Hindawi
Security and Communication Networks
Volume 2017, Article ID 2057260, 11 pages
https://doi.org/10.1155/2017/2057260

WILEY | Hindawi

Review Article

A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives

Chalee Vorakulpipat, Soontorn Sirapaisan, Ekkachan Rattanalerdnusorn, and Visut Savangsuk

National Electronics and Computer Technology Center, 112 Thailand Science Park, Phahonyothin Road, Khlong 1, Khlong Luang, Pathum Thani 12120, Thailand

Correspondence should be addressed to Chalee Vorakulpipat; chalee.vorakulpipat@nectec.or.th

Received 1 September 2016; Revised 3 November 2016; Accepted 15 November 2016; Published 12 January 2017

Academic Editor: Alexandre Viejo

Today, many organizations allow their employees to bring their own smartphones or tablets to work and to access the corporate network, which is known as a bring your own device (BYOD). However, many such companies overlook potential security risks concerning privacy and confidentiality. This paper provides a review of existing literature concerning the preservation of privacy and confidentiality, with a focus on recent trends in the use of BYOD. This review spans a large spectrum of information security research, ranging from management (risk and policy) to technical aspects of privacy and confidentiality in BYOD. Furthermore, this study proposes a policy-based framework for preserving data confidentiality in BYOD. This framework considers a number of aspects of information security and corresponding techniques, such as policy, location privacy, centralized control, cryptography, and operating system level security, which have been omitted in previous studies. The main contribution is to investigate recent trends concerning the preservation of confidentiality in BYOD from the perspective of information security and to analyze the critical and comprehensive factors needed to strengthen data privacy in BYOD. Finally, this paper provides a foundation for developing the concept of preserving confidentiality in BYOD and describes the key technical and organizational challenges faced by BYOD-friendly organizations.

1. Introduction

Bring your own device (BYOD) policies that include smartphones and tablets have played an important role in technological enhancements over the past decade. Today, many organizations employ a BYOD policy and allow their employees to freely use BYOD. Some companies view this as an opportunity to implement new technology without investing their own resources on devices [1]. Often, employees simply bring their devices to work because they own those devices and use them to play games or watch videos while at work. On many occasions, those employees who do use these devices for work do so without prior authorization from their employer, and, in the majority of cases, there are no workplace rules regarding the use of such devices. However, many employers overlook security concerns regarding potential leaks of private or confidential information. For instance, if an employee loses his/her smartphone which may contain confidential organizational data such as email and trade secrets, there is potential of that data leaking in an unauthorized fashion to the public. This can be detrimental to the organization's reputation and profitability [2]. In light of such issues, security management can be addressed in various manners, depending on the organization's policies. An organization may allow devices to be used freely, in a limited manner with some restrictions, or not at all. A security policy may state clear guidelines regarding BYOD but not contain technical guidelines that employees can implement. Factors such as access control, intrusion detection, protocol vulnerability and threat assessment, cryptography, device and OS security, and security management should be taken into account while implementing BYOD security. A framework that addresses

these factors could provide a guideline for implementing mechanisms to control BYOD at an organization level.

The objective of this study is to provide a guiding framework for BYOD control, with an emphasis on preserving confidentiality and privacy. This paper is divided into five sections. Following this introduction, related studies are discussed regarding BYOD and security. Then, the proposed framework and an analysis of this framework are presented, respectively. The final section provides a conclusion and suggestions for further study.

2. Related Research

2.1. BYOD Overview and Comparison. The use of mobile devices, including laptops, smartphones, and tablets, is common in workplaces, and the implementation of BYOD controls would significantly reduce security breaches associated with BYOD [3]. However, trends in how employees prefer to use mobile devices have been evolving. Traditionally, companies would configure mobile devices for their employees to work within the office or on site. Because the company would have full control over these devices and the network infrastructure, they could ensure that the devices complied with company security policies. Security measures would be in place, so that the company could manage risks and control any damage that might result from policy violations. It has been reported that companies spend large portions of their budgets for such a provision of mobile devices. This strategy is known as corporate owned, personally enabled (COPE) [4], here is your own device (HYOD), choose your own device (CYOD) [5], or use what you are told (UWYT) [6]. Unlike conventional schemes, some companies have adopted a new policy, which supports the use of employees' personal mobile devices in the office and working environments and is called bring your own device (BYOD). Some employees prefer this option and have begun to bring their own devices to work with them wherever they go. This working style results in increased flexibility and agility and less frustration, as employees can work anywhere with familiar devices. Some employees and executives believe that they can enhance productivity through the integration of work and lifestyles. Regardless of the additional work required to support the use of BYOD, this policy can reduce the corporate costs of hardware provision.

A summary of the differences between HYOD and BYOD is presented in Table 1, and detailed information can be found in the work of Singh [6].

2.2. Risks and Concerns. Despite the fact that both companies and their employees can benefit from various aspects of BYOD, there are also risks and concerns accompanying the adoption of BYOD.

Often, the use of BYOD results in conflicts between usability and security [5, 7]. Typically, users tend to value usability over security, because they simply want to do their jobs effectively without worrying about cumbersome security measures. Hence, while the use of BYOD can result in higher employee satisfaction, it can also increase certain security risks and concerns, such as the following aspects.

(i) Network Access Controls. Mobile devices that can remotely connect to corporate networks from anywhere at anytime can place the corporate network and corresponding data at risk. Without proper protection, adversaries may be able to intercept corporate information or even impersonate legitimate employees and illegally gain access to networks and services.

(ii) Vulnerabilities and Exploitation. Devices that are centrally managed by an organization are generally better protected as their security profiles must meet stricter standards. This means these devices are in a more controlled environment and not as susceptible to exploitation. On the other hand, devices owned by individual employees may or may not comply with regulations and standards, hence leading to uncontrollable vulnerabilities. When vulnerable devices connect to a corporate network, they present new exploitable security holes concerning the whole network.

