access

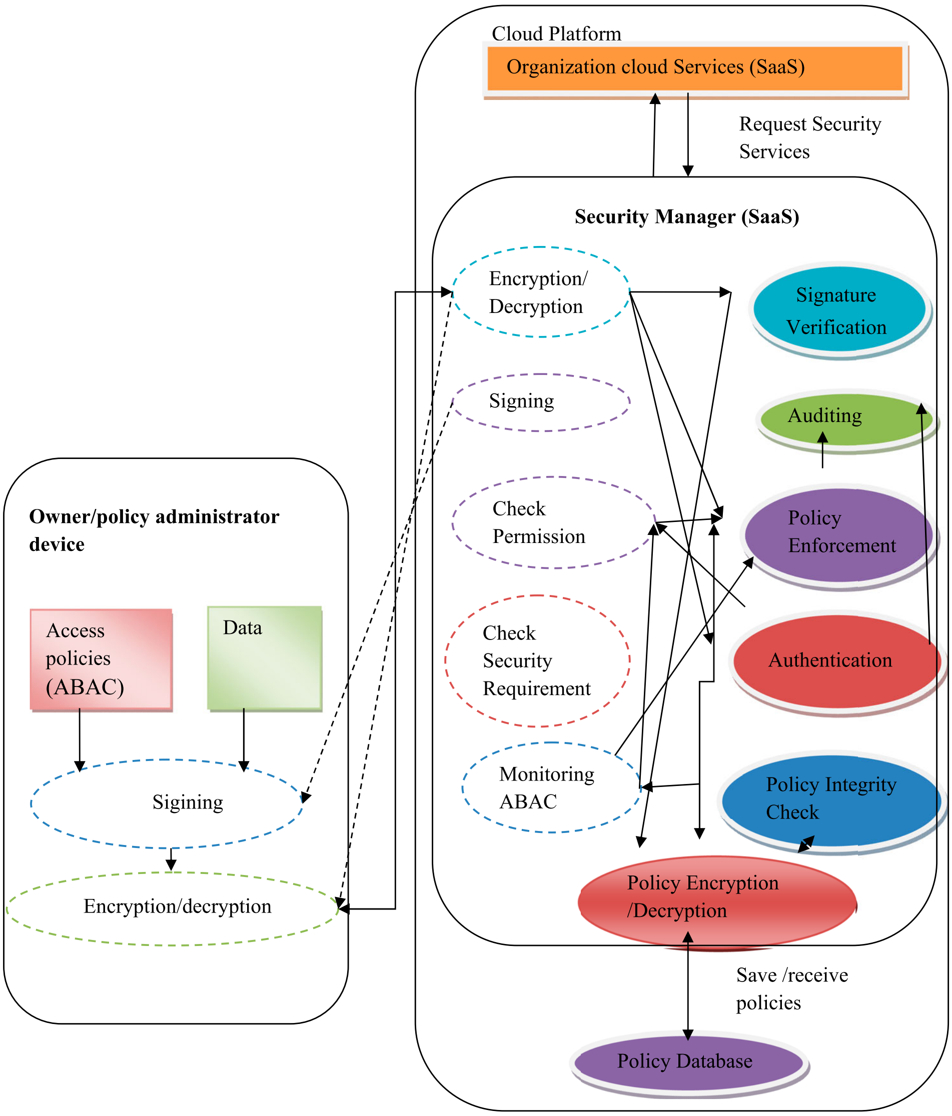


Figure 1. The recommendation framework (security manager) for cloud and BYOD security environment.

Control) policy processes. It functions as a SaaS and can be hosted on the cloud. The framework's four key tasks are managing autonomous systems, analyzing the security of BYOD parts, securing access control regulations, and enforcing access control policies.

3.1.1. *Check the security requirement component*

Verify that the controller component has configured the security needs component. Utilizing cloud-based SaaS for organizations, its objective is to assess linked devices. The verification security component ascertains whether the BYOD is a trusted device that complies with the organization's security policies.

3.1.2. *Authentication component*

When the device satisfies the requirements of the security policy, the authentication component is activated. A distinct identifier is required for each user. Using two authentication techniques for increased security, the authentication component verifies the user's identity pf to access the system.

3.1.3. *Check permission component*

When the permissions checker has finished its scan, it will immediately scan the directory to confirm the security level given to the user. If the user's access has been denied, the component in charge of checking permissions expedites the process before submitting a request to the cloud.

3.1.4. *Signature and signing verification components*

Whenever a signing or signature verification is being done, portable parts are always used. These parts are in charge of checking requests to ensure that they come from authorized users and haven't been altered in transit. Digital signatures are used to sign each JSON regulation document and each data owner request (Figure 2). The signature verification feature of the security manager validates the digital signature. The resulting unencrypted, decrypted hash code is compared to the original JSON policy to make sure they are all the same. When the values are equal, the message remains the same.

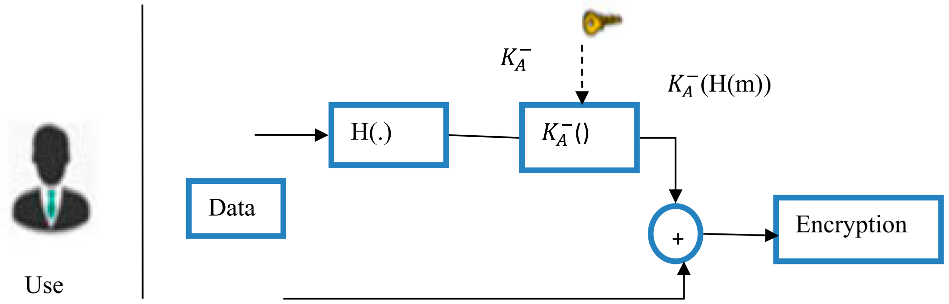


Figure 2. Establishing a Cryptographic Key on a BYOD device.

3.1.5. Components responsible for encryption and decryption

Only authorized persons and parties can view and read the information provided by the components in charge of encryption and decryption. Its objective is to guarantee the message's content's confidentiality. Before transmitting the data, this component transforms it into an unintelligible format. When the data is ready, the procedure is reversed to make it readable by humans. To encrypt messages, the component employs an asymmetric technique. This is exchanged for symmetric cryptography, which is applied to the transmission of the ABAC rule to be decoded. Figure 3 illustrates the working model of digital signature.

