applied sciences

MDPI

Review

Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions

Aljuaid Turkea Ayedh M [1,2], Ainuddin Wahid Abdul Wahab [1,*] and Mohd Yamani Idna Idris [1,3]

[1] Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia; taljuaid@su.edu.sa (A.T.A.M.)
[2] Faculty of Computing and Information Technology, Shaqra University, Shaqra 11961, Saudi Arabia
[3] Center for Mobile Cloud Computing, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia
* Correspondence: ainuddin@um.edu.my; Tel.: +60-3-7967-6383

Abstract: The number of devices connected within organisational networks through "Bring Your Own Device" (BYOD) initiatives has steadily increased. BYOD security risks have resulted in significant privacy and security issues impacting organisational security. Many researchers have reviewed security and privacy issues in BYOD policies. However, not all of them have fully investigated security and privacy requirements. In addition to describing a system's capabilities and functions, these requirements also reflect the system's ability to eliminate various threats. This paper aims to conduct a comprehensive review of privacy and security criteria in BYOD security policies, as well as the various technical policy methods used to mitigate these threats, to identify future research opportunities. This study reviews existing research and highlights the following points: (1) classification of privacy and security requirements in the context of BYOD policies; (2) comprehensive analyses of proposed state-of-the-art security policy technologies based on three layers of security BYOD policies, followed by analyses of these technologies in terms of the privacy requirements they satisfy; (3) technological trends; (4) measures employed to assess the efficacy of techniques to enhance privacy and security; and (5) future research in the area of BYOD security and privacy.

Keywords: access control policies; security techniques; BYOD security layers; risk access control; onboarding access control; authentication; attack detection; privacy and security requirements; BYOD environment

Citation: Ayedh M, A.T.; Wahab, A.W.A.; Idris, M.Y.I. Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions. *Appl. Sci.* **2023**, *13*, 8048. https://doi.org/10.3390/app13148048

Academic Editors: Antonio Fernández-Caballero, Peter R. J. Trim, Yang-Im Lee and Luis Javier García Villalba

Received: 24 February 2023
Revised: 15 June 2023
Accepted: 4 July 2023
Published: 10 July 2023

1. Introduction

The bring your own device (BYOD) paradigm, which allows employees to connect their mobile devices to the organization's network, rapidly changes organisational operations by enhancing flexibility, productivity, and effectiveness [1]. Despite these advantages, security concerns continue to affect organisational environments [2] and introduce security challenges and significant security risks [2]. One of the primary concerns with BYOD is the need for more control over employee devices. Personal devices have different security measures and software updates from company-issued devices. This disparity exposes vulnerabilities that attackers could exploit, resulting in data breaches or unauthorized access to sensitive information [3]. In addition, the variety of devices in a BYOD environment complicates the implementation of standard security policies. Different operating systems, versions, and security configurations must be considered by organizations, making it challenging to implement uniform security measures across all devices [4]. This variation heightens the possibility that cybercriminals will exploit security gaps or obsolete security software.

Furthermore, when personal devices are used for work-related purposes, the possibility of mixing personal and business information increases. This mixing of data poses the

risk of data leakage or inadvertent disclosure. It becomes more difficult for organizations on these devices to ensure that sensitive information is adequately protected and segregated from personal files. The BYOD direction also raises concerns about the possibility of device loss or theft. If an employee's device containing sensitive company information is lost or stolen, the risk of unauthorised access to that information increases [5].

To address these risks, organisations can effectively manage BYOD usage by implementing security access control and security policy technologies that address these vulnerabilities and obstacles [6]. However, there are significant gaps between the security offered by current BYOD access control policies and the desired outcomes [7]. Rhee et al. [8] provide fundamental access control policies that address security and privacy issues in three primary categories: authenticity, confidentiality, and integrity. These policies encompass network access control policies, mobile access control policies, mobile information management policies, mobile application management policies, and enterprise mobility management policies. Initially, these policies assisted organisations in managing and governing BYOD devices effectively. Nonetheless, the increasing complexity of attacks targeting BYOD devices and networks [8–10] has rendered these policies and the security requirements they fulfil insufficient [11,12]. To adequately meet the security and privacy requirements of BYOD, it is essential to adopt integrated and comprehensive BYOD security policies, emphasising the implementation of three-tiered policies and a thorough understanding of security and privacy requirements, as mentioned by Bello et al. [13] in their work on consumerization.

There have been few systematic reviews of the security of BYOD, as seen in Table 1. However, most earlier research has systematically ignored examining security and privacy needs in the BYOD context. Additionally, previous survey studies have yet to investigate the most commonly used security policy techniques based on a three-tiered BYOD policy architecture with the appropriate technology to fulfill security and privacy requirements. For instance, in [14], Oktavia et al. presented a survey on privacy concerns and BYOD challenges. This study examined these issues in depth. However, the analysis of policy mechanisms based on security and privacy requirements was not included and was limited to raising concerns.

Similarly, Jamal et al. [15] surveyed BYOD authentication techniques, focusing on authenticity criteria while giving less attention to other security and privacy criteria. The term "other security and privacy criteria*" indicates additional privacy requirements in BYOD security, such as confidentiality, integrity, availability, authenticity, privacy preservation, non-repudiation, and attack detection. Furthermore, Palanisamy et al. [16] presented a thorough review of compliance theories that are used to interpret and predict security practices in the Bring Your Own Device (BYOD) sector. However, they did not conduct an assessment of technologies in relation to security and privacy standards. Instead, their primary focus was largely on the theoretical aspects of the subject. Additionally, Wani et al. [17] highlighted significant security problems associated with hospital BYOD practices but did not extensively address the identified concerns by analyzing technologies. While several survey studies have contributed to understanding BYOD's privacy and security challenges, most of them have provided limited information on the inherent privacy and security concerns of BYOD. Furthermore, many of these studies examined only a subset of the problem or conducted a review during the early stages of BYOD adoption. In [18], the researchers conducted a comprehensive review of attack detection strategies that utilize machine learning. However, they did not delve into other aspects related to privacy needs. To put it another way, while they extensively studied how machine learning can be used to identify cyber attacks, they did not explore other crucial components of privacy, such as data protection, anonymity, and user consent. Table 1 provides an overview of the main focus and limitations of some of the earliest (pre-2023) literature on BYOD security. Overall, while these studies have made strides in offering access control solutions and risk analyses, they exhibit limitations. Particularly, they do not critically evaluate the studies in terms of their contribution to satisfying the privacy requirements essential for BYOD systems.

Table 1. Focus and limitations of some of the key older (pre-2023) publications.

Ref	Concentrate on	Limitations
[14,17,19,20]	Focused on discussing risks and security issues related to BYOD.	Not comprehensive for all security and privacy requirements and access control based on three layers.
[15]	Focused on techniques connected to the authenticity criteria.	Other * security and privacy criteria received less attention.
[16]	Overview of the BYOD compliance theories.	Not analysing technologies based on privacy criteria.
[21]	Classification scheme for proposed solutions based on identified security issues.	Not analysing technologies based on privacy criteria.
[18]	Mapping review of attack detection strategy based on machine learning.	Other * security and privacy requirements were ignored.

* indicates additional privacy requirements in BYOD security.

Therefore, this paper extensively reviews security policies and access control in three security policy layers. It evaluates the effectiveness of existing security policies and access control mechanisms in meeting privacy requirements. The study contributes to understanding privacy-focused security measures in BYOD environments and informs future research and improvements in security policies and access control strategies. To ensure a systematic approach, we developed a review protocol that outlines the critical phases necessary to achieve the objectives of this study. The paper focuses on seven critical security and privacy criteria within the three layers of secure BYOD control policies designed for enterprises adopting BYOD practices. These criteria include confidentiality, integrity, availability, authenticity, privacy preservation, non-repudiation, and attack detection. Achieving these criteria ensures the system can eliminate potential privacy and security vulnerabilities and comply with regulatory guidelines [5,22]. The process of this study will ensure unbiased data retrieval and thorough search procedures. The contributions of this study to the overall review can be summarized as follows:

- Identifies privacy and security criteria needed in the BYOD policy setting.
- Analyses existing policy techniques based on privacy and security requirements in three security policy layers.
- Introduces a novel taxonomy that categorizes policy techniques into three layers according to their alignment with privacy and security requirements. This taxonomy provides a structured framework for understanding and organizing policy techniques, contributing to the existing knowledge in the field.
- Identifies and discusses the current trends in technology related to policy techniques by examining the technological advancements within each layer.
- Addresses the measures used to evaluate the effectiveness of policy techniques, mainly through performance analysis, by discussing these evaluation measures.
- Presents a comprehensive evaluation of policy techniques' technical advantages and limitations by highlighting the strengths and weaknesses of each technique.
- Identifies potential areas for future research and improvement in policy techniques. By pointing out the gaps and limitations in the existing techniques, the paper stimulates further exploration and encourages researchers to develop innovative approaches to address the identified challenges.

The remainder of the article is divided into the following sections: Section 2 presents the background information, while Section 3 compares the conventional BYOD security approach with the desired state and examines BYOD security policies across the three layers of BYOD architecture policy. Section 4 provides an overview of the privacy and security requirements for the development of security policies. The methodology for conducting a systematic literature review is presented in Section 5. The data analysis process is detailed

in Section 6, followed by a discussion of critical findings in Section 7. Section 8 highlights open research issues, and Section 9 concludes the paper.

2. Background and Related Concepts

This section examines the security and privacy challenges posed by the bring your own device (BYOD) environment and introduces the fundamental concepts that will be investigated in this study.

2.1. BYOD Risks

The expanding adoption of BYOD raises notable privacy and security concerns. According to a report by Hewlett-Packard [13], employees now utilize multiple mobile devices at work, creating a situation where their activities are invisible and untraceable to the IT department. Consequently, this trend poses various challenges and security threats for enterprises.

Firstly, the need for clear security expectations is a primary challenge, resulting in costly consequences, particularly when inexperienced personnel are entrusted with data security. Moreover, phishing attacks pose a serious risk by compromising employee devices and company information. Using unsecured Wi-Fi networks outside the office further amplifies security risks, as highlighted by Kaspersky Lab [23]. Additionally, malware infections and unauthorized app installations pose additional threats [23,24]. Lastly, the BYOD trend raises concerns about employees accessing social media during work hours, potentially violating company policies.

These risks associated with BYOD significantly impact organizational security, giving rise to various challenges. These challenges include implementing security policies across different BYOD operating systems and devices, effectively managing numerous BYOD devices within the organization, securing BYOD devices, tracking their activities, and monitoring their usage outside of work hours [24]. To address the above challenges, access control policies and technologies play a crucial role in mitigating risks and meeting the privacy requirements of the BYOD environment.

As a result, this study aims to investigate appropriate access control solutions and privacy requirements within the three layers of the BYOD security architecture. The objective is to effectively tackle the privacy and security issues associated with BYOD.

2.2. Security Challenges

The term "security", in the context of an organization, pertains to the safeguarding of valuable assets, including information, resources, processes, and records [13]. Companies that prioritise security allocate significant resources to establish an effective information security system to protect their data. However, despite these efforts, they remain a target for various threats [25].

Managing security poses challenges for large corporations with multiple departments or small branches sharing the same network. In the latter scenario, this structure makes it easier for cybercriminals to target small branches before moving on to headquarters. Security plays a crucial role in supporting organizational operational processes and methods. Therefore, organizations must protect confidential information from potential threats or harm resulting in damage, loss, modification, or unauthorized disclosure.

According to Whitman and Mattord [26], an organisation's security should be a complex system that includes computer systems supporting the organisational environment, software applications and databases securing data, as well as policies, procedures, training, and other human-reliant components. The primary objective of securing an organization's critical information resources and assets is to implement security policies across three layers: onboarding access control, authentication access control, and risk access control policies utilizing related technologies [13].

Whitman and Mattord further suggest that the objectives of security policies should encompass the protection of confidentiality, integrity, and availability of information-reliant entities and information-delivering systems, ultimately fulfilling privacy requirements [26].

Hence, confidentiality, integrity, and availability objectives are essential for accomplishing security policy objectives.

2.3. Privacy Challenges

Privacy is the behaviour or attitude of a company toward protecting its information resources and the personally identifiable information of its customers [27]. Organisations are increasingly leaking personal information, either deliberately or due to compromised information systems. Users of BYOD devices express concerns about their ability to manage personal data and trust organizations to protect their users. According to Johnston and Anna [28], there has been an ongoing debate on whether individuals should sign contracts with organizations to manage and safeguard their information or if it should be the responsibility of the enterprise to protect individual privacy. According to various publications, organisations devote regular financial resources to implementing safeguards and information privacy programmes to protect information from leaks and other threats. However, they fail to effectively utilise these protections and programmes [29]. This strategy can easily result in privacy breaches, which have historically been a significant concern. The primary objective of these hacking attacks is to steal, delete, or alter sensitive information. Organisations must recognise the significance and necessity of protecting personal data because it presents various privacy issues, risks, and other data breaches. New, difficult-to-detect vulnerabilities are generated for hackers as technology progresses and becomes more sophisticated [30]. BYOD has and will continue to raise concerns about data and user privacy.

2.4. Security Policies

Security policies refer to the rules established by organizational leaders to ensure the appropriate level of security is aligned with the organization's needs. The access control policy is crucial in safeguarding the organization's data and resources against internal and external threats, reducing vulnerability to cyber and physical attacks. Each access control type employs specific security techniques to meet the organization's security and privacy requirements, which will be discussed in detail in Section 3.2.

2.5. Security Technologies

Security technologies encompass control policies across various technological components to fulfil privacy and security requirements within the BYOD organizational environment. These technologies cover devices, information, applications, and communication. Each layer of the BYOD security architecture incorporates access policies and technologies that address specific security and privacy needs. For instance, the identification access control policy employs a variety of mechanisms, such as authentication algorithms or other technologies, to carry out authentication and authorization functions. Section 3.2 will comprehensively explain these techniques, where the control policies and techniques associated with each access control policy will be discussed.

2.6. Privacy and Security Requirements

Privacy and security requirements define the security standards that policies and technologies in the BYOD context should meet. Standard terms include confidentiality, integrity, availability, non-repudiation, authentication, privacy preservation, and attack detection. The rationale for selecting these requirements and the underlying concepts will be discussed in Section 4.

3. Comparison Traditional Access Control vs. Security Access Control Based on Three Layers

This section will highlight the primary differentiation between traditional BYOD security policies and contemporary approaches to BYOD security, as depicted in Figure 1. According to Macaraeg [31], traditional security policies primarily focus on

protecting devices, networks, data, and applications. These policies encompass network access control, mobile device management, mobile application management, and enterprise mobility management policies, as described in more detail in Section 3.1. While these access control policies may provide security mechanisms and solutions to protect the company's network, data, and devices, they often overlook risk control access policies. Consequently, they fail to meet the requirement for attack detection. To address this limitation, Bello et al. [1] proposed an enhanced BYOD access control approach based on three security layers, aiming to comprehensively address security and privacy requirements that fulfill organizational security needs and user privacy. This three-layered protection approach, as described in Section 3.2, includes an access control policy and corresponding mechanism within each layer. A comparison between this security approach and traditional security policies and their respective shortcomings is outlined in Table 2:

- Traditional security approaches are often deemed insufficient and potentially vulnerable in providing the required level of protection [1,31]. For example, network access control policies in traditional security heavily rely on mobile device management (MDM) technology for authenticating and managing BYOD devices within the organization. In contrast, ideal BYOD security emphasizes identification access control methods, such as biometrics and two-factor authentication. Additionally, ideal security policies for information protection encompass advanced measures like communication access control, encryption, virtual private networks (VPNs), and data wiping. On the other hand, traditional security approaches utilize mobile information management (MIM) to enforce information management policies.
- Traditional security policies lack the inclusion of risk access control policies, despite their importance in BYOD security, as recommended by Bello et al. [1].
- Traditional security policies fall short in adequately addressing all privacy requirements due to limitations in policy techniques and defense mechanisms [31]. These limitations serve as a motivation to address the challenges surrounding privacy and security and enhance security policies through the implementation of three layers of security policies, thus meeting the privacy requirements of BYOD security.

