The Bioscan AN INTERNATIONAL QUARTERLY JOURNAL OF LIFE SCIENCES 19(2): S.I (1), 722-728, 2024 www.thebioscan.com

CLUSTERED BASED TECHNOLOGICAL AND ORGANIZATIONAL ASPECTS OF MOBILE DEVICE MANAGEMENT AND THEIR SECURITY CONCERNS

Dr. L. K Suresh Kumar

Associate Professor, Department of Computer Science & Engineering, UCE, Osmania University

Email: lksureshkumar@osmania.ac.in

DOI: https://doi.org/10.63001/tbs.2024.v19.i02.S.I(1).pp722-728

KEYWORDS
Change, Management, Implementation
Mobile device management (MDM)
Security, TOE, BYOD, Cloud-based solutions,
Security concerns, Device management features,
Device management elements,
Corporate infrastructure,
Employee productivity.

Received on:

19-09-2024

Accepted on:

21-12-2024

ABSTRACT

Due to security concerns, mobile device management (MDM) is gaining importance in enterprises. Unlike permanent equipment, which may be controlled by companies and local administrations, mobile devices can move about. Android powers the vast majority of modern smartphones. Here we will go over some of the current MDM-solutions, how they work, and how they affect change management. The purpose of this study is not to argue for or against any particular MDM-system. Mobile device management segmentation in cloud-based and on-premises operations, as well as the bring-your-own-device policy in comparison to company-owned devices, are discussed in the paper. The article delves into the features, aspects, security issues, and application of mobile device management. Additionally, we cover the present state of the industry's market, the mobile device management landscape, the significance and benefits of this field, and more.

INTRODUCTION

A significant percentage of individuals inside organizations using cellphones to obtain essential corporate information. Mobile device management (MDM) technologies are becoming indispensable. It is a rapidly expanding market that increases significantly each year. In 2012, the market value exceeded $500 million with over one hundred software manufacturers, and in 2015, the market value reached $2 billion. The projected MDM market value till 2019 is $3.94 billion [1]. The proliferation of mobile devices, coupled with a heightened need for security, ensures a continuous rise in market value insights. This article examines administration and security in Android devices. This article demonstrates that although the MDM solutions accommodate many devices, Android remains the predominant operating system in the mobile industry, as seen in Fig. 1. This article focuses on ensuring the compliance of additional devices and their management. Concerning the General Data Protection Regulation (GDPR), the implementation of a Master Data Management (MDM) solution is advantageous for organizations to guarantee compliance with data protection standards. This program facilitates centralized control of a company's mobile phone policy, enabling the limitation of functionalities to avoid misuse. Inappropriate use entails the potential loss of corporate data resulting from inadequate security configurations and the threat of detrimental installs by users, such as viruses or trojans on a firm's personal computer (PC). Although managers now use robust tools for securing PCs via group rules and antivirus software on Windows systems, as well as effective monitoring of user privileges on Linux computers, mobile devices inside organizations are devoid of such solutions. Moreover, while essential server equipment for a corporation might be securely housed in restricted-access areas, those using mobile devices are often not administrators. Individuals with physical access to the devices may potentially access a business network when using corporate APNs. This becomes crucial if a mobile device is neglected or misplaced.

