BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 30 No. 4. 2025

UDC 004.42:004.7
DOI: 10.62660/bcstu/4.2025.25

Problems of protecting unstructured information on mobile devices

Evgen Brovchenko*
Postgraduate Student
Open International University of Human Development "Ukraine"
04071, 23 Lvivs'ka Str., Kyiv, Ukraine
https://orcid.org/0000-0002-1416-0385

Abstract. The relevance of the study was determined by the growing volume of unstructured data in the mobile environment, which required a rethinking of classical approaches to the protection in conditions of limited resources and dynamic use. The purpose of the study was to conduct a comprehensive analysis of methods for protecting unstructured information in the mobile environment and to identify key barriers to the effective implementation. The methodology was based on a theoretical and analytical approach, which included the systematisation of protection methods, a comparative analysis of cryptographic algorithms, an assessment of authentication and access control models, as well as an analysis of cloud security mechanisms. It was established that symmetric encryption Advanced Encryption Standard in Cipher Block Chaining mode provided effective local protection but required careful management of initialisation vectors. It was found that Elliptic Curve Cryptography outperformed Rivest-Shamir-Adleman in terms of energy efficiency and performance, and BLAKE3 outperformed Secure Hash Algorithm 256 in terms of speed, energy consumption, and parallelism support. It was generalised that access control models were insufficiently adapted to the dynamics of the mobile environment, and the most effective were context-oriented and multifactor approaches, in particular with the use of biometric and behavioural authentication. It was found that a combination of client-side encryption, identity management, and cloud backup ensured the highest level of protection with proper implementation. It was established that the effectiveness of HyperText Transfer Protocol Secure, Transport Layer Security 1.3, and Virtual Private Network protocols depended on the type of data and interaction scenario, and the use required a balance between security, performance, and the context of use. Eight key challenges were identified, the relevance of which to mobile security practice was confirmed through comparison with the OWASP Mobile Top 10 categories: data leakage, limited resources, complexity of authentication, dynamic access control, use of public networks, platform fragmentation, application opacity, and legal barriers. It was determined that the effectiveness of protection methods was conditioned by the context of application – the type of data, device architecture, interaction scenario, and available infrastructure – which required an adaptive choice of solutions. The results obtained confirmed that traditional approaches to information security required adaptation to the specifics of mobile platforms. The study has practical value for security solution developers, corporate system administrators, and policymakers in the field of cybersecurity

Keywords: environment; encryption; authentication; resource constraints; access control

INTRODUCTION

In the conditions of rapid digitalisation, mobile devices became the key tool for working with information, in particular unstructured data, which were created, stored, and transmitted in a decentralised environment. Such specifics complicated the use of traditional security tools, which were developed for stationary or server systems. The limitation of computing resources, the fragmentation of operating systems, and the changing context of mobile device usage created additional challenges for ensuring the confidentiality, integrity,

Article's History: Received: 03.07.2025; Revised: 21.10.2025; Accepted: 15.12.2025.

Suggested Citation:
Brovchenko, E. (2025). Problems of protecting unstructured information on mobile devices. *Bulletin of Cherkasy State Technological University*, 30(4), 25-37. doi: 10.62660/bcstu/4.2025.25.

*Corresponding author

and availability of data. There arose a need to critically assess how existing information security mechanisms met the requirements of the mobile environment. It was necessary to clarify whether existing methods were able to adapt to real conditions of use, and whether these methods ensured a sufficient level of protection in conditions of mobility. All this determined the relevance of searching for flexible, adaptive solutions capable of functioning effectively in the limited and dynamic conditions of mobile platforms.

In the context of general system approaches to data security, S. Spasiteleva *et al.* (2019) carried out an analytical review of threats to the security of universal data management platforms, including multimodel database management systems, Data Lake, and cloud environments. The authors highlighted a data-centric security approach and proposed cognitive technologies for automated vulnerability detection. The subject of protecting unstructured information in the mobile environment was directly addressed in a number of studies that combined cryptographic and political-organisational approaches. In the study of Y.M. Brovchenko *et al.* (2023), the focus was on protecting unstructured information on mobile devices, exploring the possibilities of combined application of local encryption, in particular Advanced Encryption Standard (AES), and access policies. The advantages of a hybrid approach were identified, although the need for precise parameter tuning was emphasised. A. Sereda *et al.* (2022) conducted a functional and cryptanalytic analysis of the resilience of algorithms AES, Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC) on Android and iPhone Operating System (iOS) mobile platforms. The study showed that ECC provided the best combination of high cryptographic strength and low energy consumption, which made it the priority choice for mobile security.

A separate strand of the literature focused on protecting communication channels and the features of implementing security mechanisms in mobile device operating systems. The work of Y. Kostiuk *et al.* (2024) focused on the analysis of authentication and key exchange protocols in wireless mobile networks. The authors found that dynamic key updates increased the security of communications, although the implementation of these mechanisms in heterogeneous operating systems (OS) remained technically difficult. In the study of S.M. Konovalov (2025), a categorisation of cyber threats to mobile operating systems was carried out, and the vulnerability to typical attacks was analysed. The effectiveness of Trusted Execution Environment security components in Android and Secure Enclave in iOS was assessed, the limited ability to resist modern attacks was identified, and ways of improving the interaction of security modules with application services were proposed.

Within the related subject area, some authors highlighted aspects of cloud security. In particular, A.R. Abibulaev & A.Z. Piskozub (2025) proposed an innovative approach to strengthening cloud infrastructure security through the introduction of Natural Language Processing (NLP) and Machine Learning (ML) methods for detecting anomalous activity and predicting risks. The authors confirmed the effectiveness of behavioural analytics for automatic threat response but emphasised the need to adapt models to resource-constrained environments, in particular mobile devices. In a related field, the work of K.G. Babayeva (2024) focused on the study of cryptographic mechanisms for protecting biometric data, with emphasis on the practical application in mobile information systems. The expediency of using specialised cryptographic algorithms for the confidentiality of biometric data was substantiated, but the need for the integration with access policies and channel protection was emphasised.

In the broader context of cybersecurity strategy formation, the contribution of O. Marchenko (2023) was important, in whose study risks in cyberspace were systematised and the effectiveness of existing approaches to the neutralisation was analysed. The author paid attention to multilevel protection models combining organisational, technical, and behavioural security components, which were relevant for protecting mobile environments. In turn, J.V. Rogushina (2019) studied methods of analysing unstructured data, covering algorithmic approaches to processing textual, multimedia, and mixed information. The results of this study formed an important basis for understanding the specifics of unstructured data before developing effective protective mechanisms in the mobile environment. Despite the diversity of scientific approaches, the analysis of sources indicated the fragmentary nature of existing research. Some works focused on encryption, cloud infrastructure, biometrics, or data analysis, but in most cases, there was a lack of an interdisciplinary approach to the problem of protecting unstructured information in the mobile environment. The need to simultaneously take into account the technical limitations of mobile devices, the specifics of unstructured data formats, the dynamics of user behaviour, and the requirements of the regulatory environment remained insufficiently disclosed.