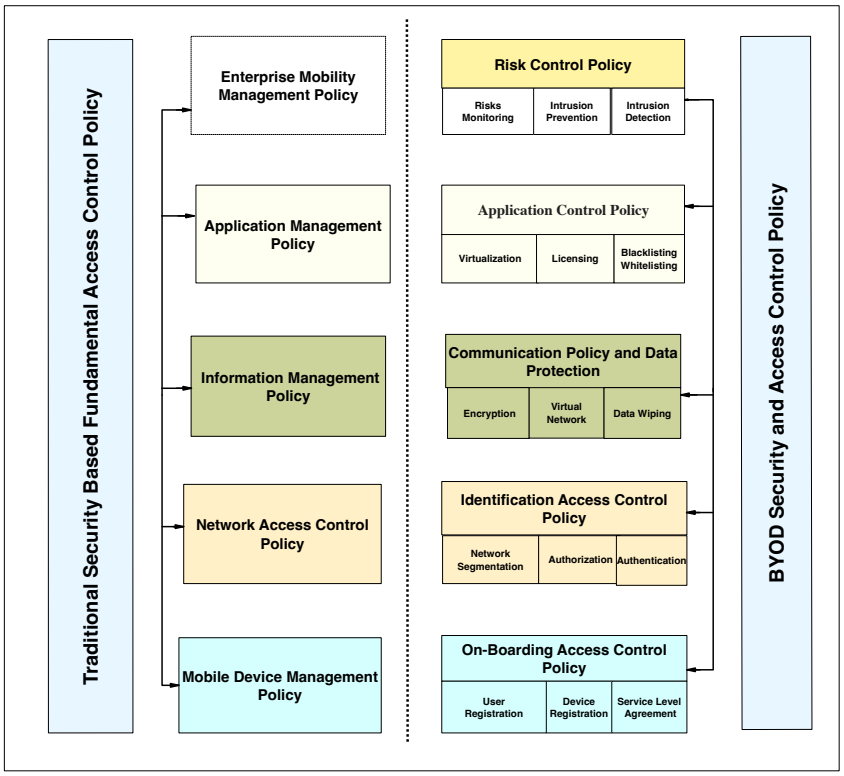

Figure 1. Comparison between traditional security policy and BYOD security.

Table 2. Comparison between traditional security policy and BYOD security.

Security Policy Approaches	Traditional Security	BYOD Security That Should Be Implemented
Mobile Device Management Policy.	✓	✓
Application Management Policy.	✓	✓
Information Management Policy.	✓	✓
Network Access Control Policy.	✓	✓
Enterprise Mobility Management Policy.	✓	✓
Security Communication Policy and Data Protection.	✗	✓
Private Network (VPN), Data Wiping and Data Backup.	✗	✓
Identification Access Control Policy.	✗	✓
Risk Access control policy.	✗	✓
Information Security Policy Compliance.	✗	✓
Comprehensive for the privacy requirements that the BYOD needs.	✗	✓

3.1. Traditional Security-Based Fundamental Access Control Policy Approaches

This section highlights and discusses several traditional management approaches and techniques utilised to control the security of organisational resources and avoid security risks to manage employee devices at work effectively. These management approaches can assist as security mechanisms, or solutions, that protect corporate networks, data, and devices while considering employees' privacy rights. The fundamental security policy approach for BYOD includes network access control policies, mobile device management policies, mobile application management policies, and enterprise mobility management policies. These access control policies may provide security mechanisms or solutions. Their shortcomings are detailed below.

3.1.1. Network Access Control Policy (NAC)

This technique focuses on the management and control of access to enterprise networks. NAC controls the devices that access the corporate network and provides secure and regulated network access to various devices from various locations. In addition, NAC can implement authentication and encryption security controls and integrate MDM tools into the network infrastructure to manage network services and resources and monitor the entire network. This strategy uses virtual local area network (LANs)to reduce network traffic by classifying users according to access control policies or functions [13]. Some network BYOD solutions, such as those developed by Cisco and Meru Networks, recommend BYOD management through network methods [13]. However, NAC is subject to the following limitations:

- Managing and accessing rich media material can contribute to network congestion.
- Malicious devices linked to the network can contaminate it.
- Malicious or infected devices can infect others on the same virtual local area network (VLAN).

3.1.2. Mobile Device Management Policy (MDM)

MDM, which manages and controls mobile devices, is based on a product or software platform [32]. MDM controls apps, cameras and the cloud on staff devices. Google Device Manager, Apple Profile Manager and Microsoft Exchange ActiveSync are among MDM technologies [13,33]. Organisations may use MDM to monitor, manage and secure mobile devices in the workplace by enforcing security requirements and ensuring devices conform to these regulations. The MDM approach can manage desktops, mobile devices and servers using the same tools. In addition, it can enforce device access regulations for all devices attached to the MDM platform. However, it has certain limitations, including:

- There is a limit on the number of devices and operating systems.
- Personal and corporate data might be combined.
- Third-party apps are required to utilise MDM functionalities fully.

3.1.3. Mobile Application Management Policy (MAM)

This differs from the MDM approach in that it controls, manages, and secures only specific enterprise software instead of the entire device. Consequently, a corporation may utilise MAM to protect and control email apps and other corporate applications on the mobile devices of its workers [33]. For instance, ZixOne is a mobile application that offers a BYOD solution, providing management access to business email via secure email encryption features [34].

3.1.4. Enterprise Mobility Management Policy (EMM)

This integrates MDM, MAM, and MIM capabilities. It is a solution for BYOD security that handles all devices, apps and data [34]. Enterprise mobility management EMM distinctive characteristics include separating work and personal data on the same device, managing threats proactively, and providing an application store for business apps. However, the EMM strategy has drawbacks such as:

- It combines all of the limitations and challenges of the strategies previously discussed.
- The user experience and satisfaction with BYOD may be compromised by this solution.
- By employing data separation techniques such as containers, corporate data can be vulnerable to security threats.

3.1.5. Mobile Information Management Policy (MIM)

MIM focused on managing BYOD-based data and documents that synchronise across many devices [33]. Mobile information management (MIM) is a device-independent security strategy that encrypts sensitive data and permits only authorised applications to access or transmit it. Mobile information management faces significant obstacles in enterprise mobility management.

3.2. Security Access Control Based on Three Layers (Ideal Security Policy)

This section will introduce the architecture of security policy layers and the control mechanisms present at each layer. According to Bello et al. [1], the security policy of BYOD is divided into three layers that organisations can manage to support comprehensive BYOD device management and security. These layers consist of the operational, tactical, and strategic layers. Figure 2 shows the three-layer BYOD policy. Each layer has a security control function and works with the other layers to manage BYOD information security and privacy. In addition, the protection function of each layer has many security control mechanisms. Bello et al. confirm in [1] that the three layers should be considered when implementing access control solutions between an organization's resources and BYOD devices in order to protect the environment from security and privacy threats, where each layer function is complementary to the function of the other layer to obtain optimal and comprehensive security, in addition to achieving the privacy and security requirements that the BYOD strategy needs, which include confidentiality, integrity, availability, authenticity, privacy preservation, non-repudiation, and attack detection. The operational layer is the primary layer, which focuses on the service level agreement (SLA) that the system owner proposes for the agreement's policies; also, BYOD users register their devices as an initial step. Following that, secure BYOD access control should be added to the tactical layer of policies concerned with authentication and confidentiality of the communication channel between the organization's resources and devices. Finally, applications should be subject to safe control policies. In addition, the strategic layer, an essential addition to the previous two, is responsible for detecting and monitoring employee-device-based attacks. Therefore, if organisations adopt a three-layer policy approach, they will achieve a more secure, competitive environment than traditional policies.

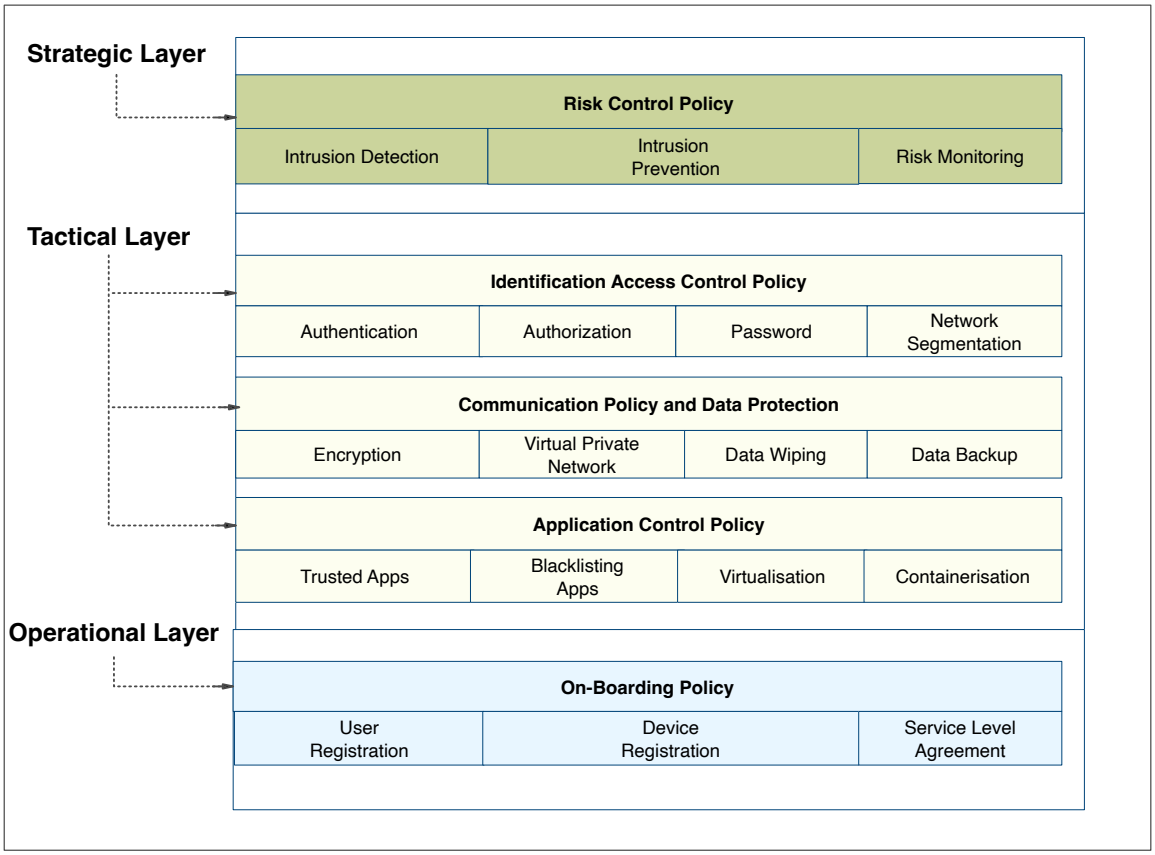

Figure 2. Secure Three-Layer Architecture for BYOD Access Control Policy [1].

3.2.1. Operational Layer

This layer encompasses onboarding access control, which facilitates the identification of authorized users who can access the organization's resources and network through their BYOD devices [1]. Within this layer, two key security functions are performed. Firstly, device account registration control allows users to create and register their accounts, requiring verifiable information such as employee ID, job role, and assigned services. Secondly, a service level agreement (SLA) is established, requiring BYOD users to agree to the terms of use and assume responsibility for the information and services provided by the corporate system.

3.2.2. Tactical Layer

The second layer, known as the tactical layer, encompasses a BYOD policy that focuses on authentication through access control, consisting of three key functions [1]. Firstly, the identification access control policy establishes access controls for BYOD devices to safeguard an organization's information services and resources from unauthorized access. Within BYOD ecosystems, activities such as illegal use or inappropriate communication in information-sensitive applications, including password authentication, authorization, and network segmentation, are strictly prohibited.

The second function is the security communication policy, also known as data protection. Its objective is to ensure the protection of confidential data while enabling secure and protected access, sharing, and transfer between BYOD devices and the organizational infrastructure. Various security control mechanisms, such as encryption, virtual private networks (VPN), data wiping, and data backup, are employed to achieve data confidentiality.

Thirdly, the application control policy is responsible for safeguarding organizations that adopt BYOD from malicious applications. The application management policy aims to prevent any confusion between personal and business data, allowing the exchange of

data between personal and company applications on BYOD devices. Control mechanisms such as virtualization, licensing, application blocklisting, application whitelisting, and containerization support this layer.

Overall, the tactical layer addresses multiple security requirements, including confidentiality, integrity, and prevention of unauthorized access.

3.2.3. Strategic Layer

The third layer, referred to as the strategic layer, encompasses a risk control policy known as risk-based access control. This policy focuses on safeguarding both BYOD devices and organizational resources from malware attacks, unauthorized access, and attacks originating from or transmitted through BYOD devices. It plays a critical role in detecting, preventing, and monitoring risks. Intrusion prevention systems (IPS) and intrusion detection systems (IDS) are examples of systems utilized within this layer to achieve these objectives [1].

4. Overview of the Privacy and Security Requirements in a BYOD Environment

Privacy requirements are the set of security and privacy requirements that BYOD security policies should achieve to provide sufficient security. Every decision made by BYOD users within an organisation is influenced by security and privacy, including permitting email on a personal device. However, this could expose the organisation to numerous risks and data loss. Employees are also concerned about how much personal data employers can access and use to control their devices, although enterprises are authorised to protect company data. Therefore, privacy requirements are insufficient for the organization's and BYOD users' security. The security access control in BYOD should consider the privacy and security requirements of both the organisation and BYOD users. Several security models have been proposed to overcome these challenges and concerns, including the CIA triad, which refers to confidentiality, integrity, and availability and is designed to guide information security policies that include confidentiality, integrity, and availability within an organisation. Also, the IAS-Octave has confidentiality, integrity, availability, accountability, auditability, authenticity, trustworthiness, non-repudiation, and privacy preservation.

The conventional CIA triad framework is inadequate for addressing emerging threats in shared environments such as BYOD, as evidenced by Mosenia and Ioannis's research [35]. The introduction of BYOD exposes organizations to various security risks, including email phishing attacks, embedded viruses in applications, and denial-of-service incidents. Consequently, the CIA triad framework fails to meet evolving security and privacy requirements, necessitating an upgrade to the more comprehensive IAS-Octave standard. Yahuza et al. [22] propose a combined approach that integrates the privacy requirements of the CIA triad model and the IAS-Octave model, as depicted in Figure 3. This upgraded model incorporates the IAS-Octave security requirements and introduces additional attack detection requirements. Muktar et al. [22] further suggest enhancing security and privacy requirements in edge computing, comprising eight essential privacy requirements, including the CIA and IAS-Octave standards, attack detection, and reliability. Adopting this same model while excluding the reliability requirement is advisable for BYOD security, as previous studies have not emphasized its significance, prioritizing other security and privacy requirements [1]. In the forthcoming sections, we will investigate each component of this model to improve privacy requirements and investigate their relevance to BYOD security.