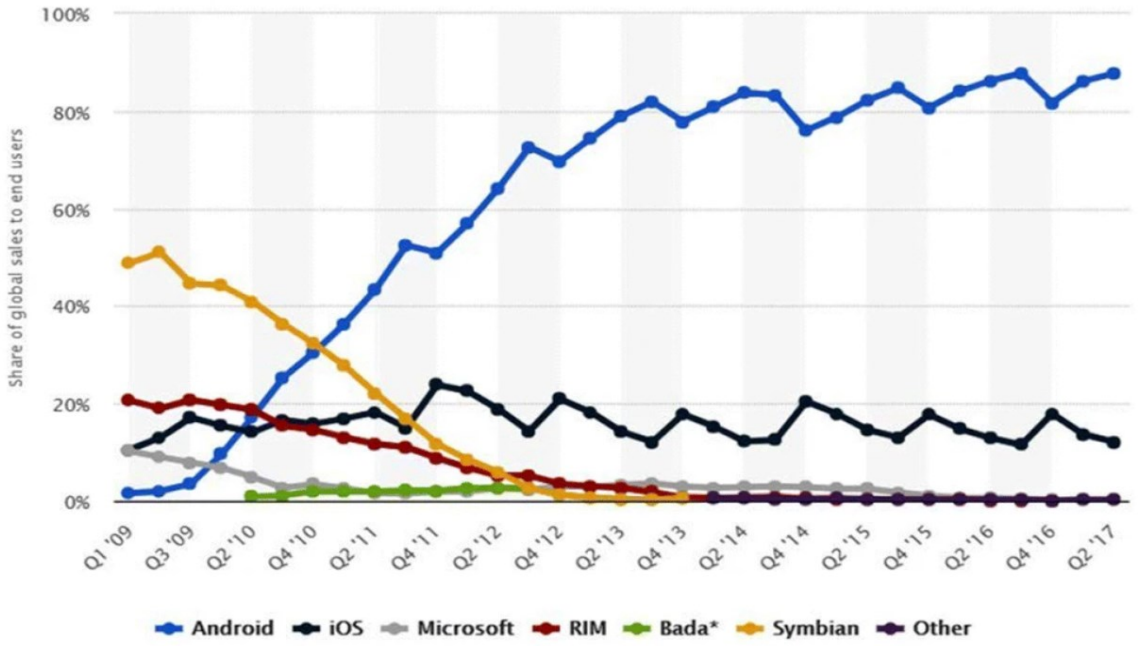

Fig. 1 Global market share held by the leading smartphone operating systems in sales to end users from 1st quarter 2009 to 1st quarter 2018 [2]

Mobile device management is a comprehensive technological term that encompasses the administration of mobile device use and the enforcement of related regulations within an enterprise. The primary objective of integrating mobile devices into the organization's IT infrastructure is to enhance efficiency and boost employee productivity. Mobile device management allows workers to use either company-owned or personal mobile devices for essential business functions while ensuring stringent security and adherence to policies. Furthermore, mobile device management may be executed across many computing environments, including on-premises and cloud-based solutions. It provides several benefits to the organization. Moreover, several components of mobile device management and the fundamental characteristics of an efficient solution exist. It has evolved as a technology, enhancing complexity and manageability over time.

Methodology

This study aims to provide an overview of one commercial and two freemium MDM solutions, focusing on their setup and centralized control via the cloud for devices used by staff members. The illustrative use case pertains to the limitation of the camera application on the mobile device. The procedures for executing this activity should serve as a framework for implementing additional situations, such as limiting use time, managing phone expenses, or geo-blocking a corporate device. This article presents organizational considerations about security for a corporation when its employees access the corporate network using personal devices.

To assess the technical aspects of adopting MDM systems, certain criteria must be satisfied. The appendix has a table that provides a decision framework for the company's management to choose the most suitable option. This article, however, cannot provide any recommendations for or against the examined MDM solutions owing to many factors that must be taken into account, such as pricing, device quantity, support, and personal preferences regarding graphical user interfaces (GUIs). The change management section will address potential implementation techniques grounded on organizational development and the Technology-Organization-Environment framework (TOE) [5], which will be applied to cloud-based Master Data Management systems. The assessed systems include the two freemium options, Miradore MDM and ManageEngine MDM, whilst Sophos MDM is offered as a comprehensive commercial solution. All systems include an on-premise installation component with supporting routines maintained in the cloud, as well as exclusively cloud-based solutions. Initially, we implemented the on-premises installation for testing reasons and then transitioned to cloud solutions. Given that all solution providers aim to relinquish their on-premises components in the MDM systems, this transition appears rational, particularly as on-premises solutions necessitate costly infrastructures such as Exchange/Sendmail servers and a messaging system to disseminate configuration profiles and compliance SMS, as illustrated at the conclusion of the appendix. Additionally, it should be noted that all solutions are compatible with web browsers.

Mobile Device Management Features

Using application programming interfaces (APIs), mobile device management solutions are mostly governed by mobile device hardware makers and operating system providers in terms of what they can and cannot do on these devices (Hong et al., 2016). Thus, these APIs may be integrated into mobile device management systems to provide device management services. Network isolation is one of the characteristics of mobile device management systems. According to Arnaud and Wright (2015), network segregation creates subnets inside the corporate network. In order to provide more secure connection inside the corporate network, each subnet is then allocated to a certain purpose and set of requirements, ensuring that only authorized or certified organizations may access the domains within those subnets. As a result, both internal and external unauthorized individuals cannot access data or other procedures.

