Interdisciplinary Description of Complex Systems 23(3), 207-216, 2025

SUSTAINABLE AND SAFE CITIES THROUGH COMPUTER APPLICATIONS

Ferenc Bálint[1, *] and Richárd Pető[2]

[1]Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

[2]Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering
Budapest, Hungary

DOI: 10.7906/indecs.23.3.2
Regular article

Received: 7 February 2024.
Accepted: 1 July 2024.

ABSTRACT

The article emphasizes the critical role and the areas of development of Mobile Device Management (MDM) in enhancing safety within urban environments by securing data and applications. It underscores the importance of protecting vital infrastructure such as government buildings, banks, utilities, transport networks, communication systems, health services, and financial institutions from threats like cyberattacks and terrorism. MDM enables the secure management of mobile devices, ensuring the safe handling of sensitive data, conducting business transactions, and accessing IT applications. This strategy aims to strengthen the security and resilience of modern cities by ensuring reliable and protected digital operations. The protection of critical infrastructure through secure technology is crucial for mitigating risks and maintaining uninterrupted operations. Each component serves distinct functions and requires specific structural considerations. Although secure buildings contribute to safer cities, they encounter various challenges in achieving this objective, including cyber threats and attempts to disrupt infrastructure. Today, many daily activities, both professional and personal, rely heavily on mobile devices. These activities encompass handling sensitive company data, conducting business via email, managing personal and professional calls, performing banking transactions, and utilizing various other IT applications. The security of any building heavily depends on a robust IT infrastructure. However, it is important to acknowledge that IT systems may be accessed and potentially disabled by authorized individuals. MDM emerges as a critical solution to address these challenges by ensuring the secure management of mobile devices utilized by companies and their employees.

KEY WORDS

mobile device management, cybersecurity, control, monitoring, AI

CLASSIFICATION

ACM: 10010405.10010406.10010426

APA: 4120

JEL: R59

*Corresponding author, η: balintf.dtp@gmail.com; -;
Nepszinhaz str. 8, 1081 Budapest, Hungary

INTRODUCTION

Mobile devices, initially designed as personal consumer communication tools, have evolved into essential components of enterprise operations, used to access networks and process sensitive data. With expanded functionality, these mobile devices have become integral to enhancing productivity but also pose unique security challenges due to their mobility and diverse threat landscape. The increasing adoption of modern technologies by consumers and enterprises has led to a rise in mobile malware and vulnerabilities [1]. To mitigate risks of sensitive data leakage, organizations are advised to implement robust policies, processes and infrastructures for managing and securing mobile devices, applications, and content effectively and efficiently.

Mobile Device Management (MDM) [2] refers to the administration and management of mobile devices, such as smartphones, tablets, and laptops, in corporate environment. It enables IT and security teams to monitor, manage, and secure all mobile devices connected to the corporate network. That includes both corporate-issued and personal (Bring Your Own Device (BYOD)) [3] devices.

With the implementation of mobile devices in the workplace, comprehensive MDM solutions are becoming absolutely critical. The various MDM solutions help organizations manage, monitor, and secure devices that are deployed across different mobile service providers and operating systems.

These MDM solutions are essential for organizations to maintain control over their various mobile devices, ensuring they remain secure, compliant and efficiently managed.

MOBILE DEVICE MANAGEMENT SOLUTIONS

MDM solutions simplify the challenge IT and security teams face in monitoring diverse mobile device fleets manually. These solutions offer extensive features like device enrollment, patch management, configuration policies, application management, and remote troubleshooting. By consolidating these functions into a single platform, MDM enables clearer visibility into device statuses without the need for multiple tools or manual updates. Moreover, MDM allows remote management through a central console, which is particularly advantageous for businesses with remote or hybrid workforces. This capability ensures all endpoints are consistently updated and secured, eliminating the need for IT teams to travel for in-person device enrollment or troubleshooting.

Remote access to mobile devices and the secure running of applications can be ensured through leading MDM solutions such as Ivanti [4], Microsoft Intune [5], and VMWare Workspace ONE Unified Endpoint Management [6]. These solutions significantly reduce the risk of data leakage by allowing secure access to internal resources while enabling the use of more secure mobile devices. MDM solutions are continuously evolving, presenting both challenges and opportunities.

The development of MDM systems involves not only mobile devices but also computers running various operating systems like Windows, Linux, and MacOS. The primary goal is to prevent malicious application leaks and protect personal and sensitive data stored by companies. With MDM solutions, both company-owned and private mobile devices can be used with minimal limitations, ensuring that company and private data remain separate due to built-in security restrictions. Android and iOS, the two most popular mobile operating systems, are fully supported for remote access to internal resources.

