Journal homepage: https://itce.vn.ua/en

Information Technologies and Computer Engineering **Vol. 23, No. 1. 2026**

Article's History: Received: 09.10.2025 Revised: 05.01.2026
Accepted: 26.03.2026 Published: 20.04.2026

ISSN 1999-9941; e-ISSN 2078-6387
UDC 004.056:004.738.5
DOI: 10.31649/vitce/1.2026.60

Method for protection of unstructured information on modern mobile platforms: Threat modelling and effectiveness analysis

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

Valeriy Samaraj
PhD in Technical Sciences, Associate Professor
Centre for Military and Strategic Studies of the National Defence University of Ukraine
03049, 28 Povitrianykh Syl Ave., Kyiv, Ukraine
https://orcid.org/0000-0003-4419-1366

Abstract. The study aimed to develop a comprehensive approach to protecting unstructured information on mobile platforms by combining cryptographic algorithms, multi-factor authentication, machine learning methods, and blockchain technologies to create an adaptive security system. The research methodology was based on a theoretical analysis of scientific sources and modelling of the architecture of a system for protecting unstructured information, focused on modern mobile platforms. The study addressed the use of devices with support for Advanced RISC Machine TrustZone and Secure Enclave, which provide hardware isolation of cryptographic operations. Advanced Encryption Standard was used as the basic encryption algorithm for symmetric data protection, and Learning with Errors was used as a quantum-resistant mechanism. As part of the research, a conceptual multi-level model of an integrated security system was developed, including four interacting layers: cryptographic, authentication, analytical (behavioural analytics and machine learning methods) and blockchain. Each layer performs a separate function: encryption and hardware isolation of operations, user authentication, anomaly detection, and data integrity assurance. Together, they form an adaptive security system for mobile platforms. Implementation of a hybrid blockchain, which combines the high performance of private chains with independent verification of transactions in public blocks, was emphasised. This approach ensured a balance between transparency, energy efficiency, and resistance to modifications. Theoretical analysis confirmed that integrating these components into a single architecture creates conditions for the formation of an adaptive security system capable of dynamically responding to threats and ensuring a high level of protection for unstructured data in mobile environments. The proposed approach can be implemented in medicine, finance, public administration, and other areas where the protection of unstructured information is critical

Keywords: multi-factor authentication; recurrent neural networks; logistic regression; adaptive encryption; hybrid blockchain architecture

Introduction

The rapid development of mobile technologies has led to smartphones and tablets becoming integral elements of the information infrastructure, widely used in business, public administration, medicine, finance and other critical sectors. According to current statistics, there are over 6.8 billion mobile devices, and a significant portion of them are used to store and process sensitive data (Kumar, 2025). Unstructured data, such as text documents, media files, electronic messages, event logs, etc., which are highly diverse and difficult to protect in a unified manner, pose a particular threat. The relevance of the problem is exacerbated by the dynamic growth in the number of cyberattacks targeting

Suggested Citation:
Brovchenko, E., & Samaraj, V. (2026). Method for protection of unstructured information on modern mobile platforms: Threat modelling and effectiveness analysis. *Information Technologies and Computer Engineering*, 23(1), 60-71. doi: 10.31649/vitce/1.2026.60

*Corresponding author

mobile systems. The number of security incidents has increased, and financial losses have reached billions (Bonnie, 2025; Smith, 2025). Modern threats are no longer limited to technical software vulnerabilities; they increasingly include social engineering, contextual manipulation, multi-vector attacks, and the use of artificial intelligence technologies to bypass traditional protection systems. An additional challenge is the prospect of quantum computing, which could render traditional cryptographic algorithms (Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and even Advanced Encryption Standard (AES)) vulnerable in the coming years. Traditional security methods such as passwords, single-factor authentication, and static encryption are becoming less effective in the modern cyber environment.

A. Shifa *et al.* (2020) proposed a multi-level encryption model focused on protecting multimedia files stored in mobile applications. The results confirmed an increase in the system's resilience, but the computational costs proved excessive for budget smartphones. G. Malik (2024) emphasised the problem of authentication and proved that combining biometric and contextual factors (access time, geolocation) reduces the risk of unauthorised access by more than six times. The disadvantage of this approach is an increase in the number of false rejections when user behaviour changes.

E.M. Brovchenko *et al.* (2023) analysed the integration of blockchain technologies into mobile case management systems. The study emphasised that the use of hybrid blockchains, which combine private and public chains, provides an optimal balance between process transparency and speed, although the issue of excessive energy consumption remains relevant. D. Prokopovych-Tkachenko *et al.* (2025) examined the use of machine learning algorithms to detect phishing attacks in a mobile environment. The results showed high classification accuracy, but the effectiveness of the model depended largely on the size and diversity of the training sample. The study by V. Mahor *et al.* (2021) analysed vulnerabilities in mobile operating systems. The author found that about 40% of successful attacks are conducted through unprotected application programming interface (API) accesses, indicating the need for comprehensive security policies at the application developer level. Y. He *et al.* (2022) proposed the concept of Zero Trust architecture for mobile devices. The results proved to be highly effective in a corporate environment, but scaling this approach proved problematic due to increased delays.

S.R. Kandula (2025) examined quantum-resistant encryption algorithms. The study emphasised that the implementation of Learning with Errors (LWE) in mobile systems guarantees a promising level of protection, although it requires additional optimisation for hardware limitations. Mehwish *et al.* (2024) emphasised the problem of data protection in public Wi-Fi networks. The study demonstrated that the use of WireGuard-based VPNs in combination with behavioural analytics reduces the likelihood of data compromise by more than 70%. A.M. Aburbeian & M. Fernández-Veiga (2024) analysed the role of multi-factor authentication in financial mobile applications. The study demonstrated that the combination of a password, biometrics and one-time tokens render brute force attacks impossible, but at the same time requires user-friendly interfaces. Lastly, M. Woźniak *et al.* (2021) proposed a model for adaptive threat monitoring in mobile systems based on recurrent neural networks. Testing showed a reduction in attack response time to one second, but this requires resource-intensive machine learning (ML) frameworks.