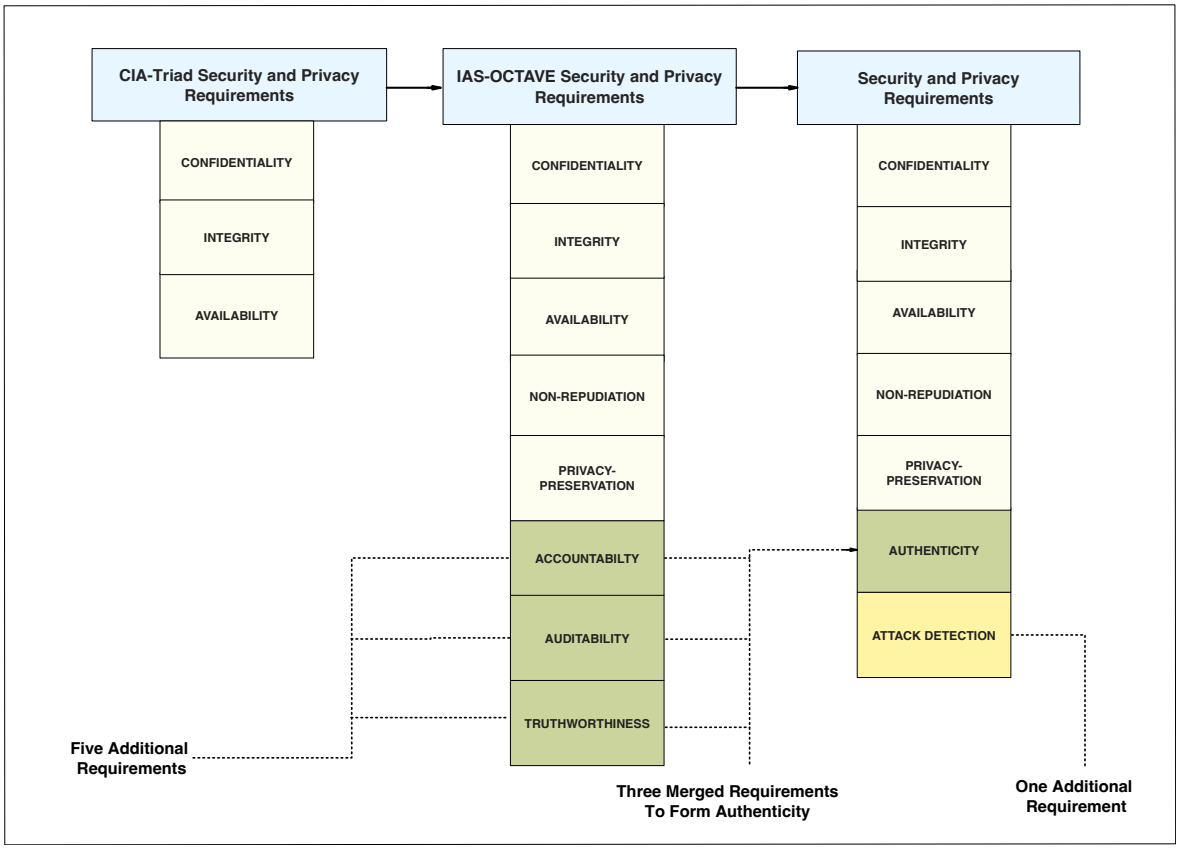

Figure 3. Development of BYOD security and privacy requirements [22].

4.1. CIA Triad Criteria Security and Privacy Requirements

The CIA triad, which encompasses the principles of confidentiality, integrity, and availability, serves as a fundamental model for the development of security systems [16]. These three categories, confidentiality, integrity, and availability, have traditionally formed a classification system for security and privacy requirements [16]. For several reasons, it is essential to include these requirements within the privacy guidelines for BYOD. Firstly, confidentiality plays a critical role in ensuring security and privacy [36]. Its primary objective is to prevent unauthorized access to sensitive company information. Cybersecurity issues may arise because BYOD devices and enterprises are connected to the internet. For instance, the man-in-the-middle (MITM) attack represents one of the threats targeting the security of BYOD users. This attack aims to intercept and steal information exchanged between two parties. Secondly, the integrity requirement ensures that data is only accessible to authorized BYOD devices and remains unmodified. Preserving data integrity becomes challenging in BYOD scenarios, as the organization loses visibility and control when a BYOD device operates outside its network, leading to potential data corruption or loss [37]. Therefore, integrity is a fundamental security requirement for organizations employing BYOD devices [38]. Lastly, availability emphasizes the continuous accessibility of devices, data, and resources, ensuring that BYOD devices always have secure access to services. In cases of an unexpected surge in data traffic volume, client-server communications may suffer from data loss [39].

4.2. IAS-Octave Security Criteria and Privacy Requirements

The IAS-Octave classification extends the CIA triad framework by introducing additional security requirements: accountability, auditability, trustworthiness, non-repudiation, and privacy preservation [22]. Accountability and auditability contribute to establishing trustworthiness, which is closely associated with the authenticity requirement. Alternatively, it has been proposed that these three requirements can be combined to

form the concept of authenticity [22]. Therefore, authenticity is essential to the standard set of privacy and security requirements for BYOD. It ensures accurate monitoring and verification of BYOD users' identities, establishing trust between BYOD devices, organizations, and their resources. Additionally, including privacy-preservation and non-repudiation requirements is crucial as part of the BYOD security framework. Privacy preservation ensures the security and monitoring of all information, end users, networks, and resources involved in the organization's BYOD implementation. On the other hand, non-repudiation guarantees that a BYOD device cannot later deny its signature's validity or an event that occurred within the organization. This requirement aids in tracing the origin of any BYOD device that poses security issues [40]. Thus, the privacy requirements for BYOD are derived from the CIA triad model and supplemented with three additional standards from the IAS-Octave framework: privacy preservation, non-repudiation, and authenticity.

4.3. Addition of Attack Detection Requirements

In the context of BYOD devices, "attack detection" refers to identifying and mitigating potential threats. When employees bring their devices to the office and connect them to the wireless network, there is a risk of theft and other malicious activities. Security threats such as phishing, malware, and potentially spreading infected devices through BYOD can compromise a company's security [41]. Hence, the security and privacy requirements for BYOD should include provisions for attack detection. Attack detection requirements are necessary to meet the required level of security by identifying and preventing attacks before they occur [42]. Also, Bello et al. [1] highlight the importance of incorporating attack detection requirements into BYOD security policies, particularly concerning risk access control policies discussed in a previous section. Attack detection requirements are intrinsically linked to risk-based access control policies, as illustrated in Figure 3. The attack detection criteria should be integrated into the existing privacy requirements and are crucial as they address the negative aspects of implementing the BYOD concept in organizations. This helps mitigate significant challenges such as attacks, risks, unauthorized access, data leakage, and user privacy concerns. By incorporating attack detection along with privacy and security requirements, organizations can effectively tackle these challenges and enhance the security of their BYOD environments. This study examines access control policies and techniques in the context of BYOD based on the privacy requirements that have been met. The aim is to determine the privacy requirements that have been thoroughly examined and to encourage researchers to enhance and propose techniques that align with privacy requirements that may need more attention and require further investigation. Table 3 comprehensively describes the privacy criteria that will be evaluated during the review process. Furthermore, Figure 3 illustrates the advancements in privacy and security requirements for BYOD security.

Table 3. Security and privacy requirements in the BYOD environment [22].

Requirement	Description
Confidentiality	Ensures that unauthorized individuals are prevented from accessing shared data within BYOD-enabled organizations.
Integrity	Ensures that data is delivered exclusively to authorized BYOD devices without any unauthorized modifications.
Authenticity	Ensures accurate monitoring and verification of BYOD users' identities, fostering trust between the BYOD devices, organizations, and their resources.
Nonrepudiation	Ensures accurate monitoring and verification of BYOD users' identities, fostering trust between the BYOD devices, organizations, and their resources.
Privacy-Preservation	Ensures the secure and monitored storage of all confidential information related to BYOD devices, including end users.
Attack Detection	ensures the timely identification and effective mitigation of any security breaches or threats targeting BYOD devices.

5. SLR Methodology

This study has conducted a systemic literature review (SLR) following Kitchenham's recommendations [43]. The literature analysis process consisted of five steps before the review:

Step 1: Define research questions and objectives to give the study a broad scope.
Step 2: Determine a search strategy for published research in available digital libraries.
Step 3: Employ a screening process that uses inclusion and exclusion criteria to decide which studies to include.
Step 4: Perform classification and data extraction, aided by keywording.
Step 5: Extract and map data.

In addition, the preparation, collection, retrieval and implementation processes were conducted to identify any study discrepancies in the previous literature and thereby contribute to the subsequent study. The primary purpose of this search was to find publications that investigated BYOD security policy techniques based on security and privacy requirements. Figure 4 illustrates the measures taken in the methodology of the analysis work.

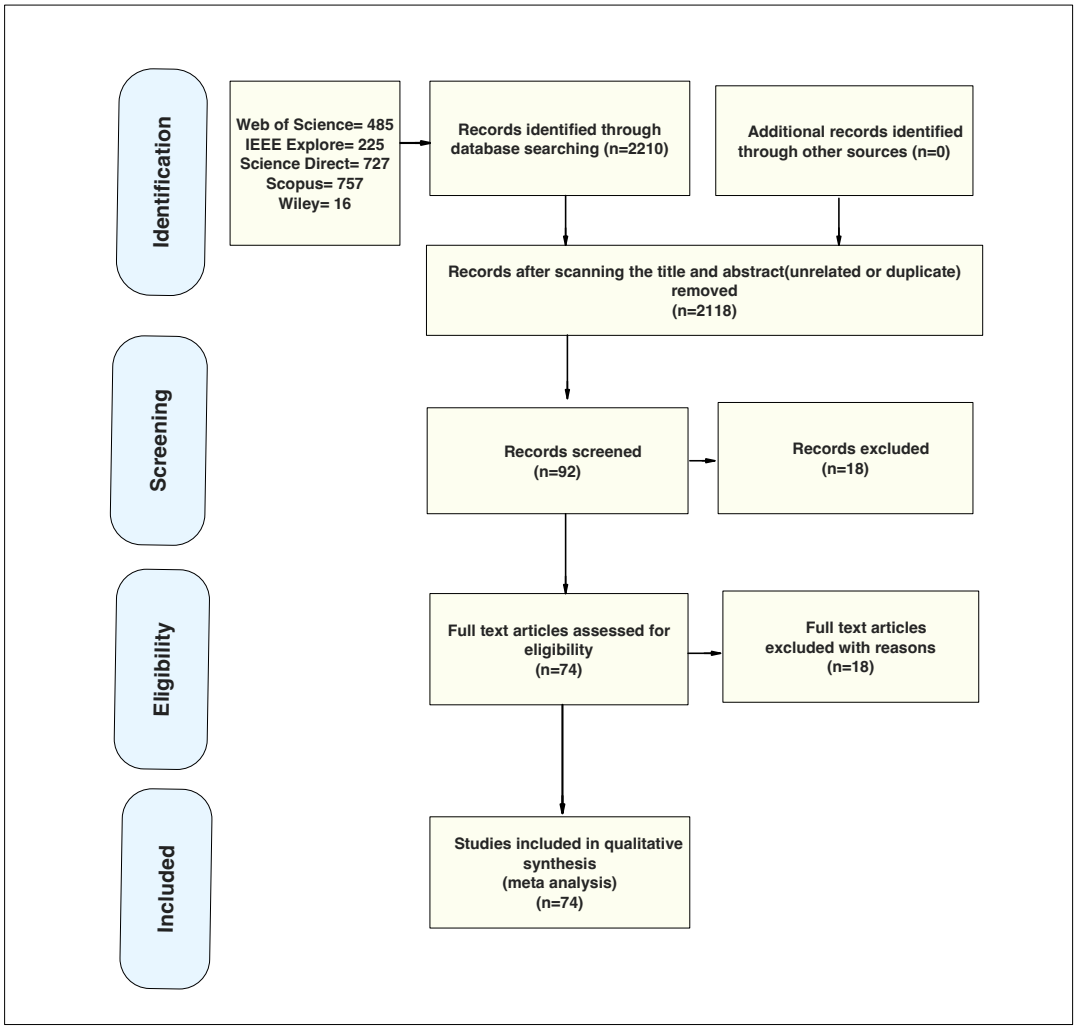

Figure 4. Flowchart of the systematic review process.

5.1. Research Questions and Objectives

This study aims to highlight the results of existing primary studies published on security policy techniques and privacy in the BYOD environment to identify current trends and open issues in the domain. Table 4 shows our research questions and the objectives of each research question.

Table 4. Research questions and objectives.

Research Question	Research Objective
RQ1: For BYOD environments, what is the classification of privacy and security criteria?	To define the security and privacy requirements to ensure the highest level of security for the data of enterprises and BYOD users.
RQ2: What policy techniques are employed to ensure security and privacy requirements have been identified?	To analyse existing solutions to security policy techniques in terms of the three layers of BYOD security policy that are used to achieve specific security and privacy requirements.
RQ3: What are the trends in technological methods used by the identified techniques?	To identify trends in technological approaches used by the indicated methodology.
RQ4: What evaluation procedures should use to evaluate the performance measurement of technologies?	To determine the appropriate evaluation metrics used in evaluating the performance of technologies.
RQ5: What future research opportunities and gaps exist in the security policy and privacy field in BYOD for researchers?	To identify the currently open issues for privacy and policy issues in BYOD.

5.2. Data Search Strategy

All defense policy research, including analysis and technical studies, was thoroughly searched in the BYOD environment. Five major electronic databases, including the Web of Science, IEEE Explore, Wiley, Science Direct and Scopus, were used in the research. The quest was limited to technology, computer technology, informatics, and engineering. In addition, the boundaries of the analysis were limited by the subject areas. The first search was conducted by screening conference papers and journals published between 2015 and June 2022. The search was restricted to the five online electronic databases. To build a search query, specific keywords with similar meanings were used. The queries were then followed up in three phases: title, abstract scanning and reading of the full text. The three phases of an inquiry are detailed below:

- "Bring your own device" OR "BYOD" AND "Security Policy" OR "Policy" AND "Security and Privacy"
- "Secure*" AND "Policy Techniques " AND "Bring your own device" OR "BYOD"
- "Access control" AND "BYOD" OR "Bring your own device" AND "BYOD" OR "Bring your own device"

5.3. Criteria for Study Selection

The inclusion criteria were established to ensure well-defined boundaries of the review topics and to facilitate article selection. The search criteria included collecting applicable data from journal articles and conference papers published in public databases from 2015 to June 2022 (see Table 5). There were a total of 2208 posts found initially. These were from Science (485), IEEE Explore (225), Science Direct (727), Scopus (757) and Wiley (16). Next, the title and abstract of the papers were scanned. Following the scan, 2118 papers were found to be outside the scope of the review and were excluded. The remaining 90 papers were subsequently selected through inclusion and exclusion procedures. If an article met the criteria of inclusion set out in Table 5, it was eligible for inclusion. Otherwise, it was excluded. The remaining 92 publications were scrutinised after the full-text review. Several articles were subsequently removed, leaving 74 articles for inclusion. The reason for including these articles was that they addressed the study's objectives, which were access control and policy techniques in terms of three layers and privacy requirements, and they met the established inclusion criteria.

Table 5. Inclusion and exclusion criteria.

Inclusion	Exclusion
IC1: Papers related to research questions.	**EC1:** The papers do not address security policies based on BYOD.
IC2: Papers from journals or conferences.	**EC2:** Techniques and models used in the security policy are not addressed.
IC3: Papers are written in English only.	**EC3:** Duplicate papers.
IC4: Papers published between 2015 and 2022.	**EC4:** Full text is unavailable.
IC5: The full text is available.	**EC5:** Non-English.
IC6: Articles that present techniques and models of security policy in a BYOD environment.	**EC6:** White papers, chapters in books and magazines.

5.4. Data Extraction

The 74 papers that met the inclusion criteria were reviewed to summarise relevant data that addressed the research questions. As a result, the following are documented: the authors, the publication year, the type of article, the policy technique under a specific category of security and privacy requirement, the category of technological approaches used and the performance metrics used in evaluating the proposed technique's performance. Additionally, the flaws of each recognised technique provided research opportunities.

6. Data Analysis

This section examines all the research that fulfilled the inclusion requirements. Section 6.1 describes general data analysis. In addition, Section 6.2 conducts an analysis to address the research questions. According to RQ1,the classification of privacy and security criteria is examined and discussed in this Section 4. This study found that seven security and privacy requirements identified to meet the needs of the BYOD organization's security and privacy users include confidentiality, integrity, availability, non-repudiation, authentication, privacy preservation, and attack detection. The RQ2 is related to analyzing access control techniques based on security and privacy requirements. These were then divided into three categories. The first are techniques that meet one of the security and privacy requirements; the second are techniques that meet more than one requirement; and the third are techniques that do not meet any requirement. In addition to RQ3, which identified policy techniques used to ensure security and privacy requirements that achieved RQ4, evaluate performance measurement, and RQ5, related to performance evaluation metrics, are discussed in detail.

