ISSN 2712-0562
Sustainable Engineering and Innovation
Original Research
Vol. 5, No. 2, December 2023, pp.247-260
https://doi.org/10.37868/sei.vi.id234

Enhancing BYOD mobile device security in a hybrid environment

Samur Ahmadov[1*]
[1] Azerbaijan Technical University, Azerbaijan

*Corresponding author E-mail: SamurAhmadov1@outlook.com

Received Nov. 4, 2023
Revised Dec. 18, 2023
Accepted Dec. 24, 2023

Abstract

Research on enhancing Bring Your Own Device (BYOD) security in hybrid environments is critically relevant and important to protect data and ensure customer and organizational trust through the development of strong security policies. The study aims to develop and implement effective strategies and interventions that will help ensure that corporate data and resources are protected when employees use personal mobile devices in an environment where both on-premises and cloud-based resources are present. The methods used include analytical, deduction, modeling, statistical, and synthesis methods. This research identified specific vulnerabilities of potential threats to BYOD mobile devices in a hybrid environment and developed security strategies that include recommendations for creating a security policy and using a mobile device management system. The research led to the development of specific technical solutions, such as recommendations for mobile device configuration. This included educating employees and managers about security rules and the importance of adhering to security policies, and updated lists of current BYOD security threats and challenges given the changing threat environment. The practical value of the work lies in providing practical relevance to organizations by providing robust protection of sensitive data and resources, increasing employee comfort and confidence in the security of personal devices, easing IT departments' tasks of device management and threat detection, and increasing customer and partner confidence in a security-layer organization.

Keywords: Data protection, Updating, Data privacy, Employee training, Management

1. Introduction

The trend of using personal mobile devices for the workplace continues to grow and stay relevant. This means that more and more sensitive corporate data and information are being transferred via mobile devices, making security in this area more critical. Research is needed to identify new threats and develop defense techniques. The challenge of enhancing Bring Your Own Device (BYOD) mobile security in a hybrid environment involves several complex and relevant issues faced by organizations and information security professionals. The main aspects of the issues are quite numerous.

The research may include analyzing threats, developing security policies, and technology solutions, training employees, and monitoring the effectiveness of security measures in a hybrid environment [1-3]. Completing this task will provide the implementation of effective security strategies and practices, helping to reduce the risks associated with employees using their own mobile devices for work purposes. BYOD mobile device security management will help organizations use resources more efficiently and reduce the burden on the information technology (IT) department. Overall, completing the task of enhancing BYOD mobile device security in a hybrid environment will enable organizations to provide a more secure and reliable working environment, which in turn will contribute to more successful operations and reduce potential risks. The result of properly configured security measures will be a reduction in security incidents and associated costs.

According to [4], the variety of devices and operating systems is very large, employees use different mobile devices (smartphones, tablets, laptops) with different operating systems, and managing such diversity requires the development of universal security strategies. This is what makes the topic of BYOD mobile device security relevant, as it is becoming an integral part of modern business. As stated by [5], there is currently a large lack of control over devices in a BYOD environment. Organizations do not always have full control over employee devices, which leads to the risk of data leakage if the device is lost or compromised. This lack of control creates significant risks to the security and privacy of an organization's data [6-7]. Currently, the use of Mobile Device Management (MDM) solutions allows organizations to remotely manage mobile devices, including the ability to lock, delete data, and configure security policies. Also, differentiating data between personal and work areas on devices helps isolate corporate data and improve data control.

[8] note that mobile devices often connect to public Wi-Fi networks, which may not be secure. This creates the risk of data interception and Man-in-the-Middle attacks. Attackers intercept and analyze network traffic between a mobile device and a Wi-Fi access point. This allows them to interfere with and even modify data exchanges, resulting in the leakage of sensitive data such as passwords, banking details, and personal information [9-10]. According to [11] applications installed on mobile devices may contain vulnerabilities that can be exploited by attackers to attack corporate networks. Many users do not update applications on their mobile devices, which leaves open vulnerabilities that have been fixed in newer versions. Additionally, there is a risk of installing malicious apps that may have been downloaded from unreliable sources. BYOD organizations lack effective management of apps on employees' mobile devices. This means that employees can install apps without transparent security checks [12]. Some apps can access device data and resources without proper verification, posing a huge risk to data privacy and security.

As argued by [13], security incidents such as data leakage and virus attacks occur in hybrid environments and cause serious damage to the organization. To avoid such incidents, regular updates of antivirus software and firewalls on mobile devices and servers are required to help prevent virus attacks. Monitoring mobile devices used in a BYOD environment and the applications installed on them helps identify potential threats and vulnerabilities. Security incidents can cause serious damage to an organization, and it is therefore important to take proactive steps to prevent and respond to them. In a hybrid environment, it is especially important to pay attention to security, as the combination of enterprise and cloud resources creates additional security challenges.

Following [14], exploring the topic of enhancing BYOD mobile security in a hybrid environment is important for several reasons. The first is that many organizations are subject to data security regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Learning about the topic helps you comply with these regulations and avoid legal repercussions. The second is reputation protection. A data leak or compromise of mobile device security can damage an organization's reputation and cause customer and partner dissatisfaction [15-17]. There must be a balance between security and convenience; employees want to be comfortable using their devices for work, and overly strict security policies can cause dissatisfaction and reduce productivity.

The study aims to develop and evaluate the effectiveness of strategies and methods for securing BYOD mobile devices in organizations operating in a hybrid environment. This objective involves analyzing and developing methods that will help to reduce the security risks associated with employees using their own mobile devices for work, as well as improve the protection of sensitive data and resources of the organization. Research into BYOD mobile security in hybrid environments plays an important role in securing organizations and protecting their data. This enables researchers and engineers to develop new methods and solutions that contribute to a more robust and secure BYOD environment.