(iii) Corporate Applications. Companies may offer certain applications and services for which they wish to allow access only to employees with sufficient privileges and appropriate roles. Traditional measures of who can access such resources may not be sufficient. Companies may need to consider, for instance, which devices can access these resources where and when.

(iv) Device Policies. The security posture of organizational owned devices is more straightforward to design and implement using a security guideline or template. Devices that are employee-owned and are not managed centrally by the organization may not meet the security standards required and thus place organizational data at risk.

(v) Data Protection. In BYOD scenarios, company data such as corporate emails, classified documents, and project photos can be stored together with users' private data. Protection measures regarding data leakage in the event of lost or stolen devices must be in place to protect corporate data. Storage encryption and remote data wiping should be considered as a line of defense in order to prevent data from falling into the wrong hands.

In 2014, the well-known security company Symantec conducted an experiment to investigate what would happen to lost mobile devices in the real world, by intentionally "losing" devices incites with high traffic. This project was called the "Honey Stick Project" [8]. In the experiment, Symantec loaded mobile phones with dummy information, including bank accounts, HR salaries, personal photos, and other documents, and installed tracking software to monitor what would happen after the phones were found. The phones were left without security protection, such as screen locks, so that their finders could do virtually anything they wanted with the phones. The phones were dropped in six Canadian cities: Vancouver, Calgary, Toronto, Ottawa, Montreal, and Halifax. The major findings of the investigation were as follows:

(i) 93% of people accessed the phones.

(ii) 63% of people viewed corporate emails.

Table 1: Differences between HYOD and BYOD.

	HYOD (employer's devices)	BYOD (employee's devices)
Information security governance	(i) Standardized devices (ii) Tightly coupled (iii) Focus on corporate control (iv) Fully controllable	(i) Diverse devices (ii) Loosely coupled (iii) Focus on flexibility and agility (iv) Partially controllable, require user awareness
Operations	(i) Full centralized management (ii) Standard hardware (iii) Standard software (iv) Acceptable use policy	(i) User is responsible for their own devices (ii) Hardware of their choice (iii) Standard and user's software (iv) Acceptable use policy and BYOD policy
Personnel	(i) Lesser level of employee technical ability (ii) Central support (iii) Lower cost for personnel training due to standard devices	(i) Higher level of employee technical ability (ii) Central support and self-service (iii) Higher cost for personnel training due to diverse devices
Information and data flow	(i) Centrally provisioned and secured information (ii) Easier to comply with rules and audit (iii) Easier to implement access control to limit information leakage	(i) Centrally provisioned, distributed security (ii) Harder to comply with rules and audit (iii) Harder to implement access control to limit information leakage (iv) Remote information wiping is required
Application	(i) Standard and corporate applications (ii) Controllable vulnerabilities and data leakage	(i) Standard, corporate, and user's applications (ii) Harder to control vulnerabilities and data leakage, sandboxed or container management (iii) Focus on open standards
System	(i) Centralized control of access to applications, systems, and information	(i) Centralized control of infrastructure, distributed control of applications and information

(iii) 83% of people viewed personal data.

(iv) 50% of people viewed private photos.

(v) 55% of people tried to return the phones.

Apparently, in the absence of proper protection measures, once mobile devices are lost, it is very likely that information on those phones will be exposed, which could result in serious data leakages.

2.3. Location-Based Service. Advances in location detecting technology for mobile devices have accelerated the development of and demand for location-based services (LBS) [9, 10]. LBS are services that leverage a user's geographical location in order to deliver personalized information. In order to better understand LBS, let us consider the following scenarios.

(i) Alice Is Currently Staying in Thailand. When she types the keywords "famous sightseeing" into the input box of a search engine, the search engine will return results for "famous sightseeing" in Thailand, such as the Grand Palace, Doi Inthanon, and Phuket. Other locations, such as the Forbidden City or Big Ben, are excluded from the search results, because they are not located in Thailand.

(ii) Bob Is Visiting His Friend at NECTEC. He wants to know the locations of the nearest big shopping malls in the area, so he opens a map application on his mobile phone and searches for "big shopping malls." The app returns Future Park Rangsit as the first result, based on his present location, rather than Siam Paragon or Central World.

(iii) Kate Uses a Social Network App on Her Mobile Phone. It has a feature called "Shake and meet new friends." When she shakes her phone, the app sends a request for a list of users who are currently staying nearby and then shows Kate a list of users that are close to her location. Then, she can begin to chat with these new friends.

These customized services are made possible by modern positioning technologies, especially on mobile devices. There are several common techniques that are used to locate positions of mobile devices. Global positioning system (GPS) is a navigation system that provides location and time data for a client to a GPS receiver, through communications with four or more GPS satellites. Other similar technologies can be used in a similar manner, such as GLONASS, IRNSS, and BeiDou-2. Furthermore, cellular triangulation uses raw radio

measurements to determine the locations of devices relative to tower bases, and the WiFi positioning system (WiPS) is mainly used for indoor positioning systems.

LBS can be utilized in a BYOD environment to track devices and enforce location-based policies. For instance, a policy may allow employees to use their mobile devices in corporate locations without screen locking, but once employees leave such areas, the devices can be locked, and employees must enter a passcode in order to unlock their device. In the case of lost or forgotten devices, devices' locations can be used to help locate and retrieve those devices.