The purpose of the work was to identify technical, organisational, and architectural barriers that complicated the implementation of effective protection of unstructured data on mobile devices through a comprehensive analysis of existing methods and security mechanisms. The hypothesis of the study was that most traditional methods of data protection, developed for stationary or server systems, were not fully effective in the mobile environment without appropriate adaptation, since the methods did not take into account resource constraints, the specifics of unstructured data, and the fragmentation of mobile platforms.

MATERIALS AND METHODS

The study had a theoretical and analytical character. The source base consisted of international technical standards, recommendations, and regulatory documents

in the field of information security. The foundation was made up of publications of the National Institute of Standards and Technology (NIST) (2023), USA, in particular: AES Federal Information Processing Standards (FIPS) 197, recommendations on the use of the Cipher Block Chaining (CBC) mode NIST Special Publication (SP) 800-38A (Dworkin, 2001), and the parameters of elliptic curves NIST SP 800-186 (Chen *et al.*, 2023). For the consideration of digital identification mechanisms and attribute-based access control, the study analysed NIST SP 800-63-3 (Grassi *et al.*, 2017) and NIST SP 800-162 (Hu *et al.*, 2014) respectively. The RSA specification was studied separately according to Request for Comments (RFC) 3447: Public-Key Cryptography Standards (PKCS) #1 (Moriarty *et al.*, 2016). In the part concerning data protection in the cloud environment, ISO/IEC 27017:2015 (2015) – the industry standard for cloud service security – was considered. In addition, to substantiate the requirements for privacy and the protection of personal information, the study took into account the main provisions of Regulation (EU) of the European Parliament and of the Council No. 2016/679 (2016) and the Law of Ukraine No. 2297-VI (2010). These documents formed the basis of the conceptual framework of the study, as well as for the formation of the criterion of compliance of protection methods with the specifics of unstructured data in the mobile environment.

The study applied a number of complementary methods, which ensured separate levels of analytical processing of source information. Content analysis served as the main tool for the systematic collection and study of regulatory and technical documents governing the requirements for data protection in the mobile environment. The classification approach in the study was used to systematise methods of data protection according to functional purpose. The basis for constructing such a structure was the categories of security measures defined in NIST SP 800-53 (Force, 2020). According to this classification, the methods were grouped into categories: cryptographic protection (including symmetric and asymmetric encryption and hash functions), user identification and authentication (including biometric and behavioural methods), access control, data protection during transmission (through secure protocols, in particular HyperText Transfer Protocol Secure (HTTPS), Transport Layer Security (TLS) 1.3, and Virtual Private Network (VPN)), and protection during storage in the cloud environment.

The functional and technical analysis envisaged a comprehensive evaluation of data protection methods, taking into account the suitability for use in the mobile environment. In particular, for asymmetric encryption algorithms RSA and ECC, the comparison was conducted according to performance indicators (encryption/decryption time), energy efficiency, and computational complexity (required key size to achieve a given level of cryptographic strength). Within the analysis of hash functions Secure Hash Algorithm 256 (SHA-256) and BLAKE3, the following criteria were determined: hashing speed, resource consumption, support for parallel data processing, as well as suitability for implementation on mobile devices with limited resources. For other categories of protection methods, such as authentication models, access control, data transmission protocols, and cloud storage tools, the evaluation was based on such parameters as adaptability to the mobile scenario, scalability, compatibility with existing standards, as well as resilience to typical threats of the mobile environment. This made it possible to carry out a comparative ranking of methods within functional categories and to identify the most suitable solutions for the protection of unstructured data. The comparison method was applied to assess the relevance of the identified technical limitations to practical threats. The comparison procedure involved a step-by-step analysis of the characteristics of the studied protection methods with the categories of threats defined in the classification of the Open Web Application Security Project (OWASP) (Mobile Top 10 2024..., n.d.). To increase the objectivity, the comparison was carried out in tabular form with the correspondence of problems to OWASP categories, which made it possible to trace the correlation between the identified barriers and the practical vulnerabilities of the mobile environment.

RESULTS

Theoretical approaches to protecting unstructured information on mobile devices

The protection of unstructured information on mobile devices required the use of a comprehensive set of methods, encompassing both technical and organisational solutions. The main approaches were based on the application of cryptographic algorithms, access control policies, cloud technologies, and information security standards. The symmetric AES algorithm was widely applied for data encryption at the device level. One of the most common and secure modes of block cipher operation was the CBC mode. In the encryption process, each message block performed an eXclusive "OR" (XOR) operation with the encrypted previous block, while for the first block an XOR operation was performed with the Initialisation Vector (IV). This "chaining" effect in the operation mode of the cipher reflected a high level of security, as it indicated the dependence of each block on the previous one. The AES algorithm in CBC mode was an effective solution for encrypting local files and large volumes of data in mobile applications, due to its simplicity of implementation and built-in support by Android and iOS platforms. A key element of security was the IV, which had to be random and unique for each encryption session, while its transmission could be carried out in the open together with the ciphertext. Table 1 systematised the results of a comparative analysis of methods for generating and transmitting the IV in the context of mobile systems.

Table 1. Approaches to IV generation and transmission for cryptographic protection of unstructured data on mobile devices

IV generation/transmission method	Advantages	Disadvantages	Usage scenarios
Random generation and transmission with data	Simplicity of implementation, suitable for one-time sessions	Risk of "padding oracle" attacks due to open transmission of IV	Secure chats, one-time transactions
Generation from encryption key	Uniqueness of IV ensured automatically when the key changes	Limited uniqueness of IV with a constant key, requires Key Derivation Function (KDF)	Local file encryption on the device
Unique number (Nonce) + counter with synchronisation	Guaranteed uniqueness and efficiency: no need to transmit full IV	Requires reliable synchronisation mechanism between clients	Streaming data (video calls), client-server systems

Source: compiled by the author based on M. Dworkin (2001), National Institute of Standards and Technology (2023)

As shown in Table 1, the choice of the method for generating and transmitting the IV for encrypting unstructured data in mobile applications was determined by a compromise between security, efficiency, and practical implementation: random generation was simple but vulnerable to attacks; a key-derived IV ensured uniqueness but required the implementation of a key derivation function; Nonce + counter was effective for streams but required additional synchronisation. Thus, the optimal choice of IV generation method depended on the specifics of the mobile application, taking into account three key factors: the level of data confidentiality, the presence of server infrastructure, and the computing capacity of the device. This analysis clearly illustrated that even the technical nuances of implementing cryptographic algorithms in the mobile environment required careful consideration of the operational context – from hardware resource constraints to the specifics of network interaction.