2. Research method

To study the problem of enhancing the security of BYOD mobile devices in a hybrid environment, various methods of scientific cognition were applied, which conducted comprehensive analyses and developed effective strategies and solutions. The analytical method in this study was used to thoroughly analyze the data and identify patterns and trends in BYOD mobile security in a hybrid environment. This method helped in structuring the information, highlighting key factors, and analyzing the security level in depth. The analytical approach facilitated a more accurate understanding of threats and risks, which in turn enabled the development of effective strategies to improve mobile device security. The modeling method was used in this study to identify which specific functions and mechanisms contribute to security in the context of employees using their own mobile devices. The modeling provided insight into how these functional elements interact and what benefits they bring to the overall security management system.

The deduction method was used in this study to draw logical conclusions about the general principles of BYOD mobile security in a hybrid environment based on known facts, data, and previously established rules. This method allowed for systematizing information, highlighting common patterns, and formulating security strategies based on logical reasoning. The static method was used to validate existing security measures and identify potential vulnerabilities at the level of configuration and security policies. This involved scrutinizing current security settings, configuration settings, and policies without actually applying them to the working environment. Using a comparative method, different security strategies, technology options and policies were compared. This identified the strengths and weaknesses of different approaches to securing BYOD mobile devices in a hybrid environment.

The synthesis method was used to provide theoretical modeling of the integration of multi-factor authentication, data encryption, and event monitoring systems. This theoretical approach enabled the creation of integrated and comprehensive security strategies for BYOD mobile devices in a hybrid environment. By applying the case study method, case studies of security incidents and successful implementations of BYOD security strategies in various organizations were examined. Through the functional analysis method, identified functional components and capabilities of the BYOD system that may be vulnerable to security threats, and analyzed each functional component for potential vulnerabilities and security threats. This method helped organizations to consider security aspects at the functional component level in a more detailed and systematic way and effectively protect them in BYOD systems.

To assess the effectiveness and convenience of the BYOD mobile application, tests were conducted for target groups. The tests were conducted based on employees of one of the companies using the application. It involved 36 employees (20 men and 16 women aged 22 to 48 years). They were asked to answer the following questions, implying “yes”, “average”, and “no” answers:

- Does the app perform basic tasks quickly?
- Are accounts and access rights easy to set up and manage?
- Do you feel your data is well protected when using the app?
- Are there any perceptions of risk in terms of data security?

3. Results

To ensure that BYOD mobile devices can be used comfortably in a hybrid environment, their security needs to be improved. Employees are increasingly using their mobile devices for work purposes, making BYOD a relevant model. Organizations need to ensure the security of corporate data residing on these devices. As the number of mobile devices in the workplace increases, so does the number of potential threats. Cybercriminals are actively targeting mobile devices to gain access to sensitive data and sensitive information. Companies are increasingly utilizing hybrid IT environments, including cloud-based resources, which creates additional challenges for securing data transferred between mobile devices and corporate resources. Devices contain sensitive information, and the loss or compromise of these devices will result in serious data breaches that can severely damage an organization's reputation. Protecting data and securing mobile devices helps to maintain the trust of customers and partners [18-20]. In this research, a strategy for enhancing BYOD mobile security in a hybrid environment has been developed using a multi-factor approach (Figure 1).

