

An efficient security analysis of bring your own device

Pullagura Soubhagyalakshmi¹, Kalli Satyanarayan Reddy²

¹Department of Computer Science Engineering, VTU-RR, Belagavi, India

²HOD of Information Science Engineering, Cambridge Institute of Technology, Bangalore, India

Article Info

Article history:

Received Jun 5, 2021

Revised Dec 28, 2021

Accepted Jan 27, 2022

Keywords:

Bring your own device

Mobile device management

Security policy

Software-defined networking

ABSTRACT

The significant enhancement in demand for bring your own device (BYOD) mechanism in several organizations has sought the attention of several researchers in recent years. However, the utilization of BYOD comes with a high risk of losing crucial information due to lesser organizational control on employee-owned devices. The purpose of this article is to review and analyze the various security threats in BYOD; further we review the existing work that was developed in order to reduce the risks present in BYOD. A detailed review is presented to detect BYOD security threats and their respective security policies. A phase-by-phase mitigation strategy is developed based on the components and crucial elements identified using review policy. Managerial-level, social-level and technical level issues are identified such as illegal access, leaking delicate company data, lower flexibility, corporate data breaching, and employee privacy. It is analyzed that collaboration of people, security policy factors and technology in an effective manner can mitigate security threats present in the BYOD mechanism. This article initiates a move towards filling the security gap present in the BYOD mechanism. This article can be utilized for providing guidelines in various organizations. Ultimately, successful implementation of BYOD depends upon the balance created between usability and security.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Pullagura Soubhagyalakshmi

Department of Computer Science Engineering, Research Scholar, VTU-RR

Belagavi, India

Email: slakshmi.p@gmail.com

1. INTRODUCTION

In last decade we have seen revolution in personal device, especially in number of smartphone, tablets and laptops; moreover, the number of users has increased enormously; these smartphones and tablets work with high-speed internet. The high-tech functionalities of these smartphones and tablets have motivated many organizations to utilize these smart devices in their workspace [1], [2]. The high utilization of these smartphones is mainly due to two reasons. First, end users can have access through a massive number of apps and can easily install them according to their requirement using demand-based mobile distribution model (MDM), which is a public application store for various platforms [3]–[6]. Second, the development of advanced mobile operating systems like Android, iOS and Windows which has given strength to the development of extensive varieties of powerful devices. A new mechanism bring your own device (BYOD) has emerged in the market especially in workplaces. Using this mechanism, organization staff can easily link their smartphones and tablets with organization network to get access to their business information, client details and corporate data and conduct daily corporate activities [7]–[9]. Moreover, employees can utilize their devices for both corporate activities and personal use. This motivates employees to involve more incorporate functionalities and work activities by utilizing their smartphones, tablets. BYOD has tremendous benefits and convenience to a variety of business functionalities such as the high amount of work efficiency,

flexibility, organization staff satisfaction, and cost reduction, reduction in IT acquisition and many productivity advantages [10]–[13]. In recent years, the utilization of BYOD mechanism has become “hot tech trend”. Recently, a survey claims that almost 95% of organizational staff utilize at least one personal device for finishing their corporate works at the work station or any remote location [14]–[16]. Some reports show that almost 70% of the enterprises in many developed countries like USA, Australia, Spain, Germany and Malaysia has already adopted BYOD [17]. However, the high utilization of smartphones and tablets in corporate institutions in recent years has led to various security issues in the organization. The staff-owned and controlled devices access organization intranet and work on several networks. Thus, sensitive corporate information and details may be compromised unintentionally while sending emails to the clients via public mail services, by utilizing public cloud storage facilities like Samsung cloud, Apple’s iCloud and Dropbox for storing corporate documents or by interacting with voice assistants through smartphones [18]. Further, a corporate employee may intentionally or wickedly incorporate malware to the corporate network using his or her own virus-infected smartphones. Numerous researchers have provided a significant amount of work to provide an efficient and secure BYOD mechanism and some of the literature. In [18], a passive security mechanism is presented for reducing threats in the BYOD devices. Here, a non-intrusive big-data technique is adopted for tracking usage patterns. In [19], a smart risk management framework is introduced for BYOD technique to deal with data breaches in a corporate environment. In [20], a BYOD security enhancement method is introduced based on techniques such as software-defined networking (SDN), enterprise mobile management (EMM) and network function virtualization (NFV). In [21], a machine learning technique is introduced in which faulty and suspicious URL’s can be detected using supervised machine learning techniques. However, the malicious activities and security threats have widely enhanced in recent time hence the efficiency of these above techniques is reduced in practical implementation for a BYOD environment.