Asymmetric encryption algorithms, such as RSA and ECC, played a key role in ensuring security on mobile devices, especially when working with unstructured data. RSA was based on the factorisation of the product of large prime numbers, whereas ECC was based on elliptic curves over finite fields. Both algorithms were applied to provide secure data exchange between the client application and the cloud infrastructure. Encryption/decryption performance and energy efficiency indicators were decisive factors in the choice of data protection tools in a mobile environment with limited resources. High encryption overheads could slow down device performance, reduce battery life, or worsen the user experience. In Table 2, a comparative characteristic of the efficiency parameters of the considered asymmetric algorithms for different levels of protection and data volumes was presented.

A comparative analysis of asymmetric algorithms demonstrated the advantages of ECC over RSA in the context of mobile devices. ECC ensured an equivalent level of security with significantly smaller key sizes (160 bits versus 1,024 bits for an 80-bit level of protection), which directly affected the reduction of memory usage. The algorithm also turned out to be more energy efficient – at 128-bit protection, ECC consumption was 3.7 times lower than RSA (15.43 MWh and 56.78 MWh respectively). A separate subject of analysis was the dynamics of data processing time. Although RSA demonstrated better results in encrypting small volumes of data, its decryption was slower due to the complexity of operations with large exponents. In contrast, ECC showed more balanced performance, especially at high levels of protection, where decryption time became shorter than encryption time. These results confirmed that ECC was the optimal choice for systems with constant data exchange, while RSA could be appropriate for rare encryption operations. The choice of a specific algorithm had to take into account not only cryptographic strength but also energy efficiency and the computing capabilities of mobile devices.

Table 2. Efficiency of asymmetric encryption algorithms

Security level (bits)	Key size (bits)		Data size (bits)	Total time (ms)		Encryption time (ms)		Decryption time (ms)		Energy consumption (MWh)	
	RSA	ECC		RSA	ECC	RSA	ECC	RSA	ECC	RSA	ECC
80	1,024	160	8	785	1,815.2	30.7	488.5	754.3	1,326.7	17.86	9.05
			64	5,673.8	8,078.4	136.6	2,168.5	5,537.2	5,909.9		
			256	19,877.2	30,809.1	559.6	7,924	19,317.7	22,885.1		
112	2,048	224	8	2,737.5	3,789.3	29.9	2,203	2,707.5	1,586.3	21.55	17.38
			64	20,574.3	16,978.8	163.5	9,985.5	20,410.8	6,933.3		
			256	102,615.3	66,033.9	581.5	39,700.8	102,033.7	26,333.1		

Continued Table 2.

Security level (bits)	Key size (bits)		Data size (bits)	Total time (ms)		Encryption time (ms)		Decryption time (ms)		Energy consumption (MWh)	
	RSA	ECC		RSA	ECC	RSA	ECC	RSA	ECC	RSA	ECC
128	3,072	256	8	6,971.4	5,645.3	30.5	3,876.3	6,940.9	1,769	56.78	15.43
			64	46,645.4	22,446.6	167.2	15,088.2	46,478.2	7,358.4		
			256	210,169.7	85,844.6	561.1	58,438.6	209,608.6	27,406		

Source: compiled by the author based on K. Moriarty *et al.* (2016), Z. Vahdati *et al.* (2019), L. Chen *et al.* (2023)

In mobile security systems, hash functions were used to verify the integrity of unstructured data such as multimedia files, text documents, event logs, or cached content. Hashing made it possible to quickly detect unauthorised changes in content by comparing the current hash with the control value. In mobile applications, hash functions were used to verify the integrity of files during storage or synchronisation (for example, during offline access to images or videos), to control cache stability, as well as to validate access tokens or the authenticity of update packages. Some applications implemented additional checksum verification in the background to avoid reproducing corrupted or modified data. The most commonly used algorithms were SHA-256 and BLAKE3. SHA-256 was a standardised solution compatible with traditional cryptographic protocols, whereas BLAKE3 was designed with an emphasis on hardware capabilities. Both algorithms were used mainly to verify data integrity and did not provide encryption functions. A detailed comparative analysis of the characteristics of hash algorithms in the context of mobile devices was presented in Table 3.

Table 3. Comparison of SHA-256 and BLAKE3 algorithms in the context of mobile systems

Parameter	SHA-256	BLAKE3
Processing speed (Advanced RISC Machine (ARM), 1 thread)	300-400 MB/s	1,000 MB/s
Energy consumption (indicative assessment)	Higher: longer computation time → more Central Processing Unit (CPU) cycles	Lower: shorter computation time, efficient use of cache and Single Instruction Multiple Data (SIMD)
Multithreading support	Limited	Full (parallelised across cores)
Adaptation to the mobile environment	Needs optimisation	Designed with weaker CPUs in mind
Application scenarios	Standardised protocols (TLS, Hash-based Message Authentication Code (HMAC)) and legacy systems	Local data verification, background scanning, cache synchronisation

Source: compiled by the author based on B. Kibar (2023)

According to the comparative characteristics, BLAKE3 demonstrated higher performance when processing large volumes of unstructured data, reducing file integrity verification time and energy consumption. The algorithm supported parallel processing, which corresponded to the architecture of the latest generation of multicore mobile processors. SHA-256 remained relevant for scenarios where compliance with cryptographic standards or compatibility with existing protocols was required. Both algorithms could be used in combined data protection systems. Access control was one of the key mechanisms for ensuring the confidentiality and integrity of unstructured information on mobile devices. Effective implementation of access ensured that only authorised users or applications gained access to system data, resources, or functions. In the mobile environment, these mechanisms had to adapt to limited computing resources, the high dynamics of network connections, and frequently changing usage contexts. Despite the diversity of access control models, the implementation in mobile operating systems and applications was accompanied by a number of limitations and vulnerabilities, which reduced the overall level of protection of unstructured data. Table 4 presented a classification of access control models with an analysis of the implementation in the mobile environment.

Table 4. Comparative characteristics of access control models in the mobile environment

Access model	Principle of operation	Implementation in mobile systems	Typical application examples
Discretionary Access Control (DAC)	The user independently determined who had access to the data	Configuring data sharing in applications, system permissions of the file system (Android Storage Access Framework)	Granting access to files for other applications

Continued Table 4.