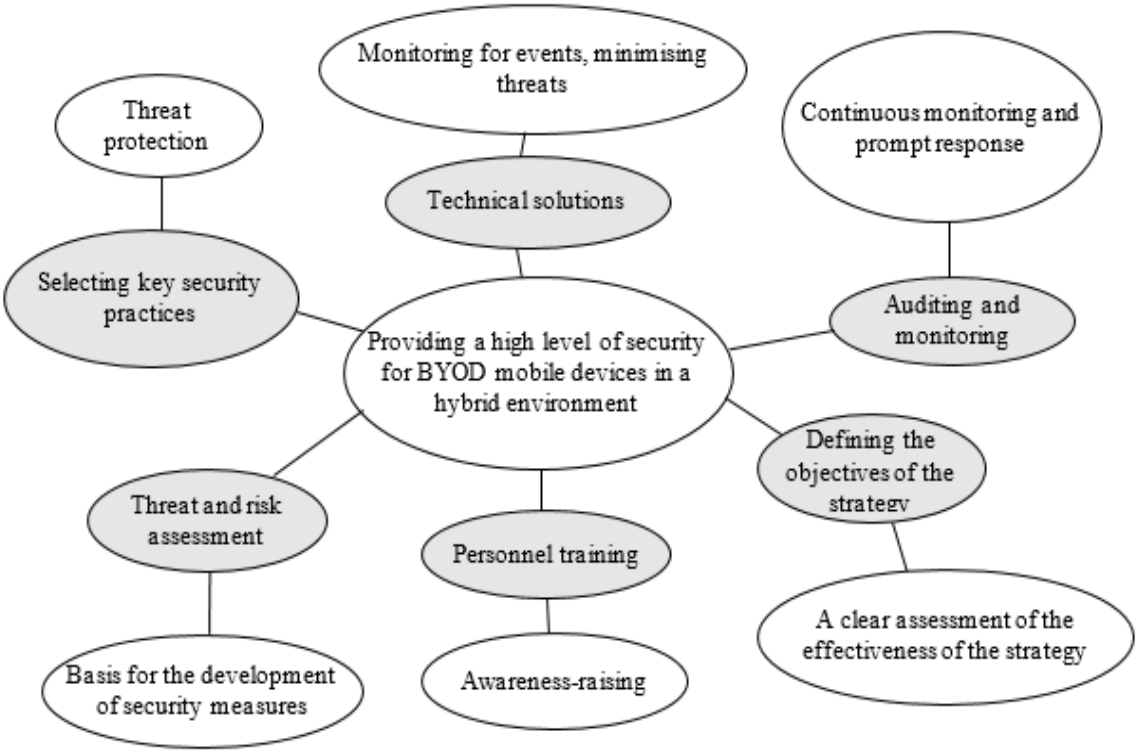

Figure 1. Schematic of the strategy developed

The existing threat and risk assessment included analyzing current security levels, identifying vulnerabilities and risks, and considering the characteristics of the hybrid environment. The study identified potential threats associated with the use of BYOD mobile devices in a hybrid environment, such as the possibility of data loss, attacks on public Wi-Fi networks, and malicious applications. Specific security aspects in a hybrid environment due to the combination of cloud and on-premises resources were considered. Network scans were conducted to identify vulnerabilities, and malware detection tools were used. Implemented an intrusion detection system (IDS) for real-time anomaly tracking [21]. The assessment identified threats such as weak passwords, vulnerable points in the network, and potential attacks. This became the basis for developing more accurate security measures.

The strategy identified specific objectives, including risk mitigation, protection of sensitive data, legal compliance, and security enhancement. These goals were formulated considering the specifics of the hybrid environment and focused on securing BYOD mobile devices. Developed key performance indicators (KPIs) for each goal, set security metrics, and implemented a KPI monitoring system. Specific goals were set that were measurable and analyzable. This provided a clear assessment of the effectiveness of the strategy. Decided to

implement multi-factor authentication, mobile device management systems, and technical tools to comprehensively secure BYOD mobile devices in a hybrid environment. Implemented technical tools including firewalls, Security Information and Event Management (SIEM), and MDM systems to secure BYOD mobile devices in a hybrid environment to meet the unique needs of the organization. These methods provide comprehensive protection against various threats, creating multiple barriers to potential attacks. Employee training programs covering security principles and the use of new authentication methods have been developed to enhance staff training in securing BYOD mobile devices in a hybrid environment [22-23].

Developing online security courses, conducting simulations of phishing attacks, and training using MDM and multi-factor authentication (MFA). Training of staff not only raised their awareness but also gave them practical skills in using new security techniques. Implemented procedures for regular audits and event monitoring to ensure that potential threats were promptly identified and responded to. Automated audit processes using tools to check compliance with security policies and installed a system to monitor network changes. Regular audits ensured continuous monitoring and enabled prompt response to security changes. Developed a mechanism for systematic updating of the strategy, which allows adapting to new threats and changes in information security of BYOD mobile devices in a hybrid environment. KPIs such as reduced security incidents, increased employee awareness, and successful implementation of new security practices were utilized. Continually updating the strategy ensures that the strategy adapts to new threats and maintains a high level of security. The results of the performance evaluation indicate successful risk mitigation and a stable level of security for BYOD mobile devices in a hybrid environment [24-25].

Properly configured security measures help employees be more productive knowing that their mobile devices are secure. Public Wi-Fi and Man-in-the-Middle networks pose serious risks to mobile devices. Improved security also reduces the likelihood of successful attacks [26]. Considering these factors, improving the security of BYOD mobile devices in a hybrid environment is a necessary and critical task for organizations. Security must be embedded into the corporate culture and infrastructure to ensure that data and business processes are protected [27]. It is also important to note that this research and the development of methods and recommendations to improve security, impacts the result of data protection, legal compliance, and improved employee productivity. These improvements contribute to more sustainable and successful organizations in today's information-driven world where security is critical.

Developing and evaluating the effectiveness of a strategy to secure BYOD mobile devices in organizations operating in a hybrid environment is a key research objective [28-29]. Strategy development is the creation of a specific plan of action and a set of practices that have been used and implemented previously to secure BYOD mobile devices. This strategy included technical solutions, security policies, and employee training. The main goal of all the work is to provide a high level of security for mobile devices that are used by employees as part of BYOD. This means protecting data, applications, and networks from threats and attacks. Given that organizations operate in a hybrid environment where employees may use their devices on both corporate and external networks, the goal is to create a strategy that ensures security in both environments. The ultimate goal is to improve the level of security in organizations operating in a hybrid environment involving BYOD mobile devices. This means reducing risk, protecting sensitive data, and complying with legislation. The research and strategy development under this objective was aimed at improving security and confidence in data protection in organizations where BYOD mobile devices play an important role.

The development of security policies was of paramount importance in this study. These policies were formulated and implemented to ensure robust protection of data and resources related to employees' use of their mobile devices in a hybrid environment. The policies included technical security measures such as password requirements, data encryption, and deletion of remote devices. Rules were established for access to corporate resources and use of mobile devices, including conditions for their use as part of BYOD. Policies included requirements for security training for employees when using BYOD mobile devices. Policies were developed to manage security events and incidents, including procedures for responding to potential attacks or data

breaches, and also considered compliance with legal requirements and security standards in a hybrid environment. The developed security policies became the basis for ensuring the reliable protection of data and resources of the organization working with BYOD mobile devices in a hybrid environment. Testing was initiated in the methodology and the results of the testing are summarized below in graphical form (Figure 2).