BYOD can enhance a significant amount of productivity of an enterprise. Moreover, this technique can reduce the cost of the organization, enhances flexibility as well as increases employee productivity. It gives a new interaction medium to the staff for communicating with clients as well as their colleagues resulting in productivity enhancement and permits staff to work from any remote location efficiently. This technique can become a bridge to fulfil the gap between corporate technologies and client solutions. Hence, this review article provides a detailed analysis of security. Further, this research focuses on various security issues, which can be experienced while utilizing BYOD policies are discussed and several secured methods are discussed to eliminate these issues. In addition, an effort has been made to provide guidelines for various organizations about several security policies and their proficient implementation. A discussion on the effects, which can be seen in various organizations in terms of security threats and their reduction by implementing these guidelines, has been presented.

This paper is organized: in section 2, security-related issues in BYOD policies are discussed and tackling these issues through various approach has been highlighted. In section 3, a detailed analysis of security issues, how to mitigate those issues and various security policies is discussed. In section 4, a detailed analysis about mentioned security policies in BYOD mechanism is presented and section 5 concludes the paper.

2. RELATED WORK

BYOD mechanism has been the demand of hour in recent days due to various situation, one of them being pandemic related. This technique can reduce the high costs required for the institutional set up to work in a company as well as a hefty investment needed for the distribution of hardware devices to employees from companies. However, security is the major concern for BYOD technique as both corporate and personal information remain on stake due to daily enhancement in malicious activities, which may concern employees as well as company authorities. Moreover, there are several mechanisms that have been proposed as a BYOD security solution, some of them were light weighted less complex with easy policy which follows the integration into other hardware domain such as given [22]–[31]; although these method does provide a fair and secure integration, they ignored some of the basic protocol of security due to major focus on IoT-domain. Furthermore, we have reviewed some of the important work that has mainly focused on the BYOD Security policy. In [32], a border patrol technique is adopted which works upon fine-grained contextual data to secure BYOD network. This method avoids unwanted functionalities like advertisements, analytical functionalities and unwanted cookies by blocking their packets. In [33], a virtual micro security technique is introduced for BYOD mechanism based on information protection abstraction, which can track malicious data packages. Throughput is considered high using this phenomenon. In [34], a deep learning context-based framework is introduced to reduce the security threats in BYOD environment. Here, artificial neural network and machine learning techniques are adopted to identify threat attacks and suspicious activities in smartphones. In [35], a BYOD evaluation mechanism is introduced to assess dynamic security threats in smartphones. This assessment mechanism is utilized for BYOD vulnerability evaluation based on their vulnerability score. However, tracking and accessing an extensive amount of relevant information is a very challenging process.

In [36], security threats, challenges, policies and their solutions for a BYOD mechanism are reviewed. Here, an inclusive security policy mechanism is introduced which tells about characteristics of a flexible and secured policy. In [37], a behaviour identification model is adopted for BYOD mechanism using theoretical determinants. This model evaluates that certain activities are malicious or not based on their behaviour patterns. This model is tested upon various employees of Oman. In [38], some necessary factors for the implementation of BYOD mechanism in schools are discussed. The data of 204 teachers are tested which is collected from 5 different schools. This study discusses the factors such as network security, content filtering and training for the maintenance of BYOD mechanism. Few researchers provided solutions to counter these threats which are associated with high overhead. And most of the researchers have provided review and evaluation model for BYOD mechanism. These issues are illegal access policies, leaking delicate company data, lower flexibility, corporate data breaching, employee privacy compromised, misuse, stolen device, and security unbalancing. Based on above factors, a detailed analysis of security issues present in the BYOD mechanism, their effects, mitigation strategies, various security policies and implementation of those policies in future work are discussed. Moreover, security guidelines are provided for organizations to mitigate security threats occur in BYOD mechanism.