2.4. Operating System Level. To secure BYOD at an operating system (OS) level, the White House in the United States (US) suggests that virtualization, walled gardens, and limited separation should be included in a BYOD policy to allow access to personal and corporate data on the same device [11], which was also confirmed in [12, 13]. Virtualization is employed as a virtual desktop solution or thin client, which allows computing resources to be accessed remotely on personal devices without data being stored or apps being processed [12, 14]. Therefore, mobile device management (MDM) may not be required, because data processing takes place on a corporate server. In addition, a virtualization-based technique called virtual machine (VM) is used to separate an enterprise space from a personal space. A hypervisor or virtual machine monitor (VMM) is implemented to create a VM. Either a Type-1 or Type-2 hypervisor can be selected [12]. However, the criteria of selection are based on separation levels, performance, and OS kernels. For example, a Type-1 hypervisor provides the best separation between personal space and corporate space, but the performance is poorer. A Type-2 hypervisor is more flexible, but the OS security can be compromised. Nevertheless, it is clear that mobile visualization faces some practical challenges. For example, hardware level virtualization requires the support of mobile device vendors, whereas software level virtualization is not fully secure against malware [15]. A study that considers OS-level virtualization for containers describes the two crucial drawbacks of additional resource constraints and severe performance limitations [16]. Despite this, it has been suggested that, in order to minimize user reactance and enable seamless, transparent personas, the use of universal standards are required for VMs (instead of limiting reliance on vendors), such as TCP/IP and loosely coupled architectures [15].

Regarding walled gardens or walled sandboxes, corporate data and apps are processed within a separate secure partition or secure application on the personal device, and this can ensure the separation between personal and corporate data [11]. A secure application can provide MDM services in the form of cloud-based software-as-a-service, in order to synchronize emails, calendars, and contacts [11]. To apply a walled garden in a BYOD enterprise architecture, internal services can be either logically or physically separated when accessed by personal devices and corporate-owned devices [17]. In fact, physical separation reduces the risk of data leakage [17]. Sensitive information storage methods usually employ a walled garden approach. For example, in cancer research, private personal information is simply moved to a walled garden, from where it is securely combined with public datasets [18]. Furthermore, tutors at the Open University can provide online courses using a secure messaging service via a walled garden [19]. In terms of app development, walled gardens are used to separate app developer areas from manufacturer areas and in most cases are associated with licensing issues [20]. Today, mobile device platforms (e.g., iOS and Android) operate within a strict walled garden, which results in severe limitations for organization-based applications [21]. The introduction of a cross-platform message delivery system is highly recommended [21].

While the separation between personal data and corporate data ensures security, it can inhibit seamless operations. A limited separation allows personal and corporate data to be processed on the same device, while enforcing policies to ensure that minimum security requirements are met [11, 22, 23]. The combination of policies, practices, and technical controls must be implemented successfully in order to be accepted by mobile device users [24]. An organization must provide MDM solutions for limited separation implementation to ensure security and privacy. For example, the data on a mobile device can be remotely wiped when a user violates the BYOD policy. Because of this, limited separation can be confronted with both technical and management issues. Limited separation may be the least expensive solution, owing to (a) the lack of requirements; (b) the ease of implementation, because it can work with existing infrastructures; and (c) the existence of this function in the two well-known operating systems iOS and Android [25].

In addition, trusted boot in mobile devices has recently become increasingly important for improving the security of the boot sequence. This falls into the following two categories of (a) secure boot where the boot sequence is evaluated and aborted if a suspicious component attempts to be loaded and (b) trusted boot where a log is maintained during the boot process for later audit [26]. Secure boot has been criticized for locking down devices, resulting in limited functionality. On the other hand, trusted boot lacks the enforcement of run-time verification [26]. Therefore, a software-only approach cannot fully secure software applications on mobile devices against cyberattacks, especially for operating systems with end-user access, which can be hacked [27]. A number of studies have proposed a dedicated security hardware-assisted solution, to customize trusted boot and thus to tackle the above problems [26–28]. Using a phone-centric approach, a trusted boot technique can protect data once the device has been switched on [29].

3. Proposed Framework

3.1. Policy. An organization must have a clear policy regarding BYOD use, whether that is to support its use fully, partially, or not at all [30]. This choice will depend on the level of security required in the organization. In addition, business requirements and productivity should also be considered. If an organization chooses to fully support BYOD, then that organization must accept security risks, and the adoption of BYOD policies is highly recommended. Many control mechanisms must be implemented to support these

policies. A top-down approach is generally used to distribute BYOD policies to employees. The corresponding mechanisms should be ready to employ prior to announcing the policy. However, if an organization does not allow BYOD, then that organization will avoid the associated security risks and BYOD policies or control mechanisms may not be required. Furthermore, the scope of the use of BYOD covered in the policy must be clearly defined. For example, a CIO should be able to decide whether or not the policy will cover a scenario in which a device is used at home to connect to the corporate network or where a device is used in an organization but does not connect to the corporate network or is offline.

3.2. Registration. If an organization allows the use of BYOD, then it is important to know the identities of devices and their owners. A device owner is required to register their identification (e.g., employee number, name, and email) and device identification (e.g., International Mobile Station Equipment Identity (IMEI)). This registration process can be automatic. The registration system can link device identification data to personal information stored in the organization's database system (such as a human research database). The registration process is the most important aspect of BYOD. The impact of a lack of registration may be equivalent to that of a lack of log storage.

3.3. Provision. If an organization fully supports BYOD use, then devices must be configured so as not to allow unauthorized users to gain access to the corporate network. There are several possible controls. For example, all devices must be protected by a passcode, to prevent unauthorized use. Failure to enter this correctly would be reported to the administrator or would result in the suspension of the use of BYOD. In addition, inappropriate use, such as jailbreaking or rooting a device that may result in an increase of vulnerability, should not be allowed, be closely monitored, or be allowed on a case-by-case basis (e.g., in the case of research purposes). Moreover, in some organizations, policies may limit the use of certain functions in BYOD, such as cameras. A mechanism to disable these functions can be implemented. For example, the camera app icon can be disabled or hidden.

3.4. Centralized Control. BYOD control mechanisms essentially involve data sanitization, compliance control, and centralized configuration control [31]. Moreover, all activities can be monitored and detected by an administrator. A dashboard is employed to signal misuses of BYOD. This helps to ensure that BYOD policy is followed. In terms of the preservation of confidential data, the administrator can force a factory reset to wipe all data or force selective wiping through a designated channel, such as Google Cloud Messaging for Android or another cloud-based system [31]. This mechanism helps to protect an organization's information assets in cases of lost or stolen BYOD devices. It is important that a communication channel through which a user can send a request to the administrator to wipe data exists. An appropriate authentication method is required to identify users. This is similar to an authentication method for mobile banking transactions. As mentioned, all such controls are completely centralized, and an agent connecting to the centralized control must be installed on the device.