6.1. Analysis of General Data

The review included 74 papers from various journals and conference proceedings indexed in five electronic databases. The percentage of papers published from 2015 to 2022 is shown in Figure 5. According to the review results, research on security policy techniques in the BYOD environment only gained popularity in 2017. Fifteen percent and 17 percent of all publications in 2017 and 2018, respectively, were found in journals. Journal articles accounted for 17 percent of all publications identified from review efforts in 2020. From 2021 to December 2022, this rose to 20 percent, suggesting more researchers had become interested in the field. Figure 6 illustrates the distribution of publications throughout the various databases covering a wide range of subjects. WOS provided the majority of the articles, followed by the IEEE database. Scopus was the second most popular database, followed by Science Direct and Wiley, with the lowest percentages.

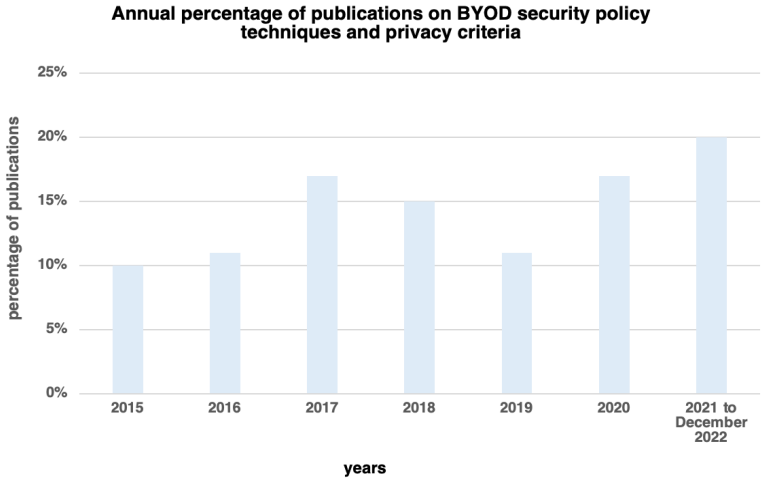

Figure 5. Percentage of publications related to BYOD security policy techniques per year.

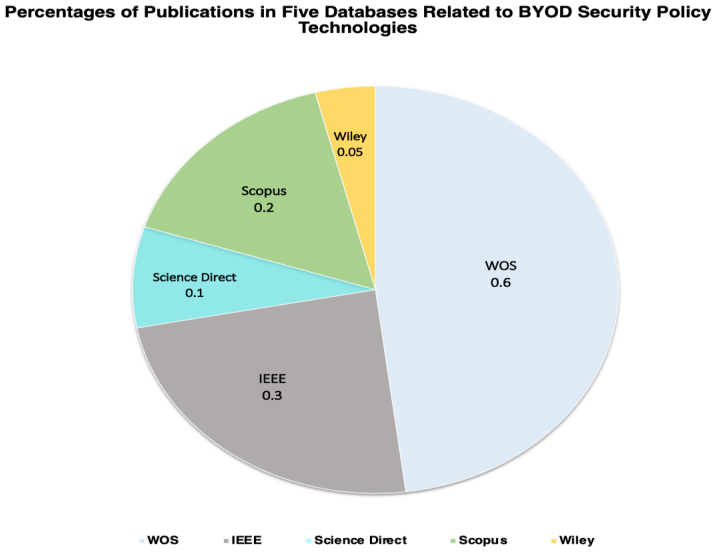

Figure 6. Percentages of publications in five databases relevant to security policy in BYOD.

6.2. *Analysis of BYOD Security Policy Techniques Based on Privacy and Security Requirements*

The purpose of this section is to present an analysis of the results. Firstly, we analysed existing policy techniques based on privacy and security requirements to ensure specific criteria were met. Then, we examined the trends in technical approaches used by the methodologies identified. According to the prior studies of policy techniques in BYOD security, the analysis was divided into three categories based on the privacy requirements they fulfilled. The first group includes technologies that meet one of the privacy requirements, such as techniques that achieve authenticity, confidentiality, and attack detection, as discussed in Section 6.2.1. In the second group, some techniques address more than one requirement, such as confidentiality and authentication, confidentiality and attack detection, and others that combine the requirements for authentication, attack detection, and confidentiality as explained in Section 6.2.2. The third group relates to security policy methods that did not address any of the suggested privacy requirements as stated in Section 6.2.3. Finally, our analysis identifies the performance measures and metrics that evaluate the effectiveness of the techniques discussed in Section 6.2.4. In addition, the tables summarize techniques within specific categories of privacy and security requirements, providing a brief overview of the methodology, the technology used, the performance assessment analysis, the main advantages and the limitations. Table 6 summarises the techniques that address the authenticity requirement. Moreover, the techniques that address confidentiality

requirements based on cryptography are summarised in Table 7. Table 8 summarises the techniques that address confidentiality requirements based on isolation. The techniques that address the attack detection requirement are investigated in Tables 9 and 10. Table 11 focuses on approaches that address more than one criterion. Table 12 summarises the technologies that do not meet the privacy as mentioned above and security standards. Finally, Tables 13 and 14 summarises the performance measures and evaluation metrics used to evaluate the effectiveness of the techniques mentioned.

Table 6. Summary of authentication techniques.

Ref	Technology Employed	Performance Analysis	Advantage	Limitation
[44]	MDM-based model.	Prototype implementation.	It can identify whether the BYOD device is disabled or enabled.	Only a limited number of devices and operating systems.
[45]	Pattern lock method and four-digit PIN(CirclePIN).	Experiment analysis and real dataset.	Protect against side-channel, shoulder-surfing and single-recording threats.	Less secure technologies.
[46]	Based on WPA2-Enterprise.	Experimental analyses, case study.	It eliminates shared password risks.	Increase processing power.
[47]	Set policies based on IEEE 802.1X/Certificated.	Case study of a Greek school.	Introduces security issues and their resolution.	Secure but vulnerable if authentication policies are simple.
[48]	Co-proximity authentication protocol(fingerprint sensors and biometric).	Prototype implementation and behavioural, biometric dataset.	Context-aware authentication.	Complex and time-intensive.
[49]	EZ-Net system.	Experimental analysis, Case study on campus.	Low-cost, high-performance.	Each user's monthly authentication time is limited.
[50]	Lightweight network access control (NAC) module.	Prototype implementation, OpenWrt, NAC module.	Improves administrator management and OpenWrt is a free wireless router.	Unsuitable for all systems.
[51]	Pseudo-code-based two-factor authentication.	Mathematical analysis.	Simple to implement and inexpensive.	It is difficult to do while utilising a mobile phone rather than a laptop because the keyboard is different.
[52]	NFC technology.	Simulation (computer simulation experimental).	More secure, fast and convenient authentication.	Limited number of nodes.
[53]	AppShield scheme, certificate-based authentication.	Prototype implementation, synthetic dataset (1000 data access operations).	Most secure BYOD infrastructure control.	Complicated and time-consuming.
[54]	Fine-grained security policies (set policy as an individual, group for user and device).	Prototype implementation.	Very low cost.	Network address interpretation is weak.

Table 7. Summary of cryptographic techniques.

Ref	Technology Employed	Performance Analysis	Advantage	Limitation
[55]	Cryptography-based algorithm (self-encryption).	Prototype implementation, (Encryption and decryption for Several files).	Effective in data storage units in enterprises that use BYOD.	Limitation in the execution time, compression.
[56]	RSA-based algorithm, property-based token attestation (PTA).	Mathematical analyses, a scyther tool for verification.	Secure enterprise network access.	Cloudlet-based BYOD models require modification of this PTA protocol.
[57]	MAC-based algorithm (symmetric key cryptographic), file-grained data.	Prototype implementation.	Sets policy rules in the endpoint and achieves confidentiality.	Makes use of the shared key.
[58]	ABE scheme-based algorithm.	Algorithmic proof.	Confidentiality.	Time increase due to sensor data collection and processing to determine attributes.
[59]	Based on the algorithm (RSA-Tokens).	Prototype implementation and Private cloud.	It reduces authentication time and information exchange from 3000 ms to 2000 ms using TLS.	It transfers data slowly.
[60]	Based on symmetric algorithm.	Prototype implementation.	BYODENCE is low-cost and delivers high accuracy and speed.	More complex.

Table 8. Summary of isolation techniques.

Ref	Technology Employed	Performance Analysis	Advantage	Limitation
[61]	VNF scheme-based virtualization technique.	Prototype implementation and testing in real word network.	Improved security, mobility, and response time with virtual and dynamic networks.	Synchronization of physical and virtual security.
[62]	Remote mobile screen (RMS) system based virtualization method.	Experimental analysis.	RMS ensures data confidentiality, policy compliance and space isolation.	It poses numerous security risks.
[63]	vNative-based virtualization method.	Prototype implementation, evaluation testbed configuration.	Data confidentiality and isolation.	Limited availability of BYOD/mobile devices.
[64]	Multi-level architecture for isolation.	Experimental analyses.	Provided privacy for android end-user.	The solution is only for android.
[65]	Brahma-based virtualization method.	Prototype implementation (KVM Module, Zenfone).	Privacy.	Less security.
[66]	EMM, SDN and NFV.	Prototype implementation.	SDN can enhance NFV performance with virtualization.	SSDN and NFV are independent.
[67]	MSS system-based virtualisation method.	Experimental analysis.	MSS secures sensitive data and security activities in a separate domain.	The MSS is only for one environment.
[68]	MSS system.	Experimental analyses.	Confidentiality.	Low cost.

Table 9. Summary of the attack detection techniques.

Ref	Technology Employed	Performance Analysis	Advantage	Limitation
[69]	Risk access scheme, NGFW technique based deep-packet inspection firewall.	Experiment analyses and Case study (Tokyo University).	Reduces costs while increasing security.	It is weaker because package content should be verified instead of only filtered network traffic.
[70]	Forensics investigation method.	Experiment analyses, real dataset (Android log).	Works well to detect and analyse BYOD malware.	Only deal with log files without applications.
[71]	Forensic investigation model.	Simulation performed in three stages (computer, simulation, and experimental)	tracked BYOD user's traffic.	Forensic investigation requires an end-to-end ecosystem.
[72]	Clustering algorithms	Simulation, public malware dataset, branchy model.	High precision and lower traffic.	long training time.
[73]	Risk-detection-based ML random forest algorithm.	Experimental analysis, tested by comparing infected, unaffected android, public malware App dataset.	The method examines the whole issue to see if BYOD is legal.	Less efficient.
[74]	Risk access control model based on a risk estimation algorithm (fuzzy model)	Prototype implementation and Smart contracts dataset.	Making access decisions based on anomalies.	The method requires further development.
[75]	Andrologger tool.	Experimental analyses, Real dataset.	Automatically sending BYOD data and user actions to the company's server for analysis.	The method only works on android phones.
[76]	OPPRIM-based risk policy model	simulations (AnyLogic), Mathematical Analysis.	Adaptability, cost reduction.	Simulating risk will result in conservative behaviours from attackers.
[77]	Neural network-based algorithm to detect HTTP botnets.	Simulations (Anylogic), Drebin dataset, PRISM model checker and Mathematical analysis (Correlation).	High accuracy.	Complexity.
[78]	IDS model-based ML algorithm.	Prototype implementation, NSL KDD dataset.	Able to detect DoS, probing and torrent traffic.	The dataset quantity is large.
[79]	Behaviour-based abnormality detection model, Pattern Analysis (data mining).	Mathematical analysis.	Analyzing user behaviour to detect abnormal behaviour.	High false alarm rate.
[80]	System based SDN.	Simulation (NS2), attacks dataset (SYN attack, ICMP flood, Dos attack).	Self-adaptive network can defend against internal threats and reduce attack reaction time.	Should be extended and improved to detect sophisticated APTs.
[81]	Malware identification scheme based supervised classification algorithms/ML.	Prototype implemented-android applications dataset.	High accuracy.	The decision limit may be overtrained.
[82]	MUSES framework based fuzzy Logic, ML.	Prototype implementation.	Enhanced security and provided intrusion detection systems.	Difficult interpretation.

Table 10. Summary of the attack detection techniques.

Ref	Technology Employed	Performance Analysis	Advantage	Limitation
[83]	ANN algorithm (deep learning).	Experimental analysis, Real data from the Media Lab of MIT dataset (incoming, outgoing, type of call).	Precision and accuracy of over 99%.	ANN has difficulty converting data into numerical values.
[84]	Border patrol system.	Prototype implementation, 2000 apps of Google Play an android emulator.	Introduced new policies for corporate networks to manage organised activities.	Limited ability to block malicious apps.
[85]	Anomaly detection method based ML algorithms.	Prototype implementation, a proof-of-concept and Spark dataset.	Detecting intrusions and anomalies.	Need more verification.
[86]	CVSS system-based decision engine logic algorithm.	Simulation (Computer simulation and experimental).	Privacy for the infrastructure layer.	The assessment time is still a major concern.
[87]	IFT technique based on a clustering algorithm/ML.	Experimental analyses, Public data set containing packet IAT features.	Employed the packet inter-arrival time feature to detect abnormal behaviour.	Need to improve the algorithm within large datasets.
[88]	Real-time traffic classification system based on ML.	Experimental analyses, proof of concept and real dataset.	Employed a fine-grained, real-time traffic classification.	Required a change in the entire network infrastructure to implement SDN protocol.
[89]	Detection technique-based novel algorithm.	Prototype implementation.	Reduced network risk and increased BYOD infrastructure security.	The analysis should include traffic instead of just the login log.
[90]	Other methods (white box method).	Prototype implementation.	Benefits both end-users and organisational use.	Exploiting apps makes security testing difficult.
[41,91]	DFRM model based honeypot technology (digital forensic readiness).	Prototype implementation.	Efficient method.	limited in digital evidence.
[92]	DFR framework-based honeypot technology.	Prototype implementation.	DFR improves BYOD security and reduces issues.	Honeypots only gather data when attacked.
[93]	Roving proxy server framework.	Prototype implementation and SMS spam dataset.	Efficient with a small dataset.	Need more work on a massive dataset.
[94]	Classification framework.	Correlation analysis, Real malicious traffic logs.	Useful for the network administrator.	Only classifies cyber-attack patterns and not types.
[95]	Based on dynamic decision tree algorithm (ML).	Experimentation and IBM's internal network dataset.	Reducing enterprise risk.	Limited application installation.
[96]	Network scanning technique-based algorithm.	Proof-of-concept, Experimental analysis and Public dataset(Attack)	Preventing network eavesdropping and spoofing.	It should be implemented on the switch for better security.
[97]	SIDD system.	Prototype implementation, network attacks dataset (e.g., zero-day, worms, DoS).	Validate up to 99% and help to detect zero-day malware.	Should be applied to various attacks to ensure effectiveness.
[98]	ARANAC, a Novel access control	Experimental analysis, Case study using more than 80 Android devices at a university campus	ARANAC has monitoring, risk estimation, and attack detection modules.	Need to extend the model to estimate risk values for the remaining features.

Table 11. Summary of techniques based on multiple security and privacy requirements.

Privacy Requirements	Ref	Technology Employed	Performance Analysis	Advantage	Limitation
Confidentiality and Authentication.	[99]	AES,HMAC algorithm	Prototype implementation.	Authentication-based cryptography secures networks and users.	Certificate management challenges.
Confidentiality and Authentication.	[100]	Optimizing and encrypting Schema-Based Access Control.	Prototype implementation.	Protects data from key leakage.	Secure but complicated.
Confidentiality and Authentication.	[101]	Biohashing technique.	Mathematical analysis, Experimental.	Increases security and lowers error rates.	Data increases collision probability.
Attack Detection, Authentication, and Confidentiality.	[102]	SDN and 2FA (TOTP)-based virtualization method.	Prototype implementation, Proof of concept.	Security and assault reduction.	ARP spoofing is the only attack allowed with this method.
Confidentiality and attack detection.	[103]	PHE encryption, tracing, and revoking (tracing algorithm, public revocation algorithm).	Simulation, experimental analysis (an RBAC simulation system with ten classes and around ten users per class).	Tracking and key service interruptions provide safety.	It needs big master public keys.