The sender performs the following actions to sign a message:

1. Creates a message's hash value.
2. computes the signature using his/her private key (m,c)

$$S = Nc \; mod \; m \qquad (1)$$

3. Send S signature to the receiver

To verify the communication, the receiver takes the following actions:

1. Utilize the sender's public key (m,f) to compute the hash value

$$V = Sf \; mod \; m \qquad (2)$$

2. Retrieving the message's hash value
3. The signature is valid if both hash values match.

3.1.5.1. Key generation algorithm.

1. It is necessary to create two gigantic random primes, i and j, that are almost identical in size for their product, $m = ij$, to have the required amount of bits.
2. Calculate $m = ij$ and $\varphi = (i - 2)(j - 2)$.
3. Select an integer $f, 2 < f < \varphi$, such that $gcd(f, \varphi) = 2$.
4. Calculate the secret exponent $c, 2 < c < \varphi$, such that $fc \equiv 2(mod\varphi)$.
5. The public key is (m, f), and the private key is (c, i, j). Keep all c, i, j, and φ secret values. Where
   (a) a)m is called the modulus
   (b) b)f is called the public exponent or the cryptographic exponent or simply the exponent.
   (c) c)c is called the secret exponent or the decryption exponent

3.1.5.2. Encryption.

1. Get receiver B's public key (m, f).
2. Uses positive integer $n, 2 < n < m$ to represent the plaintext message. $h = nfmodm$ is used to calculate the ciphertext.
3. Send ciphertext h to B

3.1.5.3. Decryption.

1. Calculates $n = hcmodm$ using his private key (m,c).
2. The message representation n is used to extract the plaintext.

The message is authenticated using the digital signature. If the signature is genuine, the recipient will be able to verify that the message was sent by the legitimate user and was unaltered by using an asymmetric encryption algorithm and again encrypting the message using the public key.

3.1.6. Policy enforcement component

A fixed system called an authorization policy uses access control policies to decide who has access to the cloud. It intends to improve access control. The security control component assesses the ABAC policy to determine whether the user satisfies the required categorization.

3.1.7. Components responsible for policy monitoring and integrity checks

The component in charge of the service keeps a copy of the original owner's hash each time it is generated or altered. It regularly compares these against manually generated hash values for an equivalent ABAC scheme.

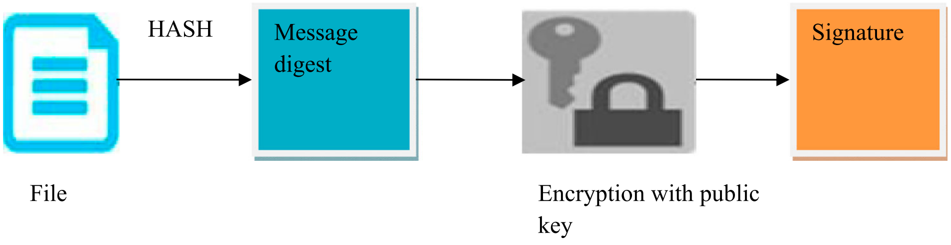


Figure 3. Work model of RSA with the digital signature technique.

3.1.8. Component responsible for auditing

The checked element has been corrected. Responsible for tracking all system accesses, both successful and unsuccessful. The component keeps track of all access decisions made by policy enforcement components, including those that grant and refuse access.

3.1.9. Policy encryption and decryption component

After being encoded and decoded by designated components, i.e. encoding and decoding components, the accessible data is transferred. When connecting to an access control database, the storage is protected using a symmetric encryption algorithm (AES).

3.1.10. Policy database component

The database is managed by a standalone application that communicates with a distributed DBMS (database management system) and the database as a service. This component exchanges data while transmitting messages using various software architecture designs and patterns.

3.2. Devices representing policy/Owner administrator

The person responsible for managing the BYOD customer access control policy also supervises the mechanism's application.

3.2.1. Access policies

The term "Attribute-Based Access Control" (ABAC) refers to a novel logical access control mechanism that restricts access to things after evaluating the regulations defining the characteristics of specific entities (i.e. subjects and objects), their behaviours, and the surrounding environment in connection with the request.

3.2.2. Data

Data includes documents sent over the internet and stored in the cloud.

4. Experimental results

To validate and confirm that the suggested framework is a workable solution, it must be put into practice and tested. Testing and implementation show that the system is error-free and faultless. Two processes are used in the prototype implementation: a client-side owner application and an online SaaS-operating security agent.

Table 1. Various cases of untrusted and trusted devices and users.

Status under various cases	Trusted devices	Untrusted devices
Allowed authorized access to Trusted	Case 2	Case 1
Unauthorized access by a trusted owner	Case 3	Case 1
Untrusted owners	Case 4	Case 1

4.1. Trusted and untrusted users and devices testing

Four distinct cases are used to evaluate trustworthy and untrustworthy people or devices. As shown in Table 1, some cases discuss the results of implementing BYOD.

The "check security requirement component" analyzed these cases and found an untrusted device that did not meet the firm's standards. In Figure 4, this is depicted. In this instance, connecting to the cloud is not allowed for the application.

In the second instance, the "check security requirement component" has been activated, allowing the gadget to connect to the Google cloud since it is a trusted gadget. The system recognizes users who want to use unauthorized resources in the third case, as depicted in Figure 5. This is accomplished through contrasting ABAC policies.

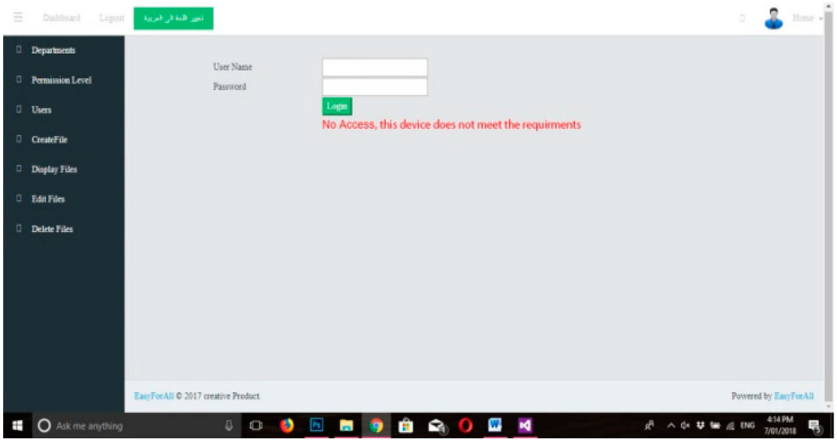
The final scenario concerns untrustworthy users who are permitted to access the system but do not meet the ABAC security requirements. In this case, the "Authenticator component" identifies these operators and denies them access to the network. Figure 6, is depicted.