3. SECURITY ANALYSIS IN BYOD MECHANISM

A comprehensive security analysis of BYOD framework is presented in the following section: in general BYOD has the security policy which helps in minimizing the threat, hence we have named it as security threat reduction policy framework aka security threat reduction policy (STRP) and analyze the different security framework, along with various challenges. A security threat reduction policy framework for BYOD mechanism is presented for the identification of security issues present in BYOD and provide solutions to mitigate these issues. STRP framework combines seven steps to form a decisive and proficient solution to reduce security threats in BYOD and incorporates a comprehensive life cycle of BYOD mechanism. The life cycle of a BYOD mechanism starts from granting permission to an employee from the organization to use their devices for corporate activities and work. This BYOD life cycle ends when those particular devices are revoked. STRP framework is designed to introduce a risk assessment system for BYOD security threats. These seven steps are strategize, recognize, defend, detect, retaliate, retrieve, evaluate and observe. These steps help to design a security threat reduction policy framework which can mitigate security threats in BYOD mechanism. Several crucial elements of the STRP framework can be identified based on the mechanism which mainly depends upon three categories. First, people involved in security procedures. Second, the security policy factors which helps to design a security guideline manual for ideal employee behavior concerning BYOD security. Third, a technology which holds up security procedures. The following section discusses major security challenges faced in the BYOD mechanism which are identified from various literature.

3.1. Security challenges identified in BYOD

Security challenges in BYOD plays a major role, security challenges identification helps in reducing the different kind of threats. Although there are number of security challenges, this section discusses several security challenges which has major impact while designing the BYOD security framework. Furthermore, this section mostly focuses from data center perspective.

3.1.1. Recognition, validation and access control challenges

BYOD implies that several employees of an organization perform various corporate activities with their own devices. For security reasons, these devices need to be protected using very essential in-built device authentication and locking mechanism such as PIN, passwords, patterns, face recognition and fingerprint access to protect crucial information present in the employee devices. However, various surveys show that a massive number of employees do not utilize this type of authentication security features [39]. There is minimal control of an organization on their employees in the way they access their devices, which is a reason for excess information breach in several organizations. Moreover, the possibilities of information breaching may enhance when employees work from a remote location or access corporate functionalities from outside the company perimeter. Moreover, cybercriminals can easily hack these BYOD devices and can utilize employee details to access unauthorized information of an organization and cause harm to their business activities.

3.1.2. Device and information security problems

Employee-owned devices are susceptible to various malicious activities like malware, virus, worms, and spyware. Additionally, organizational authorities have no clue what type of applications or programs,

employees are running on their devices. In contrast, company-maintained devices generally have all the applications or programs prior installed with severe security policies incorporated in those devices. Therefore, the possibility of data leakage of an organization is more in employee-owned devices than company-maintained devices. Recently, several applications, websites and software utilizes 'caches' which is a temporal repository for storing information. The 'caches' may keep crucial information about the organization and may expose to unauthorized people. Moreover, employees can attract well-designed programs or applications, which have minimal security encryption policies, enhancing the possibility of information leakage. The utilization of BYOD mechanism means several devices, which are owned by employees, are connected to a single organization network in which many devices may consist of malicious software and applications. Finally, employee-owned devices may get stolen or lost which remain unprotected and unencrypted in major cases and can be easily exposed by intruders which may cause severe security threats. Most information breach cases are registered at the time of device lost or stolen.