Fig -2: Mobile Device Management

Application management is a component of mobile device management that enables a corporation to maintain a library of proprietary application software accessible to workers. These programs are securely maintained and distributed to workers in a controlled environment. They may be efficiently administered and enhanced with updated security and functional features.

Mobile device management systems provide monitoring capabilities (Hayes et al., 2020). This is accomplished using real-time network packet analysis of incoming and outgoing requests. The company's information technology management may remotely execute operations on these devices, including transmitting logs, diagnosing and rectifying faults, or locking and erasing the device's sensitive data in the event of a security breach. Policy enforcement is an additional aspect of mobile device management. The corporation may implement many corporate rules to regulate devices, including device-specific and platform-specific regulations (Hayes et al., 2020). Device or platform-specific rules provide the sophisticated administration of devices via their foundational operating system or platform suppliers. A personal policy is the second category that the corporation might implement to regulate device use in accordance with the corporate environment. Compliance policies are the third category of regulations established by the organization, dictating the rules to be followed in the use and management of mobile devices.

Additional typical mobile device management functionalities include virtual private network setup, predetermined network settings, remote data erasure, device locking, remote deactivation of native programs, whitelisting and blacklisting, enforcement of data encryption, and monitoring of device inventory.

Related work-security and compliance in general-technological aspects

Mobile Data Management (MDM) is essential for safeguarding a company's data. M. Pierer categorizes the notion of MDM systems into the following areas: definition of security policies, over-the-air policy distribution, compliance control, maintenance and monitoring, and response to policy violations. The practice of employees using their own devices with self-installed software is increasingly recognized as a trend and a catalyst for Mobile Device Management (MDM) and corporate rules [4]. Conversely, almost all mobile devices need a manufacturer account for proper use. This implies that individuals may inadvertently upload data to cloud servers. This occurs almost every time normal settings are used. All evaluated solutions have functionalities to limit settings in Android for the establishment of security profiles. The only issue was the potential consequences of using outdated technology. The only system, or more accurately its agent, proficient in maintaining an outdated Android version was Sophos. This system provides plugins for many hardware manufacturers of devices. However, the drawback is that both the agent and the plugin for the particular device must be installed. Both freemium systems provide a single client, but at least provide distinct support for Samsung mobile devices. The limits imposed by MDM differ between devices due to the diversity of Android platforms. The criteria for the assessed systems are not the quantity of potential limits, but rather the operational environment, particularly the configuration procedure, administration, and expenses. The evaluated systems included Sophos Mobile Device Management as a commercial solution, and Miradore and Mobile Device Manager Plus as freemium options. The criterion catalog is included in the appendix. The results indicated that the commercial system, owing to its compatibility with several plugins for various devices and a total cost of ownership over five years that is cheaper than that of a freemium system, would be the optimal selection. In terms of management, application deployment, and limitations, the characteristics of the evaluated systems exhibit little variation, as previously noted, as these configurations are contingent upon the controlled device and its Android operating system. Samsung smartphones equipped with Samsung KNOX, beginning with Android 5, impose much more limitations compared to Android devices without Samsung KNOX. The selection of the system to adopt must be determined by the quantity of controlled devices and the necessary security measures. It is essential to consider the need for supplementary server hardware in on-premises systems, while an outsourced cloud solution offers more flexibility and scalability. The evaluated freemium systems are only applicable for a corporation upon payment for premium services. Otherwise, customers face limitations on the number of devices and limits on profiles.