Access model	Principle of operation	Implementation in mobile systems	Typical application examples
Mandatory Access Control (MAC)	Access policies were set centrally	SELinux mechanism on Android	Android kernel security
Role-Based Access Control (RBAC)	Access was determined by the user's role	In Mobile Device Management (MDM) systems, corporate platforms	Defining employee access rights to data according to the position
Attribute-Based Access Control (ABAC)	Access depended on user, environment, and resource attributes (time, location, device type)	Application Programming Interface (API) of the new generation, mobile Software Development Kit (SDK)	Applications with geo-zones, Internet of Things (IoT) systems with time-restricted access
Multi-Factor Authentication (MFA)	Access was allowed after passing several levels of authentication	Use of biometrics, passwords, and one-time codes	Banking applications, cloud storage

Source: compiled by the author based on V.C. Hu *et al.* (2014), P.A. Grassi *et al.* (2017), J.T. Force (2020)

The analysis of the main access models demonstrated that traditional approaches had limitations in the mobile context. DAC, although intuitive for users, often became a source of misconfigurations due to excessive dependence on the human factor. MAC ensured a higher level of protection, but its complexity limited its application mainly to system components. RBAC proved effective in corporate environments, but its lack of flexibility complicated adaptation to dynamic mobile scenarios. ABAC and MFA offered more promising solutions, as these approaches took usage context into account. However, the implementation was accompanied by additional resource costs and raised issues concerning privacy protection. These observations indicated the necessity of developing hybrid solutions that combined the advantages of different models, taking into account the technical features of mobile platforms and patterns of user behaviour. The optimal system had to ensure an adequate level of security while maintaining performance and usability. For the effective protection of unstructured data in the cloud environment, a comprehensive approach was necessary, combining three key methods: client-side encryption, Identity and Access Management (IAM), and backup mechanisms. These technologies jointly ensured confidentiality, integrity, and availability of data when working with mobile devices. Table 5 presented the results of a comprehensive analysis of methods for protecting unstructured data in the cloud environment.

Table 5. Methods for protecting unstructured data in the cloud environment

Protection method	Main functions	Objectives	Key advantages	Client-cloud interaction
Client-side encryption	Data encryption before uploading to the cloud, key management on the device	Preventing data leakage in case of cloud storage compromise	Full control over keys, absence of cloud provider access to data content	Client encrypts data → transfers the data to the cloud → decrypts only when downloading to the device
IAM	Centralised access management, authentication, authorisation	Control of user rights, prevention of unauthorised access	Flexible access policies, integration with MFA, activity audit	Cloud verifies access rights → grants/blocks data operations for the client
Backup	Automatic creation of data copies, the encryption, recovery in case of loss	Ensuring availability, protection against data loss	Reliability, ability to roll back to previous file versions	Client configures backup schedule → cloud stores versions → client initiates recovery

Source: compiled by the author based on Law of Ukraine No. 2297-VI (2010), ISO/IEC 27017:2015 (2015), Regulation (EU) of the European Parliament and of the Council No. 2016/679 (2016)

The results presented in Table 5 of the analysis of cloud protection methods testified to the need for a differentiated approach to processing unstructured data in the mobile environment. Client-side encryption, despite increased demands on computing resources, remained the optimal choice for confidential information, while IAM systems realised the potential best in corporate solutions with clearly defined user roles. Backup mechanisms, being critically important for data integrity, required individual configuration for each type of content, taking into account its value and update frequency. These findings emphasised that effective protection of unstructured data in the cloud required not only the technical implementation of separate mechanisms but also a deep understanding of the context of the use. The optimal strategy envisaged a combination of protection methods, adaptation to the type of data and usage scenarios, realistic assessment of the capabilities of mobile devices, and a balance between security and performance.

Data transmission protocols of the latest versions played a crucial role in protecting unstructured data when working with mobile devices. A direct correlation was established between the type of transmitted data and the choice of an appropriate protocol: for API requests and processing of confidential information, it was advisable to use HTTPS, which provided basic encryption; transmission of large volumes of data (media content, backups) was more efficiently implemented through TLS 1.3, which combined high performance and cryptographic protection; in corporate scenarios, the optimal solution was the implementation of VPN for secure connections via open networks. Such a differentiated approach allowed taking into account the specifics of mobile applications and the type of data being processed. The analysis results confirmed that none of the reviewed protection methods were universal in the context of mobile devices. Each method had technological and contextual limitations associated with resource constraints, peculiarities of the operating environment, and modelling of user behaviour. Only the combination of complementary approaches allowed the formation of a resilient protection system for unstructured data. Accordingly, the hypothesis about the limited effectiveness of traditional security tools developed for stationary or server platforms in the mobile context was confirmed.

Challenges and limitations of protecting unstructured data in the mobile environment

Despite the active development of information protection methods, the effective implementation of these technologies in the dynamic mobile environment, particularly regarding unstructured data, faced a number of challenges. These challenges arose both at the level of technical implementation and due to the peculiarities of the mobile environment, user behavioural factors, and legal-regulatory restrictions. Within this study, the following key challenges were identified and systematised, which complicated the implementation of effective protection of unstructured data in the mobile environment (Table 6). To ensure the objectivity and relevance of the analysis, the identified problems were compared with the most widespread and critical risks defined in the industry standard OWASP Mobile Top 10 (Mobile Top 10 2024…, n.d.).

Table 6. Key problems of protecting unstructured information on mobile devices

No.	Challenge	The essence of the problem	Correspondence to OWASP Mobile Top 10 for 2024
1	High vulnerability to unstructured data leakage	The absence of centralised accounting, classification, and access control complicated protection of data from unauthorised access or loss	M5, M6, M9
2	Limited computing resources of mobile devices	Technical limitations of mobile devices restrained full implementation of cryptographic protection without harming performance	M10
3	Complexity of ensuring continuous authentication	Traditional authentication mechanisms did not provide sufficient resilience in mobile use and were subject to compromises between convenience and security	M1, M3
4	Access control in a dynamic environment	Variability of usage context complicated the application of static access policies, requiring adaptive management models	M3, M8
5	Use of public networks and cloud services	Unsafe transmission and storage of confidential data without end-to-end encryption increased the risk of interception or modification	M2, M5, M6, M9
6	Fragmentation of platforms and ecosystems	Uneven updates and differences between platforms hindered the creation of unified protection tools	M7, M8
7	Lack of transparency in mobile applications	Lack of openness in mobile applications created preconditions for hidden data collection, processing, or leakage	M4, M6
8	Legal and ethical aspects of protecting unstructured information	Inconsistency of international norms complicated compliance with data protection requirements during the processing in different jurisdictions	M6, M9

Source: compiled by the author based on Mobile Top 10 2024: Final release updates (n.d.)

