FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 277-285 | e-ISSN: 2347-470X

# An Evaluation of the Proposed Security Access Control for BYOD Devices with Mobile Device Management (MDM)

**Jimshith V.T[1] and Mary Amala Bai V[2]**

[1]*Research Scholar, Department of Computer Information Technology, Noorul Islam University, Thackalay, Tamil Nadu, India; jimshith345vt@outlook.com*
[2]*Associate Professor, Department of Computer Information Technology, Noorul Islam University, Thackalay, Tamil Nadu, India; marybmalabai852v@gmail.com*

***Correspondence:** Jimshith V.T.; jimshith345vt@outlook.com

**ABSTRACT-** Bring Your Own Device (BYOD) at Work is a growing practice that has significantly increased network security vulnerabilities. This development has tremendous implications for both businesses and individuals in every organization. As a result of the extensive spreading of viruses, spyware, and other problematic downloads onto personal devices, the government has been forced to examine its data protection legislation. Dangerous apps are downloaded into personal devices without the user's awareness. As a result, both people and governments may suffer disastrous repercussions. In this research, proposed BYODs are troublesome since they can change policies without consent and expose private information. This type of privacy violation has a domino effect, resulting in substantial legal and financial consequences as well as decreased productivity for enterprises and governments. Governments have a daunting problem since they must protect networks from these threats while simultaneously considering user rights and privacy legislation. The framework of this paper that decreases the number of system limits and access control methods that are established for BYODs and cloud environments has been presented by the researchers of the study. They also attempted to protect user privacy by implementing Mobile Device Management (MDM) technology. The study's preliminary findings were optimistic, implying that the framework might reduce access control difficulties.

**Keywords:** BYOD, Cloud environment, Data security, Malicious programs, Network security.

**ARTICLE INFORMATION**

**Author(s)**: Jimshith V.T1 and Mary Amala Bai V.;
**Received**: 02/01/2024; **Accepted**: 08/02/2024; **Published**: 28/03/2024;
**e-ISSN**: 2347-470X;
**Paper Id**: IJEER 0201-01;
**Citation:** 10.37391/IJEER.120138
**Webpage-link**:
https://ijeer.forexjournal.co.in/archive/volume-12/ijeer-120138.html

**Publisher's Note:** FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

## 1. INTRODUCTION

BYOD is the practise of allowing employees in a company or institution to use their own devices or equipment to finish their work. It was expected that 5.22 billion people utilise mobile devices for work-related tasks, and that there will be roughly 6.3 billion smartphone users worldwide in 2021. Smartphone users are constantly increasing every year dominant device to access internet resources. Approximately 87% of businesses rely on their employees to use their own devices for work-related tasks, as per the current BYOD trend. [1-2] The following gadgets are covered by BYOD: audio players, e-book readers, tablet computers, smartphones/handhelds, laptops, and netbooks. Two-thirds of the respondents said they used a smartphone for work, indicating the growing use of smartphones as work tools [3-4].

BYOD also improves employee satisfaction, productivity, and flexibility. Although the BYOD trend promises many advantages, it also introduces a number of security risks that can damage an organization's reputation in addition to its revenue, such as device loss, data contamination, and data leakage. One in five businesses (21%) experienced a mobile device security breach as a result of connecting to rogue Wi-Fi hotspots and malware [5]. Attackers may gain access to a stolen or lost device or use phishing or malware to infect the device of a working employee [6-8].

Malware frequently most of the time, users are not aware that their smartphone has been compromised. One effective way to prevent employees from accessing illegal software while connected to business networks is to implement containerization, which allows employees to utilise their personal devices without any restrictions [9].

Because of BYOD, private information can be accessed and viewed on devices that are not under an organization's control. Therefore, it is essential to encrypt data both moving and stationary. Encryption allows you to protect important file content even in the worst case of device loss or hacking. Actually, encrypting every piece of data that is transferred to employee devices can be challenging. Security and operations teams need to take into account any scenario when a user downloads or saves a file locally, including opening emails with attachments and retrieving files from company cloud storage. In each of these scenarios, the BYOD device's software must ensure that the data is secured. Furthermore, if the encryption procedure fails, users may not have access to crucial files that they require to perform their duties [10–12].

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 277-285 | e-ISSN: 2347-470X

***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.
• NAC is a networking solution composed of a collection of protocols that develop and implement a policy for securing users' first access to network services.
• 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.
The following are the contributions made by this review paper:
• Enforcing user access regulations and limiting access to authorised users.
• MDM increases the security of an organization's corporate data by encrypting it and preventing unauthorized access.
• By combining Network Access Control with Mobile Device Management, the provision of policies and endpoint device authentication in a BYOD network creates a framework for network monitoring and configuration setting control of mobile devices.

This review is organised as follows for the remainder of it. The need for study is highlighted by the presentation of earlier studies on BYOD security in the following section. The security provisioning mechanism for BYOD devices is then discussed. The results are then reported, and the suggested methodology is then discussed. Finally, we wrap up the article by discussing the implications for future research.