The MDM process involves setup or registration, the addition of devices, and ensuring compliance. Initially, an agent must be installed on the device. This agent must be obtained from the Google Play Store for Android devices or from the solution vendor as an APK file. Downloading these agents from other sources is inadvisable due to the potential for tampering. Depending on the device, plugins may exist for interfacing with the MDM. They are analogous to the hardware abstraction layers used in Windows or certain kernels in Linux. Samsung smartphones with Sophos MDM need the installation of the Sophos Mobile Control Application and the Sophos Samsung Plugin. Moreover, connection between the MDM and the smartphone must be activated. Companies reserve a static IP address for this purpose and establish a contract with a mobile network provider for each respective Access Point Name (APN). The benefit is that any smartphone using this APN may be included into an individual's workplace network. Regardless of whether a user opts for a personal device (BYOD) or one provided by the organization, the selection of a personal device (CYOD) pertains only to comfort. It is crucial that every mobile device utilizes your corporate firewall and can access only the resources

inside your network that have been granted to it. Once a device is compliant, management may be executed via rules tailored to the company's requirements. The deployment and management process (Fig. 3), including the enrollment of a mobile device to the issuance of security instructions, is an integral component of any MDM system.

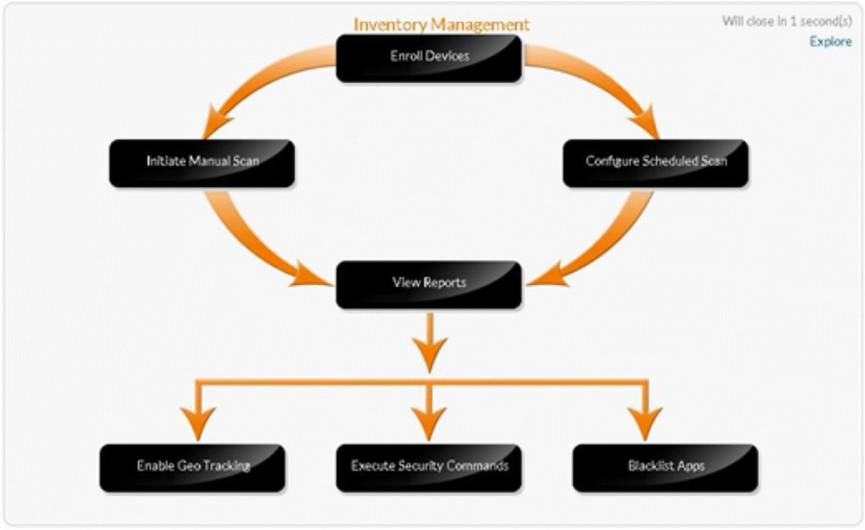

Fig. 3 The deployment and management process for the introduction of a MDM-soltion [1]

Moreover, the Play Store may be entirely deactivated. The setup of mobile devices is executed using the over-the-air standard (OTA), which is supported by all MDM systems. This standard guarantees the setup of devices using several channels such as near field communication (NFC), Bluetooth, Wireless Fidelity (WiFi)/wireless local area network (WLAN), or the mobile network itself [1]. Nearly all configurations available via the Android system may be limited. The primary advantage of MDM is the deployment of apps. This implies that you may do almost any task, such as managing Group Policy Objects (GPOs), inside a Windows context. Consequently, all mobile devices may be maintained at a uniform level, with similar program versions, thereby facilitating support and precluding users from independently upgrading their applications and testing compatibility prior to corporate approval of an update. The appendix will provide more information on the limitations on program use.

For security purposes, if a device is lost or reset, MDM guarantees that it can no longer access the corporate network, while administration is conducted via a web browser from any place [6]. The implementation of comprehensive security profiles is more critical than the distribution of APKs in preventing users from independently installing applications or modifying device specifications. The profiles prevent unauthorized adjustments to the settings. This also encompasses altering the APN, using SD cards for the storage of enterprise data, accessing WLANs, and employing the camera. The latter is an aesthetically pleasing attribute in crucial areas where photography is prohibited. Examples of this limitation are included in the appendix, along with the configuration of the MDM solutions.

Mobile Device Management Security

Security is a fundamental problem in mobile device management. Mobile devices are used to handle essential business data, including client information, database entries, emails, documents, and enterprise apps. The security of this data is crucial, since it might dictate the company's success or failure. Mobile device management solutions are therefore constructed using the most advanced cryptography methodologies. They are constructed using the principle of containerization, whereby essential data is handled inside these containers (Jaramillo et al., 2013). Containerization guarantees the segregation of users' personal data from business data on mobile devices.