3.5. Monitoring and Tracking. Besides the monitoring of activities related to access to the corporate network, the monitoring and tracking of locations are necessary. This is crucial when a device is an asset of an organization. Organizations sometimes place restrictions on the use of devices (either BYOD or organization-owned devices), where a user cannot use or bring the device outside of designated areas. A mechanism for tracking the locations of users could ensure that users do not bring devices outside of specific locations. This can be underpinned by GPS or a mobile network. Moreover, not only should information regarding physical locations be monitored and tracked, but rather contextual information (e.g., time-based, behavioral-based, and statistical-based information) should also be considered to control access [32]. Issues regarding privacy concerns may be raised, but monitoring and tracking systems can only be active during specific times, such as when a user borrows an organization-owned device for ad hoc work, or when a user is connecting to the corporate network using their BYOD device during working hours.

3.6. Location Privacy. Information regarding the locations of users' devices is legally collected for tracking purposes. This implies that user locations are also known to the company. If this location data is not stored under proper protection and is accessed by adversaries or malicious attackers, then the attackers may learn user identities, corporate interests, working routines, and so on and use this information for their own benefit. Hence, it is essential that location privacy is considered, in order to protect the privacy of users. The risks of location data exposure can be mitigated through several approaches. Location perturbation [33] is the simplest technique for preserving anonymity, by providing a dummy location back to the system. For instance, a random position in the legitimate range is reported back instead of the exact location of the user, as long as the user is still in the permitted area. Spatial cloaking [34–36], also referred to as location cloaking or location blurring, is a technique used to blur the user's exact location with a bigger area, called a "cloaked region." It is reported that location privacy depends strongly on the size of the cloaked region. The bigger the cloaked region, the more strongly the location privacy protected, and vice versa. For example, if a user is currently located at the NECTEC building, a larger fuzzy area name, such as Thailand Science Park or even the Khlong Luang District, can be employed as a cloaked region to disguise the user's location. An approach called k-anonymity [37–43] is used to blend the exact location of the user with other locations of users nearby that are impossible or difficult to distinguish. This approach uses a similar idea as spatial cloaking to blur the real location of the user but uses locations from a group of k users instead of a cloaked region. For instance, if Alice is currently located at NECTEC, while Bob, Charlie, and Dave are located at other buildings nearby, then Alice can hide her real location by

reporting the locations of all of these users, including hers, back to the system.

3.7. Password and Challenge Response. Passwords represent one authentication technique [44–46] that has been widely employed in many application domains over a longtime. In parlance of security terminology, this is categorized as a "something you know" authentication method. This leverages a concept where a service provider shares a secret with its users. The provider may share secrets with either a single individual or a group of users. Only valid users know this secret and use it to validate their identities and prove that they are who they claim to be. The password authentication scheme does not increase the cost of implementation, because it does not require special hardware or software. The protection it provides is as strong as its length, complexity, and difficulty to guess. A good password should be of reasonable length, mix various types of characters, and be difficult to guess for other people.

One major weakness of the password method is that if a password is discovered by an adversary by guessing, intercepting, brute force, or other means, then they can impersonate the identity of the user. To prevent password exposure through interception, guessing, or brute force attacks, a technique called a challenge-response mechanism can be introduced to reduce the risks posed by adversaries. Instead of simply relying on the password alone, a service provider will send a challenge value to a user, and the user then computes the response value and replies with this. The challenge-response authentication scheme is deployed in many well-known protocols, such as CHAP, CRAM-MD5, SCRAM, and Session Initialization Protocol. It can also be implemented as a solution to prevent bots from carrying out brute force attacks or accessing services, for example, using CAPTCHA or re-CAPTCHA. As a response to password guessing and cracking techniques becoming more sophisticated, the one-time password (OTP) technique has been introduced to solve the resulting problems. In practice, this has proved to be a considerably efficient authentication method, owing to the fact that it is volatile, unique, and only usable for a short period of time.

3.8. Public-Key Cryptography. Public-key cryptography [47, 48], also referred to as asymmetric cryptography, is a cryptographic algorithm that uses a pair of generated keys. These consist of a public key, which can be distributed widely in public spaces, and a private key, which is only accessible to the owner. The strength of the public-key cryptography system is a reflection of the difficulty of calculating the private key from its corresponding public key. Cryptographic algorithms are usually based on complex mathematical problems, such as integer factorization, discrete logarithm, and elliptic curve problems. One of the most widely employed public-key cryptography systems is RSA (Rivest-Shamir-Adleman), which is based on the practical difficulty of factoring products of two large prime numbers.

The private key-public key pair is used to encrypt and decrypt a message. If the private key is used to encrypt the message, then the message must be decrypted using the public key. In this manner, the message is guaranteed to originate from the real author only if it can be decrypted using the author's public key. Similarly, if the public key is used to encrypt the message, then the private key is used to decrypt it. This ensures that only the owner of the private key can view a message that is encrypted using their public key. A secure channel is not required for the exchange of public keys. However, the authenticity and the integrity of a public key are usually assured through a digital certificate issued by a "certificate authority (CA)" [49]. Today, certificateless signatures (CLSs) are used as a security model for managing the key escrow problem of identity-based signatures, with an emphasis on public-key replacements and strong unforgeability [50].

Owing to the computational complexity of public-key cryptography, it is commonly employed for small chunks of data, such as the exchange of a session key (symmetric key) that is used to secure a communication channel. The use of public-key cryptography can strengthen the security of BYOD communications. In the context of mobile commerce, cryptography algorithms and standards are taken into account for the purpose of energy-aware consumption [51].