4.2. Malicious activity detection

This study has investigated detection mechanisms and implemented appropriate security controls to identify internal infrastructure risks.

4.2.1. Byod users face malicious internet traffic detection

This section's main focus was on BYOD mobile roaming customers who were entirely connected to the internet. Results are sequentially recorded and examined.

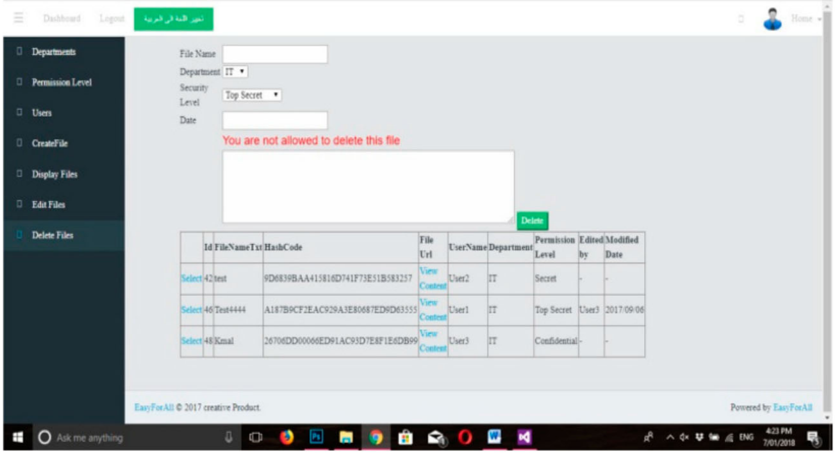


User Name
Password

No Access, this device does not meet the requirments

EasyForAll © 2017 creative Product. Powered by EasyForAll

Figure 4. Untrusted BYOD interface.



File Name
Department IT
Security Level Top Secret
Date

You are not allowed to delete this file

	Id	FileNameTxt	HashCode	File Url	UserName	Department	Permission Level	Edited by	Modified Date
Select	42	test	9D6839BAA415816D741F73E51B583257	View Content	User2	IT	Secret	-	-
Select	46	Test4444	A187B9CF2EAC929A3E80687ED9D63555	View Content	User1	IT	Top Secret	User3	2017/09/06
Select	48	Kmal	26706DD00066ED91AC93D7E8F1E6DB99	View Content	User3	IT	Confidential	-	-

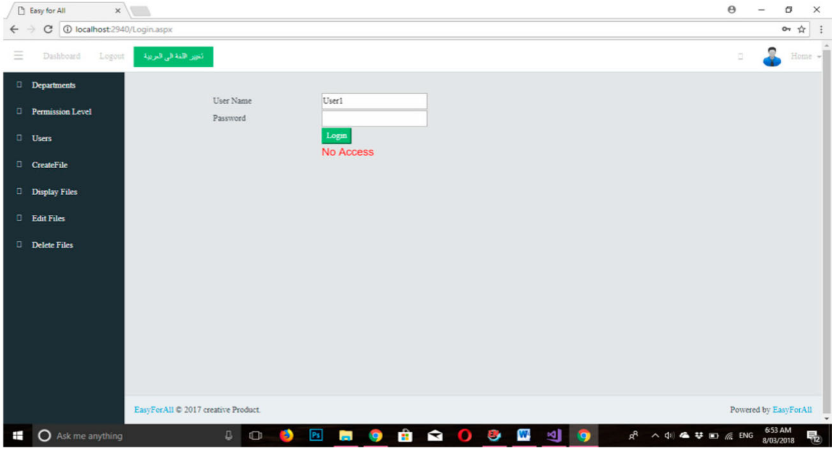
EasyForAll © 2017 creative Product. Powered by EasyForAll

Figure 5. An interface displaying the classification of forbidden access to illegal resources.

The main issues with remote users are a variety of harmful behaviours, data leaks, security events, and security compliance.

The BYOD device information that was further explored is also shown in this result. Finally, it examined the summary of attack vectors, threat variables, and event classifications for the entire infrastructure and discovered crucial information that was helpful in the overall scheme of things, as depicted in Figure 7.

All BYOD endpoints adhere to security standards, regardless of the functionalities of the various technologies they employ. Results are displayed in Figure 8. The Security Compliance Dashboard also showed all BYOD devices, the top threats, hazards, and security incidents.



User Name User1
Password

No Access

EasyForAll © 2017 creative Product. Powered by EasyForAll

Figure 6. An interface showing the prohibition of unauthorized users from accessing the system.

This dashboard offers guidance on security policy for the entire platform.

4.2.2. Internal segment connected BYOD users for malicious traffic detection

Figure 9 depicts the connection between an android smartphone's mac address 2E:79:8E:93:DF:5A and the IP address 182.27.61.137 for the testing username Indra.

4.2.3. Detection of malicious internet traffic facing BYOD users with VPN

The Prisma cloud gateway then verified any communications that were directed at an Internet destination. The following image shows the DNS security landscape, with 5.96 K of the traffic falling under the Spyware DNS security category. Threats that would be investigated and blocked are listed in Figure 10.

4.3. BYOD policy configuration

For this particular policy, Figure 11 shows editing the identity source sequence. Go to MyDevices _Portal _Sequence in ISE by selecting Administrative > Identification Management > Identity Source sequences. At the top of the selected column, place the AD (Active Directory) server on this policy.