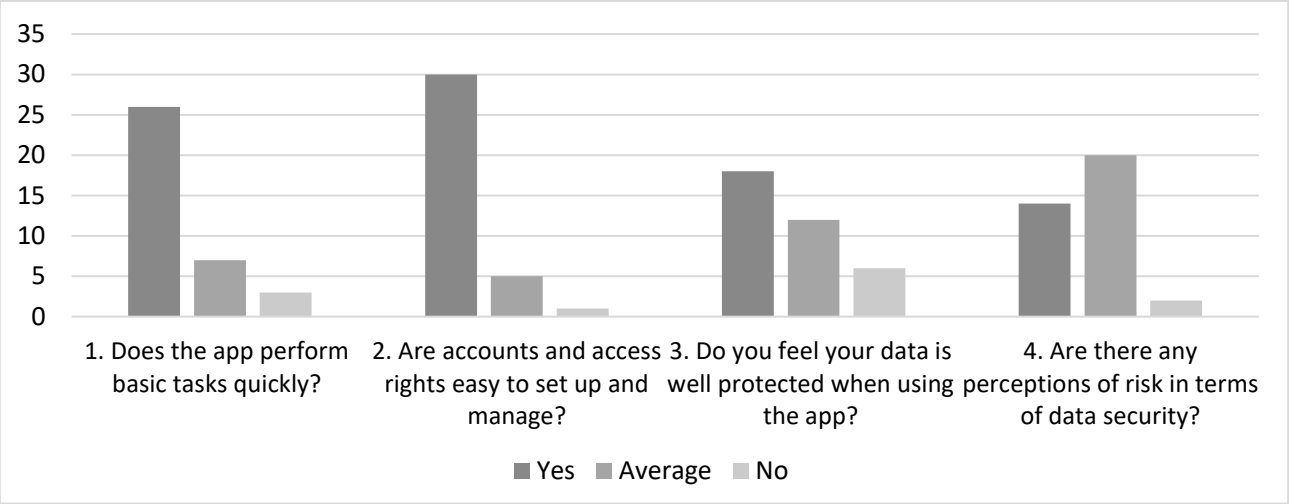

Figure 2. Results of BYOD testing on the target group

The majority of survey participants believe that the level of BYOD mobile security in their organization is quite high. However, it is worth noting that some respondents have an "average" opinion. This may indicate that there are some shortcomings or weaknesses in the security system. By surveying the employees of one of the organizations and analyzing the statistics of security incidents, it was found that users identified several main security threats, including device loss, malicious applications, attacks on public Wi-Fi networks, and Man-in-the-Middle attacks. These threats are typical and require attention from the organization. The majority of respondents recognize that employees within the organization need additional training on security when using BYOD mobile devices. This emphasizes the importance of training and awareness amongst staff regarding secure practices and security policies. The lack of strict security policies or their lack of enforcement may be the reason for the middle opinion among some respondents. This indicates the need for more stringent policies to be developed and implemented, as well as enforced by employees.

It is important to note that the topic of BYOD mobile device security is generating interest among respondents, which may confirm a willingness to further improve security strategies and practices. Overall, the survey results emphasize the importance of continually monitoring and improving BYOD mobile device security in a hybrid environment. Working to increase employee awareness, tighten security policies, and threat management training is an integral part of securing the field. Overall, the survey results emphasize the importance of continuously monitoring and improving BYOD security in a hybrid environment. Addressing employee awareness, tightening security policies and training in threat management is an integral part of providing security in the field [30]. Based on these results, more effective security strategies and training for employees began to be developed, and measures were taken to comply with security policies and legal requirements.

The study enabled the selection and successful implementation of technical solutions, in particular MDM mobile device management systems. These solutions provided the organization with the ability to effectively monitor and manage mobile devices used by employees as part of the BYOD strategy in a hybrid environment. MDM systems have become a central element of security in the BYOD context [31]. The study looked at various MDM platforms and selected those that best meet the needs of the organization such as MobileIron, AirWatch by VMware, and Microsoft Intune. With MDM, hundreds and even thousands of mobile devices can be managed from a single console. This made it easier for the IT department to monitor and maintain the devices. MDM allowed security policies to be set and applied to all devices simultaneously, including password, encryption,

and data wipe requirements. If a device was lost or stolen, MDM provided the ability to remotely wipe data, which helped protect sensitive information. In summary, the implementation of MDM systems following the study significantly improved the security of BYOD mobile devices in a hybrid environment and provided greater protection for the organization's data and resources.

Selecting and implementing technical tools such as firewalls and SIEMs have proven to be important steps to improve the security of BYOD mobile devices in a hybrid environment. Firewalls help monitor and filter network traffic, block potentially malicious connections, and provide protection from external threats. SIEMs play a key role in detecting anomalies and potential threats in an organization's information environment. They collect, analyze, and correlate event data from a variety of sources to identify and respond to unusual activity. SIEM also integrates with other security systems, which enhances the BYOD security monitoring capability of mobile devices [32]. As a result of implementing firewalls and SIEM systems, an organization provides an additional layer of protection and monitoring of mobile devices, reducing risks and increasing the security of its information environment. These technical tools play an important role in ensuring data integrity and confidentiality in a hybrid environment.

The implementation of MFA methods is one of the effective ways to provide an additional level of security at login, including access to corporate resources from BYOD mobile devices [33-34]. MFA requires the user to provide multiple forms of identification, which significantly increases security. The choice of MFA methods for an organization includes something the person knows (password or PIN), something they have (mobile device, smart card, or USB key), and something they are (fingerprint, retina). Training employees is an integral part of the process of how to use MFA and why it is important for security. Developing an MFA policy will determine when and for which resources it is mandatory. Multi-factor authentication adds an extra layer of protection when accessing corporate resources from BYOD mobile devices, as it will be much more difficult for an attacker to complete all authentication steps, this is an important security component in a hybrid environment.

Employee training plays an important role in ensuring safety during this study. During the research process, educational programs and courses were developed to raise awareness and educate employees on the security rules for using BYOD mobile devices in a hybrid environment. These programs included training on security basics, proper authentication methods, threat detection and response procedures, and training on the proper handling of sensitive information and corporate data [35]. In addition, employees are provided with information on the importance of adhering to security policies and standards, as well as the latest trends in cybersecurity. The main objective of this training is to make employees more vigilant and responsible in security matters and reduce the risk of possible security incidents. Employee training as part of the study contributed to improved security, as well-trained employees serve as the first line of defense in preventing threats and complying with security policies in a hybrid environment.