Table 12. Summary of the techniques that did not consider any of the proposed requirements.

Ref	Technology Employed	Performance Analysis	Advantage	Limitation
[104]	Enforce access control policy architecture.	NA	Simple policy.	It is only a preliminary proposal that needs implementation
[105]	STRIDE-based BYOD threat model.	NA	Help understand how BYOD concerns affect corporate data	Only provides an initial model.
[106]	An investigation framework.	Safe-Logic experts evaluated based on particular criteria.	Excellent awareness of BYOD threats and solutions.	Only provides an initial model.
[107]	Proactive approach based GQM (goal, question, metric).	NA	Creating benchmarks for BYOD security protocols.	Only identified security metric.
[108]	OPPRIM model.	Mathematical analysis and quantitative model.	Integrating trust and risk management mechanisms with threat analysis	Only provides an initial model.
[109]	Poise policy for device, app.	Prototype implementation.	It is network analysis.	It should build and test a complete prototype.
[110]	Fine-grained policies (BYODroid model).	Case Study.	Apply policy on the infrastructure layer.	Implementation is needed to verify rules.
[111,112]	Security architecture.	Case Study.	Flexible and adaptable to various business fields.	Only provides a starting point.
[113]	Metamodeling techniques.	Case study (Interview domain experts at the Ottawa Hospital to validate).	Identify key BYOD risk assessment metamodel concepts.	Initial and limited architecture.
[114,115]	Other methods (middleboxes and alert systems).	Prototype implementation.	Accurate transparency, usability, and performance with HTTPS security.	It is only a preliminary proposal that needs implementation.
[116]	Plugin Framework Based fine-grained security policy.	Prototype implementation.	Allows correct security policy execution on any device connection network organisation.	No other systems (only Android).
[117]	BYOD security framework	Case study (Australian, questionnaire instrument)	Building new framework to improve attack and threat defence.	Discusses only the theoretical aspect.

Table 13. Summary of evaluation metrics.

Ref	Requirement under Consideration	Purpose for the Evaluation	Evaluation Metrics
[44,46,47,50,51,54]	Authenticity.	To evaluate the functionalities of the authentication policy.	Access Response (Deny or Permit).
[45]	Authenticity.	To evaluate the possibility of an authentication policy for preventing unauthorized access.	Authentication Time, Access Response and Error Rate.
[48]	Authenticity.	To evaluate the performance of biometric authentication.	Accuracy and Frequency Detection Latency.
[49]	Authenticity.	To evaluate the functionalities of the authentication policy.	Response time and Cost.
[52,53]	Authenticity.	To evaluate the performance of the authentication system.	Performance, Memory Consumption, CPU consumption, Time overhead and Code Size Execution Time.
[55]	Confidentiality.	To reduce the time when switching the key.	
[67,68]	Confidentiality.	To evaluate the performance measurement of the MSS system.	Time and Performance Measurement.
[69]	Attack detection.	To evaluate the possibility of reducing management costs for Wireless Network Monitoring.	Cost.
[72]	Attack detection.	To evaluate the possibility of reducing costs and improving detection accuracy and efficiency.	Detection Accuracy and Cost.
[73,81]	Attack detection.	To evaluate the accuracy of detecting a specific malware and abnormal application class.	Accuracy.
[74]	Attack detection.	To evaluate the risk value associated with each access request.	Risk Value, Scalability and Context Awareness
[76]	Attack detection.	To determine the impact of threat and opportunity estimations on the risk.	threat probability.
[77]	Attack detection.	To evaluate the rate of detection and accuracy.	Accuracy and rate of detection
[78]	Attack detection.	To evaluate the model's accuracy for detecting peer-to-peer traffic from torrent clients.	Accuracy and usability.
[79]	Attack detection.	To evaluate the ability to classify abnormal behavior.	Behaviour occurrence probability.
[80]	Attack detection.	To evaluate response time against internal threats.	Delay time.
[83]	Attack detection.	To evaluate the system's ability to detect unauthorized access.	Precision (PPV), recall (TPR) and accuracy (ACC).
[84]	Attack detection.	To evaluate the ability to block unwanted application functions selectively.	Overhead and latency
[85]	Attack detection.	To evaluate RAM and CPU consumption over time.	RAM usage over time. CPU usage over time.
[86]	Attack detection.	To evaluate time duration and vulnerability assessment against the cyber threat.	Time and score assessment.

Table 14. Summary of evaluation metrics.

Ref	Requirement under Consideration	Purpose for the Evaluation	Evaluation Metrics
[56]	Confidentiality.	To evaluate the performance of PTA protocol.	Computation cost and performance consumption.
[57]	Confidentiality.	To evaluate the response time for each subsequent request.	Execution time, complexity of the access policy and block size.
[58]	Confidentiality.	Protecting BYOD users and network privacy with practical effect on communication performance.	Time complexity, communication costs and communications complexity.
[59]	Confidentiality.	To ensure the proper handshaking time between clients and serves.	Cost and exchange key time.
[61,64]	Confidentiality.	To reduce the delay in access time and run time.	Access time, power consumption and switching cost.
[62]	Confidentiality.	To evaluate the scalability of the approach.	CPU usage, memory usage and boot time.
[65]	Confidentiality.	To evaluate memory resource usage and power consumption due to virtualization.	Run-time memory usage and power consumption.

6.2.1. Techniques that Satisfy Only One of the Privacy and Security Requirements

This section describes the findings of previous studies related to proposed policy technologies based on how well they meet privacy and security criteria. As stated in Section 3.2, the requirements for BYOD security were classified into seven categories.

These are confidentiality, integrity, availability, non-repudiation, authentication, privacy preservation, and attack detection. These requirements contributed to the creation of the review-related taxonomy. Figure 7 illustrates the taxonomy of security policies and privacy techniques based on the security requirements in BYOD environments, which include the seven categories described above. It can be seen that some techniques address one aspect of privacy and security criteria. For instance, confidentiality requirements have been met through cryptographic techniques and isolation techniques. Authentication algorithms can address authenticity requirements. Machine learning algorithms, deep learning algorithms, and SDN techniques have accomplished attack detection requirements. According to the review's findings, a technique that satisfies integrity, privacy, availability and non-repudiation requirements alone cannot be produced. As seen in Figure 7, we labelled this with the symbol NA, indicating non-availability. After analysing and categorising previous research results, we failed to identify any research that addressed just these categories. Other researchers have focused on the privacy and security needs of authenticity, confidentiality, and attack detection but failed to consider all the privacy and security requirements that BYOD demands. In the following section, we will examine security policy strategies that only address a single privacy and security criterion and summarize previous research.

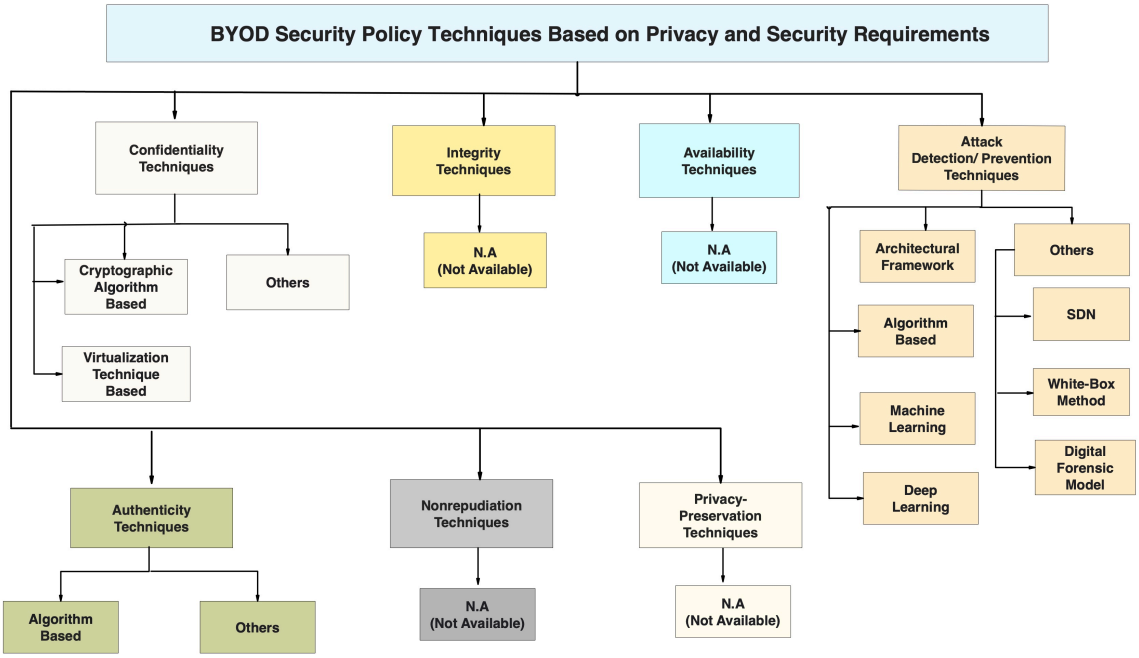

Figure 7. The taxonomy security policy and technological trends based on privacy requirements.

A. Techniques Based on Authenticity Requirements:

Authenticity requirements refer to verifying the identification of a user, process, or BYOD device and are frequently required before granting access to resources in an environment [118]. Many companies believe that the BYOD concept benefits both individuals and enterprises. However, the primary security issue is how to restrict BYOD device access to organisational information. As a result, when a BYOD client accesses a company network via their device, the device must be authenticated in some way. Lee et al. [44] proposed a secure authentication for BYOD devices that would be able to select disablers and enablers, determining if a BYOD device is either a disabler or an enabler. The proposed solution involved a mobile application acting as an MDM client, connecting to a server-side MDM server. However, the proposed method is only compatible with a limited number of devices and a specific operating system. Guerar et al. [45] presented CirclePIN, a novel authentication technique geared towards BYOD, particularly smart watches, that is both

resilient to most common threats and was highly rated in actual tests with real users. It enhanced authentication between BYOD and the company network and gave protection against unauthorised access. However, it still performed at a similar level to other less secure alternatives. The review also showed that previous researchers had put much effort into achieving authenticity based on authentication techniques. In Table 6, a summary of the technology used, performance analysis, advantages and limitations is presented.

B. Cryptographic Techniques Based on Confidentiality Requirements:

Confidentiality requirement refers to the protection of organisational data from unauthorised parties' access to records. In other words, it ensures that no unauthorised users can access the data shared in BYOD-enabled enterprises. Therefore, in BYOD situations, encryption mechanisms should be seen as the first line of defence that must be in place to protect company data. Previous researchers have studied confidentiality requirements based on cryptographic techniques. For example, Vinh et al. [56] implemented property-based token attestation (PTA) to protect users and company networks in BYOD environments. These data are processed as binary and property-based attestation and the method is effective in data storage units in enterprises. Nevertheless, the PTA protocol must be changed to make a more secure BYOD model based on the Cloudlet idea. Rahardjo et al. [55] implemented the self encryption algorithm into various applications. However, the proposed method has limitations in terms of execution time and compression. Catuogno et al. [57] addressed the problem of preserving data access control over a mobile device's storage space while running different and distinct third-party applications. To that end, they proposed a general-purpose protected file system capable of providing fine-grained data protection at the operating system level. Facilities for trusted execution environments (TEE) are used for data encryption, critical protection, and policy compliance, providing safe access to corporate networks. Table 7 represents additional efforts made by researchers to accomplish confidentiality requirements using cryptographic techniques.

C. Isolation Techniques Based on Confidentiality Requirements:

There are numerous methods for achieving confidentiality, such as encryption, which we discussed previously, and isolation strategies. The difference is that cryptographic techniques based on confidentiality aim to protect the confidentiality of data stored in systems or transmitted over the organisation's network and BYOD. However, isolation techniques based on confidentiality are utilised to isolate corporate space, enforce security policies, and protect corporate data when using BYOD. In addition, security isolation methods allow users to separate personal data from corporate space. In these various ways, cryptographic and isolation techniques constitute a requirement for confidentiality.

In a BYOD scenario, personal and company data are stored on the same device. There are numerous benefits to integrating BYOD devices into the company infrastructure. However, this causes safety issues such as space isolation, data confidentiality, policy compliance and vulnerabilities since small and medium-sized enterprises cannot afford a suitable product solution that allows personal and professional data to coexist securely on employees' devices. Previous research has suggested isolation-based methods. Ocano et al. [62] proposed a remote mobile screen (RMS) based on the virtualization method to solve these problems. RMS allows for data confidentiality and space isolation. However, the complexity of managing physical roles is challenging. In addition, an essential real-world scenario in BYOD requires individuals to be isolated from the enterprise's privileged information access, according to Kim et al. [61]. They proposed an architecture called vNative that builds one foreground virtual machine (FVM), providing data confidentiality and isolation. However, the proposed solution is restricted to a few mobile intelligent devices. The proposed virtual network function (VNF) scheme is described in [63].

The suggested approach enables users to take advantage of the NFV server's more powerful corporate resources and increases service quality regarding security, mobility, and response time. It features a prototype technique [64] that takes advantage of virtualization characteristics common in today's mobile processors to fulfill this isolation demand.

In addition, this solution offers typical Android users security and privacy features. Table 8 summarises the isolation strategies discussed in previous studies.

D. Technique-Based Attack Detection Requirement:

According to previous research, there are numerous approaches for identifying attacks and preventing and monitoring risks. Kim and Lee [70] suggested a network-based risk identification tool based on the ML algorithm. The goal was to detect and evaluate malware on infected mobile devices under BYOD. However, this strategy cannot be employed for applications using log files. Aldini et al. [76] improved the method based on a machine learning algorithm to detect denial of service assaults, probing attacks, and torrent traffic in BYOD. The proposed approach is adaptable and flexible, lowering costs. Ammar et al. [80] proposed a supervised classification-based malware detection technique for Android BYOD devices. It provides a self-adaptive network capable of protecting critical services and defending against internal attacks and should be upgraded and expanded to detect advanced APTs. Ref. [72] proposed method based on clustering algorithms that may improve malware detection in BYOD was used with a simulation data set and a public dataset and achieved high precision. Ref. [69] employed a risk access scheme based on NGFW (next-generation firewall) technology, and a deep packet inspection firewall is used to protect a campus network. This method tracks and categorises risk packages. The experiment was analysed using a case study (Tokyo University). It reduced costs while increasing security. However, it is weaker because package content needs to be verified for network traffic filtering.

Furthermore, Ali et al. [71] proposed a risk-based access control model based on a dynamic risk estimation method, using features to analyse each request's security risk. The algorithm evaluates access based on user context, resource sensitivity, action severity, and risk history to represent an end-to-end ecosystem. Zungur et al. [84] presented a framework for detecting anomalous behaviour and unauthorised access to BYOD devices using artificial neural networks (ANN and data mining. A real dataset used in the evaluation had a precision of over 99 percent. One of the study's goals by [90] was to identify anomalous behaviour in BYOD devices connected to a corporate platform and then submit those devices to access control system management (ACSM) for platform access using an intelligent filtering technique. This method can set end-user access control policies and protect against malicious mobile apps, but security testing becomes difficult when apps are constantly attacked. The author in [79] proposed a behaviour-based abnormality detection method based on data mining that examines vulnerabilities and patterns in diverse information use contexts. Finally, ref. [83] provided a methodology using ANN techniques for detecting unusual behaviour and identifying unauthorised access to BYOD devices. It performed well on a real-world dataset, with a precision and accuracy of more than 99%. The experimental analysis assisted organisations in addressing three types of legitimate user behaviour. ANN, on the other hand, has difficulty converting data into numerical values. Previous studies show that many techniques have been developed for detecting risk in BYOD. Some techniques, such as fuzzy models and neural networks, are based on machine learning and deep learning. Tables 9 and 10 summarise previous research on BYOD attack detection techniques.