## 2. LITERATURE REVIEW

The increasing use of mobile devices for personal and work-related tasks has driven many organizations to implement BYOD programs to facilitate remote work and increase employee productivity. (Palanisamy et al., 2022) [13]. In 2021, Abisheka, PA C., et al. presented a comprehensive solution for detecting and preventing unauthorised access to organisational records named "BYODENCE". The primary security concern for businesses using BYOD is data loss. A blockchain with more security measures, according to F. Jamal et al. (2021), will aid in the detection of data leakage incidents [14–15].

A "Comparative examination of risk evaluation models for risk-aware access control your own device environment" was put out by Ganiyu et al. (2018). In 2016, V. R. Kebande and colleagues presented a BYOD concept based on honeypot technology. Consequently, this research has proposed a substantial security model with DFR capacity. The model attempts to collect, encrypt, and digitally preserve prospective digital evidence (PDE) based on the DFR methodologies and concepts [16–17]. A good solution should respect the users' privacy and rights while also adhering to the organization's security requirements. The major goal of BYOD would be defeated if the solution limited or restricted user access. [18–19].

Implementing strong access control measures is crucial to ensuring a company that embraces BYOD's security [20]. These technological and access control regulations ought to be enforced, according to the corporation [21–22]. To lower threats to users and their devices, an efficient solution needs to work with the authorised BYOD's Windows versions [23–25]. Implement Access Control Guidelines The technical policy of the organisation that needs to be adhered to is referred to as this enforcement. This policy specifies how BYOD devices must adhere to Platform Independence's minimal security criteria. All BYOD operating systems should be compatible with the suggested solution's implementation. These devices' hazards will be decreased with the aid of this remedy. Policy for Secure Access Control Without protection, developing new approaches is pointless. All of the earlier research, we believe, only addressed a specific problem and did not offer a comprehensive solution to access control difficulties, based on the literature study. Therefore, more research is necessary as these solutions are still insufficient.

## 3. PROPOSED METHOD

The three primary architectures for cloud services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The available study suggests a new SaaS-based security manager product. With the help of this framework, an organization's cloud managers can before allow BYOD access to the cloud, do security checks.

The framework makes use of component-based software for a variety of purposes. Comparatively to creating a new component, reusing the existing one took less time. Therefore, using the software engineering process based on components would facilitate the rapid development of the system. By lowering software development costs and boosting software productivity, the competitiveness can be raised. This enables the reuse of current solutions rather than their development. In a setting where the software is being used, the system simulates the actual software. It provides a precise image of the current system before any changes or developments are made.

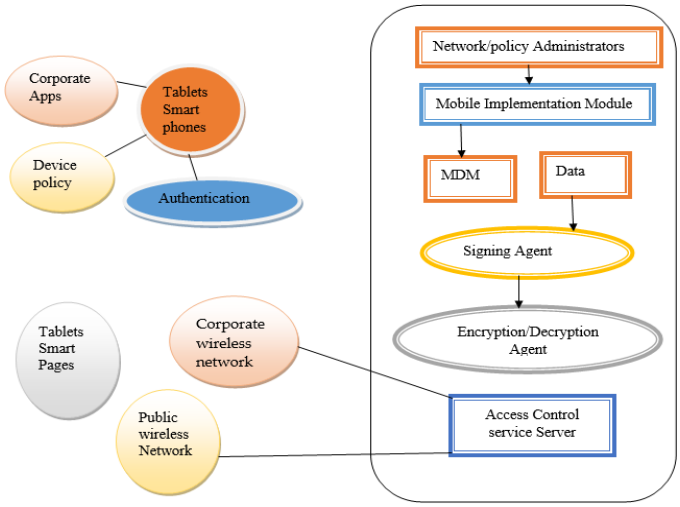


**Figure 1.** The Proposed Model for Network/Policy administrator in BYOD Security Environment.

*Table 1* shows the suggested protective paradigm with earlier methodologies it created model is a multi-component system

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 277-285 | e-ISSN: 2347-470X

that employs gateways to connect various brokers to enable software to operate independently for a network user. Owner device is the initial module in the framework. This proposed module is shown in the *figure 1* above. The placement of each software component within the framework is described in the article.

## 3.1. Network/Policy administrator

The BYOD login access management policy is implemented by the person in charge of the policy mechanism. Potential candidates may be the company's founder, the administrator of policies, or the chief security officer (CSO).