This study actively conducted regular auditing and monitoring of BYOD mobile device security systems in a hybrid environment. These processes are the systematic and continuous monitoring of events and incidents in an organization's information environment to identify anomalies and potential security threats. Regularly conducted security audits are done to assess the effectiveness of practices, identify vulnerabilities, assess compliance with security policies and procedures, and ensure compliance with legal requirements and security standards. It has assessed how effective current security practices and measures are, identifying which practices are working well and which require improvement or revision. This has allowed organizations to focus on areas that need additional protection. Helped identify vulnerabilities and weaknesses in information systems and security policies. This is important to address potential threats before they are exploited by attackers. Regular auditing and system monitoring were important components of securing BYOD mobile devices in a hybrid environment, as they enabled the identification and remediation of security issues, as well as maintaining compliance with standards and legislation [36-38].

In this study, special emphasis was placed on constantly updating the security strategy for BYOD mobile devices in a hybrid environment. This means that the strategy is not limited to one-off solutions, but constantly adapts to changing conditions and new threats in cyberspace. This comprehensive security strategy has enabled the organization to significantly improve the security of BYOD mobile devices in a hybrid environment. Thanks to it, the risks of data breaches and cyberattacks have been significantly reduced and employee productivity has been preserved.

4. Discussion

Improving BYOD mobile security in a hybrid environment is a key challenge for many organizations that allow their employees to use personal mobile devices for work purposes. This study analyzed the current environment, including the types of devices used by employees, and identified existing security threats and risks. This is an important step as understanding the current state allows for the development of effective strategies. In addition, specific objectives such as risk mitigation, protection of sensitive data, and legal compliance were identified. This helps to focus on key security aspects and develop appropriate measures [39].

According to the results of [40], analyzing the current security levels of BYOD mobile devices in a hybrid environment, included and identified several existing vulnerabilities and risks. The results contained the development of a security strategy that provided a set of measures and policies to secure BYOD mobile devices. The study evaluated the effectiveness of the selected security methods, the results indicated that the methods successfully mitigated risks and protected data. This study focused on improving the security of BYOD mobile devices, and both studies identified vulnerabilities and risks in this area. Both studies also developed security strategies and used different methods to mitigate risks and ensure data protection.

[41] determined that when investigating the security of BYOD mobile devices in a hybrid environment in an organization, the data must be representative of the employees using such devices in that organization. They must be reliable and accurate, which means that the data collection methods must be reliable, and the procedures standardized and homogeneous, errors in the data can skew the results of the study. Data are required to contain enough information to answer the research questions, this includes a variety of variables and metrics that allow analysis and conclusions to be drawn. The data should be adequately analyzed and interpreted to arrive at conclusions and recommendations that can be used. The amount of data also affects the statistical significance of the results and the ability to detect trends and patterns. However, it is more important that the data are suitably prepared and analyzed concerning the objectives of the study. This shows that there are overlaps with the work carried out by these authors, for example, the importance of methodology and quality data preparation was emphasized to produce information that can be used to develop BYOD mobile device security. However, in this paper, the emphasis was on providing data to employees rather than training them to help them better understand security threats and practices that can help them avoid threats, which will enable them to be more vigilant and cautious when using their mobile devices.

The attack modeling method is studied in [31]. This is a technique that is used to create controlled attack scenarios to assess system vulnerabilities, test its defenses, and train employees to respond to such threats [42-43]. He chose an attack scenario, a Structured Query Language (SQL) injection on an application, to test how resilient the application is to such attacks and modelled it. To do this, he created conditions close to a real-world environment, which included creating and installing fake applications. The SQL injection is run, and its effects are monitored, this includes monitoring the system response as well as the user response when the experiment is run with their participation. The results of the attack simulation were analyzed, Researchers assessed what vulnerabilities the system had and how the system reacted to the attack. With unauthorized access to the application database, an attacker can modify, delete, or extract data. An SQL injection vulnerability could be exploited to execute malicious SQL queries via user input. This method helps prevent real security incidents and protect sensitive data in a hybrid BYOD environment. But, for more correct operation, it is necessary to implement all the attack modeling techniques such as Session Hijacking, Buffer Overflow, and Denial of Service

(DoS). Therefore, there are differences with this paper in that the author did not consider all attack variants and the study was rather narrow.

[44] evaluated the effectiveness of such authentication methods as biometrics. It is an important aspect of securing BYOD mobile devices in a hybrid environment. Researchers conducted a comparative study of authentication methods such as password input (in biometrics it is a fingerprint scanner and facial recognition) and evaluated their advantages and disadvantages. The results of the study allowed a more accurate analysis of the characteristics and effectiveness of the different authentication methods. This allowed the organization's security policies and measures to be improved and updated, considering the use of multiple authentication methods, instead of being limited to a single method. Comparing the results of this study and the researchers' study showed that biometrics methods such as fingerprint scanners and facial recognition have certain advantages such as higher security and user-friendliness compared to traditional password methods.

[45] showed through their work that proper, regular updating of security strategy and techniques is very important to ensure the security level of BYOD mobile devices in a hybrid environment. In the rapidly changing world of information technology, new threats are constantly emerging, and the security strategy must be flexible and able to adapt to these changes [46-48]. Regularly updating security strategies and practices helps an organization to be prepared for new challenges and improve the protection of sensitive data and resources [49]. However, what has not been pointed out and discussed in this paper is that at this point, security strategies also have their complexities and challenges that are important to consider. Some of them contain many different aspects. By comparing the researchers' findings with this study, a common conclusion can be drawn about the importance of constantly updating and adapting the security strategy in BYOD mobile organizations. This allows for an effective response to changing conditions and new threats, ensuring that data and resources are securely protected [50].