Documents are used often in company operations and may include essential corporate information that requires safe management and usage. Mobile device management may impose limitations on the unauthorized dissemination of these materials to other domains or outside the business network domain (Kim et al., 2016). This will prevent the abuse of documents by device users. Moreover, internet connectivity is essential for remote device access and use. Mobile device management may compel users to use secure integrated browsers while restricting native browsers, therefore augmenting data security on the device and mitigating the danger of possible security breaches.

Mobile Device Management Implementation

A mobile device management system typically operates on a client-server architecture (Liu et al., 2010). Administration occurs via a client module and a server module. The server module may be situated in data centers on the firm premises or hosted on a cloud platform. The server component transmits instructions and other resources to an agent module located on the mobile device's client component. The agent is installed on the end-user device and utilizes application programming interfaces (APIs) to interact directly with the device's operating system. A single solution supplier may provide both client and server modules, while some companies offer them independently.

The server module transmits instructions and rules directly to the client component via a management console. The client component autonomously executes instructions and policies using APIs to interface with the operating systems of the client device. The mobile device management software often autonomously detects configured or connected devices and oversees their operations and setups, facilitating a user-friendly environment for information technology administrators. The automated function is essential as it enables scalability. The server and client modules are set in accordance with the company's rules. During operation, a record of connected devices is maintained, and settings and configurations are automatically sent over the air to unconfigured devices.

Mobile device management solutions have progressively advanced to enhance their efficiency. Previously, the mobile device required a connection or SIM installation to facilitate setup and settings. Subsequently, the client was required to commence the upgrading or configuring process to let the management to transmit logs and updates to the device. This method was tedious and compromised scalability and efficiency, particularly when several devices were involved. The existing solutions are fully automated using application programming interfaces.

The organizational aspect

Contemporary literature indicates that contemporary Master Data Management systems are cloud-based. Although they were not originally conceived in this manner [4], they evolved in this direction [8] and are mostly managed that so now [9]. The connection between technology, especially contemporary smartphone use, and organizational development has not been well examined in the literature. Research indicates that the fast implementation of technology may significantly impact institutional frameworks, including formal organizational

procedures, human behavior, and social interactions [10]. Organizations function within an environment that shapes their form, dictates their structure, presents possibilities, and introduces risks. Customers and rivals are important among these external influences.

An assessment of an enterprise's environment must first ascertain if a proposed change (implementation of an MDM solution) affects the organizational environment, particularly the external environment. If this is not applicable, just the internal organizational environment is taken into account.

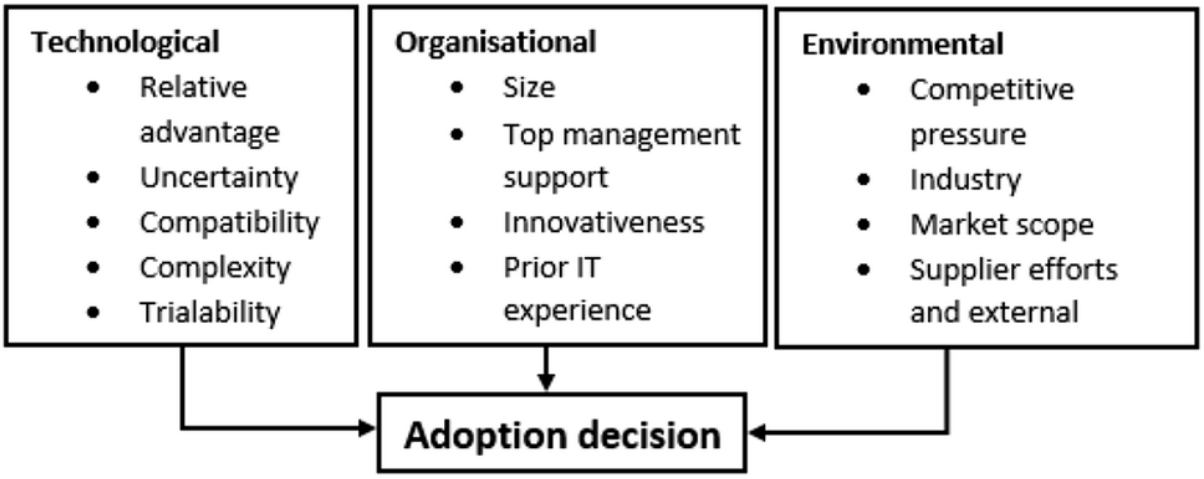

Fig. 4 The TOE framework [3]