3.1.3. Network security challenges

The utilization of BYOD mechanism shows the possibility of malicious software and applications in employee-owned devices links to the same network is much higher than in company-owned devices due to restricted access. This may lead to a high-level security threat and crucial client information may leak. A hacker can easily expose these security drawbacks of BYOD mechanism by accessing organizational network whenever employees connect to a local network in the organization. Recently, several employees have demanded data center access while work from outside company premises or work from home. This shows that risks are higher while using BYOD mechanism.

3.1.4. Management challenges

Strict guidelines and security policies are very essential for enhancing security structures in the BYOD model for employee-owned devices. Absence of these security policies and guidelines may cause higher security threats as well as misinterpretation of data, resulting in immoral security practices. Additionally, lack of knowledge in employees about secured policies may lead to severe security threats. Security enhancement in devices requires additional cost. Certain organization imposes guidelines on employees such as the utilization of long and intricate passwords, automatic session expired functionalities in certain time-period. However, these strict guidelines can affect usability and can irritate many employees.

3.1.5. Compliance challenges

The utilization of BYOD in many organizations is a very complex process. First, these organizations do not have any control on employee-owned devices. Second, all organizations need to follow several legal laws and guidelines. This shows that these organizations need to impose severe security guidelines to save their customer's crucial information.

3.2. BYOD security policy

A comprehensive discussion of a proficient and secure BYOD security policy is presented here. The seven steps mentioned in review of security threat reduction policy (STRP) framework, which are strategy, recognize, defend, detect, retaliate, retrieve, evaluate and observe. These security policies have been discussed thoroughly later in the section.

– Strategy

This phase is very crucial for authorities (higher management) in an organization for the design and implementation of BYOD mechanism. Several steps require to design the BYOD mechanism which is: At first, higher management authorities have to design a strong and efficient BYOD model by establishing a strong relationship with all the people who are involved in this BYOD model such as all the managers, employees, shareholders, managerial authorities and they need to work as one link and follow every compulsory guideline given by higher authorities. To design such a BYOD policy which works in a streamline with an organization's mission and vision. Thus, initially, a clear picture of that organization's capabilities, their functionalities and their requirement is necessary for design a proficient BYOD policy. A mobile device management (MDM) can be utilized which can control all the mobile devices linked to the internal network of the organization and can comprehensively manage their information. BYOD awareness program can be placed for employees so that their understanding of BYOD improves.

– Recognize

This phase majorly discusses the device registration of employees and their training about BYOD policy guidelines and security. Employees submit their request for registration of their devices. Then, the IT department analyzes that the requested device is permitted or not under the guidelines of BYOD policy. All the devices will have a minor background check for security measures and the people with higher access to organization resources will have a major background check. The organizational authorities can install certain

security threat management technologies or configure high-security settings; finally, a training session can be arranged for an employee for a clear understanding of BYOD security measures and how to follow them.

– **Defend**

This phase discusses the factors which can impact BYOD policy and how to deal with them; an authentication system should incorporate to defend from cybersecurity threats. The utilization of passwords, patterns and biometric authentication in BYOD devices need to make mandatory for protecting information. One-time authenticate mechanism will have to be incorporated in BYOD policy that means once an employee is authenticated to utilize one functionality of the enterprise then no need to authenticate again for other functionalities of the organization for that particular session so that they can focus more on work. An internal application and software store can be incorporated so that only trusted application or software are used which are prior tested by the IT authorities. The organizational network needs to be protected with high layer advanced encryption protocol to protect from any kind of malicious activities.

– **Detect**

This phase discusses the detection of security threats in the organization and how to mitigate them; all the employees should have a clear understanding about BYOD security threats and what are the signs that their device is affected by any kind of malware. Proper knowledge of the security threats in employees can reduce future threats. All the employees should have anti-malware and anti-virus installed in their devices suggested by IT authorities and should regularly scan them. To avoid information breaching and unauthorized data transmission, visualization software can be utilized by the organization. To avoid device loss, MDM can be utilized which can continuously track all employee devices based on their location.