MDM systems offer modern integration solutions that enhance the user experience for both employees and system operators. This integration allows for the unified operation of various services and applications on a secure network platform. Additionally, MDM can be integrated

into access control systems, management of access rights, X-ray systems [7], CCTV systems, and numerous other applications, providing a comprehensive approach to managing and securing mobile devices and their usage within an organization.

MARKET SIZE OF MOBILE DEVICE MANAGEMENT

The MDM market is experiencing significant growth and is projected to expand considerably in the coming years. In 2023, the market size was approximately USD 10.8 billion and is expected to reach around USD 77,2 billion by 2032.

Key drivers of this growth include the increasing adoption of mobile devices in enterprises, the necessity of managing these devices efficiently, and rising cybersecurity concerns. The trend of Bring Your Own Device in workplaces and the growing reliance on cloud-based MDM solutions also contribute to this expansion.

Regional analysis shows that North America holds the largest market share due to the early adoption of advanced mobile technologies, strict data security regulations, and the significant presence of major MDM vendors [8, 9]. The Asia-Pacific region is expected to experience the fastest growth, driven by increasing mobile device usage, youth population, and BYOD trends in countries like China, India, and Japan [10, 11].

In terms of industry verticals, the Banking, Financial Services, and Insurance (BFSI) sectors account for the largest market segment due to the high demand for security and compliance. Other significant sectors include healthcare, manufacturing, and retail. Large enterprises dominate the market as they require robust MDM solutions to manage vast networks of mobile devices and ensure security across multiple departments and locations.

KEY CHARACTERISTICS OF MDM

MDM solutions contribute to the simplification of the management of registered devices, while a bulk enrollment for large numbers of devices can be ensured. MDM facilitates over-the-air (OTA) provisioning of settings and applications. MDM serves as a security management tool for organizations. It enforces security policies such as password complexity and device encryption. For lost or stolen devices there is a remote lock and wipe capability ensured. The application management feature supports application deployment, updates, and removal. Application whitelisting and blacklisting capabilities are also ensured by means of MDM. Furthermore, it supports enterprise application stores for distributing in-house applications. MDM allows the configuration of device settings, such as Wi-Fi, VPN, and email. It also enables restriction settings to control device functionality.

Real-time monitoring and reporting capabilities of device status and compliance are of high importance. They track device location and usage patterns. By means of MDM, detailed reports on device usage, security incidents, and compliance can enhance risk awareness and mitigation in the company.

Content management in MDM manages the distribution and access control of corporate documents and content. It ensures secure content sharing and collaboration, offering also backup capabilities.

Compliance and policy enforcement are in-built features by automated compliance checks and policy updates.

User and device management facilitates user-based management, allowing policies to be assigned based on user roles. It supports multiple device types and operating systems and integrates with directory services like Active Directory for user authentication.

Network access control within MDM controls access to corporate networks based on device compliance status. It provides network segmentation and access control policies, supporting conditional access policies based on device health and status.

Integration and interoperability features ensure that MDM integrates with other IT management tools and systems. Support for APIs allows for custom integrations, and the system interoperates with existing infrastructure such as email servers and VPNs.

The user experience is enhanced through self-service portals for users to manage their own devices. MDM provides intuitive interfaces for both administrators and end-users, ensuring minimal impact on device performance and user productivity.

Scalability and performance are critical, with MDM solutions scaling to manage thousands of devices across multiple locations. High availability and redundancy are provided, ensuring responsive performance even with large device fleets.

These characteristics collectively enable organizations to effectively manage and secure their mobile devices, ensuring that they can be used productively without compromising on security.

DEVELOPMENT OF AN EFFECTIVE MDM ARCHITECTURE

Developing an effective MDM architecture involves several critical requirements to ensure comprehensive management, security, and scalability of mobile devices within an organization.

When designing the architecture, several important aspects must be considered. Operating in a cloud-based [12] environment is essential, along with creating a secure and separated network. Installing self-developed mobile applications or applications from reliable sources is also crucial. Integrating communications from different systems, placing them on a secure network, and managing these applications is a complex task that requires significant integration efforts.

These applications and servers require substantial storage capacity [13] with a system-wide solution. Each component needs its own storage to ensure quick access to operational data. Secure communication will be implemented using SSL (Secure Sockets Layer) [14] and TLS (Transport Layer Security) protocols.