## 3.2. Mobile Policy Implementation module

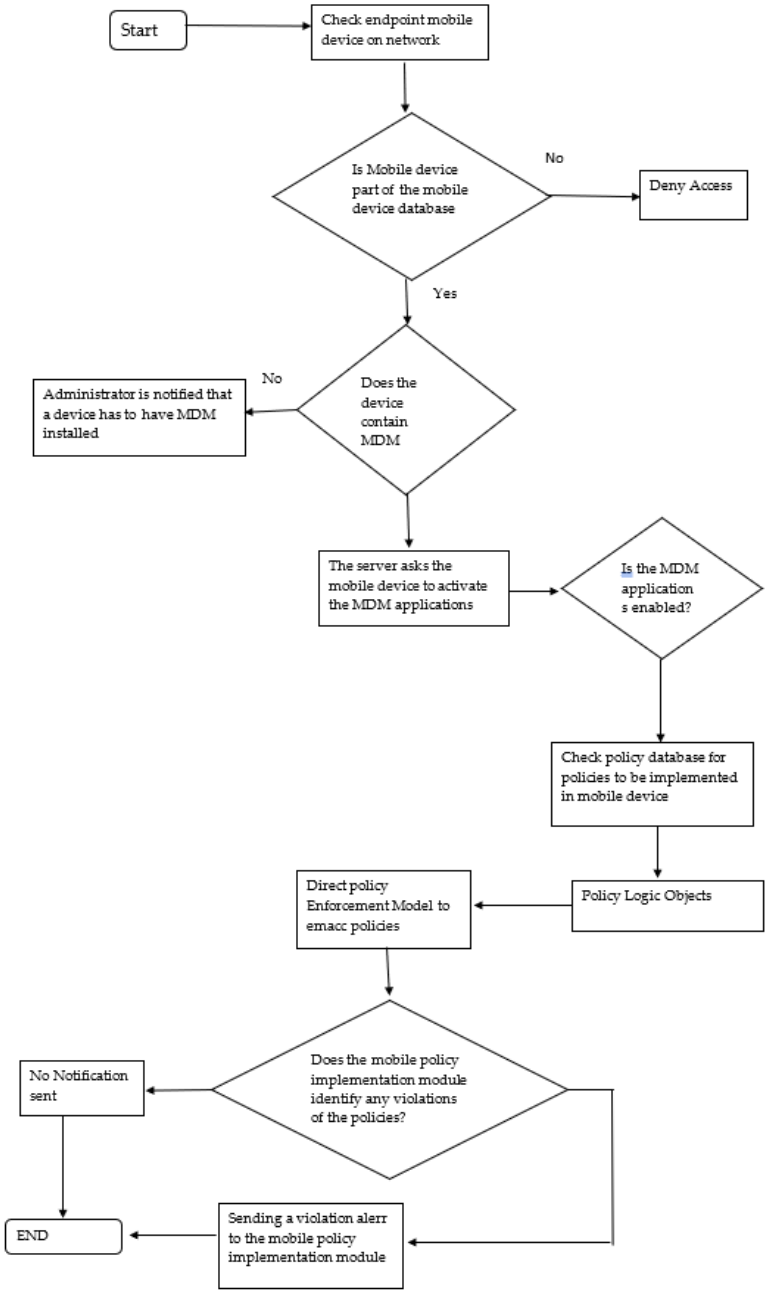


**Figure 2.** Mobile Policy Implementation Flowchart

The MDM server's mobile devices that are connected to it are subject to the normal mobile policies that are put into effect by the network/policy administrator. The module's main goal is to ensure that each policy is correctly applied to every end device that the NAC server has successfully verified according to its function. The module's main objective is to determine whether a user is disobeying any compliance checks made by devices that have been enabled, put into practise and kept in the Policy Database *(See Figure 2).*

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 277-285 | e-ISSN: 2347-470X

The module is in charge of making sure that each authenticated end device strictly abides by the established mobile regulations. This will act as the HTML-based interface that the MDM server installs. Accessing it will be easier for the MDM server administrator as a result. The module will be in charge of sending notifications, direct commands, and authorization policies to other devices in addition to managing client provisioning policies.

**Table 1. Shows the suggested protective paradigm with earlier methodologies**

| Previous Methods | Security Checks for BYOD Devices | Apply Access Control policies | Platform Independence | Access Control Security Procedures |
|---|---|---|---|---|
| RAC using on-the-fly instantiated policies | Partly | Yes | | |
| MAC using spear phishing | | Yes | | Partly |
| 2-Tier Access Control | Partly | Yes | Yes | |
| Our Proposed framework | Yes | Yes | Yes | Yes |

## 3.3. Access Policies

The alternative logical access control model known as "Attribute-Based Access Control" (ABAC) governs object accessibility following an assessment of the rules defining the attributes of certain entities (i.e., subject areas and items), their choices, and the environment relevant to the request. The essential core competences that are employed for evaluating the natural circumstances and features, upholding the legislation, and highlighting the connections between the properties and environmental conditions form the cornerstone of ABAC solutions.

## 3.4. MDM

Businesses can impose strict mobile device regulations thanks to a multifunctional framework known as mobile device management (MDM). A core component of MDM systems is situated on the network of the organisation, manages protocols, provides continuous supervision and control, and communicates and authenticates with MDM agents installed on mobile devices via certificate exchange.