For a deeper understanding of the identified barriers, it was advisable to group the barriers into three key directions: technical limitations, user factors, and regulatory challenges. Among the key technical barriers to effective protection of unstructured information in the mobile environment, several circumstances were highlighted, related to the architectural and hardware features of devices. Firstly, the decentralised nature of such data hindered centralised control, classification, and implementation of unified access policies. Secondly, limited resources of mobile devices – processor, memory, autonomy – restrained the application of full cryptographic protection without harming performance. Finally, the high fragmentation of mobile ecosystems (different OS versions, marketplace policies, hardware features) complicated the creation of unified security solutions that had to function equally across different platforms.

A separate group of challenges consisted of user-related aspects. The most critical aspect was the complexity of ensuring continuous authentication in the context of mobile use – traditional identification tools had limitations in the mobile context. Another widespread problem was incorrect configuration of access or its complete absence, which opened opportunities for abuse. An additional barrier was the low level of transparency in the operation of applications – in particular, lack of open code, insufficient documentation, and non-transparent data collection practices. At the regulatory level, the key issues remained inconsistency between national legislations in the field of data protection and the complexity of bringing mobile applications into compliance with international standards. Ensuring regulatory compliance was particularly difficult in the case of processing unstructured information, which by its nature was rarely subject to clear classification and accounting. This created risks both for data operators and for end-users. The identified challenges regarding the protection of unstructured information on mobile devices demonstrated the multidimensional nature of the problem – technical, organisational, legal, and behavioural. The challenges encompassed both internal platform aspects (computing limitations, OS fragmentation, cryptographic effectiveness) and external factors – from unpredictable environmental conditions to regulatory barriers. A separate difficulty was the dynamic context of mobile use, which required adaptive security policies. A comparative analysis with the categories of OWASP Mobile Top 10 2024: Final release updates (n.d.) confirmed the relevance of the identified challenges to mobile security practice and testified to the critical necessity of the consideration in the design of protection systems. Thus, effective resolution of these issues required an interdisciplinary approach, combining technical solutions, regulatory frameworks, and transparent interaction between the user and mobile applications.

DISCUSSION

The obtained results demonstrated that although methods of protecting unstructured information, such as symmetric and asymmetric encryption, hashing, multifactor authentication, access control, and cloud technologies, had high potential effectiveness, the implementation in the mobile environment was significantly complicated by a number of technical, organisational, and architectural barriers. The conducted analysis showed that these methods were often not adapted to the real conditions of mobile device functioning – limited energy capacity, OS fragmentation, open interfaces, and variable user behaviour. This emphasised the limitations of universal approaches developed for the server environment, while at the same time confirming the research hypothesis regarding the necessity of critically rethinking protection in the mobile context. The importance of these results lay in formulating a holistic understanding of the spectrum of challenges facing mobile security and in the analytical justification of the expediency of a comprehensive, adaptive approach to implementing systems for protecting unstructured information.

Within the conducted study, it was established that the effectiveness of cryptographic protection of unstructured information on mobile devices depended on the choice of algorithm, taking into account resource limitations. In particular, the use of AES in CBC mode required correct IV management, which was complicated in mobile systems with unstable execution contexts. Similar technical challenges were recorded in the work of K. Yu *et al*. (2022), which analysed Shamir's cryptography in distributed IoT environments. However, in that study the emphasis was shifted towards model resilience, while the impact of computational load was left unaddressed. In contrast, Y. Chen *et al*. (2020) directly pointed to the problems of energy consumption and the complexity of implementing cryptographic algorithms in mobile devices, which confirmed the findings. A comparative analysis of asymmetric encryption algorithms showed that the ECC algorithm was more suitable for the mobile environment due to its smaller key size, lower energy consumption, and faster data processing compared to RSA. This was important for protecting unstructured information, the volume of which was variable and often significant. Similar conclusions were presented in the work of R. Yuvarani & R. Mahaveerakannan (2025), where ECC showed better performance compared to RSA in the context of cloud authentication, although the authors did not focus directly on mobile devices as the local execution environment. K. Liu *et al*. (2023) confirmed the advantages of ECC in the mobile context, emphasising its effectiveness in two-factor authentication, which was consistent with the findings obtained regarding the expediency of applying ECC in scenarios of accessing encrypted data. Relevant were the results of K.S. Kumar & R. Sukumar (2019), which proved the advantage of ECC in terms of energy efficiency for Android devices, fully coinciding with the conclusions of this study about the expediency of using elliptic curves for protecting mobile data. Thus, the results of the study were confirmed by previous works, while focusing attention on the application of ECC specifically for protecting unstructured information in resource-constrained conditions.

A comprehensive review of access control models in the mobile environment demonstrated that the implementation of effective authentication and access management in the mobile environment was complicated by platform fragmentation, variability of user interaction models, and limitations of computing resources. The most effective approaches proved to be multifactor and context-dependent methods, which could ensure a balance between convenience and the level of protection. Similar conclusions were observed in the study of A. Tewari & B.B. Gupta (2020), which noted the necessity of comprehensive construction of access systems in multi-level IoT environments, with an emphasis on

adaptability and dynamic rights management. At the same time, in the mentioned work the main focus was on the general architecture of IoT, while the specifics of mobile OS and user scenarios were left beyond the analysis. In the work of H.F. Atlam & G.B. Wills (2020), the importance of considering ethical and social aspects when implementing identification mechanisms was outlined, which was relevant for the mobile environment with its high level of personalisation, although the technical parameters of access implementation were not disclosed. In contrast, in the study of J. Du *et al*. (2018) the expediency of distributed authentication models was justified to reduce the load on central nodes, which partially correlated with the mobile need for delegated processing.

The analysis of the cloud component in the context of protecting unstructured data on mobile devices confirmed the expediency of implementing client-side encryption before transferring data to the cloud, given the risks of losing control over confidential information after its upload. Such an approach was confirmed in the study of A. Musa & A. Mahmood (2021), which noted that client-side encryption significantly increased trust in cloud storage, although the authors did not consider the limitations of mobile platforms. M. da Rocha *et al*. (2020) expanded this vision, proposing the use of a trusted execution environment, which allowed keys to be stored on the client side – a similar concept corresponded with the emphasis on minimising dependence on the cloud provider. Regarding access control, the results of the study highlighted the need for dynamic rights management on the user side, which was consistent with the position of J. Mellom (2020), who emphasised the role of IAM as a basic component of cloud security. The review proposed by A.O. Akinade *et al*. (2025) confirmed the importance of combining encryption, IAM, and authentication mechanisms in cloud environments, but mainly from the standpoint of infrastructure providers, whereas in the present study the focus was on the possibilities and limitations of the mobile client.

