The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 166-172
DOI 10.37547/tajet/Volume07Issue04-22

Check for updates

Information Security Challenges in Mobile Gaming Applications

Maksim Zakopailov

CEO at uniQore LLC Orlando, FL, USA

OPEN ACCESS

SUBMITTED 24 February 2025
ACCEPTED 19 March 2025
PUBLISHED 30 April 2025
VOLUME Vol.07 Issue 04 2025

CITATION

Maksim Zakopailov. (2025). Information Security Challenges in Mobile Gaming Applications. The American Journal of Engineering and Technology, 7(04), 166–172. https://doi.org/10.37547/tajet/Volume07Issue04-22

Abstract: This article addresses the issues related to ensuring information security in mobile gaming applications. The rapid growth of this sector is accompanied by a surge in cyber threats, primarily targeting user data compromise, scenario manipulation, and unauthorized access to application functionality. The technical complexity of such systems—particularly those interacting with cloud and edge computing infrastructures—has given rise to a range of new vulnerabilities that fall outside the scope of traditional security measures. The aim of this study is to identify and systematize the problem areas in securing mobile games, particularly at the intersection of network architecture, user behavior, and cryptographic solutions. A review of the academic literature reveals a disconnect: while individual aspects such as authentication and encryption are explored in depth, architectural and behavioral risks are often treated superficially. This work categorizes the key threats and emphasizes how poor coordination between application design, technical implementation, and user practices creates a vulnerable environment—especially in the context of widespread use of third-party SDKs and monetization systems. The article presents indicative performance estimates for encryption and authentication mechanisms to provide an initial assessment of their applicability. The author's contribution lies in integrating interdisciplinary approaches to analyzing the security of mobile gaming solutions and highlighting areas that remain underexplored in the current literature. The material will be of interest to cybersecurity specialists, developers, digital communication researchers, and interface designers.

Keywords: authentication, gamification, information security, mobile gaming applications, network threats, encryption.

Introduction: Modern mobile applications, particularly in the gaming sector, are complex software systems that combine interactivity, multimedia technologies, and network integration. As the popularity of mobile games continues to rise, so does the scale of threats related to information security. The central challenge lies in designing effective protection measures that can safeguard user data and ensure the integrity of software solutions—without compromising gameplay quality or the overall user experience.

Against this backdrop, the focus of research shifts toward identifying key vectors of cyber threats, patterns in the exploitation of vulnerabilities, and contemporary approaches to implementing security mechanisms within mobile gaming applications. Recognizing the critical importance of cybersecurity is essential, especially given that many users still rely on the same passwords across platforms or choose easily guessable phrases. Human error remains a leading cause of data breaches, often due to a lack of awareness regarding necessary protective measures.

Therefore, there is a pressing need to strengthen cybersecurity efforts in the mobile gaming domain. Both developers and users must adopt more robust security practices to mitigate risks and protect sensitive information.

MATERIALS AND METHODS

The topic of information security in mobile gaming applications is receiving increasingly comprehensive attention in the academic literature. Research efforts are primarily concentrated in three interrelated areas: the protection of data transmission channels, authentication methods, and the management of user behavior in the context of system vulnerabilities.

With regard to network traffic security on mobile devices, the work by A. Agrawal et al. [1] offers a detailed overview of relevant methods, including behavioral and statistical approaches, as well as the use of machine learning. Another key research focus is authentication mechanisms, as emphasized by T. M. Hoang and colleagues [4], who examine a two-factor authentication framework integrated into intelligent management systems, highlighting the typology of related vulnerabilities. Similar issues are explored by A. G. Usman and A. M. A. Noor [9], who systematize identification methods based on biometrics, passwords, and behavioral patterns, while C. Wang et al. [10] focus on the evolution of threats and current trends, with particular attention to side-channel attacks and biometric spoofing risks.

Some studies address the interaction between mobile app architectures and elements of telecommunications infrastructure. H. Luo and H. Yu. Wei [6] highlight the orchestration of resources in edge networks, showing how properly configured distributed computing at the network edge can enhance the security of user sessions and reduce the risk of data interception.

Other publications explore the security of mobile games within more specific behavioral and commercial contexts. J. Bae et al. [2] analyze recommendation systems based on non-parametric models and highlight the risks of unauthorized data collection in user profiling. In a similar vein, D. Bank [3] raises the issue of ethical vulnerabilities arising from aggressive monetization practices, which may manipulate player decisions—especially among minors.