## 3.5. Digital Certificate

The easiest way to secure your company's data online is with digital certificates. You're internal and external communications are encrypted by digital certificates to keep hackers and phishers from stealing sensitive data. The foundation for device authentication is a digital certificate. In contrast to user certificates, passwords are inherently vulnerable to phishing attempts. It provides a hybrid authentication system in which a client's request for authentication is validated using both an attribute certificate and a general certificate. This makes it possible to put in place access control in conjunction with a multi-tiered chain of certificates *(see Figure 3).*

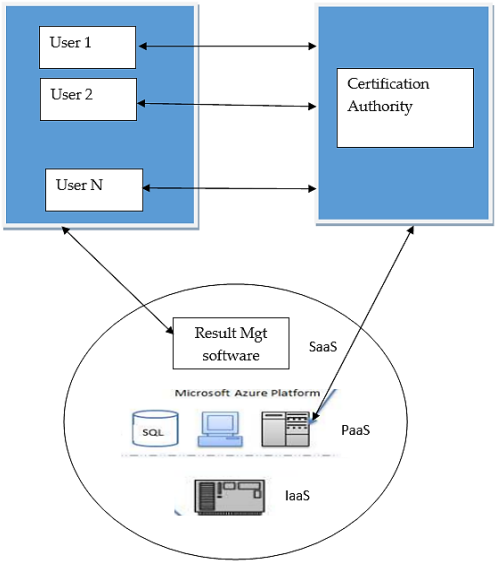


**Figure 3.** Certificate authorization in the cloud platform

Prior to delivering a message across a communication channel, a message sender first obtains an encrypted copy of the message. A hash function must be used to create a hash of the original message in order to accomplish this. In a traditional digital certificate system, the message sender first acquires an encrypted copy of the message before sending it via a communication channel. Only passing the original message through a hash function will provide a hash of the message, which is the only way to achieve this. The hash generated with the sender's private key is sent along with their digital certificate *(see Figure 4).*

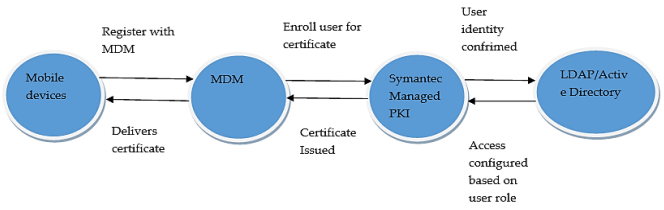


**Figure 4.** Verification of user with certificate authority

When a message is received, the recipient first verifies that the certificate that came with it is legitimate. If it is, the recipient then compares the encrypted message to the hash that was sent to him to determine whether the message has been altered.

## 3.6. Encryption/Decryption Agent

The RSA algorithm is used in both digital signatures and public key encryption. This is the most widely used public key encryption algorithm. The RSA algorithm's security rests on the mathematical impossibility of factoring sufficiently big

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 277-285 | e-ISSN: 2347-470X

integers. If the keys for an RSA algorithm have a length of at least 1024 bits, it is thought to be secure *(see Figure 5).*

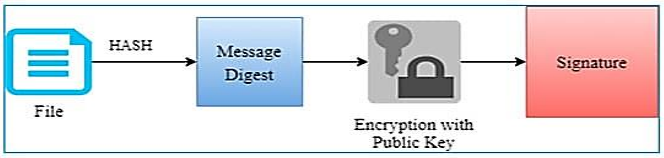


**Figure 5.** Work model of RSA with the Digital Signature technique

The sender performs the following actions in order to sign a message:

1. generates a message's hash value.
2. generates the signature using his or her private key $(n, d)$

$S = Md \bmod n$ (1)

3. Delivers the recipient's signature S.

The recipient follows these steps to confirm the message:

1. Computes the hash value using the sender's public key $(n, e)$

$V = Se \bmod n$ (2)

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

### 3.6.1. Key Generation Algorithm

1. Create two enormous arbitrary constants, $p$ and $q$, that are almost equally large so that their sum, $n = pq$, has the necessary bit length.
2. Integrate$n = pq$ and $\varphi = (p-1)(q-1)$.
3. Pick an integer $e, 1 < e < \varphi$, such that $gcd(e, \varphi) = 1$.
4. Calculate the hidden modulus $d, 1 < d < \varphi$, such that $ed \equiv 1 \ (mod \ \varphi)$. ].
5. The public key is $(n, e)$ and the private key $(d, p, q)$. Keep all the values $d, p, q$ and $\varphi$secret. Were,
   a) n is known as the modulus.
   b) e is known as the public exponent or encryption exponent or just the exponent.
   c) d is known as the hidden modulus or decryption exponent.