3.9. Cryptographic Hash Function. The cryptographic hash function [52] is a mathematical algorithm that generates a fixed size bit string from data of an arbitrary size. It inherits the property of a one-way function, which means that it is impossible to recover the original input data from an output hash string. A slight change in the input data can significantly alter the output string (avalanche effect). Despite this irreversibility property, it is theoretically possible to find other input data that can produce the same output hash string. This is called hash collision. However, in practice, it is infeasible and impractical to carry out a collision attack on a good cryptographic hash function, because it is extremely difficult to find inputs that produce the same hash string from an infinite pool of data within a limited time.

Because of the uniqueness and irreversibility properties, cryptographic hash functions are widely employed in information security applications, especially in preserving user privacy and data integrity [53, 54]. The privacy of the user is achieved by applying cryptographic hash functions to sensitive information, such as usernames and passwords for accounts or personal identification numbers. Cryptographic hash functions are also used to create identification mechanisms or to summarize messages, which is similar to fingerprinting a person. Hence, this technique is also often called message digest or checksum.

This method can be used to verify the validity of data [55]. For example, a user can download a program installer from the internet and verify its hash value to check whether the installer is complete and has not been corrupted or altered by a malicious attacker. Another use case is cryptographic hash functions in PGP [56, 57], where a sender wants to send a message to the intended receivers, and the receivers want to verify the authenticity of the message. To ensure the integrity of the message and reduce computational costs, a digest of the message is computed and signed using the sender's private key, which is called the "signature," instead of signing the

whole message. The sender then sends the message, along with the signature, to the receivers. The receivers can verify the authenticity of the message by using the sender's public key to decrypt the signature and compare it with the message digest computed from the message by themselves.

Although cryptographic hash functions have been proven to be useful in practice for many cryptographic applications, obsolete algorithms such as MD5 are discouraged and should be avoided [58, 59]. For security reasons, stronger algorithms, such as algorithms from the SHA-2 family, should be used instead.

3.10. Virtualization, Walled Garden, Limited Separation, and Trusted Boot. System architecture security in BYOD situations addresses operating system level approaches, which include virtualization, walled gardens, limited separation, and trusted boots. The first three approaches are connected to business objectives. Therefore, prior to their implementation, information asset classification must be carried out, to determine personal as well as corporate data. In a policy-based framework, the implementation should also involve an information owner, who should be the best qualified person to verify the accuracy of personal and corporate data, as well as business objectives. Although a number of existing studies only suggest that the three technical approaches of virtualization, walled gardens, and limited separation should be included in a policy-based framework, it is presently also highly recommended that trusted boot should be considered for inclusion in a BYOD policy. This is because trusted boot techniques can help to achieve lower-level protection [60]. This means that lower-level programs can ensure the security of higher-level programs that are to be activated [61]. Either a software-only approach or a hardware-assisted solution can be chosen to implement trusted boot, depending on the level of security required.

4. Framework Analysis

A framework analysis reveals a number of factors that should be addressed in the implementation of BYOD controls. A summary of this analysis can be divided into categories based on technical specifications, as depicted in Table 2. The technical specifications adapted from [10] include network structures, secure communication channels, location-based functions, identity preservation, sensitive information preservation, platform dependency, multiple device management, provisioning, and policy enforcement.

Meanings and explanations of each technical specification topic listed in Table 2 are provided as follows.

(i) Network Structure. These are networks that are used for the transmission of data and control communications between management systems and mobile devices. Some large companies may have strict policies, clearly stating that all communication traffic must pass through their own corporate trusted or secured network, and all information must be stored under their autonomous sites.

(ii) Secure Communication Channel. These are mechanisms used to secure communications between management systems and mobile devices or between mobile devices and other mobile devices. This ensures that adversaries cannot easily intercept valuable information from a network.

(iii) Location-Based Function. The location information of mobile devices and users can be utilized for more than just viewing locations on a map. For instance, this information can be used to restrict the use of devices within given areas or to require that device holders must enter a passcode to unlock devices when using them outside of certain areas.

(iv) Identity Preservation. The identities of users should be appropriately protected, in order to avoid the risks associated with leakages of identity data. The cryptographic hash function method can be used to generate fingerprints of user accounts, so that the possibility of account information being accessed is reduced. To further protect identity data, techniques of blurring identities, such as k-anonymity and area cloaking, can also greatly help to protect identities.

(v) Sensitive Information Preservation. Sensitive information, such as account information, corporate emails, prototype photos, or project documents, should be stored securely and protected by reasonable measures. Besides passwords and challenge-response mechanisms, data encryption can strongly prevent unauthorized individuals from accessing sensitive information. Another layer of protection can be provided by remote wiping, which enables users to clear important data on their devices remotely, hence preventing valuable information from falling into the wrong hands when devices are lost.

(vi) Platform Dependency. Major mobile operating systems have their own mobile device management platforms, such as Find My iPhone for iOS and Android Device Manager for Android. There are also similar services provided by third-party developers, as standalone applications or as parts of features of their applications. However, from a corporate aspect, devices need to be manageable by both the owner of the device and the company. Thus, it is necessary to have a central platform for device management.

(vii) Security Architecture. Common security architectures and models are not sufficient to secure BYOD devices and enable the seamless execution of processes. The four techniques of virtualization, walled gardens, limited separation, and trusted boot should be considered, because all of these techniques not only focus on technical issues but also address business objectives and management issues.

(viii) Multiple Device Management. Owing to the rapid development and high popularity of smart devices, many people may own multiple mobile devices, such as smart phones, tablets, and smart wearable devices. A unified platform is crucial for the management of mobile devices in a company, so that each individual, as well as the company, can manage devices effectively and comply with policies.

(ix) Provisioning. It is very common that a considerable amount of people enter and leave job positions at an office.

Table 2: A comparative analysis of device management frameworks.