As noted by [19], the implementation of technical solutions is an important step that ensures the security of BYOD mobile devices in a hybrid environment. The following technical solutions can improve the security. MDM systems provide the ability to manage mobile devices from a centralized console, allow configuring security policies, manage applications, perform remote data reset, and more, which facilitates the control of employee devices. A general focus on technical solutions and their important role in securing BYOD mobile devices can be highlighted. The study also focuses on MDM systems. Both studies confirm that technical solutions play a key role in creating a secure environment for BYOD mobile devices.

Implementing and combining these technical solutions helps to create a more secure BYOD environment and reduce the risks of data breaches and cyber threats. However, it is also important to remember to regularly update and monitor these solutions to ensure their effectiveness.

5. Conclusions

The main challenges in improving the security of BYOD mobile devices in hybrid environments are, the diversity of devices and operating systems, lack of control, public Wi-Fi networks, application vulnerabilities, security incidents in hybrid environments, balance between security and convenience, lack of employee training, and budget constraints, these challenges are and will continue to be relevant and need further research. In this paper, various methods, analyses, and recommendations have been reviewed and presented to address the pitfalls in the processes of improving BYOD mobile device security in a hybrid environment.

The study analyzed the current situation, identified threats and risks, and developed and implemented a security strategy. The research allowed the following conclusions to be drawn regarding the proposed strategy for improving the security of BYOD mobile devices in a hybrid environment. The strategy included a wide range of measures, from risk assessment and selection of key security methods to technical solutions and staff training, providing an integrated approach to security. The introduction of staff training on security principles and the use of new authentication methods helped foster a secure culture among staff. The selection and implementation

of technical tools such as MDM systems, firewalls, and SIEMs support effective device management and real-time response to events. Regular auditing and monitoring procedures ensure the rapid identification of potential threats and provide the ability to adjust strategy in response to changing situations. A mechanism for continually updating the strategy ensures flexibility and adaptability to new challenges, which is especially important in a rapidly changing information security environment.

The results of the study revealed several important points. A comprehensive security strategy was developed and successfully implemented, including security policies, multi-factor authentication, technical means, and an event monitoring system. The implementation of multi-factor authentication and a mobile device management system significantly reduced risks and improved security when using BYOD mobile devices. The event monitoring system enabled continuous monitoring of events and incidents, identifying anomalies and potential threats. Employee training on the rules of security when using BYOD mobile devices increased staff awareness and responsibility.

Employee training was an important part of the strategy. Understanding security principles and using multi-factor authentication became mandatory parts of the workflow. Employees were trained on security principles and the use of multi-factor authentication as an integral part of their workflow. This has created a more secure and informed work environment where employees are better able to understand and respond to potential security threats. Research has enabled validated analysis and authentication methods to successfully secure BYOD mobile devices. By constantly updating the strategy and monitoring events, security can be adapted to changing conditions and new threats, ensuring that data and resources are well protected. This confirms the importance of relevance and continuous improvement of security practices in a dynamic cyber environment.

In summary, achieving the goal of enhancing BYOD mobile security in a hybrid environment is a success and a solid foundation for enhancing BYOD mobile security in a hybrid environment, ensuring protection from advanced threats and compliance with security standards. The organization now has an effective security strategy that protects data and increases the confidence of employees, customers, and partners in the security of information.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Ethical approval statement

All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and national research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards. A study was approved by Ethics Committee of the Azerbaijan Technical University.

Informed consent

This study aligned with the ethical principles of research, including anonymity, confidentiality, and beneficence. Ethical approval of the study was obtained from the Ethics Committee of the Azerbaijan Technical University.

Abbreviations and acronyms

BYOD	Bring Your Own Device
MDM	Mobile Device Management
GDPR	General Data Protection Regulation

HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
IDS	Intrusion Detection System
KPI	Key Performance Indicator
SIEM	Security Information and Event Management
MFA	Multi-Factor Authentication
SQL	Structured Query Language
DoS	Denial of Service

References

[1] I. H. Zinchenko and O. V. Lavdanska, "Modern technologies for evaluating the effectiveness of digitalization," *Bulletin of Cherkasy State Technological University*, no. 2, pp. 34-42, 2022.

[2] O. Horbachova, Yu. Tsapko, S. Mazurchuk and O. Tsapko, "Mobile technology of thermal modification of wood," *Ukrainian Journal of Forest and Wood Science*, vol. 13 no. 3, pp. 22-31, 2022.

[3] S. Atanasov, "State-of-the-art technologies for remote sensing of crops water status and nutrients in agriculture: A review," *Scientific Horizons,* vol. 26, no. 9, pp. 167-177, 2023.

[4] Zh. A. Aldiyarov and M. N. Imankul, "User information security in cyberspace," *South Kazakhstan Science Herald*, vol. 8, no. 4, pp. 72-78, 2019.

[5] A. T. Ayedh M, A. W. A. Wahab and M. Y. I. Idris, "Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment: State of the art and future directions," *Applied Sciences*, vol. 13, no. 14, p. 8048, 2023. https://doi.org/10.3390/app13148048

[6] S. B. Malikova, N. E. Talantuly, E. T. Alimkulov, A. K. Zhanibekov, A. B. Sharipova, "Information-psychological security in multiconfessional society," *European Journal of Science and Theology*, vol. 14, no. 1, pp. 83-92, 2018.

[7] V. Vlasovets, T. Vlasenko, S. Kovalyshyn, O. Kovalyshyn, O. Kovalyshyn, S. Kurpaska, P. Kiełbasa, O. Bilovod and L. Shulga, "Effect of various factors on the measurement error of structural components of machine parts materials microhardness using computer vision methods," *Przeglad Elektrotechniczny,* vol. 99, no. 1, pp. 323-329, 2023.