### 3.6.2. Encryption

1. Secures the public key of the recipient B$(n, e)$.
2. Uses the positive integer $m, 1 < m < n$ to represent the plaintext message. $c = me \bmod n$ is used to calculate the ciphertext.
3. Sends the cipher text $c$ to $B$

### 3.6.3. Decryption

1. Computes $m = cd$ mod n using his private key $(n, d)$.
2. From the message representative m, extracts the plaintext.

## 4. EXPERIMENTAL RESULTS

To confirm and validate the solution, the proposed framework must be put into use and tested. It is necessary to make sure that the system is fault-, error-, or failure-free. The owner/network module is present in the implemented prototype. By validating a few of the criteria employed in our suggested framework, the validation was successfully accomplished.

### 4.1. Mobile Policy Implementation Module

This session's experiment focuses on configuring BYOD devices' MDM settings. The study makes an effort to set up the mobile policies and guarantee their correct application both when the network is connected and unplugged.


**Figure 6.** Policy Enforcement Interface

The Mobile Policy Implementation modules use the Device Administration API, which is where the policies are located in the library in *figure 6.* The administrator's selections are subsequently followed when configuring and applying the policies in the Android Virtual Device Manager. This specifically covers security requirements.

The project is an attempt to collect the device's MAC address and IP address upon connecting to the network for security and device tracking purposes. The BYOD device's log-in page, which requests the user's log-in credentials as shown in *figure 7,* is depicted in the first frame. Android device login interface is shown in *figure 8.*

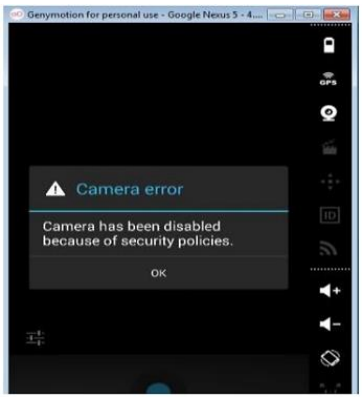


**Figure 7.** Disable camera policy enforcement

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 277-285 | e-ISSN: 2347-470X

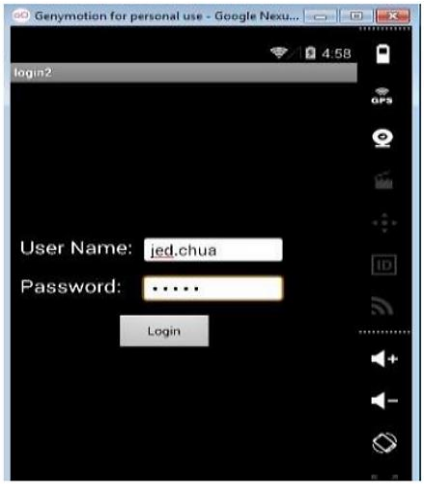


**Figure 8.** Android device login interface

Following a successful login, the phone's IP address and mac address are stored in the database under the user logs table. The account id field in the user logs table serves as a foreign key to the account id in the user accounts database since it is possible for two devices to be logged into the same account yet have different addresses. The experiment used the jed.chua account to log onto the device because it already existed in the database. The IP address and the mac address were successfully stored in the database *(see Figure 9).*


**Figure 9.** Android device database interface

## 4.2. Authentication using Digital Certificate

The application used in this work is a cloud-based result security system that utilises digital certificates for client and server authentication. Access to the site is secured using SSL, which is a crucial method for website security in the modern era.

When selecting a PKI to provide these essential characteristics, organisations must make a decision regarding whether to run PKI software in-house or to contract out PKI services to a trustworthy vendor. It should be noted that in order to enable the PKI deployment for mobile device management, all internal projects—regardless of whether an MDM is used—will require specialised modifications *(see Figure 10).*

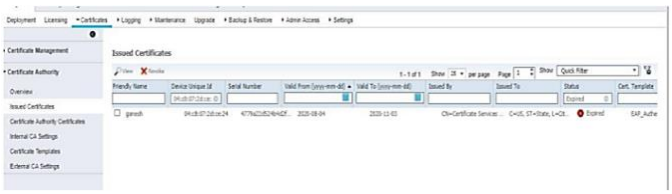

**Figure 10.** Interface showing Issue of digital certificate with expiry date

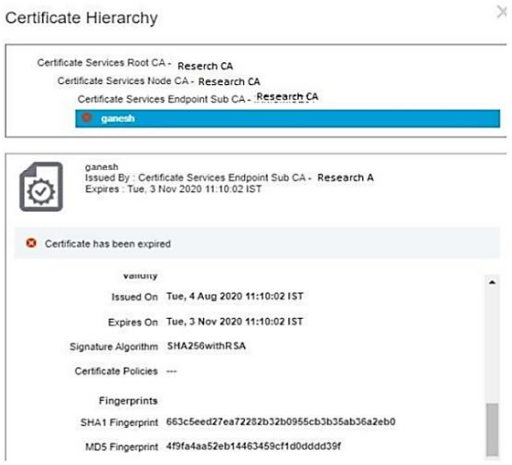


**Figure 11.** BYOD certificate expiry information

They tested the control policy's 20 accesses using various features. Five of them included the original cypher text, five contained the altered cypher text, and five contained erroneous digital signatures. The encryption and decryption agents, as shown in *figure 11*, discovered every altered access control rule, as did the signature verification agent. The number of policies that the Mobile Device Management has saved, accepted, refused, and uploaded is shown in *figure 12*.