Technical specification	Typical personal device management framework	The proposed framework
Network structure	Public network	Corporate network, trusted network, and secured network
Secure communication channel	SSL/TLS, proprietary	SSL/TLS, VPN
Location-based function	Location tracking	Location tracking and location-based policy enforcement
Identity preservation	Unknown, proprietary	k-Anonymity, area cloaking, one-way hash, and public-key cryptographic
Sensitive information preservation	Unknown, optional	Passcode locking, data/storage encryption, and remote wiping/selective wiping
Platform dependency	Platform dependent, vendor specific	Platform independent
Security architecture	Operating system security in general	Emphasis on virtualization, walled garden, limited separation, and trusted boot
Multiple device management	Managed individually	Managed individually or centrally by company
Provisioning	Not provided	Corporate network connection, corporate email, and other corporate applications
Policy enforcement	Not provided	Role-based policy enforcing and location-based policy enforcing

The tasks involved in device provisioning are nontrivial. WiFi connection settings, setting up corporate email accounts, corporate application installations, and so on are tasks that consume time and human resources. A central management platform and corporate application store can automate these processes and greatly reduce the human effort that is required for these tasks.

(x) Policy Enforcement. In order for policies issued by a company to be effective, they must be suitably enforced such that employees comply. The proposed framework can help to enforce policies by providing tools to set policies for mobile devices based on the rolls and locations of the users.

An experiment is conducted to validate the framework in a real environment. To obtain a better understanding of the metrics used for framework validation, let us consider the real scenario described as follows. Dave is an employee in an organization that takes data security and the privacy of the organization seriously. This organization has issued and enforced a BYOD policy, with which every staff member must comply. The provisioning of devices must be carried out prior to letting staff begin using mobile devices for work, such as setting up corporate email and configuring WiFi setting. There are some mandatory requirements for Dave before he can use mobile devices provided by either the company or himself for work. These devices must connect to the centralized controller, so that the organization can detect if there are any suspicious activities that do not comply with their policy and also Dave can manage these devices remotely. The communication channel between the devices and the controller must be secured, in order to prevent malicious attackers or adversaries from intercepting confidential data or exploiting vulnerabilities and illegally accessing the devices. It is also crucial and common to use a VPN to establish a secure tunnel from the devices to the corporate network before accessing some internal services. When Dave is working at an external site, keeping track of location information can benefit both the organization and Dave. The positions of the devices can be used to determine which services and functionalities are open to Dave. Dave can also use location information as concrete evidence to prove that he is really on a business trip. If any devices are lost or stolen, then Dave can track their current or last-known locations, increasing the chance of retrieving the devices. More importantly, there should be a way to enable Dave to lock the devices or even to wipe all corporate data remotely, because confidential data can be considerably important and has the potential to result in catastrophic damage to an organization if it falls into the wrong hands.

In order to comply with the BYOD policy and satisfy the requirements explained above, an implementation of the framework is achieved through a centralized mobile device management platform, which has the necessary features and can manage devices remotely and straightforwardly. The platform supports the two most commonly used mobile operating systems, Android and iOS. WSO2 is used as the

Table 3: Implementation of the proposed framework.

Features implementation		Proposed framework
Network structure	Accessing within corporate network	+
	Accessing from public network	+
Secure communication channel	SSL/TLS	+
	VPN	−
Location-based function	Location tracking	+
	Location-based policy enforcing	∗
Identities preserving	Identities blurring/hiding	−
Sensitive information preserving	Passcode locking	+
	Data encryption	−
	Remote wiping	+
Platform dependency	Support major mobile OSes	+
	Central management platform	+
Security architecture	Virtualization, walled garden, and limit separation	+
	Trusted boot	+
Multiple devices management	Individual management	+
	Central management	+
Provisioning	Network connection	+
	Corporate email	+
	Corporate apps	+
Policy enforcing	Role-based enforcing	+
	Location-based enforcing	∗

+: the feature is implemented.
−: the feature is not implemented.
∗: the feature can possibly be implemented in the future.

main tool for developing the BYOD control mechanism for the Android platform, while the iOS platform also has its own mobile device management platform.

Although the underlying implementations are different for the different operating system platforms, they share common features that provide similar functionalities. The results of using these implementations to achieve the goals of the proposed framework are summarized and discussed in Table 3.

VPN functionality is not integrated into the platform directly. However, owing to the enterprise store capability allowing an administrator to upload corporate-specific applications that only company staff can access and download, a VPN application can be deployed through the corporate store, along with other internal applications. Because the communication channel for transmitting sensitive data from mobile devices to the platform is secured using an SSL/TLS tunnel, and organizations usually have concerns regarding accountability, hiding employees' identities is not necessary (because the company already knows who uses which devices), and it is practically impossible for other parties to intercept identity information. Typically, accessing configuration data for applications on these devices is impossible without rooting or jailbreaking devices, although other data stored on shared partitions can be accessed publicly. However, full storage encryption is possible, and users can enable this feature manually.

5. Conclusions

A policy-based framework for a BYOD environment should consider the key concepts of information security and privacy. The features in the framework described in this paper should be accordingly implemented in line with a company's information security and privacy policies. An organization must clearly define the allowed scope for use of BYOD and decide the extent to which the organization will support the use of BYOD. Because a BYOD policy is strongly linked to information security, it is necessary that an information security policy must first be implemented to determine the overall requirements. Thus, a BYOD policy must be based on an organization's information security policies. A mechanism for satisfying technical requirements, including network structure, secure communication channels, location-based functions, identity preservation, preservation of sensitive information, security architecture, platform dependency, multiple device management, provisioning, and policy enforcement, must be balanced effectively and must be based on the organization's information security policies. Furthermore, security levels (regarding privacy and confidentiality) should be determined based on business objectives. Thus, different organizations that adopt the same framework may operate at different levels of security. The recommendations for the further study can be established based on this paper. The proposed framework can be further studied in conjunction

with other existing mobile device management techniques to improve effectiveness and ensure validity and reliability of the solution. Ultimately, when the proposed framework is deployed in various ways in new organizational settings, the study of organization environment such as organization history and business objectives should be conducted first. It is hoped that the present review will contribute to the ongoing debate on BYOD policy and its future evolution.