6.2.2. Techniques Based on More Than One Security and Privacy Requirement

Some techniques have satisfied more than one of the requirements, as seen in Figure 8, which shows the classification of policy technologies that consider multiple requirements. For example, some technologies fulfil multiple security and privacy requirements, according to previous studies. Firstly, some methods address both confidentiality and authentication. Many businesses have the necessary security access for BYOD to wireless networks. The network enterprise delivers WPA2 based on the 802.1X standard [46,47]. It is insufficient and should be strengthened. Pomak and Limpiyakom, proposed encryption-based authentication in [99]. They proposed employing near field communication multi-factor authentication (NFC) for secure authentication in combination

with hybrid cryptosystems. Chen et al. [100] proposed an authentication scheme for cloud data in IoT/BYOD. Participants can employ ciphertext policy attribute-based encryption to construct fine-grained access control rules (CP-ABE). The approach uses hybrid cloud infrastructure to offload expensive CP-ABE activities while protecting privacy. This way, encryption and optimization methods protect critical data at the item level, preventing leakage. Secondly, some procedures fulfil the criteria for confidentiality and detection of attacks. Zhu et al. [103] employed a new model combining anomaly detection, tracing, and revocation procedures. Partially ordered hierarchical encryption (PHE) is a novel threshold public key-based cryptosystem that implements a partial-order key hierarchy similar to RBAC roles. Tracking and large service interruptions are critical security measures. Thirdly, some techniques combine authentication, attack detection and confidentiality requirements. For instance, the technique proposed by Geber et al. [102] can enable SDN-based authentication in a BYOD setting using OpenFlo-based infrastructure. It uses SDN characteristics to create virtual networks for monitoring dynamically selected BYOD users. By employing the portal and two-factor authentication, the user is provided with a safe and convenient means for enabling access to critical applications only and barring unauthorised requests, thereby limiting the services that a potentially attacking device can access. Changes to switching streaming rules may be deployed quickly, ensuring that users always have the most up-to-date access to the network with attack predictions. Three security and privacy requirements have been fulfilled: the authentication of BYOD devices used two-factor authentication, attack detection was achieved via continuous risk monitoring, and confidentiality was based on virtual networks. Table 11 depicts those techniques that have employed more than one security and privacy requirement in previous studies in the field.

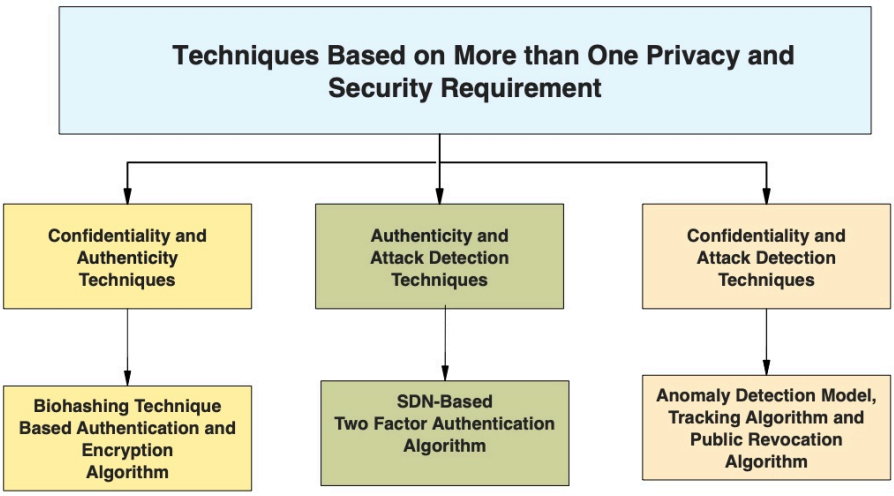

Figure 8. Techniques based on more than one privacy requirement.

6.2.3. Techniques That Did Not Fulfil Any of the Classified Security and Privacy Requirements

Figure 9 shows methods that did not identify any of the suggested requirements. Most studies in this section focus on enforcing simple policies or security architectures to improve overall security for organisations that support BYOD. These methods are preliminary models or policies, not technologies that address the identified requirements for privacy and security. For example, Selviandro et al. [104] suggested an architectural framework for enforced access control policies to reduce BYOD vulnerabilities. while Armando et al. introduced a reliable and policy-aware architecture for enforcing fine-grained security requirements on BYOD devices [105]. They implemented a user and device security policy based on existing NATO CIA guidelines (NCI Agency). Aldini et al. [108] presented an opportunity-enabled risk management (OPPRIM) approach that aimed to balance understanding primary threats with an appreciation of the increased opportunities that may emerge from BYOD. OPPRIM combines risk estimation methods

with trust and threat metrics, and the OPPRIM policy and metric formulation paradigm is formalised in this study using logic. The model was checked using qualitative tools. The next Table 12 summarises the studies that address the security of BYOD without focusing on a specific security and privacy requirement.

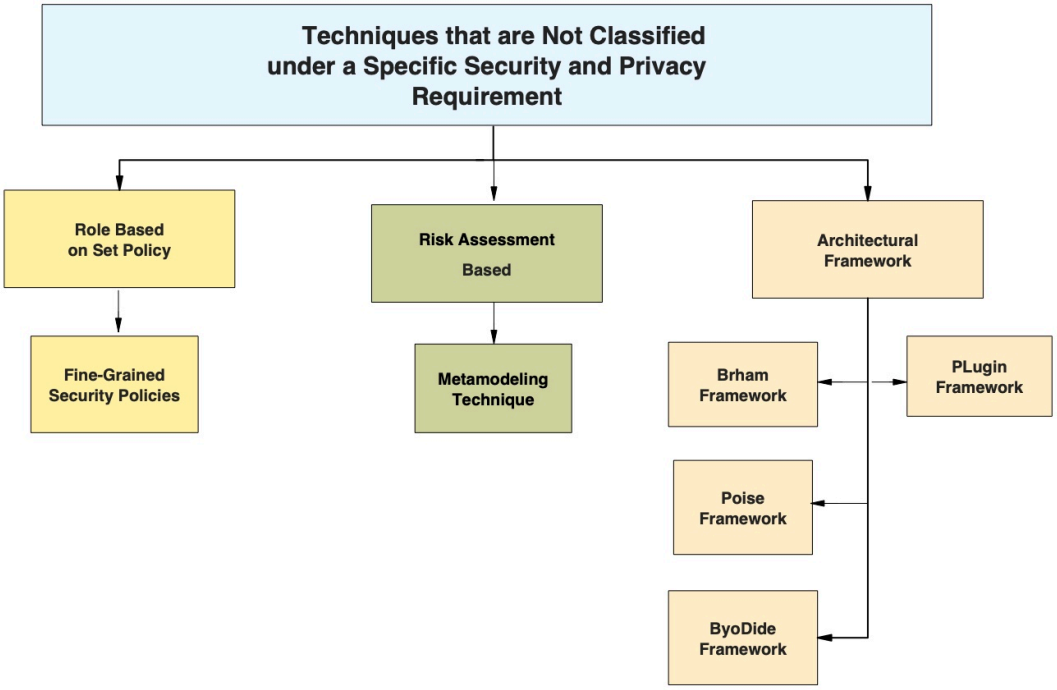

Figure 9. Techniques that did not satisfy classified privacy requirements.

6.2.4. Performance Evaluation and Metrics Employed by the Techniques

This section reviews the performance evaluation and the metrics used to evaluate the techniques. To categorize the performance evaluation analysis methods, the review distinguishes between techniques with tools (methods utilizing software or hardware in the assessment process) and methods without tools (methods relying on mathematical analysis). Figure 10 illustrates the methods using tools, including case studies, simulations (e.g., MATLAB, NS2, computer simulation experiment, and Anylogic), datasets (e.g., Public, Real, and Synthetic), formal security proofs (e.g., Scyther), and prototype implementations. Conversely, analysis without tools relies solely on mathematical analysis.

Previous research has identified specific evaluation metrics for each security and privacy requirement in technology. These metrics have been replicated in other studies to assess various security requirements. For instance, the authenticity requirement is evaluated based on response time, access response (deny or permit), and cost. The confidentiality requirement is measured using metrics such as execution time, communication costs, communication complexity, exchange key time, CPU usage, memory usage, and boot time. Attack detection requirements are assessed through metrics like accuracy, precision (PPV), recall (TPR), detection rate, RAM usage over time, CPU usage over time, overhead, and time cost. However, it is important to note that performance evaluation matrices may not adequately cover all the security and privacy requirements outlined in BYOD policies, highlighting the need for further exploration in this field.

Overall, performance evaluation and metrics provide invaluable insight into the efficacy, efficiency, and vulnerabilities of security access control systems. By employing these evaluation techniques, organizations can strengthen their access control measures, mitigate security risks, and protect sensitive resources and data. Figure 10 illustrates the classification of the performance evaluation analysis methods adopted by the techniques

examined in this review. Furthermore, Tables 13 and 14 provide a summary of the metrics used by the techniques and their respective purposes.

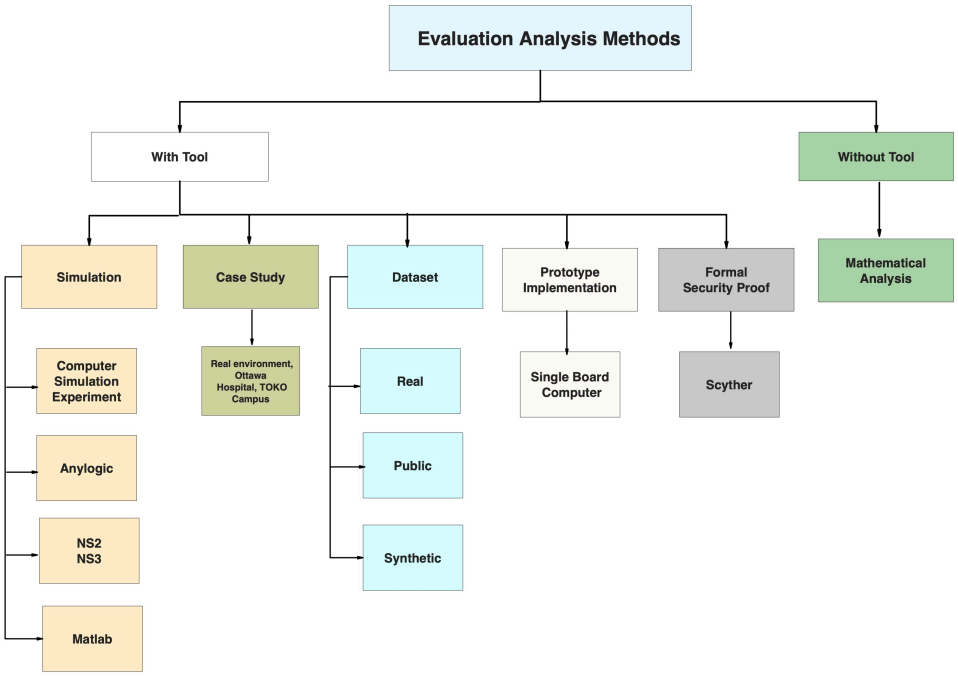

Figure 10. Classification of the performance analysis methods.

7. Discussion

The core security policy for BYOD encompasses various policies such as Network Access Control (NAC), Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Information Management (MIM), and Enterprise Mobility Management (EMM). However, the increasing number of BYOD attacks indicates that these security policies must be revised to develop BYOD security while failing to meet privacy requirements. Instead, a three-tiered security policy framework consisting of operational, tactical, and strategic layers should be implemented, working in harmony. This framework requires critical policies, including on-boarding access control policy, authentication access control policy, communication policy, application control policy, and risk control policy. These policies encompass BYOD devices and the organization's network, resources, communications, and applications while addressing seven essential security and privacy requirements: confidentiality, integrity, availability, non-repudiation, authentication, privacy preservation, and attack detection. Despite previous reviews providing foundational knowledge on the security and privacy challenges associated with BYOD policies, many still need to examine security policy techniques and privacy requirements thoroughly. Additionally, the exploration of technological methods employed to ensure compliance with these requirements still needs to be completed. This review adopts a systematic approach to comprehensively understand security policy techniques and privacy requirements within the context of a three-layered security policy architecture, which is considered ideal for optimizing BYOD security.

The study formulated and addressed five research questions (RQ1–RQ5) to accomplish its objectives. RQ1 focused on identifying the primary criteria that meet the security requirements of bring your own device (BYOD), namely confidentiality, integrity, availability, non-repudiation, authentication, privacy preservation, and attack detection. The results pertaining to RQ1 are discussed in Section 4. Similarly, the findings for RQ2 revealed the effectiveness of security policy techniques in meeting the security and privacy requirements. This analysis is presented in Section 6. The reviewed studies highlighted that among the various criteria, the most attention was given to attack detection,

with 30 proposed techniques, followed by authenticity with 11 recommended techniques. Eight techniques focused on confidentiality using isolation techniques, while six techniques centered on confidentiality using cryptography. Additionally, 13 studies did not fall under specific requirements as they presented initial suggestions within the policy architecture framework. Furthermore, five proposed techniques addressed a combination of two or more different requirements, with only three techniques addressing both authenticity and confidentiality, and one technique covering authentication, attack detection, and confidentiality requirements. Additionally, one technique fulfilled the confidentiality and attack detection requirements. However, the review study noted a lack of techniques addressing the integrity, availability, non-repudiation, and privacy preservation requirements. This indicates the need for future research to focus on these aspects. Figure 11 illustrates the distribution of techniques based on the analysed requirements.

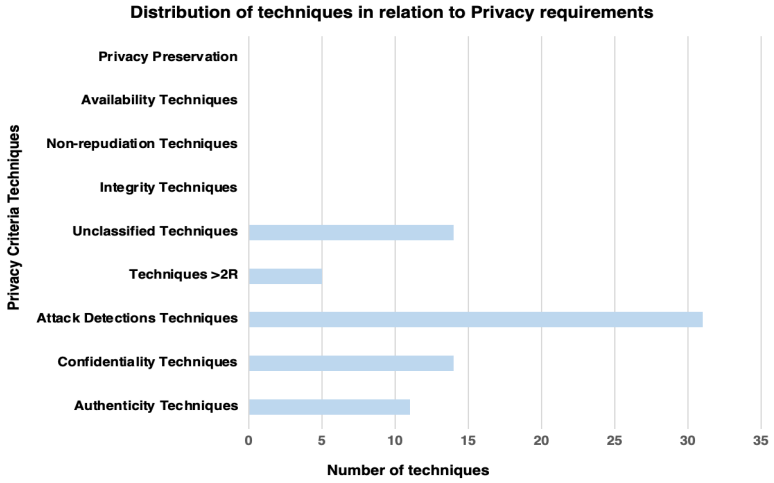

Figure 11. Distribution of techniques in relation to Privacy requirements.

Following the research review conducted under RQ3, the identified methodologies were further categorised based on their technological approaches. These approaches encompassed software-defined networking (SDN), machine learning (ML) algorithms, digital forensic models, and mobile security solution (MSS) systems. Among these, the most commonly employed technology was cryptography, specifically based on the RSA algorithm. Furthermore, the evaluation of technique effectiveness involved the examination of performance metrics, as explored under RQ4. Each category of requirements employed specific metrics to assess the performance of the techniques. Tables 13 and 14 highlight the purpose of evaluating techniques using these specific metrics. These tables provide valuable guidance for future researchers regarding the appropriate metrics for measuring technique performance. The review indicates that simulation experiments were the most frequently utilized approach for performance analysis in response to RQ4. Among the studies that employed datasets, a particular dataset emerged as the most commonly used. Prototype implementations predominantly employed embedded devices (single-board computers), while only one study utilized the Scyther tool for formal security analysis. Informal security analysis was the prevailing method utilized. Finally, based on the analysis and evaluation conducted, the study also identified significant challenges faced by the field. These challenges hold relevance for future researchers and will be expounded upon in the subsequent section.