– **Retaliate**

This particular phase highlights the actions required for a security breach or data leakage; High-security firewalls and anti-virus software can be installed in affected device and malware can be removed after successful detection. If particular application or website is infected, then it should be blacklisted for further used. In case of any malicious activities, MDM should be utilized to wipe out all the corporate details with employee properties.

– **Retrieve**

This phase will describe the prevention methods of a security breach from employee-owned devices. An organization should prevent employees to utilize shared or public data storage platforms for corporate details and activities. Maximum protection can be provided by incorporating their private cloud for data storage based on the organization's budget. Virtualization can be utilized so that the personal space of employee-owned devices is not used and employee can directly store and access information from the organization data storage center where security remains extremely high.

– **Evaluate and observe**

The last phase describes how crucial is feedback when the security policies and environment and technology is continuously changing. Therefore, certainly taken into consideration while developing any security policy. With the rise of technology and utilization of BYOD devices, regular checkups, security updates and feedbacks become very crucial. The organization has to review the entire system in a certain period and detect security gaps present in the system; further, Table 1 represents problem identification in BYOD mechanism and their solutions.

Table 1. Analysis of problem identification and their respective solutions and effects in the organization

Problem Identification	Respective Solution	Effect
Either weak or no security policies are utilized by several organizations	Ensure 2-factor authentication wherever required	Security gets enhanced and unauthorized access get denied and data security achieved
Provided Privilege misuse by employees	Use responsibility-based privilege control, incorporate automated log-off activity, a fine employee if security breached	Client access is provided based on their responsibilities and fines will ensure proper use of guidelines circulated
Possibilities of identification thefts	MDM can be utilized for validation and information storage on employee devices can be minimized	IT department can easily track and record security breaching and cybercrimes can be reduced
Utilization of virus integrated software and applications by employees	Blacklisted websites and application list should circulate to employees	Minimizes the risk of data breaching and faulty applications can be removed by regular checkups

4. ANALYSIS OF BYOD SECURITY POLICY

The main aim of this review article is to find out all the security issues faced by an organization using BYOD mechanism and required security policies to reduce those issues. The STRP framework is

extremely helpful in understanding all the issues faced by an organization, their effects and their respective mitigation policies. Moreover, very few articles have comprehensively analyzed security issues and their respective policies phase by phase, which is done in this article. This review work can be utilized for providing guidelines in various organizations. Furthermore, considering the analysis of security work in BYOD, there are other two work which has done empirical survey and strengths, weaknesses, opportunities, and threats (SWOT) analysis in [40] and [41] respectively.

5. CONCLUSION AND FUTURE WORK

BYOD is a crucial and important trend of recent time to enhance the productivity of an organization while reducing cost and establishing a stronger bond between company employees and an organization. However, security threats present in BYOD mechanism has always is a cause of concern to the authorities of the organization. However, these threats can be mitigated by following certain guidelines, installing highly-secured software and by designing a secured policy for BYOD. Several issues have been identified such as managerial-level, social-level and technical level and their effects also explained comprehensively. All the crucial elements like people, security policy factors and technology used are considered and a mitigation strategy is explained comprehensively phase by phase. It is analyzed that collaboration of people, security policy factors and technology in an effective manner can mitigate security threats present in the BYOD mechanism. Future work may involve a work on following aspects such as How BYOD is implemented in several organizations in real-time? How it remains secure from security threats and what kind of security policies and technologies are utilized? What are the security threats and how information is not compromised while working from home by employees in their own devices due to COVID-19 pandemic in 2021? Moreover, this research review article has limitations in conducting review as we have focused only on the review of BYOD security policy relevant to our work and there is other area such as efficient and productive security.