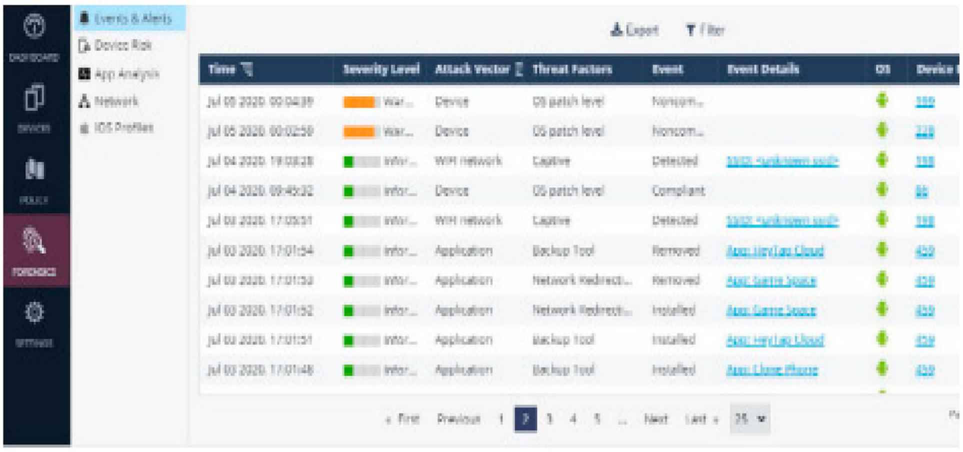
After saving this Identity Source Sequence, Figure 12 demonstrates how to alter the Guest _Portal _Sequence and place the AD server at the top of the selected column.

Make sure to choose MyDevices _Portal _Sequence from the Authentication technique drop-down on the Portal Settings page, as depicted in Figure 13.

After finishing up the MyDevices portal's modifications, as seen in Figure 14, it will make a native supplicant profile. Place a native supplicant profile by selecting Add > Native Supplicant Profile under Policy > Policy Components > Outcome > Client Provisioning > Resources.

As seen in Figure 15, it will configure the client provisioning policy after saving this profile. Go to Policy > Client Provisioning.

It is crucial to observe that in the graphical depiction of the case in Figure 16, as the number of interactions rises, the increase in the ratio between H_f and T_v becomes progressively crucial. This suggests that



Time	Severity Level	Attack Vector	Threat Factors	Event	Event Details	OS	Device
Jul 05 2020 00:04:39	War...	Device	OS patch level	Noncom...			[illegible]
Jul 05 2020 00:02:59	War...	Device	OS patch level	Noncom...			[illegible]
Jul 04 2020 19:08:28	Infor...	WiFi network	Captive	Detected	SSID: <unknown ssid>		[illegible]
Jul 04 2020 09:45:32	Infor...	Device	OS patch level	Compliant			[illegible]
Jul 03 2020 17:05:31	Infor...	WiFi network	Captive	Detected	SSID: <unknown ssid>		[illegible]
Jul 03 2020 17:01:54	Infor...	Application	Backup Tool	Removed	App: HeyTap Cloud		459
Jul 03 2020 17:01:53	Infor...	Application	Network Redirecti...	Removed	App: Game Space		459
Jul 03 2020 17:01:52	Infor...	Application	Network Redirecti...	Installed	App: Game Space		459
Jul 03 2020 17:01:51	Infor...	Application	Backup Tool	Installed	App: HeyTap Cloud		459
Jul 03 2020 17:01:48	Infor...	Application	Backup Tool	Installed	App: Clone Phone		459

« First Previous 1 2 3 4 5 ... Next Last » 25

Figure 7. An overview of all thread-related variables, attack vectors, and events.

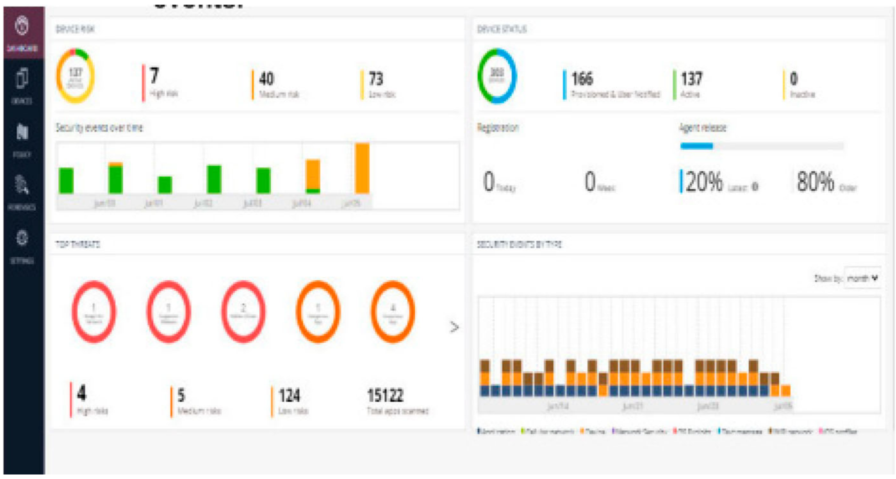
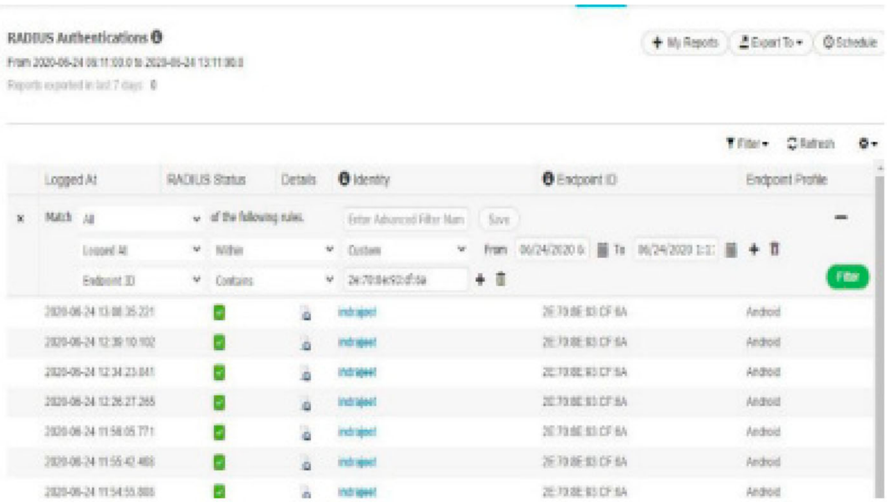


Figure 8. Security compliance dashboard.