8. Open Issues

This section aims to respond to RQ5 by discussing pertinent open research concerns regarding security policy techniques and privacy requirements. It intends to highlight opportunities for future research in this field. The following are the main open issues that merit further investigation:

8.1. Blockchain-Based Authentication Techniques

Academic researchers have proposed a variety of authentication approaches and techniques. These approaches can assist organisations in developing more secure access control between their networks, resources and BYOD. However, most techniques are designed to target either the user or the device individually. BYOD requires both the device and the user to be trusted with access to the organisation's resources. Knowledge-based authentication, possession-based authentication, biometric-based authentication and multi-factor authentication are all vulnerable to attack. As a result, more robust authentication measures are required. Most authentication systems require storing authentication information (password, ID, public key). The issue with consolidating storage is that it might become a single failure point. The initial BYOD solutions proposed by earlier academics are insufficient to secure the BYOD environment. Future research should focus on developing BYOD access control, which will address most of the issues in the BYOD environment and employ blockchain technology for security.

8.2. Secure Two-Way Communication

It is challenging to set up secure two-way communication in a BYOD environment. As a result, lightweight key exchange algorithms that suit access control in BYOD should be devised in the future to provide safe two-way communication between companies and BYOD devices.

8.3. Real-Time Authorization

BYOD encompasses a wide range of smart devices that contact the organisation's server and depend on providing real-time data access. Therefore, a delay in procuring an access decision within a BYOD environment may lead to unauthorised access to sensitive data, resulting in vulnerabilities to the system. In the scenario mentioned earlier, it can be inferred that access decision-making must remain close to the origin of access requests, which can provide the advantage of real-time data for the access control system, thus enabling access decisions with a minimal end-to-end delay. Moreover, authorised access must be ensured throughout the session, not only at the time of the request. In addition, real-time authorization means continuous access decisions throughout the session, not only when requesting access.

8.4. Context-Aware Role-Based Access Control

In security access control, many methods target communication between the organisation's platform and BYOD devices. The method of access control proposed [109] is not sensitive to contexts such as user status, location of the BYOD user, or time. According to the literature, these factors are context-aware elements. These factors are essential because they help identify BYOD devices inside the organisation. Therefore, access control based on context awareness should be given more attention to ensure the privacy of the BYOD environment. This is a major challenge and represents a promising field of study, but changes in context with access control must be adapted iteratively to avoid any risks.

8.5. Risk-Adaptive Policy Adjustments

Researchers in the field of BYOD security are interested in detecting and preventing insider attacks. Numerous methods based on behavioural models and anomaly detection approaches for addressing insider risks in BYOD environments have developed, such as [81,82,88,89]. While these methodologies do not focus on adapting access control policies to avoid insider assaults, they provide valuable insights into insider threat detection in BYOD situations. However, adaptive policy adjustment approaches pose a significant challenge and are an unexplored study area.

8.6. Evaluation Metrics Employed by the Techniques

According to the evaluation metrics, cost reduction concerning policy procedures remains a significant issue, particularly for small and growing businesses. Furthermore, it

should be noted that most attack detection techniques [72,73,93] evaluate attack detection accuracy but not adaptive policy adjustment accuracy. As a result, two evaluation metrics, time and adaptive policy adjustment accuracy, were required to evaluate adaptive policy adjustment techniques. Because there has been little research in this area, other security and privacy requirements such as integrity, availability, privacy preservation and non-repudiation should be measured using evaluation metrics.

8.7. More Effort Is Required to Fulfill Specific Privacy and Security Criteria

As previously stated, several security and privacy requirements summarised above either need to explore particular technologies fully or include them. For instance, integrity, availability, non-repudiation and privacy-preservation requirements are not taken into account by any technique on a stand-alone basis but integrated with other criteria. Therefore, future research should focus on developing techniques that consider these considerations.

9. Conclusions and Future Work

BYOD security requires applying access control policies at all three security levels: operational, tactical and strategic, considering privacy requirements. This study is the first systematic review of security policies based on the privacy criteria that they meet. It also examines current research and focuses on the following aspects: (1) categorising privacy and security requirements within bring your own device (BYOD) policies; (2) analysing advanced security policy technologies for BYOD, considering three layers of security, and assessing their alignment with privacy requirements; (3) identifying technological trends in the field; (4) evaluating the effectiveness of techniques to enhance privacy and security through various measures; and (5) identifying potential areas for future BYOD security and privacy research.

In total, 74 articles were analysed based on SLR standard procedures to extract the key findings that underpin this study. Firstly, a taxonomy of security policy techniques and privacy requirements was introduced. According to the survey, BYOD security and privacy requirements can be divided into seven categories: confidentiality, integrity, availability, non-repudiation, authentication, privacy preservation, and attack detection. Secondly, the survey found that every criterion can be fulfilled with a specific technique, except for integrity, availability, non-repudiation, and privacy-preservation requirements, which were combined with other requirements. Third, having identified contemporary trends relevant to BYOD security, the techniques identified were classified according to their associated technological methods. Fourth, there was a discussion of the performance criteria used to evaluate the effectiveness of each technique. The review effort also showed the limitations of each of the methodologies. Lastly, for the benefit of academics interested in working on BYOD security and privacy, potential research areas were identified for future studies. For future studies, researchers are encouraged to focus on developing access control to address most issues in the BYOD environment. Utilising blockchain technology for security and emphasising context-aware access control to protect the privacy of the BYOD environment are recommended. The study also emphasises the need to consider privacy requirements such as integrity, availability, non-repudiation, and privacy preservation.

Author Contributions: Conceptualization, A.T.A.M.; methodology, A.T.A.M.; validation, A.T.A.M.; formal analysis, A.T.A.M.; investigation, A.T.A.M.; resources, A.T.A.M.; data curation, A.T.A.M.; writing—original draft preparation, A.T.A.M.; writing—review and editing, A.T.A.M.; visualization, A.T.A.M.; supervision, A.W.A.W. and M.Y.I.I. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partly supported by the University of Malaya Impact Oriented Interdisciplinary Research Grant under Grant IIRG008 (A, B, C)-19IISS.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: The authors of this paper appreciate the reviewers' observations, comments and suggestions for improving the manuscript's content.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Bello, A.G.; Murray, D.; Armarego, J. A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Inf. Comput. Secur.* **2017**, *25*, 475–492. [CrossRef]
2. Agrawal, A.; Pandey, A.K.; Baz, A.; Alhakami, H.; Alhakami, W.; Kumar, R.; Khan, R.A. Evaluating the security impact of healthcare Web applications through fuzzy based hybrid approach of multi-criteria decision-making analysis. *IEEE Access* **2020**, *8*, 135770–135783. [CrossRef]
3. Beckett, P. BYOD–popular and problematic. *Netw. Secur.* **2014**, *2014*, 7–9. [CrossRef]
4. Njuguna, D.; Kanyi, W. An evaluation of BYOD integration cybersecurity concerns: A case study. *Int. J. Recent Res. Math. Comput. Sci. Inf. Technol.* **2023**, *9*, 80–91.
5. Conteh, N.Y.; Schmick, P.J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *Int. J. Adv. Comput. Res.* **2016**, *6*, 31. [CrossRef]
6. Clarke, J.; Hidalgo, M.G.; Lioy, A.; Petkovic, M.; Vishik, C.; Ward, J. Consumerization of IT: Top risks and opportunities. In *ENISA Deliverables*; European Network and Information Security Agency (ENISA) Report; European Network and Information Security Agency (ENISA): Athens, Greece, 2012.
7. Utter, C.J.; Rea, A. The" Bring your own device" conundrum for organizations and investigators: An examination of the policy and legal concerns in light of investigatory challenges. *J. Digit. Forensics Secur. Law* **2015**, *10*, 4. [CrossRef]
8. Rhee, K.; Won, D.; Jang, S.W.; Chae, S.; Park, S. Threat modeling of a mobile device management system for secure smart work. *Electron. Commer. Res.* **2013**, *13*, 243–256. [CrossRef]
9. Morrow, B. BYOD security challenges: Control and protect your most sensitive data. *Netw. Secur.* **2012**, *2012*, 5–8. [CrossRef]
10. La Polla, M.; Martinelli, F.; Sgandurra, D. A survey on security for mobile devices. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 446–471. [CrossRef]
11. Kok, J.; Kurz, B. Analysis of the botnet ecosystem. In Proceedings of the 10th Conference of Telecommunication, Media and Internet Techno-Economics (CTTE), Berlin, Germany, 16–18 May 2011; VDE: Frankfurt am Main, Germany, 2011; pp. 1–10.
12. Niehaves, B.; Köffer, S.; Ortbach, K. IT consumerization—A theory and practice review. In Proceedings of the 18th Americas Conference on Information Systems (AMCIS 2012), Seattle, WA, USA, 9–11 August 2012.
13. Garba, A.B.; Armarego, J.; Murray, D.; Kenworthy, W. Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *J. Inf. Priv. Secur.* **2015**, *11*, 38–54. [CrossRef]
14. Oktavia, T.; Yanti; Prabowo, H.; Meyliana. Security and privacy challenge in Bring Your Own Device environment: A systematic literature review. In Proceedings of the 2016 International Conference on Information Management and Technology (ICIMTech), Bandung, Indonesia, 16–18 November 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 194–199.
15. Jamal, F.; Taufik, M.; Abdullah, A.A.; Hanapi, Z.M. A Systematic Review Of Bring Your Own Device (BYOD) Authentication Technique. *J. Phys. Conf. Ser.* **2020**, *1529*, 042071. [CrossRef]
16. Palanisamy, R.; Norman, A.A.; Kiah, M.L.M. Compliance with bring your own device security policies in organizations: A systematic literature review. *Comput. Secur.* **2020**, *98*, 101998. [CrossRef]
17. Wani, T.A.; Mendoza, A.; Gray, K. Hospital bring-your-own-device security challenges and solutions: Systematic review of gray literature. *JMIR mHealth uHealth* **2020**, *8*, e18175. [CrossRef] [PubMed]
18. Eke, C.I.; Norman, A.A.; Mulenga, M. Machine learning approach for detecting and combating bring your own device (BYOD) security threats and attacks: A systematic mapping review. *Artif. Intell. Rev.* **2023**, *56*, 8815–8858. [CrossRef]
19. AL-Azazi, O.A.A.S.; Norman, A.A.; Ghani, N.B.A. BrA Systematic Literature Review and Bibliometric Analysis (2017–2022) Your Own Device Information Security Policy Compliance Framework. In Proceedings of the 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 6–7 October 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–8.
20. Soubhagyalakshmi, P.; Reddy, K.S. An efficient security analysis of bring your own device. *IAES Int. J. Artif. Intell.* **2023**, *12*, 696. [CrossRef]
21. Ratchford, M.; El-Gayar, O.; Noteboom, C.; Wang, Y. BYOD security issues: A systematic literature review. *Inf. Secur. J. Glob. Perspect.* **2022**, *31*, 253–273. [CrossRef]
22. Yahuza, M.; Idris, M.Y.I.B.; Wahab, A.W.B.A.; Ho, A.T.; Khan, S.; Musa, S.N.B.; Taha, A.Z.B. Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities. *IEEE Access* **2020**, *8*, 76541–76567. [CrossRef]
23. kaspersky. Available online: https://www.kaspersky.com (accessed on 9 May 2023).
24. Batool, H.; Masood, A. Enterprise mobile device management requirements and features. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 109–114.
25. Da Veiga, A.; Astakhova, L.V.; Botha, A.; Herselman, M. Defining organisational information security culture—Perspectives from academia and industry. *Comput. Secur.* **2020**, *92*, 101713. [CrossRef]
26. Whitman, M.E.; Mattord, H.J. *Principles of Information Security*; Cengage Learning: Boston, MA, USA, 2021.

27. Mohsin, M.K.A.; Ab Hamid, Z. Bring Your Own Device (BYOD): Legal Protection of The Employee in Malaysia. *Malays. J. Soc. Sci. Humanit. (MJSSH)* **2022**, *7*, e001609.
28. Johnston, Z.A. Exploring Privacy Concern Effect on Organizational BYOD Policies and Security Measures Compliancy. Ph.D. Thesis, Capella University, Minneapolis, MN, USA, 2022.
29. Véliz, C. Privacy and digital ethics after the pandemic. *Nat. Electron.* **2021**, *4*, 10–11. [CrossRef]
30. White, B. The Influence of BYOD Security Risk on SME Information Security Effectiveness. Ph.D. Thesis, Capella University, Minneapolis, MN, USA, 2022.
31. Macaraeg, T.A., Jr. *Bring-Your-Own-Device (BYOD): Issues and Implementation in Local Colleges and Universities in the Philippines*; ResearchGate: Berlin, Germany, 2013.
32. Herrera, A.V.; Ron, M.; Rabadão, C. National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In Proceedings of the 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, Portugal, 21–24 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–4.
33. Scarfo, A. New security perspectives around BYOD. In Proceedings of the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, Victoria, BC, Canada, 12–14 November 2012; IEEE: Piscataway, NJ, USA, 2012, pp. 446–451.
34. Alotaibi, B.; Almagwashi, H. A review of BYOD security challenges, solutions and policy best practices. In Proceedings of the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 4–6 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
35. Mosenia, A.; Jha, N.K. A comprehensive study of security of internet-of-things. *IEEE Trans. Emerg. Top. Comput.* **2016**, *5*, 586–602. [CrossRef]
36. Karimi, K.; Krit, S. Smart home-smartphone systems: Threats, security requirements and open research challenges. In Proceedings of the 2019 International Conference of Computer Science and Renewable Energies (ICCSRE), Agadir, Morocco, 22–24 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5.
37. Rodríguez, N.R.; Murazzo, M.A.; Chávez, S.B.; Valenzuela, F.A.; Martín, A.E.; Villafane, D.A. Key aspects for the development of applications for Mobile Cloud Computing. *J. Comput. Sci. Technol.* **2013**, *13*, 143–148.
38. Downer, K.; Bhattacharya, M. BYOD security: A new business challenge. In Proceedings of the 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, China, 19–21 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1128–1133.
39. Doh, I.; Lim, J.; Chae, K. Secure authentication for structured smart grid system. In Proceedings of the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Santa Catarina, Brazil, 8–10 July 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 200–204.
40. Almarhabi, K.; Jambi, K.; Eassa, F.; Batarfi, O. Survey on access control and management issues in cloud and BYOD environment. *Int. J. Comput. Sci. Mob. Comput.* **2017**, *6*, 44–54.
41. Ali, M.I.; Kaur, S. Next-generation digital forensic readiness BYOD framework. *Secur. Commun. Netw.* **2021**, *2021*, 6664426. [CrossRef]
42. Sushil, G.S.; Deshmuk, R.K.; Junnarkar, A.A. Security Challenges and Cyber Forensics For IoT Driven BYOD Systems. In Proceedings of the 2022 IEEE 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 7–9 April 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7.
43. Kitchenham, B.; Brereton, P. A systematic review of systematic review process research in software engineering. *Inf. Softw. Technol.* **2013**, *55*, 2049–2075. [CrossRef]
44. Lee, J.E.; Park, S.H.; Yoon, H. Security policy based device management for supporting various mobile os. In Proceedings of the 2015 Second International Conference on Computing Technology and Information Management (ICCTIM), Johor, Malaysia, 21–23 April 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 156–161.
45. Guerar, M.; Verderame, L.; Merlo, A.; Palmieri, F.; Migliardi, M.; Vallerini, L. CirclePIN: A novel authentication mechanism for smartwatches to prevent unauthorized access to IoT devices. *ACM Trans.-Cyber-Phys. Syst.* **2020**, *4*, 1–19. [CrossRef]
46. Yanson, K. Results of implementing WPA2-enterprise in educational institution. In Proceedings of the 2016 IEEE 10th International Conference on Application of Information and Communication Technologies (AICT), Baku, Azerbaijan, 12–14 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–4.
47. Gkamas, V.; Paraskevas, M.; Varvarigos, E. Design of a secure BYOD policy for the Greek School Network: a Case Study. In Proceedings of the 2016 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) and 15th International Symposium on Distributed Computing and Applications for Business Engineering (DCABES), Paris, France, 24–26 August 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 557–560.
48. Oluwatimi, O.; Damiani, M.L.; Bertino, E. A context-aware system to secure enterprise content: Incorporating reliability specifiers. *Comput. Secur.* **2018**, *77*, 162–178. [CrossRef]
49. Kao, Y.C.; Chang, Y.C.; Chang, R.S. EZ-Net BYOD service management in campus wireless networks. *J. Internet Technol.* **2017**, *18*, 907–917.
50. Heo, H.; Ryou, J. Design and implementation of lightweight network access control technique on wireless router. *Int. J. Serv. Technol. Manag.* **2017**, *23*, 101–116. [CrossRef]
51. Jaha, F.; Kartit, A. Pseudo code of two-factor authentication for BYOD. In Proceedings of the 2017 International Conference on Electrical and Information Technologies (ICEIT), Rabat, Morocco, 15–18 November 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–7.