From the perspective of mobile game architecture design, G. Rasool and co-authors [8] advocate for structural frameworks resilient to cyber threats, while I. Mulyawan and W. Rafdinal [7] examine decision-making mechanisms in game installation, linking trust in app security to design transparency and user perception.

As a statistical backdrop, the report by S. M. Kerner [5] provides up-to-date data on cyber threats, including those relevant to the mobile sector, allowing for a quantitative assessment of the scale of the problem.

Overall, the literature demonstrates a wide array of methodological approaches—from formal modeling and traffic analysis to behavioral analytics and ethical reflection. However, several inconsistencies emerge. On one hand, there is a notable imbalance in the attention given to different threat layers: technical issues—particularly encryption and authentication—are explored in much greater depth than the secondary use of user data and risks embedded in game architecture. On the other hand, attacks through third-party advertising SDKs integrated into games, as well as threats stemming from the compromise of game servers as part of the broader ecosystem, remain underexplored.

There is also a noticeable gap in research focused on the synergy between UX design and security mechanisms, and the literature lacks a well-grounded typology of threats specific to gamified interfaces.

The methods used in this study include comparative analysis, systematization, synthesis, statistical data

processing, and generalization.

RESULTS AND DISCUSSION

Information security in mobile gaming applications involves the comprehensive protection of user data, maintaining the integrity of gameplay, and preventing unauthorized access to system functionalities and resources. This is achieved through modern cryptographic techniques, multi-factor authentication, anomaly detection, and the development of secure architectures—all of which serve as effective responses to a wide range of cyber threats and attacks [2, 6, 7]. The threat taxonomy is presented in the diagram below (Fig. 1).

Fig. 1. Systematization of information security threats in mobile gaming applications (compiled by the author based on [1–3, 6, 9])

One of the most critical threats is unauthorized access to user information. Both personal data and in-game activity—such as achievements or in-app currency transactions—are at risk. Flaws in authentication mechanisms, insufficient data segmentation, and weak encryption protocols significantly increase the likelihood of exploitation by malicious actors.

According to Verizon's 2024 report, human error remains the most common threat vector, accounting for 68% of all data breaches, even when not driven by malicious intent [5].

Most mobile games rely on server-side logic for process synchronization and event verification. Any breach in

reward distribution algorithms, event forgery, or manipulation of server code can result not only in financial losses for developers but also in diminished user trust. Code injection and control flow manipulation by attackers necessitate the development of specialized anti-tampering methods.

Server infrastructures can also be deliberately overwhelmed via DDoS attacks, leading to service outages and disruption of gameplay. Case analyses show that even high-capacity data centers can be compromised if protective measures are not regularly updated to reflect emerging threats. Effective detection of such attacks requires a combination of real-time traffic monitoring and behavioral anomaly analysis.

Netscout reports that in the first half of 2024, nearly 8 million DDoS attacks were recorded—an increase of 13% over the previous six months. The peak observed throughput reached 960 Gbps [5].

Contemporary mobile games often integrate third-party solutions for graphics rendering, analytics, and monetization. Vulnerabilities in external libraries can be exploited to propagate attacks through otherwise isolated modules. This opens the door for attackers to take advantage of undocumented functions or flaws in data processing algorithms, emphasizing the need for regular audits of integrated software and strict vendor management.

The volume of mobile malware is on the rise. According to Kaspersky Lab, its products blocked 6.7 million mobile attacks in Q3 2024 alone [5].

Attention should also be paid to platform-specific constraints and threat vectors. Limitations in memory, energy efficiency, and computing power necessitate the development of optimized encryption and authentication algorithms. While complex cryptographic solutions offer robust protection, they can significantly degrade app performance, pushing developers to seek a balance between security and user experience.

Platform fragmentation, particularly in Android ecosystems, complicates the implementation of universal standards. Variability in OS versions, the prevalence of customized builds, and limited update cycles create fertile ground for exploit-based attacks. In contrast, iOS employs a more centralized update policy, yet vulnerabilities in system software still persist and are actively exploited.

Lastly, user behavior remains a key factor. Levels of digital literacy among mobile gamers vary significantly, leading to inconsistent risk perception and vulnerability to phishing. Security engineers must consider not only technological vectors but also psychological factors—including users' tendency to reuse weak passwords, ignore two-factor authentication, and lack awareness of modern threats.