RADIUS Authentications

From 2020-06-24 08:11:00.0 to 2020-06-24 13:11:00.0

Reports exported in last 7 days 0

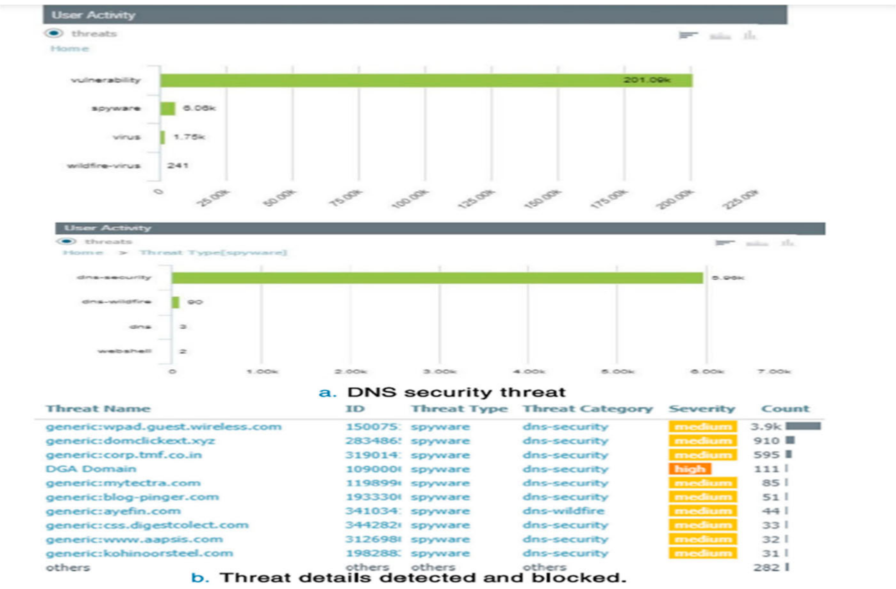
Match All of the following rules. Enter Advanced Filter Name

Logged At Within Custom From 06/24/2020 0 To 06/24/2020 1:1

Endpoint ID Contains 2e:70:8e:93:cf:8a

Logged At	RADIUS Status	Details	Identity	Endpoint ID	Endpoint Profile
2020-06-24 13:08:35.221	✓		indrajeet	2E:70:8E:83:CF:8A	Android
2020-06-24 12:39:10.102	✓		indrajeet	2E:70:8E:83:CF:8A	Android
2020-06-24 12:34:23.041	✓		indrajeet	2E:70:8E:83:CF:8A	Android
2020-06-24 12:26:27.265	✓		indrajeet	2E:70:8E:83:CF:8A	Android
2020-06-24 11:58:05.771	✓		indrajeet	2E:70:8E:83:CF:8A	Android
2020-06-24 11:55:42.485	✓		indrajeet	2E:70:8E:83:CF:8A	Android
2020-06-24 11:54:55.808	✓		indrajeet	2E:70:8E:83:CF:8A	Android

Figure 9. User recognition using the detected mac address.

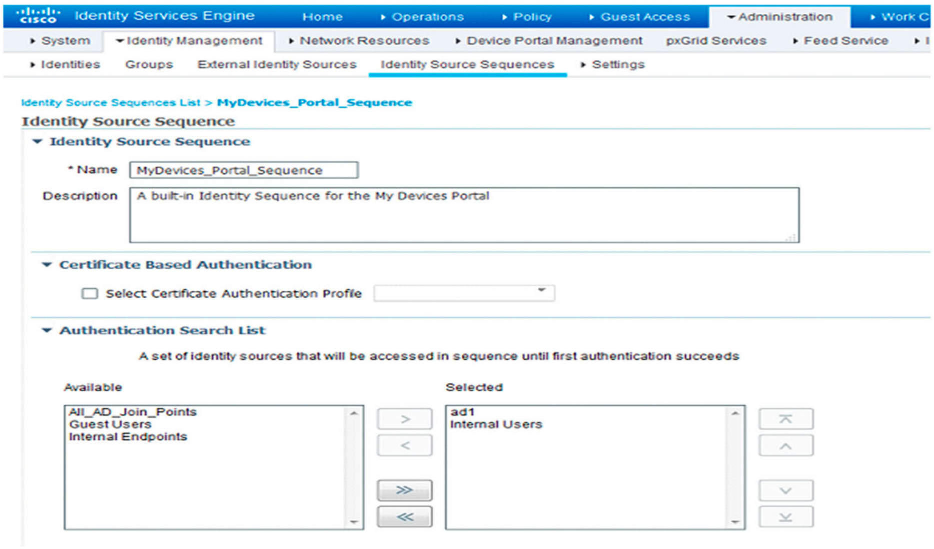


a. DNS security threat

Threat Name	ID	Threat Type	Threat Category	Severity	Count
generic:wpad.guest.wireless.com	150075:	spyware	dns-security	medium	3.9k
generic:domclickext.xyz	283486:	spyware	dns-security	medium	910
generic:corp.tmf.co.in	319014:	spyware	dns-security	medium	595
DGA Domain	109000(	spyware	dns-security	high	111
generic:mytectra.com	119899(	spyware	dns-security	medium	85
generic:blog-pinger.com	193330(	spyware	dns-security	medium	51
generic:ayefin.com	341034:	spyware	dns-wildfire	medium	44
generic:css.digestcolect.com	344282(	spyware	dns-security	medium	33
generic:www.aapsis.com	312698(	spyware	dns-security	medium	32
generic:kohinoorsteel.com	198288:	spyware	dns-security	medium	31
others	others	others	others		282

b. Threat details detected and blocked.

Figure 10. Threat landscape from Prisma.