[8] S. Siboni, A. Shabtai and Y. Elovici, "An attack scenario and mitigation mechanism for enterprise BYOD environments," *ACM SIGAPP Applied Computing Review*, vol. 18, no. 2, pp. 5-21, 2018. https://doi.org/10.1145/3243064.3243065

[9] D. Mykhalevskiy, "Evaluation of wireless information transmission channel settings of 802.11 Wi-Fi standard," *Eastern-European Journal of Enterprise Technologies,* vol. 6, no. 9, pp. 22-26, 2014.

[10] B. Orazbayev, D. Kozhakhmetova, K. Orazbayeva and B. Utenova, "Approach to modeling and control of operational modes for chemical and engineering system based on various information," *Applied Mathematics and Information Sciences,* vol. 14, no. 4, pp. 547-556, 2020.

[11] I. Tairov and I. Donchev, "Mobile applications use for business growth," in *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*. New York: IEEE, pp. 223-226, 2023. https://doi.org/10.1109/PICST57299.2022.10238668

[12] A. Lavdanskyi, E. Faure, S. T. Tynymbaiev and A. Skutskyi, "System for secure information exchange of text data through the radio channel in the ism band," *Bulletin of Cherkasy State Technological University*, no. 3, pp. 41-48, 2022

[13] D. N. Issabayeva, U. M. Abdigapbarova, G. A. Abdulkarimova, A. A. Kanatbekova and A. Seitova, "Experience in using BYOD approaches in teacher education," in *ICFET '23: Proceedings of the 2023 9th International Conference on Frontiers of Educational Technologies*. Bali: Undiknas University, pp. 102-108, 2023. https://doi.org/10.1145/3606150.3606167

[14] A. Alkandari, N. Alawadhi, A. Alonaizi, A. Alshehab and D. Almutiri, "Implementation of survey mobile application: A voting algorithm for social influence minimization using GPS," *Journal of Theoretical and Applied Information Technology*, vol. 101, no. 11, pp. 4119-4129, 2023.

[15] L. Nykyforova, N. Kiktev, T. Lendiel, S. Pavlov and P. Mazurchuk, "Computer-integrated control system for electrophysical methods of increasing plant productivity," *Machinery & Energetics*, vol. 14, no. 2, pp. 34-45, 2023.

[16] V. Panov, "The scientific process of two interferometers (optical) development and the mitigation of external influence," *Scientific Herald of Uzhhorod University. Series "Physics"*, no. 53, pp. 19-30, 2023.

[17] I. N. Shopina, D. G. Muliavka, S. K. Hrechaniuk and V. V. Fedchyshyna, "Improvement of social control as a direction of crime prevention" *Russian journal of criminology*, vol. 13, no. 3, pp. 447-454, 2019.

[18] E. L. Hasanov, "Ennovative basis of research of technologic features of some craftsmanship traditions of ganja (On the sample of carpets of XIX century)," *International Journal of Environmental and Science Education*, vol. 11, no. 14, pp. 6704-6714, 2016.

[19] C. I. Eke, A. A. Norman and M. Mulenga, "Machine learning approach for detecting and combating bring your own device (BYOD) security threats and attacks: A systematic mapping review," *Artificial Intelligence Review*, vol. 56, pp. 8815-8858, 2023. https://doi.org/10.1007/s10462-022-10382-3

[20] O. Skydan, O. Nykolyuk, P. Pyvovar and P. Topolnytskyi, "Methodological foundations of information support for decision-making in the field of food, environmental, and socio-economic components of national security," *Scientific Horizons*, vol. 26, no. 1, pp. 87-101, 2023.

[21] Iu. M. Shynkariuk, "Alternative representation of space and time: Geometric solution of problems of relativity theory", *Scientific Herald of Uzhhorod University. Series "Physics"*, no. 51, pp. 74-82, 2022.

[22] P. Soubhagyalakshmi and K. S. Reddy, "An efficient security analysis of bring your own device," *IAES International Journal of Artificial Intelligence*, vol. 12, no. 2, pp. 696-703, 2023. http://doi.org/10.11591/ijai.v12.i2.pp696-703

[23] B. Orazbayev, E. Dyussembina, G. Uskenbayeva, A. Shukirova and K. Orazbayeva, "Methods for modeling and optimizing the delayed coking process in a fuzzy environment," *Processes*, vol. 11, no. 2, p. 450, 2023.

[24] G. A. Safdar and A. Mansour, "Security and trust issues in BYOD networks," *IT Professional*, vol. 25, no. 4, pp. 45-51, 2023. https://doi.org/10.1109/MITP.2023.3293714

[25] A. P. Aueshov, A. B. Satimbekova, K. T. Arynov, A. K. Dikanbaeva and A. A. Bekaulova, "Environmental and Technological Aspects of Acid Treatment of Serpentinite Waste from Chrysotile Asbestos Mining and Processing," *International Journal of Engineering Research and Technology*, vol. 13, no. 6, pp. 1215-1219, 2020.

[26] G. Gilmore and P. Beardmore, "Finely tuning your BYOD strategy, policy and guidelines," in *Mobile Security & BYOD for Dummies*. G. Gilmore and P. Beardmore, Eds. Hoboken: John Wiley & Sons, Ltd., pp. 35-40, 2012.

[27] P. Mikhailov, Z. Ualiyev, A. Kabdoldina, N. Smailov, A. Khikmetov and F. Malikova, "Multifunctional Fiberoptic Sensors For Space Infrastructure," *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 5-113, pp. 80-89, 2021.