52. Cai, C.; Weng, J.; Liu, J. Mobile authentication system based on national regulation and NFC technology. In Proceedings of the 2016 IEEE First International Conference on Data Science in Cyberspace (DSC), Changsha, China, 13–16 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 590–595.
53. Deng, R.; Weng, J.; Ren, K.; Yegneswaran, V. Security and privacy in communication networks. In Proceedings of the Security and Privacy in Communication Networks: 12th International Conference (SecureComm 2016), Guangzhou, China, 10–12 October 2016; Springer: Berlin/Heidelberg, Germany, 2017; Volume 198.
54. Seneviratne, B.; Senaratne, S. Integrated Corporate Network Service Architecture for Bring Your Own Device (BYOD) Policy. In Proceedings of the 2018 3rd International Conference on Information Technology Research (ICITR), Moratuwa, Sri Lanka, 5–7 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
55. Rahardjo, M.R.D.; Shidik, G.F. Design and implementation of self encryption method on file security. In Proceedings of the 2017 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, 7–8 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 181–186.
56. Vinh, T.L.; Cagnon, H.; Bouzefrane, S.; Banerjee, S. Property-based token attestation in mobile computing. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e4350. [CrossRef]
57. Catuogno, L.; Galdi, C. A Fine-grained General Purpose Secure Storage Facility for Trusted Execution Environment. In Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP 2019), Prague, Czech Republic, 23–25 February 2019; pp. 588–595.
58. Li, F.; Rahulamathavan, Y.; Conti, M.; Rajarajan, M. Robust access control framework for mobile cloud computing network. *Comput. Commun.* **2015**, *68*, 61–72. [CrossRef]
59. Gupta, S. Single Sign-On beyond Corporate Boundaries. In Proceedings of the 2018 8th International Conference on Intelligent Systems, Modelling and Simulation (ISMS), Kuala Lumpur, Malaysia, 8–10 May 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 38–42.
60. Abisheka, P.C.; Azra, M.F.; Poobalan, A.; Wijekoon, J.; Yapa, K.; Murthaja, M. An Automated Solution For Securing Confidential Documents in a BYOD Environment. In Proceedings of the 2021 3rd International Conference on Advancements in Computing (ICAC), Colombo, Sri Lanka, 9–11 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 61–66.
61. Kim, J.; Kim, T.Y.; Kim, D. Network based vByod scheme in NFV platform. In Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 18–20 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1143–1145.
62. Ocano, S.G.; Ramamurthy, B.; Wang, Y. Remote mobile screen (RMS): An approach for secure BYOD environments. In Proceedings of the 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 16–19 February 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 52–56.
63. Dong, Y.; Mao, J.; Guan, H.; Li, J.; Chen, Y. A virtualization solution for BYOD with dynamic platform context switching. *IEEE Micro* **2015**, *35*, 34–43. [CrossRef]
64. Averlant, G. Multi-level isolation for android applications. In Proceedings of the 2017 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Toulouse, France, 23–26 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 128–131.
65. Chiueh, T.C.; Lin, H.; Chao, A.; Wu, T.G.; Wang, C.M.; Wu, Y.S. Smartphone virtualization. In Proceedings of the 2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS), Wuhan, China, 13–16 December 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 141–150.
66. Ketel, M. Enhancing BYOD security through SDN. In Proceedings of the SoutheastCon 2018, St. Petersburg, FL, USA, 19–22 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–2.
67. Kim, G.; Jeon, Y.; Kim, J. Secure mobile device management based on domain separation. In Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 19–21 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 918–920.
68. Kim, G.; Kim, J. Secure voice communication service based on security platform for mobile devices. In Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 18–20 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1190–1192.
69. Mishima, K.; Sakurada, T.; Hagiwara, Y.; Tsujisawa, T. Secure Campus Network System with Automatic Isolation of High Security Risk Device. In Proceedings of the 2018 ACM SIGUCCS Annual Conference, Orlando, FL, USA, 7–10 October 2018; pp. 107–110.
70. Kim, D.; Lee, S. Study of identifying and managing the potential evidence for effective Android forensics. *Forensic Sci. Int. Digit. Investig.* **2020**, *33*, 200897. [CrossRef]
71. 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**, *8*, 172770–172782. [CrossRef]
72. Tan, X.; Li, H.; Wang, L.; Xu, Z. End-Edge Coordinated Inference for Real-Time BYOD Malware Detection using Deep Learning. In Proceedings of the 2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Republic of Korea, 25–28 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
73. Watkins, L.; Kalathummarath, A.L.; Robinson, W.H. Network-based detection of mobile malware exhibiting obfuscated or silent network behavior. In Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–4.

74. Atlam, H.F.; Alenezi, A.; Walters, R.J.; Wills, G.B.; Daniel, J. Developing an adaptive Risk-based access control model for the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 655–661.
75. Tiwari, P.K.; Velayutham, T. Andrologger: Collecting and correlating events to identify suspicious activities in android. In Proceedings of the 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, India, 3–5 July 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–7.
76. Aldini, A.; Seigneur, J.M.; Lafuente, C.B.; Titi, X.; Guislain, J. Design and validation of a trust-based opportunity-enabled risk management system. *Inf. Comput. Secur.* **2017**. [CrossRef]
77. Eslahi, M.; Yousefi, M.; Naseri, M.V.; Yussof, Y.; Tahir, N.; Hashim, H. Mobile botnet detection model based on retrospective pattern recognition. *Int. J. Secur. Appl.* **2016**, *10*, 39–44. [CrossRef]
78. Joshi, P.; Jindal, C.; Chowkwale, M.; Shethia, R.; Shaikh, S.A.; Ved, D. Protego: A passive intrusion detection system for android smartphones. In Proceedings of the 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, India, 19–21 December 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 232–237.
79. Kim, T. A Study on the Detection of Abnormal Behavior and Vulnerability Analysis in BYOD. In Proceedings of the International Internet of Things Summit; Springer: Berlin/Heidelberg, Germany, 2015; pp. 162–167.
80. Ammar, M.; Rizk, M.; Abdel-Hamid, A.; Aboul-Seoud, A.K. A framework for security enhancement in SDN-based datacenters. In Proceedings of the 2016 8th IFIP international conference on new technologies, Mobility and security (NTMS), Larnaca, Cyprus, 21–23 November 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–4.
81. Akhuseyinoglu, N.B.; Akhuseyinoglu, K. AntiWare: An automated Android malware detection tool based on machine learning approach and official market metadata. In Proceedings of the 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 20–22 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–7.
82. De las Cuevas, P.; Mora, A.; Merelo, J.J.; Castillo, P.A.; Garcia-Sanchez, P.; Fernandez-Ares, A. Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Comput. Commun.* **2015**, *68*, 83–95. [CrossRef]
83. Petrov, D.; Znati, T. Context-aware deep learning-driven framework for mitigation of security risks in BYOD-enabled environments. In Proceedings of the 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), Philadelphia, PA, USA, 18–20 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 166–175.
84. Zungur, O.; Suarez-Tangil, G.; Stringhini, G.; Egele, M. Borderpatrol: Securing byod using fine-grained contextual information. In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Portland, OR, USA, 24–27 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 460–472.
85. Lima, A.; Rosa, L.; Cruz, T.; Simões, P. A Security Monitoring Framework for Mobile Devices. *Electronics* **2020**, *9*, 1197. [CrossRef]
86. Nikoloudakis, Y.; Pallis, E.; Mastorakis, G.; Mavromoustakis, C.X.; Skianis, C.; Markakis, E.K. Vulnerability assessment as a service for fog-centric ICT ecosystems: A healthcare use case. *Peer-to-Peer Netw. Appl.* **2019**, *12*, 1216–1224. [CrossRef]
87. Muhammad, M.A.; Ayesh, A.; Zadeh, P.B. Developing an intelligent filtering technique for bring your own device network access control. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge UK, 19–20 July 2017; pp. 1–8.
88. Uddin, M.; Nadeem, T. TrafficVision: A case for pushing software defined networks to wireless edges. In Proceedings of the 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Brasilia, Brazil, 10–13 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 37–46.
89. Ali, M.I.; Kaur, S. BYOD Cyber Threat Detection and Protection Model. In Proceedings of the 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 19–20 February 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 211–218.
90. Alghamdi, A.M.; Almarhabi, K. A Proposed Framework for the Automated Authorization Testing of Mobile Applications. *Int. J. Comput. Sci. Netw. Secur.* **2021**, *21*, 217–221.
91. Kebande, V.R.; Karie, N.M.; Venter, H. A generic Digital Forensic Readiness model for BYOD using honeypot technology. In Proceedings of the 2016 IST-Africa Week Conference, Durban, South Africa, 11–13 May 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–12.
92. Asante, A.; Amankona, V. Digital Forensic Readiness Framework Based on Honeypot Technology for BYOD. *J. Digit. Forensics Secur. Law* **2021**, *16*, 1–17.
93. Eshmawi, A.; Nair, S. The Roving Proxy Framewrok for SMS Spam and Phishing Detection. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
94. Awan, M.S.; AlGhamdi, M.; AlMotiri, S.; Burnap, P.; Rana, O. A classification framework for distinct cyber-attacks based on occurrence patterns. In Proceedings of the 8th International Conference on Security of Information and Networks, Sochi, Russia 8–10 September 2015; pp. 165–168.
95. Stoecklin, M.P.; Singh, K.; Koved, L.; Hu, X.; Chari, S.N.; Rao, J.R.; Cheng, P.C.; Christodorescu, M.; Sailer, R.; Schales, D.L. Passive security intelligence to analyze the security risks of mobile/BYOD activities. *IBM J. Res. Dev.* **2016**, *60*, 9–1. [CrossRef]
96. Chen, Y.; Hu, H.c.; Cheng, G.z. Design and implementation of a novel enterprise network defense system bymaneuveringmulti-dimensional network properties. *Front. Inf. Technol. Electron. Eng.* **2019**, *20*, 238–252. [CrossRef]

97. Yang, C.; Hong-Chao, H.; Guo-Zhen, C. A software-defined intranet dynamic defense system. In Proceedings of the 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, China, 8–11 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 849–854.
98. Gómez-Hernández, J.A.; Camacho, J.; Holgado-Terriza, J.A.; García-Teodoro, P.; Maciá-Fernández, G. ARANAC: A Bring-Your-Own-Permissions Network Access Control Methodology for Android Devices. *IEEE Access* **2021**, *9*, 101321–101334. [CrossRef]
99. Pomak, W.; Limpiyakom, Y. Enterprise WiFi Hotspot Authentication with Hybrid Encryption on NFC-Enabled Smartphones. In Proceedings of the 2018 8th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 15–17 June 2018; IEEE: Piscataway, NJ, USA, 2018, pp. 247–250.
100. Qi, S.; Lu, Y.; Wei, W.; Chen, X. Efficient data access control with fine-grained data protection in cloud-assisted IIoT. *IEEE Internet Things J.* **2020**, *8*, 2886–2899. [CrossRef]
101. Zheng, Y.; Cao, Y.; Chang, C.H. Facial biohashing based user-device physical unclonable function for bring your own device security. In Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 12–14 January 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
102. Gebert, S.; Zinner, T.; Gray, N.; Durner, R.; Lorenz, C.; Lange, S. Demonstrating a personalized secure-by-default bring your own device solution based on software defined networking. In Proceedings of the 2016 28th International Teletraffic Congress (ITC 28), Würzburg, Germany, 12–16 September 2016; IEEE: Piscataway, NJ, USA, 2016; Volume 1, pp. 197–200.
103. Zhu, Y.; Gan, G.; Guo, R.; Huang, D. PHE: An efficient traitor tracing and revocation for encrypted file syncing-and-sharing in cloud. *IEEE Trans. Cloud Comput.* **2016**, *6*, 1110–1124. [CrossRef]
104. Selviandro, N.; Wisudiawan, G.; Puspitasari, S.; Adrian, M. Preliminary study for determining bring your own device implementation framework based on organizational culture analysis enhanced by cloud management control. In Proceedings of the 2015 3rd International Conference on Information and Communication Technology (ICoICT), Nusa Dua, Bali, Indonesia, 27–29 May 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 113–118.
105. Flores, D.A.; Qazi, F.; Jhumka, A. Bring your own disclosure: analysing BYOD threats to corporate information. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; IEEE: Piscataway, NJ, USA, 2016, pp. 1008–1015.
106. Zulkefli, Z.; Singh, M.M.; Malim, N.H.A.H. Advanced persistent threat mitigation using multi level security–access control framework. In Proceedings of the International Conference on Computational Science and Its Applications; Springer: Berlin/Heidelberg, Germany, 2015; pp. 90–105.
107. Hajdarevic, K.; Allen, P.; Spremic, M. Proactive security metrics for bring your own device (byod) in iso 27001 supported environments. In Proceedings of the 2016 24th Telecommunications Forum (TELFOR), Belgrade, Serbia, 22–23 November 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–4.
108. Aldini, A.; Seigneur, J.M.; Lafuente, C.B.; Titi, X.; Guislain, J. Formal modeling and verification of opportunity-enabled risk management. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; IEEE: Piscataway, NJ, USA, 2015; Volume 1, pp. 676–684.
109. Morrison, A.; Xue, L.; Chen, A.; Luo, X. Enforcing Context-Aware BYOD Policies with In-Network Security. In Proceedings of the 10th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 18), Boston, MA, USA, 8–9 July 2018.
110. Armando, A.; Costa, G.; Merlo, A.; Verderame, L.; Wrona, K. Developing a NATO BYOD security policy. In Proceedings of the 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 23–24 May 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
111. Samaras, V.; Daskapan, S.; Ahmad, R.; Ray, S.K. An enterprise security architecture for accessing SaaS cloud services with BYOD. In Proceedings of the 2014 Australasian Telecommunication Networks and Applications Conference (ATNAC), Southbank, VIC, Australia, 26–28 November 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 129–134.
112. Perini, V.L.; de Fátima Webber do Prado Lima, M. BYOD Manager Kit: Integration of Administration and Security Tools BYOD. In Proceedings of the XIV Brazilian Symposium on Information Systems, Caxias do Sul, Brazil, 4–8 June 2018; pp. 1–9.
113. Zain, Z.M.; Othman, S.H.; Kadir, R. Security-Based BYOD Risk Assessment Metamodelling Approach. In Proceedings of the 21st Pacific Asia Conference on Information Systems (PACIS 2017), Langkawi, Malaysia, 16–20 July 2017.
114. Liu, X.; Qian, F.; Qian, Z. Selective HTTPS traffic manipulation at middleboxes for BYOD devices. In Proceedings of the 2017 IEEE 25th International Conference on Network Protocols (ICNP), Toronto, ON, Canada, 10–13 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–10.
115. Koesyairy, A.A.; Kurniawan, A.; Hidayanto, A.N.; Budi, N.F.A.; Samik-Ibrahim, R.M. Mapping Internal Control of Data Security Issues of BYOD Program in Indonesian Banking Sector. In Proceedings of the 2019 5th International Conference on Computing Engineering and Design (ICCED), Singapore, 11–13 April 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5.
116. Chu, P.Y.; Lu, W.H.; Lin, J.W.; Wu, Y.S. Enforcing enterprise mobile application security policy with plugin framework. In Proceedings of the 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan, 4–7 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 263–268.

117. Downer, K.; Bhattacharya, M. BYOD security: A study of human dimensions. *Informatics* **2022**, *9*, 16. [CrossRef]
118. Ali, S.; Qureshi, M.N.; Abbasi, A.G. Analysis of BYOD security frameworks. In Proceedings of the 2015 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, 18 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 56–61.