An analysis of research has shown that despite significant progress in the field of mobile platform cybersecurity, a range of substantial aspects remain insufficiently studied. In particular, there is a lack of in-depth analysis of the comprehensive integration of various protection methods – cryptography, multi-factor authentication, behavioural analytics, machine learning and blockchain – into a single adaptive system. There is also insufficient research on mechanisms for dynamic adaptation of security systems in real time, capable of automatically changing policies and resource allocation depending on the threat context. A significant gap is the issue of energy consumption and performance, as most modern ML models are characterised by high computational costs, which limit their practical application on mobile devices with limited hardware resources. Optimalisation of quantum-resistant algorithms for mobile platforms requires additional attention, as their use remains theoretically promising but practically limited. Equally relevant is the problem of combining blockchain with mobile systems, as the issues of scalability and energy consumption do not have a comprehensive solution.

Given these limitations, the study aimed to develop and justify an adaptive multi-component system for protecting unstructured information on modern mobile platforms, combining cryptography, multi-factor authentication, machine learning and blockchain technologies to improve the effectiveness of countering current and future cyber threats. The research tasks were to theoretically substantiate, develop, and test an integrated architecture for protecting unstructured information on mobile platforms using machine learning methods, multi-factor authentication (MFA), cryptographic algorithms and blockchain technologies, as well as evaluating the effectiveness of the proposed system in terms of prediction accuracy, speed, energy consumption and resistance to attacks.

Materials and Methods

The research was theoretical in nature and based on a combination of conceptual, analytical-synthetic and model types of analysis, which ensured a systematic interpretation of approaches to protecting unstructured information on mobile platforms and the formation of our own integrated security architecture. The theoretical analysis was based on a study of peer-reviewed scientific articles on machine learning and cryptography published in journals indexed in the Scopus and Web of Science scientific databases, monographs, and official technical documentation

for mobile operating systems (Android Keystore Documentation, Apple Platform Security Guide). The criteria for selecting literature were relevance to the issue of mobile security, publications for the period 2020-2025, the availability of comparative characteristics of protection methods and empirical results that can be used to compare the effectiveness of different technologies. The research materials also included technical specifications for Android Keystore API and Apple Secure Enclave, which provide hardware isolation for cryptographic operations (iOS Security: iOS 12.3., 2019; Martín *et al.*, 2021; Google for Developers, 2025). Scientific reliability was ensured by using authoritative and peer-reviewed sources, comparing theoretical models with empirical results presented in technical reports and publications by researchers. Different technologies were compared based on the following criteria: threat prediction accuracy, speed, energy consumption, level of resistance to attacks, and the possibility of integration into mobile platforms.

The analytical and synthetic review method was used to analyse scientific sources that explore the possibilities of using recurrent neural networks (RNN) and ensemble models to detect anomalies in the behaviour of mobile system users. Studies demonstrating the ability of ML models to predict threats in time series mode and support adaptive authentication were emphasised. Based on the generalisation of these data, theoretical prerequisites for further modelling of an integrated protection architecture were formed.

The theoretical analysis considered the use of Trusted Execution Environment (TEE) and StrongBox environments, which, according to official standards, ensure the execution of critical operations outside the main operating system. This was used to assess the hardware level of protection of mobile platforms and their role in the overall security architecture. They were compared in terms of resistance to compromise, supported authentication mechanisms, integration capabilities, and energy efficiency in a mobile environment. The AES-256 cryptographic algorithms and the quantum-resistant LWE approach were considered separately, which was used to evaluate their effectiveness in terms of performance, energy consumption, and resistance to classical and quantum attacks. A separate area of focus was the analysis of hybrid blockchain architecture based on Hyperledger Fabric and Ethereum, which was used for a theoretical assessment of the balance between the performance of private chains and the transparency of public blocks.

The theoretical research algorithm included several interrelated stages. At the first stage, a theoretical review and classification of modern approaches to mobile platform protection was conducted, covering cryptographic methods, multi-factor authentication, behavioural analytics, machine learning, and blockchain technologies. The second stage involved an analytical and synthetic comparative analysis of technologies, assessing their advantages and limitations and comparing methods according to key criteria: speed, energy consumption, threat detection accuracy, and resistance to attacks. The third stage identified systemic limitations in the application of individual methods and theoretically justified the need for an integrated approach to mobile platform protection capable of compensating for the weaknesses of each technology. The fourth stage was devoted to the formation of a conceptual multi-level model of an integrated security system that combines cryptographic, authentication, analytical and blockchain levels and describes the interaction of technologies within an adaptive architecture. In the final, fifth stage, the theoretical results were summarised, and conclusions were formulated, which determined the effectiveness and prospects of the proposed model for protecting unstructured information on mobile platforms. This methodological logic ensured consistency between the source base, analysis methods and the theoretical results of the study.

Results

Cryptography is a fundamental element of information security on mobile platforms and ensures the confidentiality, integrity, and authenticity of data. Both symmetric and asymmetric algorithms are actively used in modern mobile solutions. The most common symmetric standard is AES, which is used to encrypt locally stored files and protect data during transmission over the network. Its main advantages are high performance and reliability in a classic computing environment. However, AES is vulnerable to future quantum attacks, which raises questions about its long-term effectiveness.

Among asymmetric algorithms, RSA and ECC are central. RSA is a traditional solution for key management and digital signatures, but it is inferior in terms of speed and requires large key sizes to ensure sufficient security. ECC is a more optimised option that can ensure equivalent security with smaller key sizes and, accordingly, less load on the computing resources of mobile devices. At the same time, both RSA and ECC remain vulnerable to quantum computing algorithms, in particular Shor's algorithm, as highlighted by N.S.M. Shamsuddin & S.A. Pitchay (2020).

To ensure long-term security, researchers are turning to quantum-resistant cryptographic algorithms. One of the most promising is LWE, which involves building cryptosystems based on the complexity of linear algebra problems with errors. The use of LWE in mobile systems guarantees increased resistance to quantum attacks, but requires additional optimisation for the hardware limitations of smartphones, as it requires significant computing resources (Asif, 2021). Another important area is hardware encryption using secure environments such as ARM (Advanced RISC Machines) TrustZone or Secure Enclave, which can isolate cryptographic operations from the main operating system. This minimises the risks of attacks at the software level but does not eliminate threats associated with physical access to the device or side channels (e.g., power consumption analysis).

Despite progress in the development of cryptographic solutions, their implementation on mobile platforms has

several limitations. First, the high complexity of algorithms leads to increased energy consumption, which is critical for devices with limited battery capacity. Secondly, most methods do not provide sufficient flexibility in dynamic threat environments, as they are implemented in a static form without adaptation mechanisms. Thirdly, the problem of compatibility between different cryptographic protocols and platforms remains unresolved, which complicates the practical application of complex systems, as emphasised by R. Banoth & R. Regar (2023). Thus, modern cryptography provides a high level of protection for mobile platforms against classic attacks but does not guarantee long-term stability in the context of the development of quantum computing and requires integration with other approaches – machine learning, behavioural analytics and blockchain (Yadav, 2021).