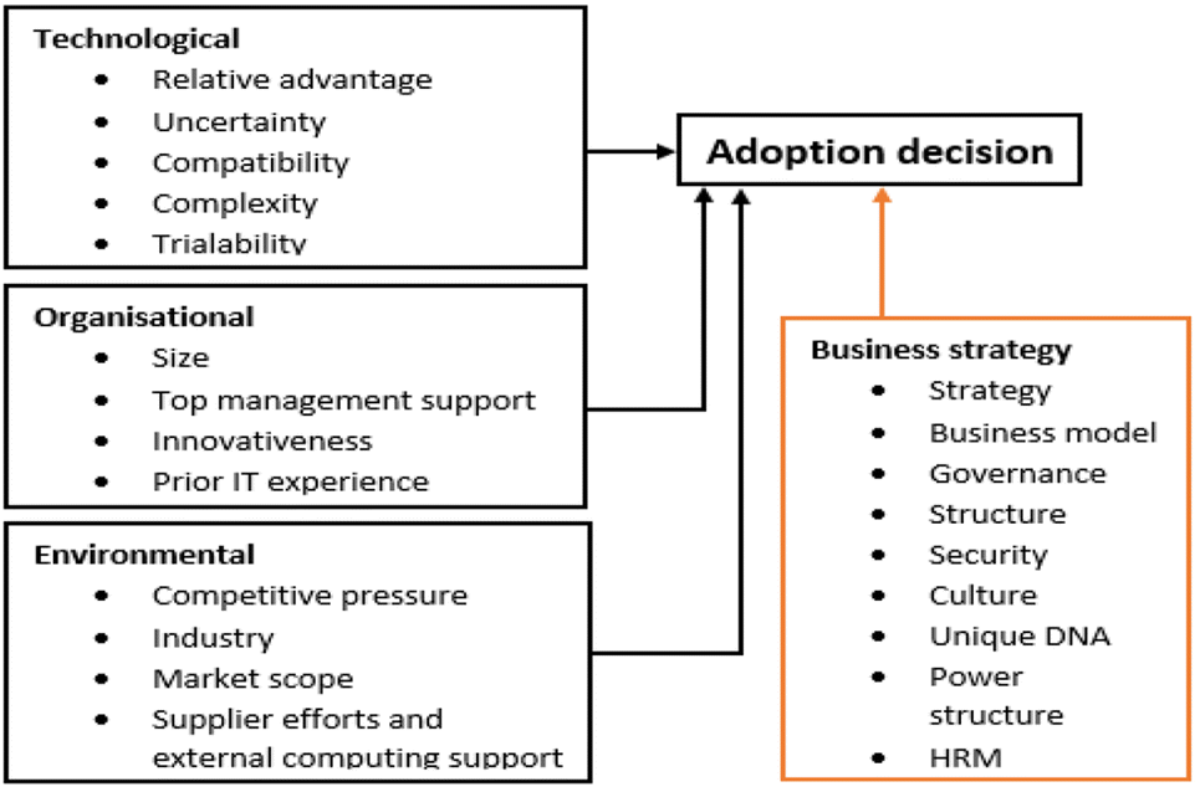

Fig. 5 The extended TOE framework [4]

While the implementation of an MDM solution may be perceived, as noted by Butterfield, "as a concrete discrete change with a defined timeframe and minimal emotional impact" [11], the introduction should not solely adhere to a Systems Intervention Strategy (SIS); rather, it should utilize this as a framework for a Change process and be supplemented by a pragmatic approach. The TOE framework is an organizational theory that delineates one aspect of how company environments affect the adoption and implementation of innovations, as seen in Fig. 4.