A runnable environment can be created on the cloud infrastructure that can serve the entire application complex simultaneously. Authentication is necessary to identify users, which can be achieved with a cloud solution such as Microsoft Entra ID [15]. This component will function as an independent service to assign and manage appropriate authorizations for users.

Log management is another critical service that must operate as a system-wide service, essential for system monitoring. Monitoring involves collecting hardware and software operating indicators to ensure that the applications and servers function correctly. It is the operators' responsibility to analyze this data to secure high system availability.

Additionally, orientation, including the display and approach of areas affected by mobile device management and integrated services, must be considered to facilitate user intervention and interaction effectively.

CREATING A ROBUST IT ENVIRONMENT

The creation of development, test and live IT environments is an important prerequisite. The test and production environments will function with several integrated systems. This means more virtualized environments. Several automated processes need to be created on these virtual servers, including backup, archive and restore processes. This must also be recorded in a separate document. The run cycle of the backups is, for example, a full, differential or

incremental backup. A full backup includes saving all selected data as well as configurations. A full backup is the starting point for the differential backup. The differential backup means only the backup of the added or changed data, compared to the full backup which includes the entire data set. The incremental backup is also based on the full backup. It differs from the differential backup in a sense that in this case the new data backups use the previous backups as a comparison reference.

Setting up user profiles, establishing access rights, file and folder structures, predefined operational tasks, and analysis of logs are also listed among the tasks to be developed. It is essential to perform the necessary testing on the built systems. According to the generally accepted testing, to reduce business costs and testing costs, a testing optimum should be determined.

INTEGRATION OF A CENTRAL LOG ANALYSIS SYSTEM

Even with the most securely structured IT systems and regulations, security gaps and incidents can still occur. One effective method for prevention and detection is connecting all devices to a central log analysis system that employs algorithms to analyze and categorize log entries. This process is crucial for detecting ongoing attacks, preventing further damage, and investigating incidents post-event. Centralized log collection and event management systems serve these purposes effectively, with Security Information and Event Management (SIEM) [16] systems providing an excellent solution for managing security incidents and events.

FEATURES OF THE SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEM

SIEM is a security solution that assists organizations in identifying and addressing potential security threats and vulnerabilities before they can disrupt business operations. SIEM systems enable enterprise security teams to detect anomalies in user behavior and leverage artificial intelligence [17] to automate many manual processes associated with threat detection and incident response. Long-term data storage is necessary for thorough analysis and retrievability, which includes analyzing (and displaying) data, recognizing patterns, and searching for activities or data that deviate from normal patterns.

Correlation Analysis: SIEM systems are designed to sort data into interpretable units that share similarities and common points. The primary objective of correlation is to transform raw data into useful and transparent information, which significantly enhances the effectiveness of threat detection and response.

Alarms and Alerts: SIEM systems establish alarm thresholds for the collected data to identify potential security issues. When these thresholds are breached, the systems can trigger protocols to warn users. These warnings can be delivered through various means, such as push notifications, automated emails, or text messages sent to dashboards or mobile devices managed by MDM systems.

Data Aggregation: SIEM systems are capable of collecting data from a wide array of connected systems, including servers, hardware, networks, databases, software, and complex operating applications. This comprehensive data aggregation facilitates extensive monitoring and analysis across the entire IT infrastructure.

Given the vast amount of log data generated by IT and security devices, analyzing the correlations between log lines is nearly impossible without a security log analysis system. It is crucial to distribute internal resources effectively to ensure the operation of the SIEM system, including the investigation of incidents deemed suspicious by the system.

Integrating a central log analysis system, such as a SIEM, is essential for maintaining the security and integrity of an organization's IT environment. By leveraging AI for threat detection, automating incident response processes, and enabling long-term data analysis, SIEM systems enhance the ability to prevent, detect, and respond to security incidents effectively.

INCIDENT MANAGEMENT AND MONITORING SOLUTIONS

Tools and applications that are integral to IT and security systems generate log files, which are crucial for monitoring the security status and activities within these systems. It is essential to determine the optimal range of events to log and the specific data to record for each event. Security event logs must be retained for the duration prescribed by law, making it imperative to consider this when defining backup procedures.

To ensure accountability and auditability, security logs must enable the post-incident determination of security events that occurred within the system. The system must be capable of registering every action performed by each user or group of users.