Blockchain technologies are increasingly seen as a promising tool for ensuring transparency and data integrity in mobile systems. Their main advantage lies in the creation of an immutable transaction ledger, which guarantees the authenticity of information and makes it impossible to falsify without the collective consent of network participants. In the context of mobile platforms, blockchain is used for several key tasks: protecting unstructured data, managing user identities, secure authentication, and transaction verification.

The main areas of blockchain use are public chains (e.g., Ethereum) and private/consortium solutions (e.g., Hyperledger Fabric). Public networks provide a high level of transparency and independence from a specific provider but suffer from scalability issues and high energy costs when verifying transactions. Private blockchains, on the other hand, demonstrate better performance and lower energy consumption, but have a limited level of decentralisation. Mobile case management systems most often use a hybrid architecture that combines the speed of private blocks with the transparency of public ones. This approach stores confidential data in a private chain and critical parameters or hashes in a public chain, ensuring integrity control without high computational costs.

One substantial use case for blockchain is managing user authentication and identification. Thanks to its distributed nature, blockchain makes it possible to create decentralised access control systems where accounts, keys, and biometric identifiers are not stored centrally, reducing the risk of mass leaks. In addition, blockchain increases the level of trust in multi-factor authentication, as each identity verification transaction can be recorded in the blockchain, as emphasised by Y. Liu *et al.* (2020).

Another substantial area is the use of blockchain to protect event logs and logs in mobile systems. Since attacks are often aimed at changing or deleting traces of activity, storing such data in a blockchain makes it immutable and available for further analysis. This creates an additional level of protection during incident investigations and promotes transparency in information processes.

Despite its advantages, the use of blockchain in mobile systems has several limitations. First, it has high energy consumption and places a heavy load on device resources, especially when using public chains. Secondly, the issue of scalability remains relevant: an increase in the number of transactions slows down the system, which is critical for mobile scenarios where a quick response is required. Thirdly, integrating blockchain into mobile platforms requires specialised optimisation protocols and a combination with other technologies (ML, cryptography, MFA) to compensate for its shortcomings.

Thus, blockchain is an effective means of protecting unstructured information in mobile systems, but its practical application requires a balance between security, performance, and energy efficiency. The most promising are hybrid architectures that combine private and public chains and integrate with other cyber defence mechanisms, forming a multi-level and adaptive security system as described by X. Wei (2022).

Behavioural analytics is one of the most promising areas of mobile platform security, as it incorporates individual device usage patterns and can be used for the detection of anomalies that cannot always be identified by traditional security measures. Models of this type analyse a wide range of characteristics: text input speed, touchscreen pressure intensity, smartphone holding posture, app usage frequency, geolocation data, network activity, etc. Based on these characteristics, a user profile is created, which is then used to detect suspicious behaviour. Machine learning methods are substantial in the development of behavioural analytics. The most common approach is the use of RNNs, which are well-suited to processing time series and can predict future user actions based on their historical activity. The use of RNNs in mobile systems ensures high accuracy in detecting attacks, but requires significant computing resources, which limits their use in low-performance devices.

Another approach is logistic regression and ensemble methods (Random Forest, Gradient Boosting), which provide a balance between prediction accuracy and energy efficiency. Such algorithms are well-suited for constrained mobile environments where resource consumption must be minimised. However, their limitation is the complexity of processing large numbers of multidimensional parameters characteristic of behavioural data.

Behavioural biometrics, which is based on unique user characteristics such as gait, typing rhythm, and screen interaction, is also receiving significant attention. Machine learning models ensure continuous authentication, which increases the level of protection even in cases of theft or temporary use of the device by third parties (Lim *et al.*, 2020). Federated learning is special in mobile systems, as it can be used to train models without the need for centralised collection of personal data. This reduces the risk of confidential information leaks while maintaining high prediction accuracy. However, this approach requires optimisation of model synchronisation algorithms and consideration of the heterogeneity of computing resources across different devices (Acien *et al.*, 2020).

Despite their significant potential, the application of behavioural analytics and ML models in mobile systems has several limitations. First, there is energy consumption: complex neural networks can quickly drain a device's battery. Second, there is the problem of false positives, when normal deviations in user behaviour are mistakenly identified as attacks. Third, the issue of data privacy remains relevant, as large amounts of personal information are often required to train models.

Thus, behavioural analytics and machine learning create new opportunities for protecting unstructured information on mobile platforms, but their effectiveness directly depends on the balance between prediction accuracy, resource costs, and user privacy (Martín *et al.*, 2021). The most promising direction would be to integrate various ML algorithms with multi-factor authentication and cryptographic methods into a single adaptive architecture.

Modern approaches to the protection of unstructured information in mobile systems are characterised by their multi-component nature and diversity of technological solutions. They include cryptographic algorithms, multi-factor authentication, behavioural analytics, machine learning, and blockchain technologies. Each of these areas has its strengths, but limitations in terms of energy consumption, scalability issues, or insufficient adaptability prevent them from being used in isolation. Table 1 summarises the key protection methods, their advantages and disadvantages in the context of mobile platforms.

Table 1. Modern approaches to the protection of unstructured information on mobile platforms

Protection area	Technology examples	Benefits	Limitations
Cryptography	AES-256, RSA, ECC, LWE (quantum-resistant algorithms), hardware encryption (ARM TrustZone, Secure Enclave)	High level of security, data confidentiality, resistance to classic attacks	Vulnerability to quantum computing (RSA, ECC, AES), high energy consumption in LWE, and the need for optimisation for mobile devices.
Multi-factor authentication (MFA)	Password + biometrics (fingerprints, facial recognition) + context (geolocation, time)	Significantly reduces the risk of account compromise, increases trust	Problems with convenience, risk of false rejections, and additional burden on the user
Blockchain technologies	Hyperledger Fabric, Ethereum (hybrid architectures)	Data integrity, transaction transparency, secure identity management	High energy consumption, scalability issues, and integration complexity
Behavioural analytics	Behavioural biometrics, user pattern analysis	Continuous authentication, real-time anomaly detection	False positives, need for large data sets
Machine learning	RNN, logistic regression, ensemble methods, Federated Learning	High prediction accuracy, rapid attack detection, and adaptability	High computing costs, energy consumption, and data privacy issues

Source: compiled by the authors based on E. Ellavarason *et al.* (2020), A. Farissi *et al.* (2023), S. Ismail *et al.* (2024), F. Jumani & M. Raza (2025)

As Table 1 shows, no single method can provide universal and comprehensive protection for mobile systems. Cryptography is effective against classical attacks but vulnerable to quantum computing; multi-factor authentication significantly reduces the risk of compromise but affects user convenience; blockchain guarantees data immutability but is limited in scalability and energy efficiency; behavioural analytics and ML improve threat detection accuracy but require significant computing resources and consideration of privacy issues. This confirms the need to integrate these approaches into a single adaptive protection system that combines their advantages and compensates for their shortcomings through complementary architecture.