Min et al. assert that the Frameworks are predicated on three dimensions of a business context: Technological, Organizational, and Environmental. These factors influence choices linked to internet technology (IT) innovation, such as Master Data Management (MDM) and the implementation of technical advancements inside enterprises [13]. The technical context encompasses all technologies pertinent to the firm, those already used by the company, and those accessible in the marketplace but not presently utilized. The organizational environment encompasses the attributes and resources of a corporation, including the interconnections among personnel, internal communication channels, corporate scale, and the quantity of accessible resources. The environmental setting encompasses the

industry's structure, the accessibility of technological service providers, and the regulatory framework [14]. The descriptions of the components indicate that there are significant overarching business concerns that must be addressed. Consequently, an adaption of the TOE framework was undertaken, as seen in Fig. 5. As previously stated, these elements of the TOE are deemed crucial, as shown by several research. The likelihood of adopting ES increases with the apparent proportional benefit it offers [16,17]. Secondly, compatibility—defined as the extent to which perceived alignment exists with existing infrastructure, attitudes, and beliefs—enhances the likelihood of adoption [16, 17]. Thirdly, a lesser perceived complexity increases the likelihood of adoption [16, 17]. Moreover, the capacity to experiment with MDM facilitates its acceptance [16, 17]. Support from top management may foster a motivated atmosphere for the dissemination of innovation via verbal communications [18]. The likelihood of adoption increases with the level of support from senior management [16, 17]. An organization and its decision-making management must endeavor to evaluate and scrutinize potential alterations in organizational culture, processes, and work relationships to mitigate the adverse effects associated with the implementation of MDM solutions. Furthermore, experience is seen as a crucial element. The higher the level of knowledge inside the firm, the greater the likelihood of adoption, particularly with the use and familiarity with mobile devices. The sensation of trust is a crucial juncture. Trust is essential for fostering productive relationships across different settings, and competitive pressure serves as a potent motivator. Industry competition is widely acknowledged to favorably impact IT adoption, including MDM. The help from trade partners, namely the Provider of Device Management, significantly enhances adoption [17]. Security is a significant problem associated to trade partners, including not just authenticity, authorization, and responsibility but also focusing on data security, disaster recovery, and business continuity. Given that addressing security issues has always been a priority for most organizations, MDM should not provide atypical or supplementary difficulties. In several cases, the limited configuration or customization options of MDM evidently posed less security threats [18]. Additionally, the BYOD idea is a component of the security framework for organizations. Security and privacy must be prioritized as a comprehensive and cohesive process that encompasses the whole enterprise. The notion is currently widespread in several firms globally, and an effective plan may provide advantages for both people and enterprises. From an employee's perspective, it may enhance mobility, flexibility, and the capacity to embrace preferred technologies. Furthermore, it may result in enhanced work satisfaction and a rise in staff productivity inside firms. Contemporary Mobile Device Management (MDM) is essential for enabling employees to utilize their devices, as it facilitates the segregation of corporate and personal data, allowing both employers and employees to reap the advantages of using preferred devices (within specified constraints, such as operating system requirements) while mitigating risks. Moreover, the absence of an MDM solution is the primary cause of structural issues with BYOD [20]. Corporate Owned, Personal Enabled (COPE) serves as an alternative to the Bring Your Own Device (BYOD) method. The company purchases the mobile device, allowing the individual to use it for personal purposes. Despite the substantial initial expenditure for the company, the costs associated with auditing and monitoring are minimal. Furthermore, the end-user's familiarity with the mobile device is attributed to their propensity to use preferred mobile devices for professional activities.

Consequently, production and efficiency may be enhanced. Organizations often use a mix of these efforts. In departments that significantly hold sensitive data, it is prudent to choose the Corporate Owned Business Only (COBO) strategy.

CONCLUSION

Mobile device management offers crucial business support features for companies that use mobile devices in their operations, both company-owned and employee-owned devices. Mobile device management enables organizations to remotely and effectively manage mobile devices signed into their network. With the rise in the adoption of mobile devices in company operations, security threats have increased as these devices have become malware targets. Companies are therefore mandated to take responsibility for securing their vital data being processed and stored on these devices through mobile device management solutions. The solutions have evolved to address issues and challenges that have come up, such as diverse platforms. Different solutions have been created to cater to different organizational needs. However, there are core elements that each mobile device management solution must have to be deemed effective. Mobile device management offers many advantages to companies, especially in terms of security and automation. Mobile device management is a critical technology resource that companies can utilize to improve efficiency and productivity while allowing the simplicity of operations in a secure and regulations-compliant manner.