Log entries generated from system startups and shutdowns are particularly valuable in the event of an error, incident, or planned intervention, as they help in identifying the causes of downtime more easily. Additionally, system clock settings, such as changes due to daylight saving time, are critical events for log entries. During a clock reset, it is important to save the logs because the critical one-hour period must be preserved to prevent new logs from overwriting those created in the previous hour.

Identification and authentication processes must track various activities to ensure security and accountability. This includes logging successful logins, login attempts, and logouts, as well as monitoring user-initiated and system-forced password changes, which are essential for maintaining password integrity. The system should also record account locking and unlocking events, whether automatic or manual, and document actions such as prohibiting or deleting user accounts, especially when an employee's access rights are revoked.

Application Management: Application and service activities must be diligently monitored. The system needs to log the start and stop events of applications, services, or tasks, including orderly shutdowns that occur due to errors or incidents. This helps in diagnosing and resolving issues more effectively.

Configuration Files and Scripts Management (Linux, Windows): The management of configuration files and scripts is critical. Activities involving these files must include the creation, deletion, modification, and querying processes, ensuring that all changes are documented for future reference and accountability.

Resource Management: Changes in system resources, such as CPU, memory, and storage, must be meticulously recorded. This includes documenting the creation, deletion, increase, or reduction of these resources, which is essential for maintaining optimal system performance and resource allocation.

Employee Actions: The actions performed by employees with different levels of authorization that impact system operation and security must be carefully tracked. This involves creating user accounts, including technical users running background scripts, modifying user authorizations, and banning or deleting users. Similarly, any changes in Active Directory roles, including their creation, authorization, and modification or deletion, need to be logged to ensure comprehensive tracking of user activities.

Activity and Sensitive Data Queries: Monitoring equipment activity and handling sensitive data require precise documentation. The system must record the creation, modification, deletion, copying, and moving of sensitive data, ensuring that all actions are transparent and traceable.

Event and Security Alarm Management: In managing events and security alarms, it is crucial to document the time of event detection and the root cause, with efforts to identify the root cause if unknown. A detailed description of the event, including its short-term and long-term business impacts, must be provided. Maintenance activities related to the event should also be recorded, along with the success or failure of the event. The system must prioritize security alerts, identify the range of users and user groups connected to the event, and determine the objects and buildings related to it. Additionally, the users and groups tasked with resolving the event and the precautionary measures that triggered the event must be clearly documented.

By adhering to these detailed expectations, identification and authentication processes can ensure a secure and accountable IT environment facilitating the effective management of applications, resources, employee actions, data activities, and security events.

DATA CARRIERS

Protection measures for data carriers (including paper and digital formats) must be carefully developed and implemented. Access should be restricted to authorized personnel only, and access permissions should be regularly reviewed during entry, exit, and periodically throughout the year. Special attention is required when acquiring and disposing of data carriers, focusing on proper labeling, secure transport, and storage practices to prevent compromising organizational integrity. Data carriers should be stored in secure, enclosed locations to safeguard against unauthorized access or theft.

SECURITY SYSTEM PLANS

MDM is essential for safeguarding urban environments against a variety of challenges, especially amidst natural disasters. It ensures uninterrupted access to critical data and communication channels during events such as floods, earthquakes, and hurricanes. MDM's efficient protocols facilitate swift response coordination, enabling timely alerts, rescue coordination, and the continuity of essential services even in adverse conditions. Beyond disaster scenarios, MDM also mitigates risks posed by cyber-attacks, safeguarding data integrity amidst potential vulnerabilities. Additionally, it addresses human errors by enforcing consistent security measures across mobile devices, minimizing the risk of inadvertent data breaches or operational disruptions. Integrating robust MDM strategies into disaster preparedness plans bolsters urban resilience, fortifying infrastructure and enhancing public safety against natural disasters, cyber threats, and human error alike.

Auditing requirements also necessitate the development of security system plans tailored to each system. These plans must assess the protection levels required for critical infrastructure systems. Systems are categorized on a scale of 1 to 6, with higher numbers indicating greater security demands. Compliance involves specifying the system's type, version number, and establishing its development lifecycle for comprehensive planning. Documentation is crucial for defining roles, authorization matrices, and daily operations. Additionally, the system plan must outline functions, network elements, protocols, and services. Security limits and protective functions of the system must be clearly defined to achieve these goals. Integration is facilitated by a connection diagram, and thorough testing and assessment of system codes are imperative for operational readiness.