One of the central challenges identified in the study was the high vulnerability to leakage of unstructured data in the mobile environment, caused by the absence of a centralised model of accounting, classification, and access control. This risk was aggravated by the fact that mobile applications often gained access to such data without clear restrictions and proper informed consent of the user. Similar observations were described in the work of Y. Guo *et al*. (2021), which emphasised that unstructured data was easily extracted, particularly due to the lack of transparent information processing policies in mobile applications. At the same time, in the mentioned study the main emphasis was on the technical aspects of data extraction, while in the present study the emphasis was shifted to the systemic absence of mechanisms to prevent leakage. An additional barrier was identified in the fragmentation of mobile platforms, which complicated the implementation of unified solutions for information protection. As noted in the study of S. Garg & N. Baliyan (2021), the differences between Android and iOS – in security approaches, update frequency, and access configuration – created unequal conditions for the implementation of protection standards. Thus, the obtained results were confirmed: effective protection of unstructured information on mobile devices had to take into account not only general technical mechanisms, but also the architectural specifics of mobile ecosystems.

Among the identified challenges of protecting unstructured information on mobile devices, a special place was occupied by the problem of continuous user authentication. As shown in the results of the study, traditional authentication methods, such as passwords, Personal Identification Number codes, or one-time tokens, did not provide an adequate level of resilience under conditions of mobile use, characterised by environmental variability, short sessions, and limited user attention. At the same time, alternative approaches, such as biometric parameters or behavioural patterns, remained vulnerable to attacks, recognition errors, and breaches of confidentiality. Similar limitations were reflected in the study of M. Papaioannou *et al*. (2023), which noted that although behavioural biometrics showed potential for continuous identification, it significantly depended on the context of use and the device. The work of Y. Yang *et al*. (2019) confirmed this assessment, emphasising the difficulties in maintaining stable accuracy of behavioural models in the dynamic conditions of the mobile environment. Similar conclusions were presented in the study of P.M.A.B. Estrela *et al*. (2021), which showed that the implementation of continuous authentication in mobile banking required complex infrastructure and a balance between convenience and security.

Insufficient protection of data during transmission via public networks or storage in cloud environments was identified as one of the challenges that increased the risks of unauthorised access to unstructured information. The study emphasised the lack of end-to-end encryption on the mobile device side, which made data vulnerable to Man-in-the-Middle attacks and interception. A similar problem was identified by Y. Yao *et al*. (2023), who proposed a complex secure transmission scheme, which, however, required high resources and did not correspond to the limitations of mobile devices. In addition, the observations of M. Sangeen *et al*. (2023) about the low awareness of users regarding the dangers of public networks resonated with the results of the present study, where behavioural aspects were identified as an additional risk factor. Unlike the mentioned authors, the present study detailed the problem precisely in the context of unstructured data and the mobile environment, emphasising the insufficiency of basic protection models.

Legal and regulatory restrictions were considered a significant barrier to ensuring the confidentiality of unstructured data. The present work indicated that the complexity of auditing such information and

the fragmentation of legal requirements complicated compliance with privacy standards. This conclusion was consistent with the arguments of W. Hartzog & N.M. Richards (2020), who pointed to the institutional lack of adaptation of law to digital dynamics. Similarly, J. Wong & T. Henderson (2019) emphasised the technical difficulties of implementing the right to portability under GDPR. However, while in the mentioned works attention was focused on general regulatory approaches, the present study supplemented these approaches by highlighting how the unstructured nature of mobile data made full legal regulation impossible. This comparison confirmed that legal challenges were no less critical than technical ones and required integrated solutions. The analysis of the results of the study reflected that the identified challenges – in particular the problems of unstructured data leakage, limited mobile resources, authentication difficulties, and regulatory barriers – were systemic and largely confirmed by other studies. At the same time, the conducted comparison showed that the present study expanded existing approaches by comprehensively covering the technical, behavioural, and legal aspects specific to the mobile environment. Such a comprehensive analysis allowed not only the identification of current problems, but also the critical evaluation of the applicability limits of existing solutions in the context of protecting unstructured information.

CONCLUSIONS

Within this study, a comprehensive analysis was carried out of methods of protecting unstructured information on mobile devices, taking into account technical, organisational, and legal-regulatory factors. The results of the theoretical analysis of cryptographic algorithms showed that symmetric AES encryption in CBC mode was suitable for protecting local data, but required careful IV management. A comparative assessment of RSA and ECC confirmed the advantage of the latter in terms of energy efficiency and speed, which made it more optimal for mobile application. The analysis of hash functions confirmed the higher effectiveness of BLAKE3 compared to SHA-256 due to its lower energy consumption, higher speed, and support for parallel data processing, which were critical for mobile platforms.

Traditional authentication mechanisms proved insufficiently adapted to the mobile environment, while promising approaches were those combining behavioural biometrics with a context-dependent approach. The analysis of cloud protection methods demonstrated the effectiveness of a combination of client-side encryption, IAM systems, and backup, particularly in ensuring the confidentiality of unstructured information during its transmission and storage. The analysis of modern secure transmission protocols, in particular HTTPS, TLS 1.3, and VPN, confirmed the high effectiveness in ensuring data confidentiality during transportation in open networks. It was established that the effectiveness of protection methods directly depended on the type of processed data, the architecture of the mobile device, resource limitations, and environmental conditions, which necessitated an adaptive choice of protection solutions.

Special attention was paid to the identification of key challenges complicating the implementation of unstructured data protection on mobile devices. Eight problems were systematised, covering technical, behavioural, and regulatory aspects: from the risk of data leakage and mobile resource limitations to application transparency issues and legal barriers. The comparison with OWASP Mobile Top 10 made it possible to verify the relevance of these challenges to current security practices. The results of the study confirmed the hypothesis that traditional protection tools, oriented towards stationary or server environments, proved insufficiently effective in the mobile context, requiring a comprehensive and adaptive approach. The study had limitations related to the theoretical nature of the analysis, the absence of empirical testing, and the inaccessibility of full technical specifications of mobile OS and commercial applications. In further research, it would be expedient to focus on the practical testing of the effectiveness of cryptographic algorithms optimised for the limitations of mobile devices, as well as on the development of adaptive authentication systems and the creation of cross-platform solutions for data protection.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Abibulaev, A.R., & Piskozub, A.Z. (2025). Analysis of possibilities for improving cloud infrastructure security using NLP and ML. *Modern Information Security*, 2(62), 124-140. doi: 10.31673/2409-7292.2025.026884.