Competing Interests

The authors declare that they have no competing interests.

References

[1] A. M. French, C. J. Guo, and J. P. Shim, "Current status, issues, and future of bring your own device (BYOD)," *Communications of the Association for Information Systems*, vol. 35, pp. 191–197, 2014.

[2] D. Sangroha and V. Gupta, "Exploring security theory approach in BYOD environment," *Smart Innovation, Systems and Technologies*, vol. 28, no. 2, pp. 259–266, 2014.

[3] N. Zahadat, P. Blessner, T. Blackburn, and B. A. Olson, "BYOD security engineering: a framework and its analysis," *Computers & Security*, vol. 55, pp. 81–99, 2015.

[4] J. Holleran, "Building a better BYOD strategy," *Risk Management*, vol. 61, pp. 12–14, 2014.

[5] A. Ghosh, P. K. Gajar, and S. Rai, "Bring your own device (BYOD): security risks and mitigating strategies," *Journal of Global Research in Computer Science*, no. 4, pp. 62–70, 2013.

[6] N. Singh, "BYOD genie is out of the bottle-'devil or angel,'" *Journal of Business Management Social Sciences Research*, vol. 1, pp. 1–12, 2012.

[7] B. Tokuyoshi, "The security implications of BYOD," *Network Security*, vol. 2013, no. 4, pp. 12–13, 2013.

[8] Symantec, *The Symantec Smartphone Honey Stick Project*, Symantec, Cupertino, Calif, USA, 2012.

[9] S. Teerakanok, C. Vorakulpipat, S. Kamolphiwong, and S. Siwamogsatham, "Preserving user anonymity in context-aware location-based services: a proposed framework," *ETRI Journal*, vol. 35, no. 3, pp. 501–511, 2013.

[10] S. Teerakanok, M. Pattaranantakul, C. Vorakulpipat, S. Kamolphiwong, and S. Siwamogsatham, "A privacy-preserving framework for location-based service: a review of structural design and analysis," *IETE Technical Review*, vol. 31, pp. 422–439, 2014.

[11] The White House, "Bring Your Own Device," 2012, https://www.whitehouse.gov/digitalgov/bring-your-own-device.

[12] J. M. Chang, P.-C. Ho, and T.-C. Chang, "Securing bYOD," *IT Professional*, vol. 16, no. 5, pp. 9–11, 2014.

[13] S. Earley, R. Harmon, M. R. Lee, and S. Mithas, "From BYOD to BYOA, phishing, and botnets," *IT Professional*, vol. 16, no. 5, pp. 16–18, 2014.

[14] Y. Dong, J. Mao, H. Guan, J. Li, and Y. Chen, "A virtualization solution for BYOD with dynamic platform context switching," *IEEE Micro*, vol. 35, no. 1, pp. 34–43, 2015.

[15] A. Hovav and F. F. Putri, "This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy," *Pervasive and Mobile Computing*, vol. 32, pp. 35–49, 2016.

[16] L. Xu, Z. Wang, and W. Chen, "The study and evaluation of ARM-based mobile virtualization," *nternational Journal of Distributed Sensor Networks*, vol. 11, no. 7, pp. 1–10, 2015.

[17] Centre for the Protection of National Infrastructure and CESG, "BYOD Guidance: Enterprise Considerations," 2014, https://www.gov.uk/government/publications/byod-guidance-enterprise-considerations/byod-guidance-enterprise-considerations.

[18] F. M. De La Vega, Y. Wu, T. Shmaya et al., "Abstract LB-308: a novel data safe haven approach to bring analyses to the International Cancer Genome Consortium data," *Cancer Research*, vol. 75, no. 15, pp. LB-308–LB-308, 2015.

[19] H. Farley and A. Pike, "Engaging prisoners in education: reducing risk and recidivism," *Journal of the International Corrections and Prisons Association*, vol. 1, pp. 65–73, 2016.

[20] A. Bhardwaj, K. Pandey, and R. Chopra, "Android and iOS security—an analysis and comparison report," *International Journal of Information Security and Cybercrime*, vol. 5, no. 1, pp. 32–44, 2016.

[21] D. Jaramillo, R. Newhook, and R. Smart, "Cross-platform, secure message delivery for mobile devices," in *Proceedings of the IEEE SoutheastCon*, Jacksonville, Fla, USA, April 2013.

[22] L. Rafferty, B. Kroese, and P. C. K. Hung, "Toy computing background," in *Mobile Services for Toy Computing*, P. C. K. Hung, Ed., pp. 9–38, 2015.

[23] CIO Council, "A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs," 2012, https://cio.gov/wp-content/uploads/downloads/2012/09/byod-toolkit.pdf.

[24] A. Cormack, "BYOD toolkit," 2012, https://community.jisc.ac.uk/blogs/regulatory-developments/article/byod-toolkit.

[25] J. Booker, S. Peng, S. Meduri, and J. German, "Bring Your Own Device: An Interactive Report," 2015, http://apps.pittsburghpa.gov/cis/BYOD_interactive.pptx.pdf.

[26] J. González, M. Hölzl, P. Riedl, P. Bonnet, and R. Mayrhofer, "A practical hardware-assisted approach to customize trusted boot for mobile devices," in *Proceedings of the in International Conference on Information Security*, Hong Kong, China, October 2014.

[27] M. Baentsch, P. Buhler, L. Garcés-Erice et al., "IBM secure enterprise desktop," *IBM Journal of Research and Development*, vol. 58, no. 1, Article ID 6717139, 2014.

[28] V. Chandra and R. Aitken, "Mobile hardware security," in *Proceedings of the IEEE Hot Chips 26 Symposium (HCS '14)*, pp. 1–40, IEEE, Cupertino, Calif, USA, August 2014.