REFERENCES

- [1] M. Ratchford, O. El-Gayar, C. Noteboom, and Y. Wang, "BYOD security issues: a systematic literature review," *Information Security Journal: A Global Perspective*, vol. 31, no. 3, pp. 253–273, May 2022, doi: 10.1080/19393555.2021.1923873.
- [2] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: security and privacy considerations," *IT Professional*, vol. 14, no. 5, pp. 53–55, Sep. 2012, doi: 10.1109/MITP.2012.93.
- [3] N. Atanassov and M. D. M. Chowdhury, "Mobile device threat: malware," in *2021 IEEE International Conference on Electro Information Technology (EIT)*, May 2021, pp. 7–13, doi: 10.1109/EIT51626.2021.9491845.
- [4] M. I. Ali and S. Kaur, "BYOD cyber threat detection and protection model," in *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Feb. 2021, pp. 211–218, doi: 10.1109/ICCCIS51004.2021.9397105.
- [5] X. Tan, H. Li, L. Wang, and Z. Xu, "End-edge coordinated inference for real-time BYOD malware detection using deep learning," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, May 2020, pp. 1–6, doi: 10.1109/WCNC45663.2020.9120765.
- [6] K. Su, P. Liu, L. Gu, W. Chen, K. Hwang, and Z. Yu, "vMobiDesk: desktop virtualization for mobile operating systems," *IEEE Access*, vol. 8, pp. 213541–213553, 2020, doi: 10.1109/ACCESS.2020.3041304.
- [7] R. Palanisamy, A. A. Norman, and M. L. M. Kiah, "Compliance with bring your own device security policies in organizations: A systematic literature review," *Computers & Security*, vol. 98, p. 101998, Nov. 2020, doi: 10.1016/j.cose.2020.101998.
- [8] J. A. Gomez-Hernandez, J. Camacho, J. A. Holgado-Terriza, P. Garcia-Teodoro, and G. Macia-Fernandez, "ARANAC: a bring-your-own-permissions network access control methodology for android devices," *IEEE Access*, vol. 9, pp. 101321–101334, 2021, doi: 10.1109/ACCESS.2021.3097152.
- [9] S. O. Ganiyu and R. G. Jimoh, "Extended risk-based context-aware model for dynamic access control in bring your own device strategy," in *Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics*, Cham: Springer International Publishing, 2021, pp. 295–315.
- [10] B. Morrow, "BYOD security challenges: control and protect your most sensitive data," *Network Security*, vol. 2012, no. 12, pp. 5–8, Dec. 2012, doi: 10.1016/S1353-4858(12)70111-3.
- [11] A. Scarfo, "New security perspectives around BYOD," in *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*, Nov. 2012, pp. 446–451, doi: 10.1109/BWCCA.2012.79.
- [12] T. Shumate and M. Ketel, "Bring your own device: benefits, risks and control techniques," in *IEEE SOUTHEASTCON 2014*, Mar. 2014, pp. 1–6, doi: 10.1109/SECON.2014.6950718.
- [13] M. Ketel and T. Shumate, "Bring your own device: security technologies," in *SoutheastCon 2015*, Apr. 2015, pp. 1–7, doi: 10.1109/SECON.2015.7132981.
- [14] A. Angelogianni, I. Politis, P. L. Polvanesi, A. Pastor, and C. Xenakis, "Unveiling the user requirements of a cyber range for 5G security testing and training," in *2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Oct. 2021, pp. 1–6, doi: 10.1109/CAMAD52502.2021.9617776.
- [15] D. Petrov and T. Znati, "Context-aware deep learning-driven framework for mitigation of security risks in BYOD-enabled environments," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, Oct. 2018, pp. 166–175, doi: 10.1109/CIC.2018.00032.
- [16] G. Thomson, "BYOD: enabling the chaos," *Network Security*, vol. 2012, no. 2, pp. 5–8, Feb. 2012, doi: 10.1016/S1353-4858(12)70013-2.
- [17] S. Kalhor, M. Rehman, V. Ponnusamy, and F. B. Shaikh, "Extracting key factors of cyber hygiene behaviour among software engineers: a systematic literature review," *IEEE Access*, vol. 9, pp. 99339–99363, 2021, doi: 10.1109/ACCESS.2021.3097144.
- [18] M. P. Stoecklin et al., "Passive security intelligence to analyze the security risks of mobile/BYOD activities," *IBM Journal of Research and Development*, vol. 60, no. 4, pp. 9:1–9:13, Jul. 2016, doi: 10.1147/JRD.2016.2569858.