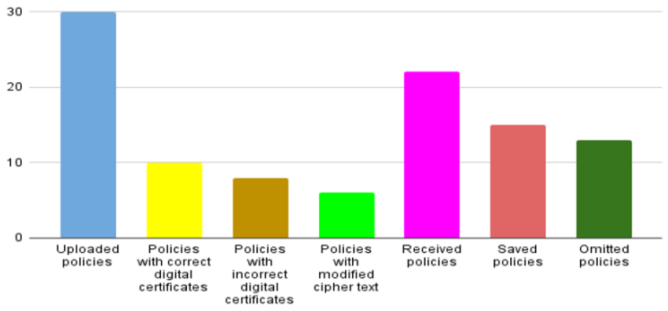


**Figure 12.** Statistics depicts the quantity of policies that were saved, rejected, and received

*Figure 13* displays a graphical representation of a device interaction together with the number of prior interactions, positive interactions, and the computed trusted value.

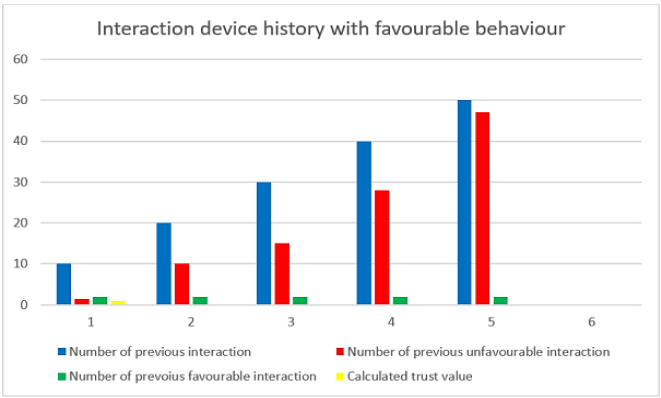


**Figure 13.** Graph showing interaction of device with favourable behaviour

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 277-285 | e-ISSN: 2347-470X

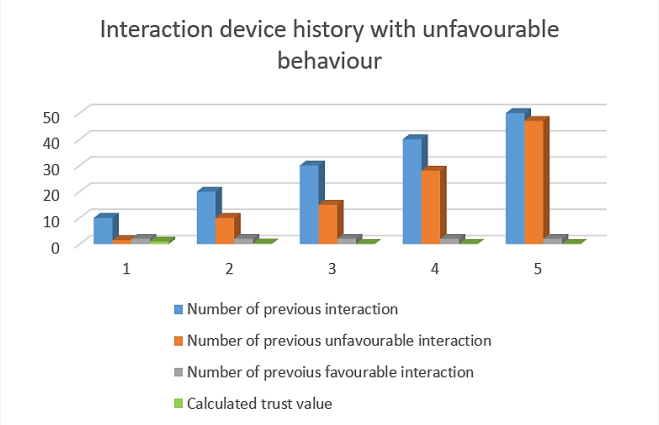


**Figure 14.** Graph showing interaction of device with unfavourable behaviour

*Figure 14* shows the graphical interaction of device with number of previous interactions, unfavourable interaction and calculated trusted value.

**Table 2. Device interaction history with favourable behaviour**

| Number of prior interactions | Number of unfavourable interactions in the past ($H_u$) | Numerous prior positive interactions($H_f$) | Determined trust value ($T_v$) | Access Decision |
|---|---|---|---|---|
| 10 | 1.5 | 2 | 1 | Pass |
| 20 | 1.5 | 10 | 0.575 | Pass |
| 30 | 1.5 | 21 | 0.704 | Pass |
| 40 | 1.5 | 32 | 0.879 | Pass |
| 50 | 1.5 | 43 | 0.929 | Pass |

*Table 2* displays a trust value resulting from prior node interactions. This ultimately led to a network access decision. The trust value is also determined using *equation (3).*

**Table 3. Device's past interactions with undesirable behaviour**

| Number of prior interaction | Number of previous unfavourable interaction in the past($H_u$) | Numerous prior positive interactions($H_f$) | Determined trust value($T_v$) | Access Decision |
|---|---|---|---|---|
| 10 | 1.5 | 2 | 1 | Pass |
| 20 | 10 | 2 | 0.1943 | Deny |
| 30 | 15 | 2 | 0.0603 | Deny |
| 40 | 28 | 2 | 0.0584 | Deny |
| 50 | 47 | 2 | 0.0437 | Deny |

*Table 3* displays a decrease in confidence as a result of malicious node interactions in the past. The network consequently experienced access denials as a result of this. The trust value is also determined using *equation (3).*

## 5. PERFORMANCE TESTING

To assess performance and scalability, we 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. The JMeter tool was another piece of software we tested for scalability using. Since JMeter is an open-source programme, it is simple to use. The load, memory use, and traffic were also measured using the Google cloud platform. The outcomes of the numerous tests we ran are listed here, along with explanations for each test's specific results.