[2] Akinade, A.O., Adepoju, P.A., Ige, A.B., & Afolabi, A.I. (2025). Cloud security challenges and solutions: A review of current best practices. *International Journal of Multidisciplinary Research and Growth Evaluation*, 6(1), 26-35. doi: 10.54660/.IJMRGE.2025.6.1.26-35.

[3] Atlam, H.F., & Wills, G.B. (2020). IoT security, privacy, safety and ethics. In M. Farsi, A. Daneshkhah, A. Hosseinian-Far & H. Jahankhani (Eds.), *Digital twin technologies and smart cities* (pp. 123-149). Cham: Springer. doi: 10.1007/978-3-030-18732-3_8.

[4] Babayeva, K.G. (2024). Using cryptographic methods, mechanisms, and tools for protecting biometric data. In *Radioelectronics and youth in the 21st century: Materials of the 28th international youth forum* (pp. 88-90). Kharkiv: Kharkiv National University of Radio Electronics. doi: 10.30837/IYF.PCEIP.2024.088.
[5] Brovchenko, Y.M., Samarai, V.P., Datsenko, I.P., Pavlenko, V.I., & Sereda, A.V. (2023). Protection of unstructured data on mobile devices. *Infocommunications and Computer Technologies*, 1(5), 194-200. doi: 10.36994/2788-5518-2023-01-05-21.
[6] Chen, L., Moody, D., Randall, K., Regenscheid, A., & Robinson, A. (2023). *Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-186.
[7] Chen, Y., Zheng, B., Zhang, Z., Wang, Q., Shen, C., & Zhang, Q. (2020). Deep learning on mobile and embedded devices: State-of-the-art, challenges, and future directions. *ACM Computing Surveys*, 53(4), article number 84. doi: 10.1145/3398209.
[8] da Rocha, M., Valadares, D.C.G., Perkusich, A., Gorgonio, K.C., Pagno, R.T., & Will, N.C. (2020). Secure cloud storage with client-side encryption using a trusted execution environment. In *Proceedings of the 10th international conference on cloud computing and services science* (pp. 31-43). Setubal: SciTePress. doi: 10.5220/0009130600310043.
[9] Du, J., Jiang, C., Gelenbe, E., Xu, L., Li, J., & Ren, Y. (2018). Distributed data privacy preservation in IoT applications. *IEEE Wireless Communications*, 25(6), 68-76. doi: 10.1109/MWC.2017.1800094.
[10] Dworkin, M. (2001). *Recommendation for block cipher modes of operation: Methods and Techniques*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-38A.
[11] Estrela, P.M.A.B., Albuquerque, R.D.O., Amaral, D.M., Giozza, W.F., & Júnior, R.T.D.S. (2021). A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications. *Sensors*, 21(12), article number 4212. doi: 10.3390/s21124212.
[12] Force, J.T. (2020). *Security and privacy controls for information systems and organizations*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-53r5.
[13] Garg, S., & Baliyan, N. (2021). Comparative analysis of Android and iOS from security viewpoint. *Computer Science Review*, 40, article number 100372. doi: 10.1016/j.cosrev.2021.100372.
[14] Grassi, P.A., Garcia, M.E., & Fenton, J.L. (2017). *Digital identity guidelines*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-63-4.
[15] Guo, Y., Liu, J., Tang, W., & Huang, C. (2021). Exsense: Extract sensitive information from unstructured data. *Computers & Security*, 102, article number 102156. doi: 10.1016/j.cose.2020.102156.
[16] Hartzog, W., & Richards, N.M. (2020). Privacy's constitutional moment and the limits of data protection. *SSRN*, article number 3441502. doi: 10.2139/ssrn.3441502.
[17] Hu, V.C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). *Guide to attribute based access control (ABAC) definition and considerations*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-162.
[18] ISO/IEC 27017:2015. (2015). *Information technology – security techniques – code of practice for information security controls based on ISO/IEC 27002 for cloud services*. Retrieved from https://www.iso.org/standard/43757.html.
[19] Kibar, B. (2023). *Comparing Blake3 and Sha-256 data integrity algorithms & integrating Blake3 with Golang*. Retrieved from https://surl.lu/vdnytl.
[20] Konovalov, S.M. (2025). Analysis of types of cybersecurity in mobile phone operating systems. *Taurida Scientific Herald. Series: Technical Sciences*, 2, 100-104. doi: 10.32782/tnv-tech.2025.2.11.
[21] Kostiuk, Y., Bebeshko, B., Kriuchkova, L., Lytvynov, V., Oksanych, I., Skladannyi, P., & Khorolska, K. (2024). Information protection and data exchange security in wireless mobile networks with authentication and key exchange protocols. *Cybersecurity: Education, Science, Technique*, 1(25), 229-252. doi: 10.28925/2663-4023.2024.25.229252.
[22] Kumar, K.S., & Sukumar, R. (2019). Achieving energy efficiency using novel scalar multiplication based ECC for Android devices in Internet of Things environments. *Cluster Computing*, 22(5), 12021-12028. doi: 10.1007/s10586-017-1542-8.
[23] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2297-17#Text.
[24] Liu, K., Zhou, Z., Cao, Q., Xu, G., Wang, C., Gao, Y., Zeng, W., & Xu, G. (2023). A robust and effective two-factor authentication (2FA) protocol based on ECC for mobile computing. *Applied Sciences*, 13(7), article number 4425. doi: 10.3390/app13074425.
[25] Marchenko, O. (2023). Cybersecurity and information protection: Analysis of risk and threat impact with modern effective cyberspace defense strategies. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 50-59. doi: 10.32782/IT/2023-3-6.