SAFEGUARDING OF OPERATION AND SUPERVISION

To ensure accurate operation, a dedicated 24/7 team of IT professionals must be established for continuous supervision and remote management of all IT security systems. Additionally, contracts should be secured with external support groups and suppliers to swiftly address

emergent issues and incidents. It is crucial to swiftly replace any malfunctioning devices. Compliance with ITIL [18] guidelines is essential, as they dictate best practices in IT system operation and development.

Passwords should adhere to stringent criteria: a maximum length of 120 characters and a minimum of 12 characters, including lowercase, uppercase, numbers, and special characters. Data integrity is maintained using robust algorithms [19] like SHA-512/256, SHA3-224, and SHA3-256, while TLS 1.2 secures network traffic and data connections.

AREAS OF CONTINUOUS IMPROVEMENT

MDM systems have become essential for securing data and managing applications, particularly in the context of critical infrastructure and urban safety. However, MDM systems have several areas where they can be significantly improved to enhance their effectiveness and usability. Among the crucial functions are user identification, access to the company's internal resources, integrated event management within the email system, application usage tracking, device tracking, and logging of unauthorized access attempts. Operationally, it is essential to ensure uninterrupted operations of critical infrastructures. Integrated systems enhance the efficiency of these infrastructures.

Enhanced security measures, such as incorporating AI and machine learning for advanced threat detection and adopting zero trust security models with granular access controls, are essential to counter increasingly sophisticated cyber threats. Scalability and performance are critical, necessitating improvements in handling increased device loads and optimizing resource utilization to prevent performance degradation. Compliance and reporting can be bolstered by integrating automated compliance monitoring and offering more detailed and customizable reporting features for better insights and decision-making. Statistics on daily, weekly, monthly, and annual events can highlight unexpected occurrences and allow for advanced preparation. Incorporating AI supports managing the changing number of incidents and requests, aiding user support, and adapting to evolving trends through modern technology and security measures. Unified Endpoint Management should be adopted to manage all types of endpoints, including mobile, desktop, and IoT devices, from a single platform. Enhanced application management capabilities are also necessary for better application deployment, monitoring, and security.

MDM systems must support emerging technologies such as 5G networks and IoT devices, and integrate edge computing capabilities for faster data processing and reduced latency. Enhancing data protection through better encryption methods and providing users with more control over their privacy settings is vital for maintaining trust and security.

Remote management capabilities can be improved with enhanced tools for remote diagnostics, issue resolution, and streamlined processes for deploying updates and patches. The examination of cost-effective integration possibilities is vital. For instance, displaying application maps on the MDM interface and defining the scope of problems for easier intervention, as well as automatically filling incident-based forms and assigning tasks via the company's mail system, can streamline operations. Notifications are sent via email to the relevant colleagues to reduce tasks requiring physical contact, thereby minimizing infection risks during pandemics and improving reaction and execution times through clear indications.

Comprehensive training programs and improved customer support services are essential for helping users and IT staff effectively utilize MDM systems. Providing tailored policies and flexible deployment options, including on-premise, cloud-based, and hybrid solutions, will allow organizations to customize MDM systems to their specific needs. By addressing these

areas, MDM systems can become more robust, user-friendly, and capable of meeting the evolving demands of modern enterprises and critical infrastructure management.

EXAMPLES FOR IMPROVEMENT OF URBAN SAFETY

To enhance urban safety, MDM systems must support various critical functions. For instance, integrating multiple alarm options such as fire, intrusion, and detection of prohibited objects into the system is essential. It is crucial to quickly identify the location of alarm events, access live camera images near the alarm, and determine the GPS coordinates of colleagues to plan the shortest route to the alarm point. This integration also involves planning emergency exit routes during evacuations and ensuring that the building's emergency sound system and signals are visible on mobile devices.

MDM facilitates continuous coordination with security patrols by calculating changing patrol routes, making it easy to track and support patrol performance using camera system images. Digital signage plays a significant role in displaying dynamic content at busy junctions, aiding security interventions such as diversions. These displays can show broadcast videos, emergency visual support, and important public information. Ensuring that messages on digital signs are accessible on mobile devices is vital for quick emergency interventions.

By incorporating these examples, MDM systems can significantly enhance the safety and efficiency of urban environments, ensuring that critical infrastructure and public safety measures are effectively managed and maintained.

CONCLUSION

Ensuring the security of urban infrastructure relies heavily on implementing strong MDM practices. This is essential for mitigating a wide range of threats.