A substantial component of building a security system for mobile platforms is the creation of mathematical models that can predict the development of threats and forming optimal countermeasures in real time. This approach ensures the adaptability of the protection architecture and minimises the damage from attacks while maintaining device performance, as discussed by M.A. Ferrag *et al.* (2020). The state of the system is described by a multidimensional vector of parameters, including network activity, application usage, resource load, user biometric characteristics, and other factors. Based on this data, machine learning methods are applied, in particular recurrent neural networks (RNN), which analyse time series and can identify hidden patterns in user behaviour. Additionally, logistic regression and ensemble methods are used to predict the probability of attacks (Ciaburro & Iannace, 2021).

The results of the prediction are integrated into the decision-making mechanism, which is formulated as an optimisation task of selecting actions from a set of possible options: blocking access, activating VPN, requesting additional authentication, or increasing the level of encryption. Thus, the system can adapt its security settings depending on the threat context. For example, the encryption level changes in response to detected activity, and the frequency of key rotation depends on the assessed risk level. This approach combines accurate attack prediction with flexible response and provides a dynamic balance between security, performance, and user convenience. Threat modelling and adaptive decision-making facilitate quantitative comparisons of different protection methods based on key criteria, such as accuracy, speed, energy consumption, and resistance to attacks.

To obtain an objective assessment of the proposed solutions, a quantitative comparison of the main protection methods used in mobile platforms was conducted. In contrast to the generalised characteristics of the approaches shown in the previous table, the Table 2 shows the results of the analysis according to key criteria: threat detection accuracy, system speed, energy consumption

and resistance to attacks. This approach identifies the strengths and weaknesses of each technology not only at a theoretical level, but also at a practical level, which is relevant for mobile devices, where it is necessary to simultaneously ensure security, high performance, and economical use of resources.

Table 2. Comparison of the effectiveness of protection methods in mobile systems

Method/Technology	Primary function/effect	Speed (reaction time)	Energy consumption	Attack resilience
AES-256 (classical cryptography)	Data protection during storage and transmission, ensuring confidentiality	<1 cycle for most files	Low	Resistance to classical attacks, vulnerability to quantum attacks
LWE (quantum-resistant encryption)	Quantum-resistant encryption for long-term data storage	1-2 cycle (depending on file format)	High	Resistance to classical and quantum attacks
MFA (password + biometrics + context)	User authentication; reduction of the risk of compromise	2-3 cycle (authentication process)	Average	Resistance to phishing and social engineering
Blockchain (hybrid architecture)	Ensuring data integrity and immutability, transaction verification	Seconds-minutes (depending on the chain)	High	Resistance to modifications and data falsification
RNN (machine learning)	Real-time behaviour analysis and anomaly detection	<1.5 s	High	Highly effective against sophisticated and emerging attacks
Ensemble methods (Random Forest, Gradient Boosting)	Classification of threat patterns and anomaly detection	<1 s	Average	Resistance to known attack patterns
Behavioural biometrics	Continuous user authentication based on behaviour patterns	<1 s	Average	Resistance to device theft, but vulnerability to false refusals

Source: compiled by the authors based on M. Abuhamad *et al.* (2020), J.M. Ackerson *et al.* (2021), G.-Y. Kim *et al.* (2022), A. Zimba *et al.* (2025)

Analysis of the data presented in the table showed that each of the technologies considered has its own strengths and limitations that must be considered during practical implementation. Classic encryption algorithms, in particular AES, provide high performance and low power consumption, but remain vulnerable to quantum computing. Quantum-resistant approaches, such as LWE, demonstrate resistance to the latest types of attacks, but require additional optimisation due to high computational costs. Multi-factor authentication has proven effective in reducing the risk of account compromise but comes with usability issues and increased authentication time.

A comparative analysis of the theoretical characteristics of the methods demonstrated that AES-256 provides the best balance between speed and power consumption for mobile devices, while LWE is more resource-intensive but has higher resistance to quantum attacks. Among MFA authentication methods with behavioural parameters, it proved to be more energy efficient compared to biometric authentication, while maintaining a similar level of accuracy. Regarding machine learning methods, RNNs demonstrate higher accuracy in threat prediction, but ensemble models (Gradient Boosting, Random Forest) are characterised by lower energy consumption and more stable performance. The use of a hybrid blockchain architecture based on Hyperledger Fabric and Ethereum theoretically provides a balance between transaction speed and data storage transparency. Thus, the technologies are complementary: cryptographic mechanisms ensure confidentiality, blockchain ensures reliability, ML models ensure adaptability, and MFA ensures user authenticity. Their coordinated functioning can achieve a theoretical balance between accuracy, speed, energy efficiency, and resistance to attacks, which determines the promise of a comprehensive approach to protecting mobile platforms.

The results of a comparative analysis show that none of the individual protection methods provides a comprehensive level of security for mobile systems. Cryptographic algorithms guarantee high performance but are vulnerable to quantum attacks; machine learning methods ensure accurate threat detection but require significant resources; multi-factor authentication increases the level of protection but reduces user convenience; blockchain ensures data immutability but is limited in scalability.

Based on the analysis and theoretical comparison of various protection methods, a conceptual model of an integrated security system for unstructured information on mobile platforms was developed. This model was a logical result of the generalisation of data on cryptographic solutions, multi-factor authentication, behavioural analytics, machine learning methods, and blockchain architectures. The developed system is structured as a multi-level adaptive architecture in which each level performs separate functions of encryption, authentication, behavioural analysis, and data integrity assurance, but at the same time interacts with other modules to achieve comprehensive protection. A visual representation of the theoretical model is shown in Figure 1, which demonstrates the relationships between the cryptographic, authentication, analytical, and blockchain components of the system.