- [19] K. Al Harthy, N. Shah, and A. Shankarappa, "Intelligent risk management framework for BYOD," in *2018 IEEE 15th International Conference on e-Business Engineering (ICEBE)*, Oct. 2018, pp. 289–293, doi: 10.1109/ICEBE.2018.00055.
- [20] M. Ketel, "Enhancing BYOD security through SDN," in *SoutheastCon 2018*, Apr. 2018, pp. 1–2, doi: 10.1109/SECON.2018.8479230.
- [21] M. Al-Janabi, E. de Quincey, and P. Andras, "Using supervised machine learning algorithms to detect suspicious URLs in online social networks," in *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*, Jul. 2017, pp. 1104–1111, doi: 10.1145/3110025.3116201.
- [22] K. AlHarthy and W. Shawkat, "Implement network security control solutions in BYOD environment," in *2013 IEEE International Conference on Control System, Computing and Engineering*, Nov. 2013, pp. 7–11, doi: 10.1109/ICCSCE.2013.6719923.
- [23] P. K. Gajar, A. Ghosh, and S. Rai, "Bring your own device (BYOD): Security risks and mitigating strategies," *Journal of Global Research in Computer Science*, vol. 4, no. 4, pp. 62–70, 2013.
- [24] T. Weil and S. Murugesan, "IT risk and resilience-cybersecurity response to COVID-19," *IT Professional*, vol. 22, no. 3, pp. 4–10, May 2020, doi: 10.1109/MITP.2020.2988330.
- [25] M. Mahinderjit Singh, S. Sin Siang, O. Ying San, N. H. A. Hassain Malim, and A. R. Mohd Shariff, "Security attacks taxonomy on bring your own devices (BYOD) model," *International Journal of Mobile Network Communications & Telematics*, vol. 4, no. 5, pp. 1–17, Oct. 2014, doi: 10.5121/ijmnet.2014.4501.
- [26] F. Jamal, M. T. Abdullah, A. Abdullah, and Z. M. Hanapi, "Enhanced bring your own device (BYOD) environment security based on blockchain technology," *International Journal of Engineering and Technology*, vol. 7, no. 4, pp. 74–79, 2018, doi: 10.14419/ijet.v7i4.31.23345.
- [27] G. Salles-Loustau, L. Garcia, K. Joshi, and S. Zonouz, "Don't just BYOD, bring-your-own-app too! protection via virtual micro security perimeters," in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Jun. 2016, pp. 526–537, doi: 10.1109/DSN.2016.54.
- [28] V. R. Kebande, N. M. Karie, and H. S. Venter, "A generic digital forensic readiness model for BYOD using honeypot technology," in *2016 IST-Africa Week Conference*, May 2016, pp. 1–12, doi: 10.1109/ISTAfrica.2016.7530590.
- [29] A. Marotta and M. McShane, "Integrating a proactive technique into a holistic cyber risk management approach," *Risk Management and Insurance Review*, vol. 21, no. 3, pp. 435–452, Dec. 2018, doi: 10.1111/rmir.12109.
- [30] N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. Pangalos, "Improving forensic triage efficiency through cyber threat intelligence," *Future Internet*, vol. 11, no. 7, p. 162, Jul. 2019, doi: 10.3390/fi11070162.
- [31] D. A. Flores, F. Qazi, and A. Jhumka, "Bring your own disclosure: analysing BYOD threats to corporate information," in *2016 IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 1008–1015, doi: 10.1109/TrustCom.2016.0169.
- [32] O. Zungur, G. Suarez-Tangil, G. Stringhini, and M. Egele, "BorderPatrol: securing BYOD using fine-grained contextual information," in *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Jun. 2019, pp. 460–472, doi: 10.1109/DSN.2019.00054.
- [33] N. A. Abu Othman, A. A. Norman, and M. L. Mat Kiah, "Information system audit for mobile device security assessment," in *2021 3rd International Cyber Resilience Conference (CRC)*, Jan. 2021, pp. 1–6, doi: 10.1109/CRC50527.2021.9392468.
- [34] X. Liu, M. Xu, T. Teng, G. Huang, and H. Mei, "MUIT: a domain-specific language and its middleware for adaptive mobile web-based user interfaces in WS-BPEL," *IEEE Transactions on Services Computing*, vol. 12, no. 6, pp. 955–969, Nov. 2019, doi: 10.1109/TSC.2016.2633535.
- [35] P. Mateko B, S. Mateko Z, and I. K, "Current BYOD security evaluation system: future direction," *Journal of Information Technology & Software Engineering*, vol. 08, no. 03, 2018, doi: 10.4172/2165-7866.1000235.
- [36] B. Alotaibi and H. Almagwashi, "A review of BYOD security challenges, solutions and policy best practices," in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, Apr. 2018, pp. 1–6, doi: 10.1109/CAIS.2018.8441967.
- [37] I. M. Al-Harthy, F. A. Rahim, N. Ali, and A. P. Singun, "Theoretical bases of identifying determinants of protection intentions towards bring-your-own-device (BYOD) protection behaviors," in *2019 First International Conference of Intelligent Computing and Engineering (ICOICE)*, Dec. 2019, pp. 1–9, doi: 10.1109/ICOICE48418.2019.9035139.
- [38] Y. H. Yeop, Z. Ali Othman, S. N. Huda Sheikh Abdullah, U. Asmar Mokhtar, W. F. Paizi Fauzi, and N. Ahmad, "Key factors to implement BYOD in schools," in *2018 Cyber Resilience Conference (CRC)*, Nov. 2018, pp. 1–3, doi: 10.1109/CR.2018.8626864.
- [39] G. Martin, P. Janardhanan, T. Withers, and S. Gupta, "Mobile revolution: a requiem for bleeps?," *Postgraduate Medical Journal*, vol. 92, no. 1091, pp. 493–496, Sep. 2016, doi: 10.1136/postgradmedj-2015-133722.
- [40] P. Soubhagyalakshmi and K. S. Reddy, "Empirical survey on BYOD security and usage," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 1, pp. 2784–2788, 2019.
- [41] P. Soubhagyalakshmi and K. Satyanarayan Reddy, "SWOT analysis of BYOD (bring your own device)," in *Emerging Technologies in Data Mining and Information Security*, Springer Singapore, 2021, pp. 681–688.