Following the authentication procedure and policy configuration, the following test displays the time response for access permitted and access denied, as shown in *figure 15* it permitted and access refused services as response time.

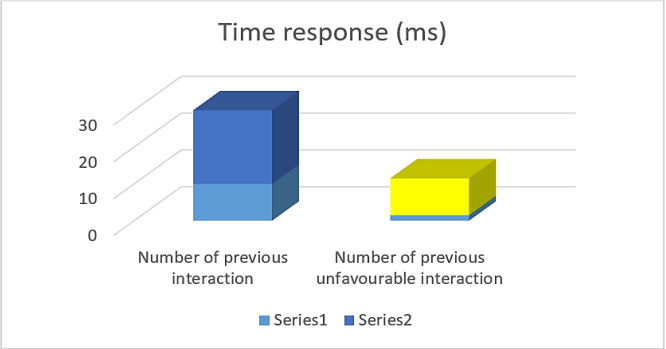


**Figure 15.** Time response for allowed and denied access

## 6. DISCUSSION AND EVALUATION

The system was tested for defects, mistakes, and faults using both white and black boxes to validate and verify it. The test findings are highlighted in this case. The proposed system could first tell apart between known and unknown operators and gadgets. Untrusted devices cannot connect to the cloud, and untrusted operators cannot use the system thanks to the framework. Secondly, the proposed architecture identified attacks related to access control rules at the storage, processing, and transfer stages. This prohibited using the updated measures after getting in touch with the system owner.

Finally, when the overall number of users climbed during a significant increase in response time, according to conventional analysis, for the execution that managed the local device's access. Scalability of the system is examined in one of these performance evaluations. This study has shown the effects of employing BYOD to enhance acceptance of technology and productivity in various industries. You will be able to complete a variety of jobs competently, successfully, and discreetly if you take use of the advantages of the digitalization and have access to the cloud's data.

## 7. CONCLUSIONS

The researchers in this paper have put up a strategy to deal with the problems with access control that BYODs and cloud environments provide. They set out to develop a technique for maintaining the more adaptable and mobile BYOD features. This solution was built around four primary requirements: assessing the security of BYOD devices, putting the access control mechanism in place, using distinct systems, and protecting the authentication scheme. The researchers developed a component-based computer programming paradigm that was scalable, economical, successful, and easy to maintain while taking these needs into mind. After the implementation of the policy, they have also made an effort to

International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 277-285 | e-ISSN: 2347-470X

improve the system's mobility and adaptability while lowering the number of constraints. They also made an effort to safeguard user privacy by putting Mobile Device Management (MDM) technologies in place. The scientists have created that the very first working model of their platform by putting their suggested architecture into practise and testing it there. Their systems' validation and verification produced encouraging findings and favourable comments. The experts aim to enhance the efficiency of its system by making it accessible and growing the current system so that it can support the federated cloud computing system in the future.

**Acknowledgments:** The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

**Author Contributions:** The following statements should be used "Conceptualization, Jimshith V.T and Mary Amala Bai V; methodology, Jimshith V.T; software, Mary Amala Bai V; validation, Jimshith V.T and Mary Amala Bai V; formal analysis, Jimshith V.T; investigation, Mary Amala Bai V; resources, Jimshith V.T; data curation, Mary Amala Bai V; writing—original draft preparation, Jimshith V.T; writing—review and editing, Mary Amala Bai V; visualization, Jimshith V.T; supervision, Mary Amala Bai V; project administration, Jimshith V.T; funding acquisition, Mary Amala Bai V All.

**Conflicts of Interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## REFERENCES

[1] García-Teodoro, P.; Camacho, J.; Maciá-Fernández, G.; Gómez-Hernández, J. A.; López-Marín, V. J. A novel zero-trust network access control scheme based on the security profile of devices and users. Computer Networks 2022, Volume 212, pp. 109068.

[2] Palanisamy, R.; Norman, A. A.; Mat Kiah, M. L. BYOD policy compliance: Risks and strategies in organizations. Journal of Computer Information Systems 2022, Volume 62, No 1, pp. 61-72.

[3] Wani, T. A.; Mendoza, A.; Gray, K.; Smolenaers, F. Status of bring-your-own-device (BYOD) security practices in Australian hospitals–a national survey. Health Policy and Technology 2022, Volume 11, No 3, pp. 100627.

[4] White, B. The Influence of BYOD Security Risk on SME Information Security Effectiveness (Doctoral dissertation, Capella University), 2022.