The next section introduces the current security methods and their implementation in mobile gaming, summarized in the diagram below (Fig. 2).

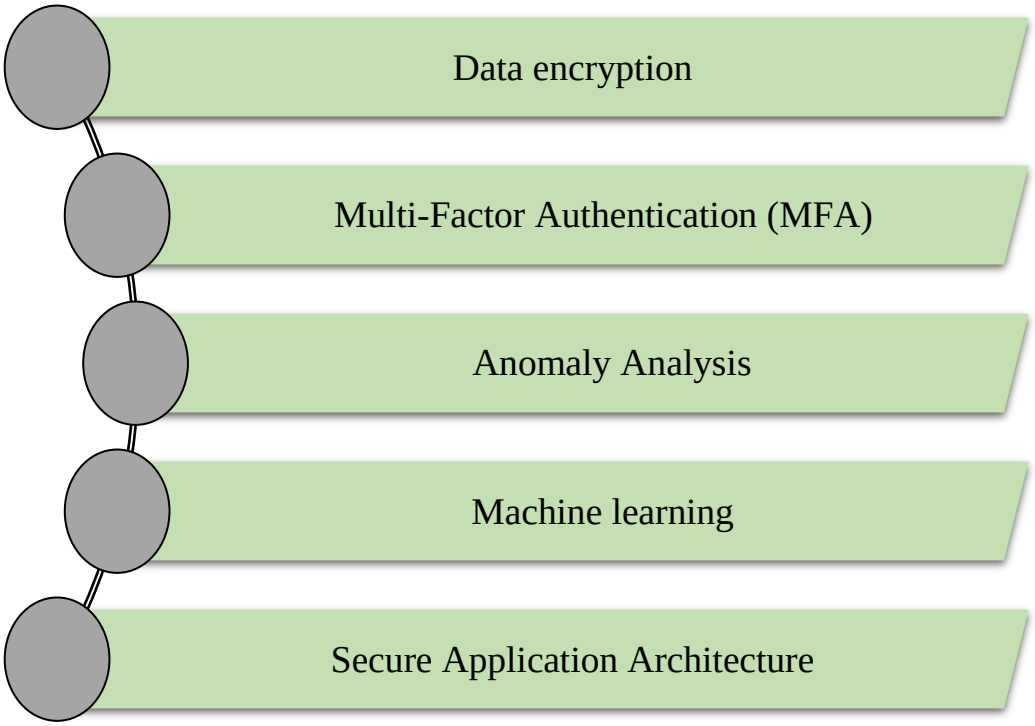

Fig. 2. Modern security methods used to enhance information security in mobile gaming applications (compiled by the author based on [2–4, 7, 8, 10])

To ensure effective protection in mobile gaming applications, both symmetric and asymmetric encryption algorithms should be used, specifically those optimized for environments with limited computational resources. Implementing TLS protocols and algorithms with short processing times helps minimize latency in client-server data transmission. In practice, hybrid solutions are recommended—combining the speed of symmetric encryption with the resilience of asymmetric methods.

Consider a hypothetical example. Suppose a mobile game uses the AES-128 symmetric encryption algorithm to secure transmitted data. On typical mobile devices, the encryption speed is around 1 MB/s. If a single data packet is 10 KB, the encryption time can be calculated as follows:

Packet size: 10 KB = 0.01 MB

Encryption time: T = 0.01 MB / 1 MB/s = 0.01 s, or 10 milliseconds

Thus, the delay introduced by encrypting one data packet is approximately 10 milliseconds—an acceptable figure for maintaining a smooth gaming experience. This calculation illustrates how the thoughtful selection of algorithms and code optimization can significantly reduce the performance impact of cryptographic protection in mobile applications.

Introducing multi-factor authentication greatly complicates unauthorized access to user accounts. The use of biometric data, SMS codes, and hardware keys increases security, though it also requires integration with external services and consideration of their latency. To optimize user experience, modern systems employ adaptive authentication, where the verification mechanism is selected dynamically based on risk assessment.

Here's another example. Assume that the login process involves two-factor authentication: after entering a password, the server sends a one-time code via SMS. If password processing takes 150 ms, SMS delivery 200 ms, and server-side code verification 100 ms, the total time is:

Password processing: 150 ms

SMS transmission: 200 ms

Code verification: 100 ms

Total time = 150 ms + 200 ms + 100 ms = 450 ms

This demonstrates the importance of optimizing each step to maintain a responsive user experience without compromising security.