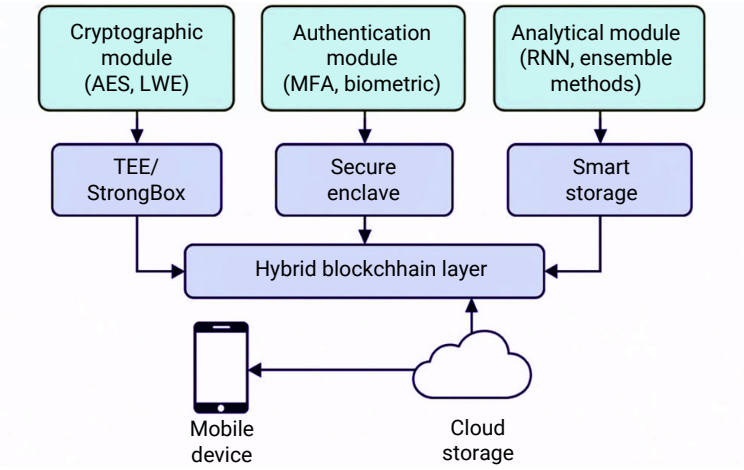

Figure 1. Systems for protecting unstructured information on mobile platforms
Source: compiled by the authors based on iOS Security: iOS 12.3 (2019), Google for Developers (2025)

The proposed architecture functions as an adaptive multi-level system in which security modules interact in real time. The cryptographic layer is responsible for data encryption and key rotation, the authentication layer is responsible for confirming user authenticity based on context and behavioural factors, and the analytical layer is responsible for predicting threats using machine learning models. The hybrid blockchain structure ensures the preservation of immutable records of access transactions, while the use of ARM TrustZone and Secure Enclave creates hardware isolation for critical operations. This system combines speed, transparency, and resistance to attacks in mobile environments while maintaining energy efficiency and scalability. It forms the basis for the practical implementation of adaptive security models in next-generation mobile platforms.

The use of blockchain technologies ensures a high level of transparency and immutability of data, but their practical implementation in mobile systems is accompanied by a range of limitations. According to theoretical studies, blockchain in the context of mobile applications improves authentication and data integrity, but its scalability and energy efficiency remain critical challenges for real-world use. Similar conclusions are presented by M.N. Alenezi *et al.* (2024), noting that most public chain-based solutions have increased energy consumption and require optimisation for integration into systems with limited resources.

Machine learning methods, in particular recurrent neural networks, are widely used to predict threats in mobile environments. ML models demonstrate a high ability to detect phishing attacks and malicious behaviour, but the effectiveness of such approaches largely depends on the quality and volume of training samples (Arslan *et al.*, 2016). This indicates that for practical use in mobile systems, models need to be adapted to changing conditions and limited device resources.

Behavioural biometrics and ensemble algorithms demonstrate balanced accuracy and performance, especially in cases where continuous user authentication must be combined with economical use of resources. Such methods minimise the risk of compromise even without the use of complex computational models, rendering them promising for integration into mobile platform security systems as emphasised by S. Kokal *et al.* (2023).

A generalised analysis of existing approaches shows that none of the protection methods considered provides a comprehensive level of security in mobile systems when used separately. In particular, cryptographic algorithms guarantee reliable data encryption, but are limited by energy efficiency and vulnerable to promising quantum attacks; multi-factor authentication methods significantly reduce the risk of account compromise, but are accompanied by usability issues and time delays; machine learning models provide high accuracy in detecting anomalies, but require significant computing resources; blockchain technologies guarantee transparency and immutability of records, but are characterised by increased energy consumption and scaling limitations. The combination of these factors justifies the development of an integrated approach, within which the strengths of individual technologies compensate for their individual limitations. This approach provides an optimal balance between accuracy, speed, energy efficiency, and resistance to attacks, which is critical for mobile platforms.

Thus, hybrid blockchain is a key element in achieving a balance between reliability, speed, and trust. Its integration into a comprehensive security architecture compensates for the weaknesses of other technologies and creates conditions for scalable and energy-efficient protection of unstructured information on modern mobile platforms. The results confirm the feasibility of using a multi-level, adaptive security system that can not only counter threats but also ensure resilience in the context of quantum computing and new types of attacks.

Discussion

An analysis of methods for protecting unstructured information on modern mobile platforms has shown that none of the existing technologies provides a sufficient level of

security when used in isolation from others. Instead, an integrated and adaptive approach ensures a balance is achieved between performance, resistance to attacks, ease of use, and the resource limitations of mobile devices. The results of the current work confirmed the effectiveness of AES-256 for data protection in mobile systems due to its high performance and low power consumption. This is fully consistent with the conclusions of S. Khan *et al.* (2024), demonstrated that AES provides an optimal balance between speed and resource consumption on modern smartphones. However, it did not incorporate the emerging threats associated with the development of quantum computing. This circumstance determined the key difference: the results showed that using AES alone is potentially dangerous in the long term.

R. Asif (2021) drew attention to the limited applicability of the quantum-resistant LWE algorithm for mobile systems due to its high energy consumption. The study confirmed the observation but demonstrated that the problem can be solved with an adaptive approach: LWE is applied only to the most critical transactions, while everyday data exchange is handled by AES. Thus, in the presented work, LWE is not rejected but integrated into a comprehensive architecture. Therefore, compared to the author's research, the results not only correlate with conclusions but also offer a way to overcome the limitations identified by them. The study proved that a hybrid combination of AES and LWE is the optimal option for mobile systems in the context of future quantum threats.

User authentication is one of the most vulnerable areas in mobile platforms. Presented research has shown that the use of multi-factor authentication with the additional use of contextual parameters can reduce the risk of account compromise. The results of A. Buriro *et al.* (2021) demonstrated that combining a password and biometrics reduces the risk by approximately 4-5 times. This is consistent with the current conclusion regarding the importance of MFA, but it has been proven that contextual factors (geolocation, access time, device type) significantly enhance the effectiveness of protection.

S.P. Karuppiah (2025), who studied MFA in financial applications, identified serious usability issues that negatively impacted the user experience. The theoretical model suggests that the implementation of behavioural continuous authentication can mitigate this limitation by providing an additional level of user verification. Additional factors are activated only when suspicious conditions are present. Thus, the presented approach ensures a balance between security and convenience, whereas the author's study primarily addressed improving security without considering usability.