[26] Mellom, J. (2020). *The role of identity access management (IAM) in cloud security*. Retrieved from https://sonraisecurity.com/blog/the-role-of-identity-access-management-iam-in-governing-cloud-security/.
[27] Mobile Top 10 2024: Final release updates. (n.d.). Retrieved from https://owasp.org/www-project-mobile-top-10/.
[28] Moriarty, K., Kaliski, B., Jonsson, J., & Rushc, A. (2016). *PKCS #1: RSA cryptography specifications version 2.2*. Retrieved from https://datatracker.ietf.org/doc/html/rfc8017.
[29] Musa, A., & Mahmood, A. (2021). Client-side cryptography based security for cloud computing system. In *2021 international conference on artificial intelligence and smart systems (ICAIS)* (pp. 594-600). Coimbatore: IEEE. doi: 10.1109/ICAIS50930.2021.9395890.
[30] National Institute of Standards and Technology. (2023). *Advanced Encryption Standard (AES)*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.FIPS.197-upd1.
[31] Papaioannou, M., Mantas, G., Panaousis, E.M., Essop, A., Rodriguez, J., & Sucasas, V. (2023). Behavioral biometrics for mobile user authentication: Benefits and limitations. In *2023 IFIP networking conference (IFIP networking)* (pp. 1-6). Barcelona: IEEE. doi: 10.23919/IFIPNetworking57963.2023.10186419.
[32] Regulation (EU) of the European Parliament and of the Council No. 2016/679 "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance)". (2016, April). Retrieved from http://data.europa.eu/eli/reg/2016/679/oj.
[33] Rogushina, J.V. (2019). Methods and tools for analyzing unstructured data. *Problems in Programming*, 1, 57-77. doi: 10.15407/pp2019.01.057.
[34] Sangeen, M., Bhatti, N.A., Kifayat, K., Alsadhan, A.A., & Wang, H. (2023). Blind-trust: Raising awareness of the dangers of using unsecured public Wi-Fi networks. *Computer Communications*, 209, 359-367. doi: 10.1016/j.comcom.2023.07.011.
[35] Sereda, A., Datsenko, I., Pavlenko, V., & Samarai, V. (2022). Stability and efficiency of cryptographic algorithms used in mobile devices. *Infocommunications and Computer Technologies*, 2(4), 178-190. doi: 10.36994/2788-5518-2022-02-04-21.
[36] Spasiteleva, S., Zhdanova, Y., & Chychkan, I. (2019). Security problems of universal data management systems. *Cybersecurity: Education, Science, Technique*, 2(6), 122-133. doi: 10.28925/2663-4023.2019.6.122133.
[37] Tewari, A., & Gupta, B.B. (2020). Security, privacy and trust of different layers in internet-of-things (IoTs) framework. *Future Generation Computer Systems*, 108, 909-920. doi: 10.1016/j.future.2018.04.027.
[38] Vahdati, Z., Yasin, S., Ghasempour, A., & Salehi, M. (2019). Comparison of ECC and RSA algorithms in IoT devices. *Journal of Theoretical and Applied Information Technology*, 97(16), 4293-4308.
[39] Wong, J., & Henderson, T. (2019). The right to data portability in practice: Exploring the implications of the technologically neutral GDPR. *International Data Privacy Law*, 9(3), 173-191. doi: 10.1093/idpl/ipz008.
[40] Yang, Y., Guo, B., Wang, Z., Li, M., Yu, Z., & Zhou, X. (2019). BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics. *Ad Hoc Networks*, 84, 9-18. doi: 10.1016/j.adhoc.2018.09.015.
[41] Yao, Y., Shu, F., Li, Z., Cheng, X., & Wu, L. (2023). Secure transmission scheme based on joint radar and communication in mobile vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*, 24(9), 10027-10037. doi: 10.1109/TITS.2023.3271452.
[42] Yu, K., Tan, L., Yang, C., Choo, K.-K.R., Bashir, A.K., Rodrigues, J.J.P.C., & Sato, T. (2022). A blockchain-based Shamir's threshold cryptography scheme for data protection in industrial Internet of Things settings. *IEEE Internet of Things Journal*, 9(11), 8154-8167. doi: 10.1109/JIOT.2021.3125190.
[43] Yuvarani, R., & Mahaveerakannan, R. (2025). Enhancing IoT security: Performance evaluation of RSA and ECC in QR code-based authentication systems with cloud integration. In *2025 6th international conference on mobile computing and sustainable informatics* (pp. 308-315). Goathgaun: IEEE. doi: 10.1109/ICMCSI64620.2025.10883058.

Проблеми захисту неструктурованої інформації на мобільних пристроях

Євген Бровченко

Аспірант
Відкритий міжнародний університет розвитку людини «Україна»
04071, вул. Львівська, 23, м. Київ, Україна
https://orcid.org/0000-0002-1416-0385

Анотація. Актуальність дослідження зумовлена зростанням обсягів неструктурованих даних у мобільному середовищі, що потребує переосмислення класичних підходів до їх захисту в умовах обмежених ресурсів і динамічного використання. Мета дослідження полягала у комплексному аналізі методів захисту неструктурованої інформації в мобільному середовищі та виявленні ключових бар'єрів для їх ефективного впровадження. Методологія базувалася на теоретико-аналітичному підході, що включав систематизацію методів захисту, порівняльний аналіз криптографічних алгоритмів, оцінку моделей автентифікації та контролю доступу, а також аналіз хмарних механізмів безпеки. Встановлено, що симетричне шифрування Advanced Encryption Standard у режимі Cipher Block Chaining забезпечує ефективний локальний захист, але вимагає ретельного управління векторами ініціалізації. Досліджено, що Elliptic Curve Cryptography перевершує Rivest-Shamir-Adleman за енергоефективністю та швидкодією, а BLAKE3 – Secure Hash Algorithm 256 за швидкістю, енергоспоживанням і підтримкою паралелізму. Узагальнено, що моделі контролю доступу недостатньо адаптовані до динаміки мобільного середовища, а найбільш ефективними є контекстно-орієнтовані й багатофакторні підходи, зокрема з використанням біометричної та поведінкової автентифікації. Отримано, що комбінація клієнтського шифрування, управління ідентичністю та резервного копіювання у хмарі забезпечує найвищий рівень захисту за належного впровадження. Встановлено, що ефективність протоколів HyperText Transfer Protocol Secure, Transport Layer Security 1.3 і Virtual Private Network залежить від типу даних і сценарію взаємодії, а їх застосування потребує балансу між безпекою, продуктивністю та контекстом використання. Ідентифіковано вісім ключових викликів, релевантність яких до практики мобільної безпеки підтверджено через зіставлення з категоріями OWASP Mobile Top 10: витік даних, обмежені ресурси, складність автентифікації, динамічний контроль доступу, використання публічних мереж, фрагментація платформ, непрозорість застосунків і правові бар'єри. Установлено, що ефективність методів захисту зумовлюється контекстом застосування – типом даних, архітектурою пристрою, сценарієм взаємодії та доступною інфраструктурою, що вимагає адаптивного вибору рішень. Отримані результати підтверджують, що традиційні підходи до інформаційної безпеки потребують адаптації до специфіки мобільних платформ. Дослідження має практичну цінність для розробників безпекових рішень, адміністраторів корпоративних систем та політиків у сфері кібербезпеки

Ключові слова: середовище; шифрування; автентифікація; обмеження ресурсів; контроль доступу