Machine learning algorithms offer new opportunities for detecting suspicious activity by analyzing network traffic and user behavior. Trained models can identify subtle patterns that traditional monitoring systems might miss. Clustering techniques, in particular, enable prompt responses to unusual behavioral shifts, helping to prevent potential incidents.

When designing a secure architecture for mobile games, it is critical to apply principles such as segmentation, least-privilege access, and containerization for isolating critical components. The use of microservices supports functional modularization, facilitating scalability and reducing the risk of widespread compromise through a single vulnerable element.

The development prospects and emerging challenges in the field of information security are summarized in the diagram below (Fig. 3).

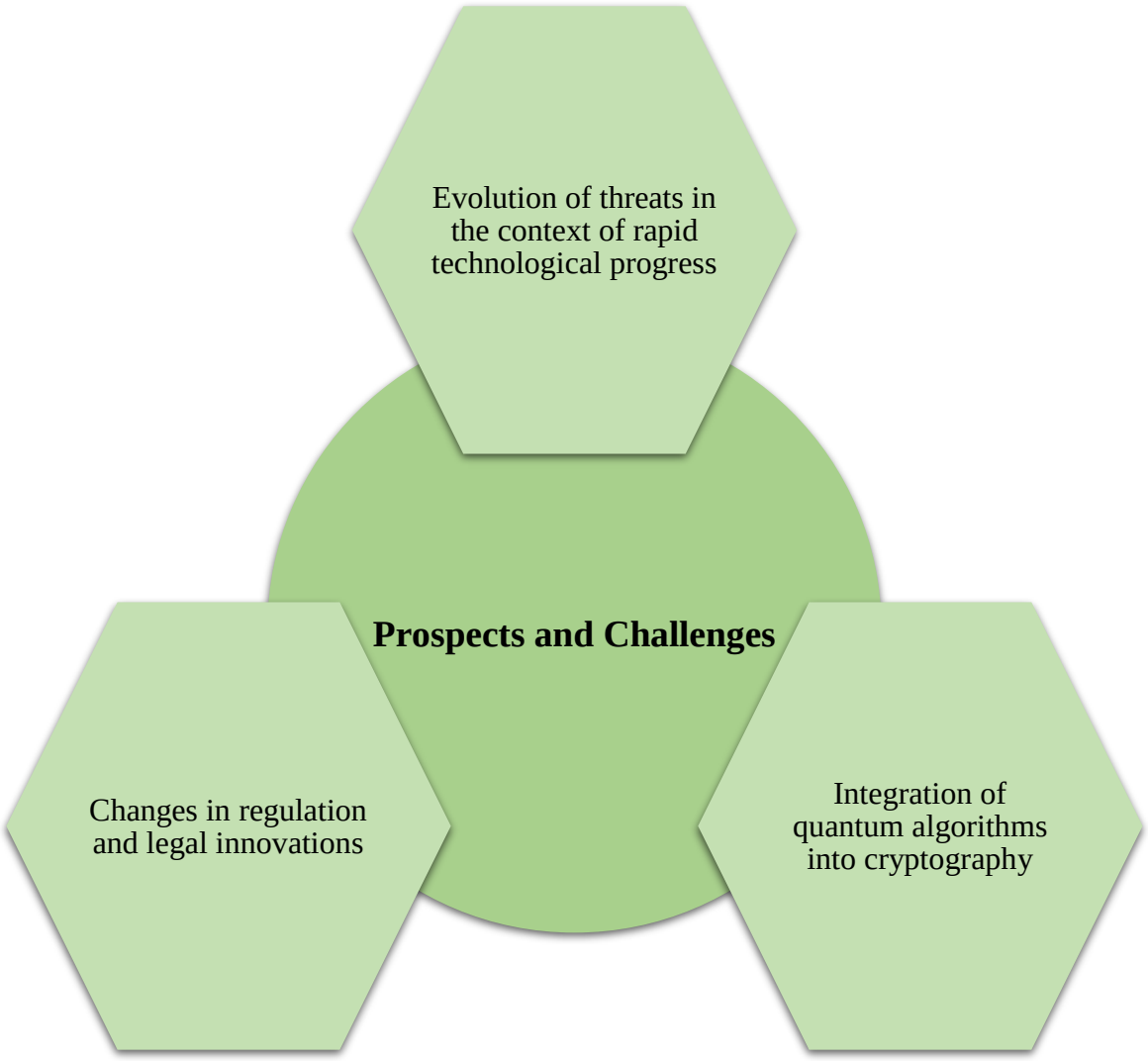

Fig. 3. Development of the information security sphere: prospects and challenges (compiled by the author on the basis of [2, 6, 9])