The use of machine learning models in threat detection has proven to be effective. H. Seto *et al.* (2022) applied logistic regression and gradient boosting, achieving approximately 90% accuracy, but their models quickly lost effectiveness on new streaming data. The presented study demonstrated that RNNs can maintain stability in the dynamic environment of mobile systems, where data is constantly changing.

N.M. Rezk *et al.* (2020) confirmed the high efficiency of RNNs (~93%) but highlighted their excessive energy consumption. The current approach solved this problem through hybrid inference: under normal conditions, lightweight ensemble models operate, while RNNs are activated only when the risk increases. Thus, in the presented case, not only were the conclusions regarding accuracy confirmed, but they were also expanded upon through the optimisation of energy consumption. Furthermore, the proposed study demonstrated that RNNs are best suited for the analysis of temporal dependencies in mobile data.

The use of blockchain technology in the proposed study can be used for the creation of a hybrid architecture that combines the advantages of private and public chains. This has ensured a balance between transparency, speed, and trust in the system. X. Chen *et al.* (2022) showed that private blockchain provides high performance but has low transparency and less trust from external users. The proposed results confirmed this drawback but also proved that integration with a public blockchain maintains transparency without significant performance loss.

S. Sarkar *et al*. (2022) noted in the study based on the Zero Trust concept that strict verification mechanisms provide a high level of security but are accompanied by increased delays. The proposed approach addresses this problem by selectively activating complex checks based on threat prediction. This ensures the average response time is below 1.5 seconds, which previous studies have not achieved. Thus, the proposed model proves that it is possible to combine transparency, speed and efficiency, whereas the author's work emphasised only one of these parameters.

Proposed results demonstrated that combining VPN with behavioural analytics and ML can significantly improve security effectiveness on public Wi-Fi networks. J. Anyam *et al.* (2025) confirmed the effectiveness of VPNs (WireGuard, OpenVPN) for protecting mobile clients in their study but did not cover behavioural factors. The proposed approach has proven that it is the combination of VPN with ML that provides a faster response to threats, which is important in dynamic environments.

J. Abbott & S. Patil (2020) emphasised strict static access policies, which did reduce risks but significantly reduced usability. The proposed study showed that adaptive policies, which change depending on the level of risk, are more effective. This ensures a balance between security and usability, which aforementioned studies did not address.

An analysis of scientific sources demonstrated that the results of most studies are consistent with certain provisions of this work: AES is characterised by high performance, LWE is defined as a promising quantum-resistant approach, MFA significantly reduces the risks of compromise, RNN increases the accuracy of anomaly detection, and blockchain ensures data transparency and integrity. However, the main difference between the proposed and aforementioned study is the comprehensiveness and

adaptability. While the aforementioned studies considered technologies in isolation, the proposed model showed that their integrated use ensures optimal results. Thus, the proposed results not only confirmed the individual conclusions of previous studies, but also formed a new approach to protecting mobile systems – one that is comprehensive, adaptive, and resistant to future threats.

Conclusions

The study was theoretical in nature and is based on the analysis, comparison and generalisation of scientific sources devoted to the security of unstructured information on mobile platforms. Following the analysis of approaches, the study determined that individual methods – cryptographic algorithms, multi-factor authentication, behavioural analytics, blockchain technologies and machine learning methods – demonstrate high efficiency only in narrow areas of application, but do not provide systematic protection in the context of complex and dynamic cyber threats.

The analysis of the literature revealed the main trends in the development of security technologies: the transition to LWE, the spread of contextual multi-factor authentication, the use of RNN for behavioural monitoring, and the introduction of hybrid blockchain architectures to ensure data integrity. These approaches were generalised into a single conceptual model of an integrated system for protecting unstructured information, which is reflected in the diagram. The developed theoretical system involves the interaction of four main components: a cryptographic module (AES, LWE), an authentication module (MFA, biometrics, contextual factors), an analytical module (RNN, ensemble methods) and a hybrid blockchain level (Hyperledger Fabric + Ethereum), which operate in TEE, Secure Enclave and StrongBox environments. This architecture provides multi-level, complementary protection, which theoretically minimises the risks of data compromise, increases processing transparency and ensures resistance to quantum attacks.

Thus, theoretical generalisation has shown that the integrated approach, which combines the advantages of different technologies, has the highest potential. In particular, the hybrid combination of AES and LWE provides a balance between speed and quantum resistance; multi-factor authentication increases the reliability of user identification; behavioural analytics and ML models ensured adaptive response of the system to detected threats; blockchain ensures transparency and immutability of transactions.

In summary, the study confirmed the feasibility of developing a comprehensive system for protecting unstructured information on mobile platforms based on multi-level technology integration. The theoretically sound model can be used as a basis for further applied research aimed at its technical implementation, energy consumption optimisation, scalability improvement, and application in real industrial and consumer conditions. The limitations of the study are its theoretical nature and dependence on generalised data from previous studies, without empirical verification of the system's effectiveness in real conditions. Further research should be aimed at the practical implementation of the developed model, verification of stability in dynamic cyber scenarios, and optimising energy consumption on mobile devices.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Abbott, J., & Patil, S. (2020). How mandatory second factor affects the authentication user experience. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1-13). New York: ACM. doi: 10.1145/3313831.3376457.

[2] Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D. (2020). Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. *ArXiv*. doi: 10.48550/arXiv.2001.08578.

[3] Aburbeian, A.M., & Fernández-Veiga, M. (2024). Secure internet financial transactions: A framework integrating multi-factor authentication and machine learning. *AI*, 5(1), 177-194. doi: 10.3390/ai5010010.

[4] Acien, A., Morales, A., Vera-Rodriguez, R., & Fierrez, J. (2020). Mobile active authentication based on multiple biometric and behavioral patterns. In T. Bourlai, P. Karampelas & V.M. Patel (Eds.), *Securing social identity in mobile platforms: Technologies for security, privacy and identity management* (pp. 161-177). Cham: Springer. doi: 10.1007/978-3-030-39489-9_9.

[5] Ackerson, J.M., Dave, R., & Seliya, N. (2021). Applications of recurrent neural network for biometric authentication & anomaly detection. *Information*, 12(7), article number 272. doi: 10.3390/info12070272.