Identity Source Sequences List > MyDevices_Portal_Sequence

Identity Source Sequence

▾ Identity Source Sequence

* Name MyDevices_Portal_Sequence

Description A built-in Identity Sequence for the My Devices Portal

▾ Certificate Based Authentication

□ Select Certificate Authentication Profile

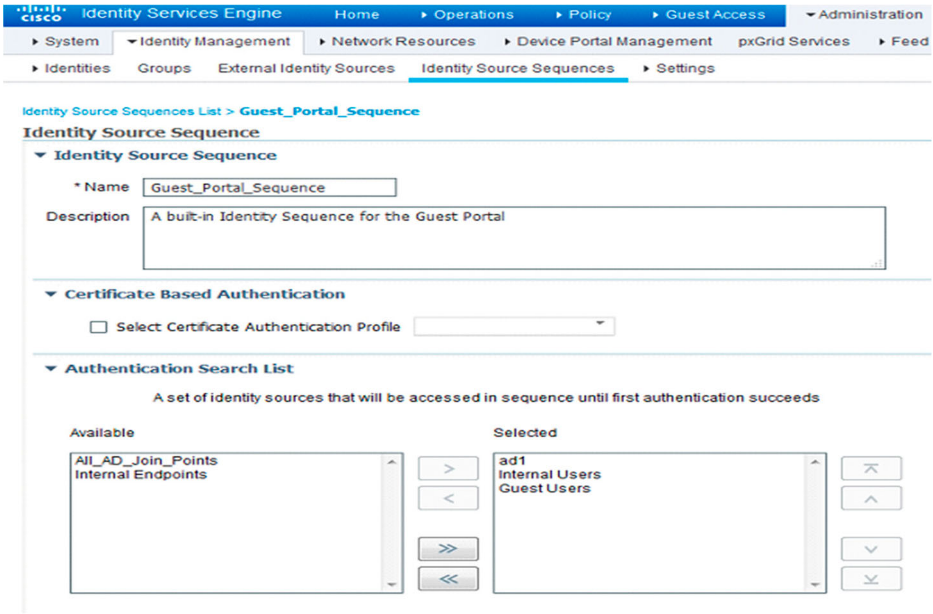
▾ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available: All_AD_Join_Points, Guest Users, Internal Endpoints

Selected: ad1, Internal Users

Figure 11. Editing the MyDevices_Portal_Sequence and the identity source sequence.



Identity Source Sequences List > Guest_Portal_Sequence

Identity Source Sequence

Identity Source Sequence

* Name: Guest_Portal_Sequence

Description: A built-in Identity Sequence for the Guest Portal

Certificate Based Authentication

□ Select Certificate Authentication Profile

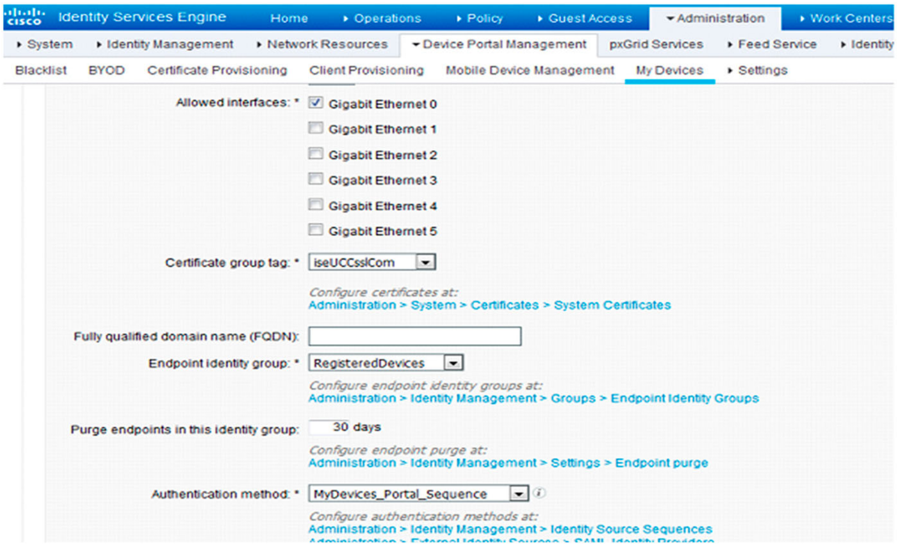
Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available:
All_AD_Join_Points
Internal Endpoints

Selected:
ad1
Internal Users
Guest Users

Figure 12. Edit the Guest_Portal_Sequence after saving this identity source sequence.



Allowed interfaces: * ☑ Gigabit Ethernet 0
□ Gigabit Ethernet 1
□ Gigabit Ethernet 2
□ Gigabit Ethernet 3
□ Gigabit Ethernet 4
□ Gigabit Ethernet 5

Certificate group tag: * iseUCCsslCom

Configure certificates at:
Administration > System > Certificates > System Certificates

Fully qualified domain name (FQDN):

Endpoint identity group: * RegisteredDevices

Configure endpoint identity groups at:
Administration > Identity Management > Groups > Endpoint Identity Groups

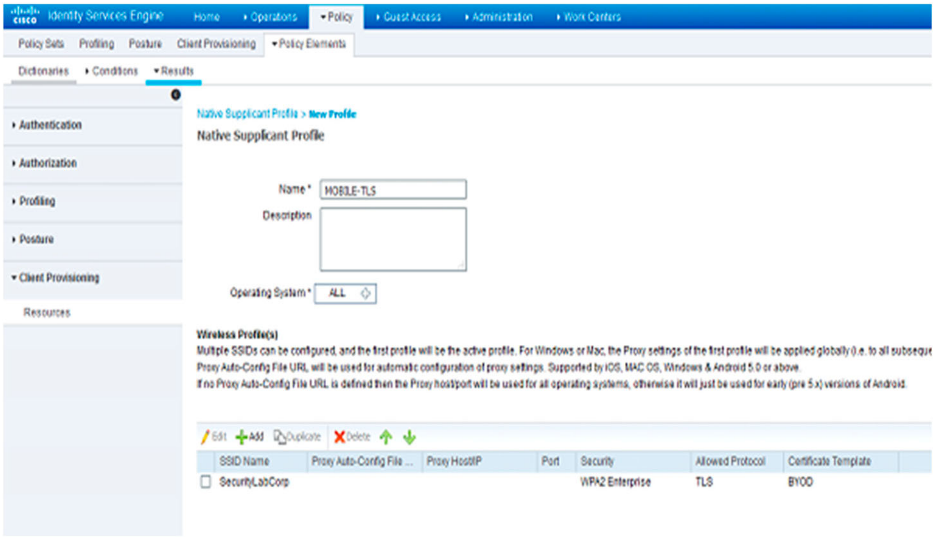
Purge endpoints in this identity group: 30 days

Configure endpoint purge at:
Administration > Identity Management > Settings > Endpoint purge

Authentication method: * MyDevices_Portal_Sequence

Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences
Administration > External Identity Sources > SAML Identity Providers

Figure 13. Selecting MyDevices_Portal_Sequence from the authentication method.