The diagram reflects the ongoing evolution of cyber threats facing mobile gaming systems—threats that continuously adapt and transform alongside technological advancements. Emerging attack strategies, including the use of artificial intelligence to automate vulnerability discovery, require security professionals to regularly update their knowledge and

protective toolkits. Looking ahead, it is essential to conduct systematic research focused on identifying system weaknesses and developing methods to address them.

In this context, the transition toward quantum-resistant encryption algorithms is seen as a promising direction for the mobile industry.

The evolution of information security regulations further highlights the need for developers to ensure strict compliance with legal frameworks. Security challenges in mobile games increasingly intersect with personal data protection concerns, obliging developers to conduct regular audits and modify systems in accordance with international standards. In the future, engagement with regulatory authorities will become an integral component of development strategy.

CONCLUSIONS

Information security issues in mobile gaming applications constitute a multifaceted domain that demands a comprehensive research approach and continuous technological innovation. Today's threats—including data breaches, manipulation of game logic, and targeted attacks on server infrastructure—illustrate the scale and complexity of the challenges developers must address. The use of advanced cryptographic techniques, multi-factor authentication, anomaly detection, and secure architecture design significantly contributes to strengthening protection in this domain.

The findings suggest that achieving sustainable security requires not only technically sound implementation of individual components but also systematic monitoring, regular security audits, and active collaboration with experts across disciplines. Such an integrated approach enables adaptation to evolving threat landscapes and provides defense against attacks at both local and global levels.

In conclusion, research on information security in mobile gaming applications remains a critical priority within the broader cybersecurity field. The development of effective defense mechanisms, along with the ongoing refinement of existing solutions, is fundamental to maintaining user trust and supporting the long-term growth of the industry.

REFERENCES

Agrawal A. A survey on analyzing encrypted network traffic of mobile devices / A. Agrawal, A. Bhatia, A. Bahuguna, K. Tiwari, K. Haribabu, D. Vishwakarma, R. Kaushik // International Journal of Information Security. – 2022. – Vol. 21. – No. 4. – Pp. 873-915.

Bae J. A recommending system for mobile games using the dynamic nonparametric model / J. Bae, J. Park, J. Choi, Soh S. Bum // Journal of Business Research. – 2023. – Vol. 167.

Bank D. Problematic monetization in mobile games in the context of the human right to economic self-determination / D. Bank // Computers in Human Behavior. – 2023. – Vol. 149.

Hoang T.M. An integrated two-factor authentication scheme for smart communications and control systems / T.M. Hoang, V.H. Bui, N.H. Nguyen // Mendel. – 2023. – Vol. 29. – No. 2. – Pp. 181-190.

Kerner S.M. 35 cybersecurity statistics to lose sleep over in 2025 / S.M. Kerner // URL: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020 (date of request: 04/14/2025).

Luo H. Resource orchestration at the edge: intelligent management of MMWAVE ran and gaming application QOE enhancement / H. Luo, H.Yu.Wei // IEEE Transactions on Network and Service Management. – 2023. – Vol. 20. – No. 1. – Pp. 385-399.

Mulyawan I. Mobile games adoption: an extension of technology acceptance model and theory of reasoned action / I. Mulyawan, W. Rafdinal // IOP Conference Series: Materials Science and Engineering. – 2021. – Vol. 1098. – No. 3.

Rasool G. Design patterns for mobile games based on structural similarity / G. Rasool, Ya. Hussain, T. Umer, Ja. Rasheed, S.F. Yeo, F. Sahin // Applied Sciences (Switzerland). – 2023. – Vol. 13. – No. 2. – P. 1198.

Usman A.G. Review on user authentication on mobile devices / A.G. Usman, A.M.A. Noor // Journal of Advanced Research in Applied Sciences and Engineering Technology. – 2024. – Vol. 46. – No. 2. – Pp. 26-36.

Wang C. User authentication on mobile devices: approaches, threats and trends / C. Wang, Y. Chen, J. Liu, Y. Wang, H. Liu // Computer Networks. – 2020. – Vol. 170. – Pp. 107-118.