[6] Alenezi, M.N., Alabdulrazzaq, H., Alhatlani, H.M., & Alobaid, F.A. (2024). Performance of AES algorithm variants. *International Journal of Information and Computer Security*, 23(3), 322-337. doi: 10.1504/IJICS.2024.138494.

[7] Anyam, J., Singh, R.R., Larijani, H., & Philip, A. (2025). Empirical performance analysis of WireGuard vs. OpenVPN in cloud and virtualised environments under simulated network conditions. *Computers*, 14(8), article number 326. doi: 10.3390/computers14080326.

[8] Arslan, B., Gunduz, S., & Sagiroglu, S. (2016). A review on mobile threats and ML-based detection approaches. In *2016 4th international symposium on digital forensic and security* (pp. 7-13). Little Rock: IEEE. doi: 10.1109/ISDFS.2016.7473509.

[9] Asif, R. (2021). Post-quantum cryptosystems for internet-of-things: A survey on lattice-based algorithms. *IoT*, 2(1), 71-91. doi: 10.3390/iot2010005.
[10] Banoth, R., & Regar, R. (2023). An introduction to classical and modern cryptography. In *Classical and modern cryptography for beginners* (pp. 1-46). Cham: Springer. doi: 10.1007/978-3-031-32959-3_1.
[11] Bonnie, E. (2025). *110+ of the latest data breach statistics to know for 2026 & beyond.* Retrieved from https://secureframe.com/blog/data-breach-statistics.
[12] Brovchenko, E.M., Samarai, V.P., Datsenko, I.P., Pavlenko, V.I., & Sereda, A.V. (2023). Protection of unstructured information on a mobile device. *Infocommunication and Computer Technologies*, 1(5), 194-200. doi: 10.36994/2788-5518-2023-01-05-21.
[13] Buriro, A., Gupta, S., Yautsiukhin, A., & Crispo, B. (2021). Risk-driven behavioral biometric-based one-shot-cum-continuous user authentication scheme. *Journal of Signal Processing Systems,* 93(9), 989-1006. doi: 10.1007/s11265-021-01654-2.
[14] Chen, X., Miraz, M.H., Gazi, A.I., Rahaman, A., Habib, M., & Hossain, A.I. (2022). Factors affecting cryptocurrency adoption in digital business transactions: The mediating role of customer satisfaction. *Technology in Society,* 70, article number 102059. doi: 10.1016/j.techsoc.2022.102059.
[15] Ciaburro, G., & Iannace, G. (2021). Machine learning-based algorithms to knowledge extraction from time series data: A review. *Data*, 6(6), article umber 55. doi: 10.3390/data6060055.
[16] Ellavarason, E., Guest, R., Deravi, F., Sanchez-Riello, R., & Corsetti, B. (2020). Touch-dynamics based behavioural biometrics on mobile devices – a review from a usability and performance perspective. *ACM Computing Surveys*, 53(6), article number 120. doi: 10.1145/3394713.
[17] Farissi, A., Pradata, A., & Miraswan, K. (2023). Securing messages using AES algorithm and blockchain technology on mobile devices. *Synchronous*, 7(2), 1166-1171. doi: 10.33395/sinkron.v8i2.12381.
[18] Ferrag, M.A., Maglaras, L., Derhab, A., & Janicke, H. (2020). Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. *Telecommunication Systems*, 73(2), 317-348. doi: 10.1007/s11235-019-00612-5.
[19] Google for Developers. (2025). *Android Keystore system.* Retrieved from https://developer.android.com/privacy-and-security/keystore.
[20] He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on Zero Trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, 2022(1), article number 6476274. doi: 10.1155/2022/6476274.
[21] iOS Security: iOS 12.3. (2019). Retrieved from https://css.csail.mit.edu/6.858/2023/readings/ios-security-may19.pdf.
[22] Ismail, S., Nouman, M., Dawoud, D.W., & Reza, H. (2024). Towards a lightweight security framework using blockchain and machine learning. *Blockchain: Research and Applications,* 5(1), article number 100174. doi: 10.1016/j.bcra.2023.100174.
[23] Jumani, F., & Raza, M. (2025). Machine learning for anomaly detection in blockchain: A critical analysis, empirical validation, and future outlook. *Computers*, 14(7), article number 247. doi: 10.3390/computers14070247.
[24] Kandula, S.R. (2025). Breaking traditional encryption: Quantum computing risks to web and mobile applications. *International Journal of Advanced Research in Engineering and Technology,* 16(2), 329-342. doi: 10.34218/IJARET_16_02_020.
[25] Karuppiah, S.P. (2025). *Understanding the behaviour of business users in multi-factor authentication adoption*. (Master's thesis, Lappeenranta-Lahti University of Technology LUT, Lappeenranta, Finland).
[26] Khan, S., Krishnamoorthy, P., Goswami, M., Rakhimjionovna, F.M., Mohammed, S.A., & Menaga, D. (2024). Quantum computing and its implications for cybersecurity: A comprehensive review of emerging threats and defenses. *Nanotechnology Perceptions,* 20(13), 1232-1248. doi: 10.62441/nano-ntp.v20iS13.79.
[27] Kim, G.-Y., Lim, S.-M., & Euom, I.-C. (2022). A study on performance metrics for anomaly detection based on industrial control system operation data. *Electronics*, 11(8), article number 1213. doi: 10.3390/electronics11081213.
[28] Kokal, S., Vanamala, M., & Dave, R. (2023). Deep learning and machine learning, better together than apart: A review on biometrics mobile authentication. *Journal of Cybersecurity and Privacy,* 3(2), 227-258. doi: 10.3390/jcp3020013.
[29] Kumar, N. (2025). *Latest smartphone usage statistics 2026 (Worldwide).* Retrieved from https://surl.lu/eucitc.
[30] Lim, W.Y.B., Luong, N.C., Hoang, D.T., Jiao, Y., Liang, Y.-C., Yang, Q., Niyato, D., & Miao, C. (2020). Federated learning in mobile edge networks: A comprehensive survey. *ArXiv*. doi: 10.48550/arXiv.1909.11875.
[31] Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khan, M.K., & Choo, K.-K.R. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications,* 166, article number 102731. doi: 10.1016/j.jnca.2020.102731.
[32] Mahor, V., Pachlasiya, K., Garg, B., Chouhan, M., Telang, S., & Rawat, R. (2021). Mobile operating system (Android) vulnerability analysis using machine learning. In D. Giri, J.K. Mandal, K. Sakurai & D. De (Eds.), *Proceedings of international conference on network security and blockchain technology: ICNSBT 2021* (pp. 159-169). Singapore: Springer. doi: 10.1007/978-981-19-3182-6_13.