[29] A. B. Garba, J. Armarego, and D. Murray, "Bring your own device organisational information security and privacy," *ARPN Journal of Engineering and Applied Sciences*, vol. 10, no. 3, pp. 1279–1287, 2015.

[30] Azzurri Communications, *Azzurri's BYOD Matrix*, Azzurri Communications, Surrey, UK, 2014.

[31] C. Vorakulpipat, C. Polprasert, and S. Siwamogsatham, "Managing mobile device security in critical infrastructure sectors," in *Proceedings of the 7th International Conference on Security of Information and Networks (SIN'14)*, pp. 65–68, Scotland, UK, September 2014.

[32] D. Kang, J. Oh, and C. Im, "Context based smart access control on BYOD environments," *Information Security Applications*, vol. 8909, pp. 165–176, 2015.

[33] R. Dewri, "Local differential perturbations: location privacy under approximate knowledge attackers," *IEEE Transactions on Mobile Computing*, vol. 12, no. 12, pp. 2360–2372, 2013.

[34] P.-Y. Li, W.-C. Peng, T.-W. Wang, W.-S. Ku, J. Xu, and J. A. Hamilton Jr., "A cloaking algorithm based on spatial networks for location privacy," in *Proceedings of the IEEE International*

Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC '08), pp. 90–97, IEEE, Taichung, Taiwan, June 2008.

[35] C.-Y. Chow, M. F. Mokbel, and X. Liu, "Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments," *GeoInformatica*, vol. 15, no. 2, pp. 351–380, 2011.

[36] T. C. Li and W. T. Zhu, "Protecting user anonymity in location-based services with fragmented cloaking region," in *Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE'12)*, pp. 227–231, Zhangjiajie, China, May 2012.

[37] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1–18, 2008.

[38] L. Sweeney, "k-Anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[39] G. Zhong and U. Hengartner, "A distributed k-anonymity protocol for location privacy," in *Proceedings of the 7th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'09)*, Galveston, Tex, USA, March 2009.

[40] S. Wang and X. S. Wang, "AnonTwist: nearest neighbor querying with both location privacy and k-anonymity for mobileusers," in *Proceedings of the International Conference on Mobile Data Management, System, Services, and Middleware*, Taipei, Taiwan, 2009.

[41] T. Hashem, L. Kulik, and R. Zhang, "Privacy preserving group nearest neighbor queries," in *Proceedings of the 13th International Conference on Extending Database Technology (EDBT '10)*, Lausanne, Switzerland, March 2010.

[42] A. Masoumzadeh and J. Joshi, "An alternative approach to k-anonymity for location-based services," in *Proceedings of the International Conference on Mobile Web Information System*, Niagara Falls, Canada, 2011.

[43] R.-H. Hwang and F.-H. Huang, "SocailCloaking: a distributedarchitecture for k-anonymity location privacy protection," in *Proceedings of the International Conference on Computing, Networking and Communications ((ICNC'14)*, Honolulu, Hawaii, USA, February 2014.

[44] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[45] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell, "Stronger password authentication using browser extensions," in *Proceedings of the Usenix Security Symposium*, Baltimore, Md, USA, 2005.

[46] M. Sandirigama and A. Shimizu, "Simple and secure password authentication protocol (SAS)," *IEICE Transactions on Communications*, vol. 83, no. 6, pp. 1363–1365, 2000.

[47] M. E. Hellman, "An overview of public key cryptography," *IEEE Communications Magazine*, vol. 16, no. 5, pp. 42–49, 1978.

[48] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[49] B. A. Forouzan, *Cryptography and Network Security*, McGraw-Hill Higher Education, New Delhi, India, 2008.

[50] Y.-C. Chen and R. Tso, "A survey on security of certificateless signature schemes," *IETE Technical Review*, vol. 33, no. 2, pp. 115–121, 2016.

[51] F. Hamad, L. Smalov, and A. James, "Energy-aware security in M-commerce and the internet of things," *IETE Technical Review*, vol. 26, no. 5, pp. 357–362, 2009.

[52] B. Schneier, *One-Way Hash Functions, in Applied Cryptography*, John Wiley & Sons, Indianapolis, Ind, USA, 2015.

[53] A. H. M. Ragab and N. A. Ismail, "An efficientmessage digest algorithm (MD) for data security," in *Proceedings of the IEEE Region 10 International Conference on Electricaland Electronic Technology*, Singapore, 2001.

[54] A. Habib, D. Xu, M. Atallah, B. Bhargava, and J. Chuang, "A tree-based forward digest protocol to verify data integrity in distributed media streaming," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 7, pp. 1010–1013, 2005.

[55] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, 2011.

[56] D. Kumar, D. Kashyap, K. K. Mishra, and A. K. Misra, "Security Vs cost: an issue of multi-objective optimization for choosing PGP algorithms," in *Proceedings of the 2010 International Conference on Computer and Communication Technology (ICCCT'10)*, pp. 532–535, Uttar Pradesh, India, September 2010.

[57] W. Stallings, *Network and Internetwork Security: Principles and Practice*, Prentice Hall, Englewood Cliffs, NJ, USA, 1995.

[58] T. Xie and D. Feng, "How to find weak input differences for MD5 collision attacks," *IACR Cryptology ePrint Archive*, vol. 2009, p. 223, 2009.

[59] V. Klima, "Finding MD5 collisions on a notebook PC using multi-message modifications," *IACR Cryptology ePrint Archive*, vol. 2005, p. 102, 2005.

[60] C. Huang, C. Hou, H. Dai, Y. Ding, S. Fu, and M. Ji, "Research on Linux trusted boot method based on reverse integrity verification," *Scientific Programming*, vol. 2016, Article ID 4516596, 12 pages, 2016.

[61] Y. Inamura, T. Nakayama, and A. Takeshita, "Trusted mobile platform technology for secure terminals," *NTT DoCoMo Technical Journal*, vol. 7, pp. 25–39, 2005.