[5] Alothman, R. B.; Saada, I. I.; Al-Brge, B. S. B. A Performance-Based Comparative Encryption and Decryption Technique for Image and Video for Mobile Computing. Journal of Cases on Information Technology (JCIT) 2022, Volume 24, No 2, pp. 1-18.

[6] Ratchford, M.; El-Gayar, O.; Noteboom, C.; Wang, Y. BYOD security issues: A systematic literature review. Information Security Journal: A Global Perspective 2022, Volume 31, No 3, pp. 253-273.

[7] Ratchford, M.; El-Gayar, O.; Noteboom, C.; Wang, Y. BYOD security issues: A systematic literature review. Information Security Journal: A Global Perspective 2022, Volume 31, No 3, pp. 253-273.

[8] Abisheka, P. C.; Azra, M. F.; Poobalan, A. V.; Wijekoon, J.; Yapa, K.; Murthaja, M. An Automated Solution for Securing Confidential Documents in a BYOD Environment. In 2021 3rd International Conference on Advancements in Computing (ICAC). IEEE, 2021, pp. 61-66.

[9] AL-HARTHY, I. M.; ALI, N. A. DETERMINANTS OF BYOD PROTECTION BEHAVIOR: AN EMPLOYEE'S PERSPECTIVE. Journal of Theoretical and Applied Information Technology 2022, Volume 100, No 13.

[10] Ali, M. I.; Kaur, S. BYOD secured solution framework. Int. J. Eng. Adv. Technol. 2019, Volume 8, No 6, pp. 1602-1606.

[11] Ali, M. I.; Kaur, S. BYOD cyber threat detection and protection model. In 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) 2021, pp. 211-218. IEEE.

[12] Jamal, F.; Abdullah, M. T.; Abdullah, A.; Hanapi, Z. M. Enhanced bring your own device (BYOD) environment security based on blockchain technology. International Journal of Engineering & Technology 2018, Volume 7, No 4.31, pp. 74-79.

[13] Ganiyu, S. O.; Jimoh, R. G. Comparative analysis of risk evaluation models for risk-aware access control in bring your own device environment, 2018.

[14] Ratchford, M. M. BYOD: a security policy evaluation model. In Information Technology-New Generations: 14th International Conference on Information Technology 2018, pp. 215-220. Springer International Publishing.

[15] Zhang, D.; Han, X.; Deng, C. Review on the research and practice of deep learning and reinforcement learning in smart grids. CSEE Journal of Power and Energy Systems 2018, Volume 4, No 3, pp. 362-370.

[16] Akeju, O.; Butakov, S.; Aghili, S. Main factors and good practices for managing BYOD and IoT risks in a K-12 environment. International Journal of Internet of Things and Cyber-Assurance 2018, Volume 1, No 1, pp. 22-39.

[17] Almarhabi, K.; Jambi, K.; Eassa, F.; Batarfi, O. A Proposed Framework for Access Control in the Cloud and BYOD Environment. IJCSNS Int. J. Comput. Sci. Netw. Secur 2018, Volume 18, No 2, pp. 144-152.

[18] Kebande, V. R.; Karie, N. M.; Venter, H. S. A generic Digital Forensic Readiness model for BYOD using honeypot technology. In 2016 IST-Africa Week Conference 2016, pp. 1-12. IEEE.

[19] Raj, U. Certificate based hybrid authentication for bring your own device (BYOD) in Wi-Fi enabled environment. International Journal of Computer Science and Information Security (IJCSIS) 2015, Volume 13, No 12.

[20] Singh, M. M.; Siang, S. S.; San, O. Y.; Hashimah, N.; Malim, A. H.; Shariff, A. R. M. Security attacks taxonomy on bring your own devices (BYOD) model. International Journal of Mobile Network Communications & Telematics (IJMNCT) 2014, Volume 4, pp. 1-17.

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

[22] Ghosh, A.; Gajar, P. K.; Rai, S. Bring your own device (BYOD): Security risks and mitigating strategies. Journal of Global Research in Computer Science 2013, Volume 4, No 4, pp. 62-70.

[23] Ali, M. I.; Kaur, S.; Khamparia, A.; Gupta, D.; Kumar, S.; Khanna, A.; Al-Turjman, F. Security challenges and cyber forensic ecosystem in IOT driven BYOD environment. IEEE Access 2020, Volume 8, pp. 172770-172782.

[24] Singh, M. M.; Siang, S. S.; San, O. Y.; Hashimah, N.; Malim, A. H.; Shariff, A. R. M. Security attacks taxonomy on bring your own devices (BYOD) model. International Journal of Mobile Network Communications & Telematics (IJMNCT) 2014, Volume 4, pp. 1-17.

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 277-285 | e-ISSN: 2347-470X

[25] Raj, U. Certificate based hybrid authentication for bring your own device (BYOD) in Wi-Fi enabled environment. International Journal of Computer Science and Information Security (IJCSIS) 2015, Volume 13, No 12.