BIOGRAPHIES OF AUTHORS



Pullagura Soubhagyalakshmi    secured first class with distinction in M.Tech, Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad in 2006. She is pursuing Ph.D. (Computer Science) degree in VTU, Belagavi, Karnataka, India. She can be contacted at email: slakshmi.p@gmail.com, alternative email: pslakshmi2021@gmail.com



Dr. Kalli Satyanarayan Reddy    secured his M.Sc. and M.Phil. (Mathematics) Degrees from Nagpur University, Maharashtra State, and M. Tech (CSE with specialization in Computer Applications) from Indian School of Mines [now IIT (ISM)], Dhanbad, Jharkhand in 1987, 1988 and 2000 respectively. He was awarded Ph.D. (Computer Science) degree in the year 2012 from School of Science & Technology, Dept. of Computer Science at Dravidian University, Kuppam, AP, and India. He is currently working as Professor in the dept. of Information Science and Engineering, Cambridge Institute of Technology (affiliated to VTU Belagavi), Bangalore, Karnataka State, India. His current areas of research are High Speed Networks, Data Communications, Network Security, Wireless Sensor Networks, Big Data, and Artificial Intelligence. Currently he is guiding 7 PhD Scholars under VTU, Belagavi, Karnataka, India. He has 46 publications. He can be contacted at email: satyanarayan.reddy@gmail.com, alterenative email: ksatyanreddy@yahoo.com, official email: hod.ise@cambridge.edu.in