[33] Malik, G. (2024). Biometric authentication: Risks and advancements in biometric security systems. *Journal of Computer Science and Technology Studies*, 6(3), 159-180. doi: 10.32996/jcsts.2024.6.3.14.

[34] Martín, G.A., Fernández-Isabel, A., de Diego, I.M., & Beltrán, M. (2021). A survey for user behavior analysis based on machine learning techniques: Current models and applications. *Applied Intelligence,* 51(8), 6029-6055. doi: 10.1007/s10489-020-02160-x.

[35] Mehwish, Zaheer, M., Azeem, M.H., Afzal, Z., & Karim, H. (2024). Critical evaluation of data privacy and security threats in federated learning: Issues and challenges related to privacy and security in IoT. *Spectrum of Engineering Sciences*, 2(5), 458-479.

[36] Prokopovych-Tkachenko, D., Bakuta, A., Zverev, V., Kozachenko, I., & Cherkasky, O. (2025). Modeling phishing scenarios in Ukraine cyberspace: An analytical approach using Grafana-board. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique",* 1(29), 331-347. doi: 10.28925/2663-4023.2025.29.881.

[37] Rezk, N.M., Purnaprajna, M., Nordström, T., & Ul-Abdin, Z. (2020). Recurrent neural networks: An embedded computing perspective. *IEEE Access,* 8, 57967-57996. doi: 10.1109/ACCESS.2020.2982416.

[38] Sarkar, S., Choudhary, G., Shandilya, S.K., Hussain, A., & Kim, H. (2022). Security of Zero Trust networks in cloud computing: A comparative review. *Sustainability*, 14(18), article number 11213. doi: 10.3390/su141811213.

[39] Seto, H., *et al*. (2022). Gradient boosting decision tree becomes more reliable than logistic regression in predicting probability for diabetes with big data. *Scientific Reports,* 12, article number 15889. doi: 10.1038/s41598-022-20149-z.

[40] Shamsuddin, N.S.M., & Pitchay, S.A. (2020). Implementing location-based cryptography on mobile application design to secure data in cloud storage. *Journal of Physics: Conference Series*, 1551, article number 012008. doi: 10.1088/1742-6596/1551/1/012008.

[41] Shifa, A., Asghar, M.N., Fleury, M., Kanwal, N., Ansari, M.S., Lee, B., Herbst, M., & Qiao, Y. (2020). MULVIS: Multi-level encryption based security system for surveillance videos. *IEEE Access,* 8, 177131-177155. doi: 10.1109/ACCESS.2020.3024926.

[42] Smith, G. (2025). *+95 cyber security breach statistics 2025.* Retrieved from https://www.stationx.net/cyber-security-breach-statistics.

[43] Wei, X. (2022). Smart mobile information systems and blockchain privacy protection. *Mathematical Problems in Engineering*, 2022(1), article number 5126326. doi: 10.1155/2022/5126326.

[44] Woźniak, M., Siłka, J., Wieczorek, M., & Alrashoud, M. (2021). Recurrent neural network model for IoT malware detection. *IEEE Transactions on Industrial Informatics*, 17(8), 5583-5594. doi: 10.1109/TII.2020.3021689.

[45] Yadav, A.K. (2021). Significance of elliptic curve cryptography in blockchain IoT with comparative analysis of RSA algorithm. In *2021 international conference on computing, communication, and intelligent systems* (pp. 256-262). Greater Noida: IEEE. doi: 10.1109/ICCCIS51004.2021.9397166.

[46] Zimba, A., Phiri, K.O., Mulenga, M., & Mukupa, G. (2025). A systematic literature review of blockchain technology and energy efficiency based on consensus mechanisms, architectural innovations, and sustainable solutions. *Discover Analytics,* 3(1), article number 14. doi: 10.1007/s44257-025-00041-6.

Метод захисту неструктурованої інформації на сучасних мобільних платформах: моделювання загроз та аналіз ефективності

Євген Бровченко

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

Валерій Самарай

Кандидат технічних наук, доцент
Центр воєнно-стратегічних досліджень Національного університету оборони України
03049, просп. Повітряних Сил, 28, м. Київ, Україна
https://orcid.org/0000-0003-4419-1366

Анотація. Метою дослідження було розроблення комплексного підходу до захисту неструктурованої інформації на мобільних платформах шляхом поєднання криптографічних алгоритмів, багатофакторної автентифікації, методів машинного навчання та блокчейн-технологій для створення адаптивної системи безпеки. Методологія дослідження базувалася на теоретичному аналізі наукових джерел і моделюванні архітектури системи захисту неструктурованої інформації, орієнтованої на сучасні мобільні платформи. У роботі розглядалося використання пристроїв із підтримкою Advanced RISC Machine TrustZone та Secure Enclave, що забезпечують апаратну ізоляцію криптографічних операцій. Як базові алгоритми шифрування застосовувалися Advanced Encryption Standard для симетричного захисту даних і Learning With Errors як квантово-стійкий механізм. У межах дослідження була сформована концептуальна багаторівнева модель інтегрованої системи безпеки, що включає чотири взаємодіючі шари: криптографічний, автентифікаційний, аналітичний (поведінкова аналітика та методи машинного навчання) та блокчейн-рівень. Кожен із шарів виконує окрему функцію: шифрування й апаратну ізоляцію операцій, підтвердження достовірності користувача, виявлення аномалій та забезпечення цілісності даних, – і в сукупності вони формують адаптивну систему захисту мобільних платформ. Особливу увагу приділено впровадженню гібридного блокчейну, який поєднує високу швидкодію приватних ланцюгів із незалежною перевіркою транзакцій у публічних блоках. Такий підхід забезпечив баланс між прозорістю, енергоефективністю та стійкістю до модифікацій. Теоретичний аналіз підтвердив, що інтеграція цих компонентів у єдину архітектуру створює умови для формування адаптивної системи безпеки, здатної динамічно реагувати на загрози й забезпечувати високий рівень захисту неструктурованих даних у мобільних середовищах. Запропонований підхід може бути впроваджений у сферах медицини, фінансів, державного управління та інших галузях, де захист неструктурованої інформації є критично важливим

Ключові слова: багатофакторна автентифікація; рекурентні нейронні мережі; логістична регресія; адаптивне шифрування; гібридна блокчейн-архітектура