Native Supplicant Profile > New Profile

Native Supplicant Profile

Name * MOBILE-TLS

Description

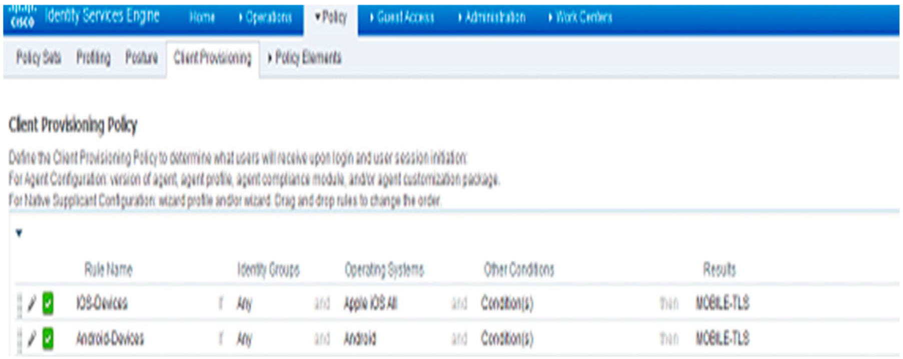
Operating System * ALL

Wireless Profile(s)

Multiple SSIDs can be configured, and the first profile will be the active profile. For Windows or Mac, the Proxy settings of the first profile will be applied globally (i.e. to all subseque
Proxy Auto-Config File URL will be used for automatic configuration of proxy settings. Supported by iOS, MAC OS, Windows & Android 5.0 or above.
If no Proxy Auto-Config File URL is defined then the Proxy host/port will be used for all operating systems, otherwise it will just be used for early (pre 5.x) versions of Android.

	SSID Name	Proxy Auto-Config File ...	Proxy Host/IP	Port	Security	Allowed Protocol	Certificate Template
□	SecurityLabCorp				WPA2 Enterprise	TLS	BYOD

Figure 14. Native supplicant profile.



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	IOS-Devices	If	Any	and	Apple iOS All	and	Condition(s)	then	MOBILE-TLS
☑	Android-Devices	If	Any	and	Android	and	Condition(s)	then	MOBILE-TLS

Figure 15. Configures the client provisioning policy.

if a node has continuously maintained a secure profile throughout time, it is highly likely that it will do so in the future, and making a security choice on this assumption will most likely lead to a positive outcome.

It relates the amount of favourable interactions to α and the amount of unfavorable interactions to$\beta; \alpha = H_f + 2,\ and\ \beta = H_u + 2$. Consequently, the predicted beta distribution value E(p) or $T_v$can be stated as follows;

$$T_v = E(p) = \frac{H_f + 2}{H_f + H_u + 3} \tag{3}$$

Where $H_f =$ Amount of favourable interactions for a particular device, $H_u =$ Amount of unfavourable interactions with the same device, and $T_v =$ the devices' level of trust.

$E(p) =$ predicted likelihood of node behaviour (favourable or unfavourable)

The interaction history of device A is shown in Table 2, with an increasing number of favourable interactions (H_f). The trust value (T_v) is calculated using Equation (3). Increase in the value of trust as the amount of interactions rises shows that trust increases with the number of favourable (secure) encounters.

The scenario is illustrated graphically in Figure 17, which explains that the steeper slope at the beginning of the curve shows how trust quickly declines when a node starts acting unfavorably.

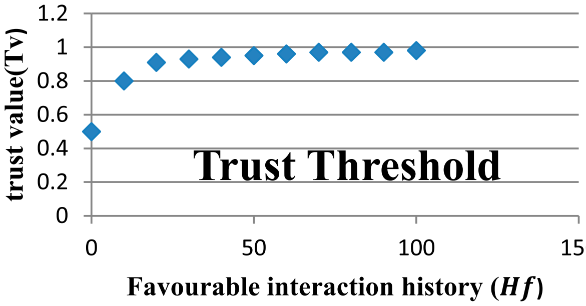


Figure 16. Effect of Favourable (secure) Interactions (H_f) on Trust Value (T_v) and access decision.

Table 2. History of interactions with device A, with increasingly favourable behaviour.

Amount of prior interactions	Amount of prior unfavourable interactions ($\boldsymbol{H_u}$)	Amount of prior favourable interactions ($\boldsymbol{H_f}$)	Computed trust value ($\boldsymbol{H_v}$)	Access Decision
20	1.6	4	0.7	Pass
30	1.6	20	0.823	Pass
40	1.6	29	0.829	Pass
50	1.6	36	0.938	Pass
60	1.6	40	0.950	Pass

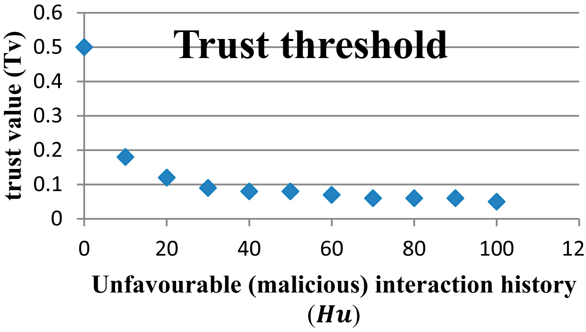


Figure 17. Effect of Unfavourable (malicious) Interactions (H_u) on Trust Value (T_v) and access decision.

Table 3. History of interactions between device B and rising unfavorable (malicious) behaviour.

Amount of prior interactions	Amount of prior unfavourable interactions ($\boldsymbol{H_u}$)	Amount of prior favourable interactions ($\boldsymbol{H_f}$)	Computed trust value ($\boldsymbol{H_v}$)	Access Decision
20	1.7	3	0.7	Pass
30	19	3	0.1655	Deny
40	29	3	0.0908	Deny
50	34	3	0.0654	Deny
60	42	3	0.0475	Deny

Table 3 displays a decrease in trust as a result of malicious node interactions in the past. To prevent these nodes from endangering the entire network, this led to access denials to the network. Trust can be lost as rapidly as it can be acquired. The trust value (T_v) in the table is also determined using equation (3).

4.4. Performance testing

To assess performance and scalability, it made use of a variety of software tools. For instance, Visual Studio 2017 includes practical tools for designing experiments that measure CPU and memory usage.