Natural disasters, including floods, earthquakes, and hurricanes, pose significant risks to critical infrastructure, endangering both physical assets and public safety. Human errors, stemming from operational oversight or negligence, further underscore the vulnerability of infrastructure systems. These errors can have far-reaching consequences, highlighting the importance of stringent management protocols and oversight. Moreover, deliberate attacks and cybercrime present formidable challenges to infrastructure security. Malevolent actors may target critical systems to disrupt operations or compromise sensitive data, posing threats to economic stability and public trust. Effective MDM strategies play a pivotal role in mitigating these risks by enforcing robust security measures, monitoring device access and usage, and swiftly responding to potential breaches.

By implementing comprehensive MDM solutions, urban environments can bolster their resilience against diverse threats, ensuring the continuity and integrity of essential services. Proactive management of mobile devices not only enhances operational efficiency but also reinforces the overall security posture, safeguarding infrastructure against evolving risks in an increasingly interconnected world. By following best practices and staying informed about emerging trends, organizations can ensure their MDM strategies remain robust and effective.

REFERENCES

[1] Muha, L. and Krasznay, Cs.: *Managing the security of electronic information systems.* Ludovika University of Public Service, Budapest 2014,

[2] Pikhart, M.: *The Use of Mobile Devices in International Management Communication: Current Situation and Future Trends of Managerial Communication*. Procedia Computer Science **171**, 1736-1741, 2020, http://dx.doi.org/10.1016/j.procs.2020.04.186,

[3] Steiner, P.: *Going beyond mobile device management.* Computer Fraud & Security **2014**, 19-20, 2014, https://doi.org/10.1016/S1361-3723(14)70483-X,
[4] Ivanti: *Everywhere Work. Elevated*. https://www.ivanti.com, accessed 21st December 2023,
[5] Microsoft: *Microsoft Intune.* https://www.microsoft.com/en-us/security/business/microsoft-intune, accessed 21st December 2023,
[6] Wmware: *space ONE Unified Endpoint Management.* https://www.vmware.com/products/workspace-one/unified-endpoint-management.html, accessed 21st December 2023,
[7] Smith detection: *Making the world a safer place.* https://www.smithsdetection.com, accessed 21st December,
[8] imarc: *Mobile Device Management Market Report.* https://www.imarcgroup.com/mobile-device-management-market, accessed 10th May 2024,
[9] imarc: *Mobile Device Management Market Report* https://www.researchandmarkets.com/reports/5946677/mobile-device-management-market-report-type, accessed 15th May 2024,
[10] Market Data Forecast: *Global Mobile Device Management Market Size, Share, Trends, & Growth Forecast Report by Solutions (Device Management, Deployment Management, Security Management, Network Service Management, and Others), Vertical (Education, Healthcare, Banking, Financial Services, and Insurance (BFSI), Retail, Manufacturing and Other) and Regional - (2025 to 2033)*. https://www.marketdataforecast.com/market-reports/mobile-device-management-market, accessed 15th May 2024,
[11] technavio: *Mobile Device Management (MDM) Market Analysis, Size, and Forecast 2025-2029: North America (US and Canada), Europe (France, Germany, and UK), APAC (Australia, China, India, Japan, and South Korea), and Rest of World (ROW)*. https://www.technavio.com/report/mobile-device-management-market-industry-analysis accessed 18th May 2024,
[12] Azure: *Adaptation and development*. In Hungarian. https://azure.microsoft.com/hu-hu, accessed 5th January 2024,
[13] Hewlett Packard Enterprise: *HPE Storage.* https://www.hpe.com/us/en/storage.html, accessed 8th January 2024,
[14] Cloudflare: *What is SSL? SSL definition.* https://www.cloudflare.com/en-gb/learning/ssl/what-is-ssl, accessed 8th January 2024,
[15] Microsoft Security: *Azure Active Directory is now Microsoft Entra ID.* https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id, accessed 10th January 2023,
[16] IBM: *What is security information and event management (SIEM)?* https://www.ibm.com/topics/siem, accessed 10th January 2024,
[17] IBM: *What is artificial intelligence (AI)?* https://www.ibm.com/topics/artificial-intelligence, accessed 10th January 2024,
[18] TechTarget: *ITIL (Information Technology Infrastructure Library).* https://www.techtarget.com/searchdatacenter/definition/ITIL, accessed 15th January 2024,
[19] Okta: *Hashing Algorithm Overview: Types, Methodologies & Usage.* https://www.okta.com/identity-101/hashing-algorithms, accessed 15th January 2024.