[28] Y. Barlette, A. Jaouen and P. Baillette, “Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers coping strategies,” *International Journal of Information Management*, vol. 56, p. 102212, 2021. https://doi.org/10.1016/j.ijinfomgt.2020.102212

[29] N. Repnikova, Yu. Berdnyk and V. Hnyp, “Improving control accuracy in multi-connected digital systems,” *Scientific Horizons*, vol. 25, no. 7, pp. 55-64, 2022.

[30] K. Almarhabi, A. Bahaddad and A. M. Alghamdi, “Security management of BYOD and cloud environment in Saudi Arabia,” *Alexandria Engineering Journal*, vol. 63, pp. 103-114, 2022. https://doi.org/10.1016/j.aej.2022.07.031

[31] U. Vignesh and S. Asha, “Modifying security policies towards BYOD,” *Procedia Computer Science*, vol. 50, pp. 511-516, 2015. https://doi.org/10.1016/j.procs.2015.04.023

[32] P. de las Cuevas, A. M. Mora, J. J. Merelo, P. A. Castillo, P. García-Sánchez and A. Fernández-Ares, “Corporate security solutions for BYOD: A novel user-centric and self-adaptive system,” *Computer Communications*, vol. 68, pp. 83-95, 2015. https://doi.org/10.1016/j.comcom.2015.07.019

[33] K. Almarhabi, K. Jambi, F. Eassa and O. Batarfi, “Survey on access control and management issues in cloud and BYOD environment,” *International Journal of Computer Science and Mobile Computing*, vol. 6, no. 12, pp. 44-54, 2017.

[34] D. Yakymenko and Y. Kataieva, “Methods and means of intelligent analysis of text documents,” *Bulletin of Cherkasy State Technological University*, no. 2, pp. 43-52, 2022.

[35] A. Barlybayev, T. Sabyrov, A. Sharipbay and A. Omarbekova, “Data base processing programs with using extended base semantic hypergraph,” *Advances in Intelligent Systems and Computing*, no. 569, pp. 28-37, 2017.

[36] J.-W. Lian, “Understanding cloud-based BYOD information security protection behaviour in smart business: In perspective of perceived value,” *Enterprise Information Systems*, vol. 15, no. 9, pp. 1216-1237, 2021. https://doi.org/10.1080/17517575.2020.1791966

[37] O. Trokhaniak, “Estimation of eddy currents and power losses in the rotor of a screw electrothermomechanical converter for additive manufacturing,” *Machinery & Energetics*, vol. 13, no. 3, 92-98, 2022.

[38] V. Kaplun, V. Osypenko and S. Makarevych, “Forecasting the electricity pricing of energy islands with renewable sources,” *Machinery & Energetics*, vol. 13, no. 4, pp. 38-47, 2022.

[39] N. Smailov, Z. Dosbayev, N. Omarov, B. Sadykova, M. Zhekambayeva, D. Zhamangarin and A. Ayapbergenova, “A Novel Deep CNN-RNN Approach for Real-time Impulsive Sound Detection to Detect Dangerous Events,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, 271-280, 2023.

[40] K. Degirmenci, M. H. Breitner, F. Nolte and J. Passlick, “Legal and privacy concerns of BYOD adoption,” *Journal of Computer Information Systems*, 2023. https://doi.org/10.1080/08874417.2023.2259346

[41] G. Costantino, F. Martinelli, A. Saracino and D. Sgandurra, “Towards enforcing on-the-fly policies in BYOD environments,” in *2013 9th International Conference on Information Assurance and Security (IAS)*. New York: IEEE, pp. 61-65, 2013. https://doi.org/10.1109/ISIAS.2013.6947734

[42] L. Pavliuk, “Electron modelling in conjunction witch vacuum modelling” *Scientific Herald of Uzhhorod University. Series "Physics"*, no. 52, pp. 27-35, 2022.

[43] V. Levchenko, O. Pogosov and V. Kravchenko, "Cobalt application in repair tools for maintenance and modernisation of NPP equipment," *Scientific Herald of Uzhhorod University. Series "Physics"*, no. 53, pp. 31-41, 2023.

[44] R. Palanisamy, A. A. Norman and M. L. M., Kiah, "BYOD policy compliance: Risks and strategies in organizations," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 61-72, 2022. https://doi.org/10.1080/08874417.2019.1703225

[45] K. Downer and M. Bhattacharya, "BYOD security: A study of human dimensions," *Informatics*, vol. 9, no. 1, p. 16, 2022.

[46] O. Havrysh, Y. Obruch, A. Chepynoga, A. Honcharov and O. Panasko, "Organizational structure of technical protection of information at the network level using vpn technology," *Bulletin of Cherkasy State Technological University*, no. 3, pp. 5-15, 2023.

[47] A. Danylkovych, O. Sanginova and A. Shakhnovsky, "Computer simulation and optimization of the composition of the hydrophobising mixture," *Bulletin of Cherkasy State Technological University*, no. 2, pp. 100-110, 2023.

[48] T. O. Prokopenko and Y. Povolotskyi, "A system of criteria for evaluating the efficiency of projects in the field of information technologies," *Bulletin of Cherkasy State Technological University*, no. 4, pp. 23-30, 2022.

[49] Z. Adanbekova, A. B. Omarova, S. Yermukhametova, S. Assanova and S. Tynybekov, "Features of an Electronic Transaction as Evidence in Court," *Revista de Direito, Estado e Telecomunicacoes*, vol. 14, no. 1, pp. 98-112, 2022.

[50] S. Shaimurunov, K. Ryspayev, A. Ismailov, A. Zhikeyev and B. Salykov, "Study of the Efficiency of Using Facilities Based on Renewable Energy Sources for Charging Electric Vehicles in Kazakhstan," *International Journal of Sustainable Development and Planning*, vol. 18, no. 4, pp. 1263-1269, 2023.