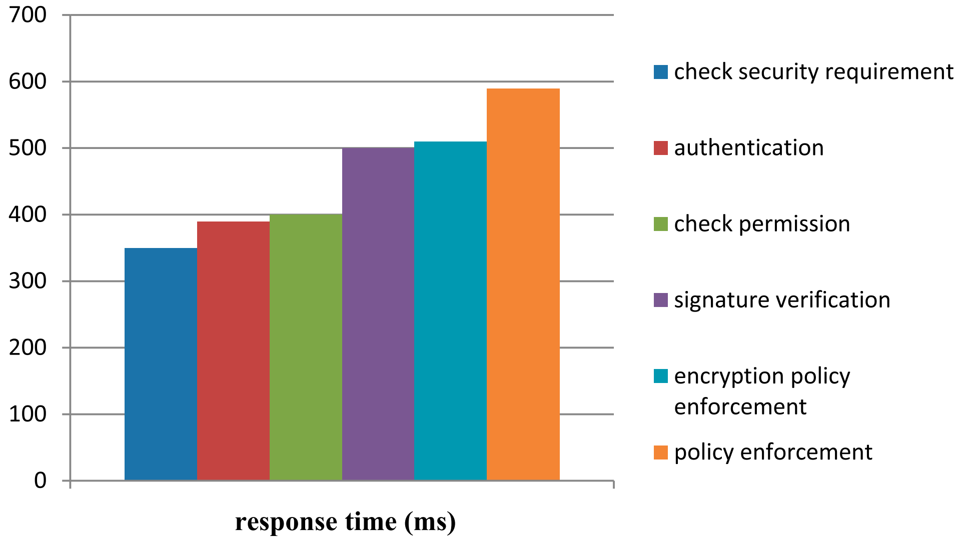


Figure 18. Response time for all functions in the suggested framework.

The response time for each function in the suggested framework is shown in Figure 18 together with the time taken to store and retrieve information from the database.

4.5. Integrity testing

After three weeks of testing, it found that the documents contained 2,850 access requests. During this time, there would be 21 policy attacks, but none of them succeeded because the system stopped them all. Understanding the likelihood that a specific type of attack will take place during a given period is crucial to assess the integrity of that attack. The integrity threat is generally recognized:

$$2 - \text{threat attack } (2 - \text{security attack equals } 2 - \text{integrity attack}) \quad (4)$$

The integrity of a software program is also determined by the total number of integrity attacks.

$$\sum \text{attack (integrity attack)} = \text{Integrity} \quad (5)$$

In this instance, the threat attack would be (21/2850) = 0.0073684, whereas the security attack would be (0/21) = 0.00. As a result, the integrity would be (1–0.0073684x (1–0.00)) = 0.9926316 $*$ 100 ≈ 100%.

5. Conclusion

Investigators offer solutions to access control problems caused by BYOD and cloud environments. They aimed to develop a technique that would preserve BYOD characteristics like better portability and flexibility. This solution was built based on four key requirements: recognizing the BYOD device security, practicing the access control policy, utilizing independent platforms, and protecting the access control policy.s To protect user privacy, they also oppose the introduction of MDM technology. The investigators performed and evaluated their suggested design under real-world conditions to create a prototype for their system. When their systems were validated and verified, the outcomes were positive. In the future, the researchers plan to increase the speed of the system by permitting access and improving the existing architecture to support federated cloud computing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

[1] Palanisamy R, Anir Norman A, Kiah MLM. BYOD policy compliance: risks and strategies in organizations. J Comput Inf Syst. 2022;62(1):61–72. doi:10.1080/08874417.2019.1703225

[2] Wani TA, Mendoza A, Gray K, et al. Status of bring-your-own-device (BYOD) security practices in Australian hospitals–A national survey. Health Policy Technol. 2022;11(3):100627.

[3] Abdulkarim S, Muhammed AI, Ahmad SK. Byod, The advancement of enterprise and mobile civilization: challenges and prevalence. J Med-Clin Res Rev. 2022;6(7):1–7. doi:10.33425/2639-944X.1281

[4] Ratchford M, El-Gayar O, Noteboom C, et al. BYOD security issues: a systematic literature review. Inf Secur J: A Global Perspect. 2022;31(3):253–273. doi:10.1080/19393555.2021.1923873

[5] Garba AB, Armarego J, Murray D, et al. Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. J Inf Privacy Secur. 2015;11(1):38–54. doi:10.1080/15536548.2015.1010985

[6] Beckett P. BYOD–popular and problematic. Netw Secur. 2014;9:7–9. doi:10.1016/S1353-4858(14)70090-X

[7] Singh MM, Chan CW, Zulkefli Z. Security and privacy risks awareness for bring your own device (BYOD) paradigm. Int J Adv Comput Sci Appl. 2017;8(2):53–62.

[8] Ali MI, Kaur S. BYOD secured solution framework. Int J Eng Adv Technol. 2019;8(6):1602–1606. doi:10.35940/ijeat.F8202.088619

[9] Muhammad M, Daniel Ani U, Aliyu Abdullahi A, et al. Device-Type Profiling for Network Access Control Systems using Clustering-Based Multivariate Gaussian Outlier Score. In The 5th International Conference on Future Networks & Distributed Systems. 2021:270–279. doi:10.1145/3508072.3508113

[10] Morrow B. BYOD security challenges: control and protect your most sensitive data. Netw Secur. 2012;12:5–8. doi:10.1016/S1353-4858(12)70111-3

[11] Jamal F, Abdullah MT, Abdullah A, et al. Enhanced bring your own device (BYOD) environment security based on blockchain technology. Int J Eng Technol. 2018;7(4.31):74–79.

[12] Eslahi M, Var Naseri M, Hashim H, et al. BYOD: Current state and security challenges. In 2014 *IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE)*, pp. 189–192. IEEE, 2014.

[13] Almarhabi K, Jambi K, Eassa F, et al. Survey on access control and management issues in cloud and BYOD environment. Int J Comput Sci Mob Comput. 2017;6(12):44–54.

[14] Costantino G, Martinelli F, Saracino A, et al. Towards enforcing on-the-fly policies in BYOD environments. In 2013 9th International Conference on Information Assurance and Security (IAS), pp. 61–65. IEEE, 2013.

[15] AlHarthy K, Shawkat W. Implement network security control solutions in BYOD environment. In 2013 IEEE International Conference on Control System, Computing and Engineering, pp. 7–11. IEEE, 2013.

[16] Shumate T, Ketel M. Bring your own device: benefits, risks and control techniques. In Ieee Southeastcon 2014, pp. 1–6. IEEE, 2014.

[17] Zahadat N, Blessner P, Blackburn T, et al. BYOD security engineering: a framework and its analysis. Comput Secur. 2015;55:81–99. doi:10.1016/j.cose.2015.06.011

[18] Ratchford MM. BYOD: a security policy evaluation model. In: Information technology-new generations. Cham: Springer; 2018. p. 215–220.

[19] Heineman GT, Councill WT. Component-based software engineering. *Putting the pieces together, addison-westley* 5 (2001).