Regarding technological aspects, Mobile Device Management can be considered a solution for enterprises to extend their security from classic internal networks to mobile devices, even when users bring their own devices (BYOD). Yet, it also plays an essential role when using COPE or COBO approach in firms for security reasons. MDM ensures these devices are compliant with corporate policies, like GPOs in Windows. That means a user cannot tamper with a device without being banned from the corporate network once a policy violation is being detected. Even for the management, it is made much more comfortable to update many mobile devices to current software version (APK-files), comparable to software distribution in Windows. A mobile device can be remotely controlled as well, monitored, and restricted in their functions to the desired level.

REFERENCES

- Glowinski, K., Gossmann, C. & Strümpf, D. Analysis of a cloud-based mobile device management solution on android phones: technological and organizational aspects. *SN Appl. Sci.* **2**, 42 (2020). https://doi.org/10.1007/s42452-019-1819-z.
- Khaja Taiyab Mohiuddin , Fayed Mohammed Akbar , Mobile Device Management and Their Security Concerns, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 10 Issue: 10 | Oct 2023.
- DePietro R, Wiarda E, Fleischer M (1990) The context for change: organization, technology, and environment. In: Tornatzky LG, Fleischer M (eds) The process of technological innovation. Lexington Books, Lexington.
- Butterfield R, Maksuti S, Tauber M, et al (2016) Towards modelling, a cloud application's life cycle. In: 6th international conference on cloud computing and services science, pp 310–319. https ://doi.org/10.5220/00059 12403 10031 9316
- Yeo R, Marquardt M (2015) Think before you act: organizing structures of action in technology-induced change. J Organ Change Manag 28(4):511–528. https ://doi.org/10.1108/ JOCM-12-2013-0247
- Alizadeh M, Hassan W (2013) Challenges and opportunities of mobile cloud computing. In: IEEE 9th international wireless communications and mobile computing conference. https :// doi.org/10.1109/IWCMC .2013.65836 36. Accessed 22 July 2018.
- Jaramillo, D., Katz, N., Bodin, B., Tworek, W., Smart, R., & Cook, T. (2013). Cooperative solutions for bring-your-own-device (BYOD). IBM journal of research and development, 57(6), 5-1.
- Kim, G., Jeon, Y., & Kim, J. (2016, October). Secure mobile device management based on domain separation. In 2016 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 918-920). IEEE.
- Liu, L., Moulic, R., & Shea, D. (2010, November). Cloud service portal for mobile device management. In 2010 IEEE 7th International Conference on E-Business Engineering (pp. 474-478). IEEE.

- Ortbach, K., Brockmann, T., & Stieglitz, S. (2014). Drivers for the adoption of mobile device management in organizations.
- Steiner, P. (2014). Going beyond mobile device management. Computer Fraud & Security, 2014(4), 19-20.
- Tairov, I. (2019). Mobile device management as a component of corporate IT infrastructure.
- Yamin, M. M., & Katt, B. (2019, January). Mobile device management (MDM) technologies,
- Fortune Business Insights. (2020, July). Mobile Device Management Market Size, Growth | Share by 2028. https://www.fortunebusinessinsights.com/mobile-device-management-market-106381.
- Hayes, D., Cappa, F., & Le-Khac, N. A. (2020). An effective approach to mobile device management: Security and privacy issues associated with mobile applications. Digital Business, 1(1), 100001.
- Gangwar H, Date H, Ramaswamy R (2015) Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. J Enterp Inf Manag. https ://doi.org/10.1108/ JEIM-08-2013-0065.
- Borgman H, Bahli B, Heier H, Schewski F (2013) Cloudrise exploring cloud computing adoption and governance with the TOE framework. In: 46th Hawaii international conference on system sciences. https ://doi.org/10.1109/HICSS .2013.132.
- McKnight DH, Chervany L (2016) The meanings of trust. Technical Report MISR 96-04, Management Information Research Center, University of Minnesota, Minneapolis.
- Bello AG, Murray D, Armarego J (2017) A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. Inf Comput Secur 25(4):475- 492. https ://doi.org/10.1108/ICS-03-2016-0025
- Butterfield R (2015) Change management tools—a support booklet, prepared for the FH-Burgenland, Eisenstadt
- Stricklen M, McHale T, Caminetsky M, Reddy V (2008) Mobile device management. https ://paten timag es.stora ge.googl eapis .com/3b/ec/bf/cfe24 b906c a78e/US200 80070 495A1 .pdf.Accessed 02 Apr 2018.
- Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519-526
- Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto)