

DETECTING ATTACKS ON MOBILE PLATFORMS USING ARTIFICIAL INTELLIGENCE: A CYBER BROTHER APPROACH

¹Abbaz Primbetov, ²Xusniddin Xamidov, ³Kamron Mamedov, ⁴Muhammadillo Xakimov

¹*Senior Lecturer, Computer Engineering Department, Tashkent University of Applied Sciences*

^{2,3,4}*Students of Information Security, Tashkent University of Applied Sciences*

abbaz0203@mail.ru, husniddinhamidov@hotmail.com, mamedovkamron2002@gmail.com,
dilloxabib@gmail.com

Abstract

The rapid expansion of mobile ecosystems has significantly increased the attack surface for cyber threats. This paper explores the application of Artificial Intelligence (AI) techniques in detecting and mitigating cyberattacks on mobile platforms. As a case study, the Cyber Brother mobile security system is analyzed, focusing on its ability to detect malicious APK files and phishing URLs in real time. The system utilizes on-device machine learning models to ensure privacy-preserving and offline threat detection. Experimental observations indicate that AI-driven approaches outperform traditional signature-based methods, especially in identifying zero-day attacks. The study highlights the effectiveness, limitations, and future potential of AI-based mobile cybersecurity solutions.

Keywords: Artificial Intelligence, Mobile Security, Cybersecurity, APK Analysis, URL Detection, Malware, On-device AI, Cyber Brother

Introduction

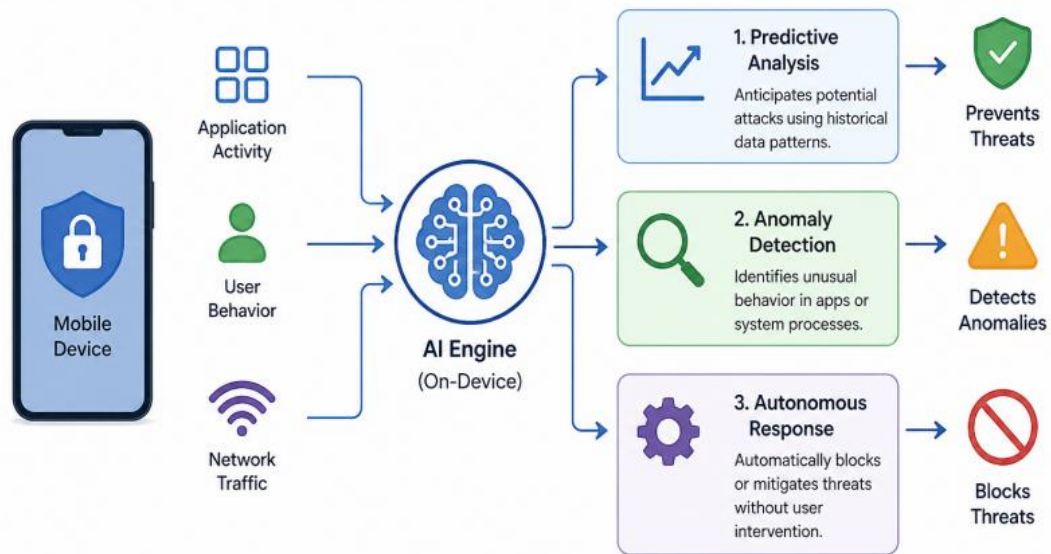
In the era of rapid digital transformation, mobile devices have evolved into critical platforms for communication, financial transactions, and access to sensitive personal data. Consequently, they have become prime targets for increasingly sophisticated cyberattacks. Modern threats, including malicious applications (APKs), phishing URLs, and AI-generated scams, have significantly surpassed the detection capabilities of traditional security mechanisms.

Conventional antivirus solutions primarily rely on signature-based detection methods, which are ineffective against polymorphic malware and zero-day vulnerabilities. As cyber threats continue to evolve in complexity and scale, the integration of Artificial Intelligence (AI) into mobile security systems has become not only beneficial but essential.

The Cyber Brother project addresses this challenge by introducing an intelligent, on-device cybersecurity system specifically designed for Android platforms. By combining behavioral analysis, machine learning, and real-time monitoring, the system is capable of detecting both known and previously unseen threats without relying on cloud-based infrastructure, thereby enhancing user privacy and response speed.

Role of Artificial Intelligence in Mobile Cybersecurity

Role of Artificial Intelligence in Mobile Cybersecurity



Artificial Intelligence (AI) has significantly transformed the field of cybersecurity by enabling systems to process large volumes of data and detect anomalies in real time. Machine learning models are capable of identifying complex patterns in user behavior, application activity, and network traffic, which are often difficult to detect using traditional methods.

In mobile environments, AI contributes in three primary ways. First, **predictive analysis** allows systems to anticipate potential cyberattacks by analyzing historical data and identifying emerging patterns. Second, **anomaly detection** enables the identification of unusual or suspicious behavior within applications or system processes. Third, **autonomous response mechanisms** allow systems to automatically react to detected threats, such as blocking malicious activity or restricting access, without requiring human intervention.

Unlike conventional signature-based approaches, AI-driven systems are capable of detecting previously unseen threats, including zero-day attacks. This ability makes AI particularly valuable in dynamic and rapidly evolving mobile threat environments, where new attack techniques continuously emerge. Furthermore, AI enhances the adaptability and scalability of cybersecurity systems, allowing them to improve over time as they are exposed to new data and threat patterns.

Cyber Brother System Architecture

Cyber Brother is a modular mobile security platform designed to operate efficiently within device constraints. Its architecture consists of several integrated components:

- a) Warning interface displayed during APK installation when a potential malicious application is detected.
- b) Application scanning module analyzing installed apps for potential security threats.

c) Real-time alert triggered when a verification code is received during a phone call, indicating a potential social engineering attack.

d)

d) Settings interface allowing users to configure security preferences and system behavior.

e)

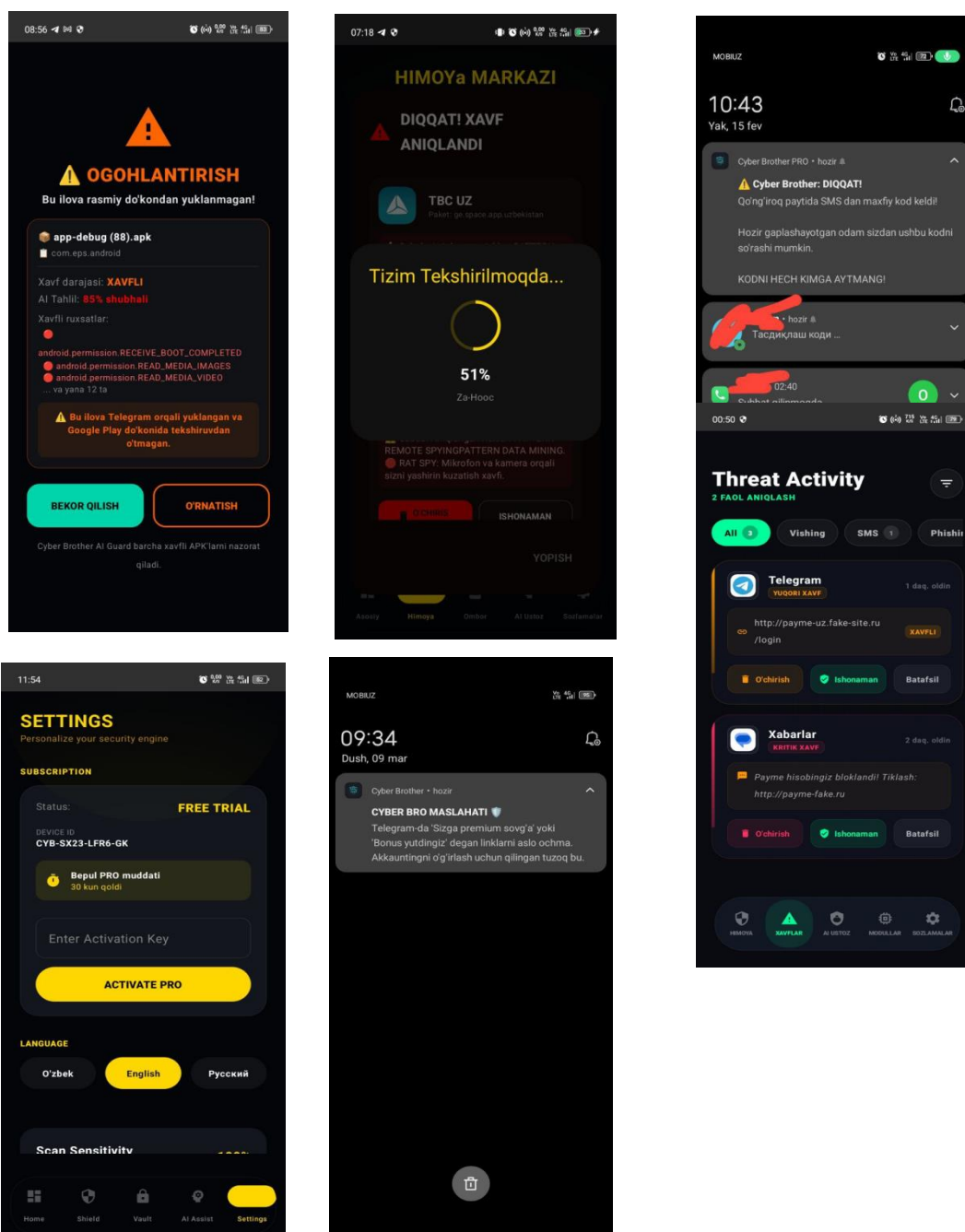
e) Daily push notification system designed to educate users about cybersecurity awareness.

f)

f) Threat history interface showing previously detected security risks and alerts.

On-Device AI Module

The core component of the Cyber Brother system is its on-device AI engine, which



performs data processing locally without transmitting sensitive information to external servers. This approach enhances user privacy and eliminates dependency on continuous internet connectivity, allowing the system to operate effectively in offline environments.

The AI model continuously learns and adapts to user behavior patterns, enabling it to detect deviations that may indicate potentially malicious activity. By leveraging behavioral analysis

techniques, the system can identify both known and previously unseen threats in real time, thereby improving the overall responsiveness and reliability of mobile security.

APK Security Analysis Module

Cyber Brother provides advanced protection against malicious APK files. The system analyzes:

- Application permissions
- Background processes
- Resource usage patterns
- Behavioral anomalies

If an application requests suspicious permissions or performs unauthorized actions, the AI model flags it as a potential threat and restricts its execution.

URL and Phishing Detection Module

The system includes a real-time URL scanning mechanism to protect users from phishing attacks. It evaluates:

- Domain reputation
- URL structure
- Redirection patterns
- Suspicious keywords

The "Red Alert" protocol is triggered when a high-risk URL is detected, immediately warning the user and blocking access.

Network Monitoring Module

Cyber Brother monitors network traffic to identify suspicious connections, unknown domains, and abnormal data transfers. This helps prevent data exfiltration and communication with malicious servers.

Detection of APK-Based Attacks

Malicious APK files are one of the most common attack vectors in Android ecosystems. Cyber Brother uses AI-based behavioral analysis to detect threats that bypass traditional signature-based systems. The system evaluates applications based on multiple parameters, including execution behavior, permission misuse, and hidden background activity. This allows the detection of spyware, trojans, and ransomware even when they are not previously known.

Detection of URL-Based Attacks

Phishing attacks often rely on deceptive URLs to trick users into revealing sensitive information. *Cyber Brother* addresses this issue using an AI-driven URL classification approach.

The model analyzes both lexical and structural features of URLs and compares them against known malicious patterns. Suspicious links are detected and blocked in real time, significantly reducing the risk of credential theft and financial fraud.

Advantages and Limitations

Advantages:

- Privacy-preserving architecture through on-device data processing
- Real-time threat detection and immediate response capabilities
- Improved resistance to zero-day attacks through behavioral analysis
- Offline functionality, enabling protection without internet connectivity
- Reduced latency compared with cloud-based scanning systems

Limitations:

Limited computational resources on mobile devices
Battery and memory consumption during continuous monitoring
Model training and update constraints in offline environments
Potential false positives that may affect user experience
Evasion techniques used by advanced malware to bypass detection

Conclusion

This study demonstrates that Artificial Intelligence plays a critical role in enhancing mobile cybersecurity by enabling intelligent, adaptive, and real-time threat detection mechanisms. The Cyber Brother system highlights the effectiveness of on-device AI in providing efficient protection against both APK-based and URL-based attacks while preserving user privacy and ensuring offline functionality.

As cyber threats continue to evolve in complexity and scale, future research should focus on improving model accuracy, minimizing false positives, and integrating advanced techniques such as federated learning to strengthen collaborative threat intelligence. Additionally, optimizing AI models for resource-constrained mobile environments remains an important challenge.

Overall, AI-driven solutions such as Cyber Brother represent a significant shift from traditional reactive defense strategies toward proactive and predictive cybersecurity models, paving the way for more resilient and intelligent mobile security systems.

References

1. OWASP Foundation, "OWASP Top 10 Mobile Risks," 2023. [Online]. Available: <https://owasp.org>
2. Android Developers, "Security Best Practices," Google, 2025. [Online]. Available: <https://developer.android.com>
3. IEEE Access, "Artificial Intelligence in Cybersecurity: A Comprehensive Survey," 2023–2024.
4. Y. Zhang et al., "Machine Learning-Based Intrusion Detection Systems: A Survey," *ACM Computing Surveys*, vol. 55, no. 1, 2023.
5. Cyber Brother Project, "Technical Documentation," 2025.
6. I. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning," MIT Press, 2016.
7. S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*, CRC Press, 2016.
8. A. Shabtai et al., "Andromaly: A Behavioral Malware Detection Framework for Android Devices," *Journal of Intelligent Information Systems*, vol. 38, no. 1, pp. 161–190, 2012.
9. N. McLaughlin et al., "Deep Android Malware Detection," *Proc. ACM CODASPY*, 2017.
10. K. Allix et al., "AndroZoo: Collecting Millions of Android Apps for the Research Community," *Proc. MSR*, 2016.
11. M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, "Analyzing Android Malware: A Survey," *Computer Communications*, vol. 89–90, pp. 1–19, 2016.
12. Google, "Android Security Overview," 2024. [Online]. Available: <https://source.android.com/security>
13. Symantec, "Internet Security Threat Report," 2023.
14. Verizon, "Data Breach Investigations Report (DBIR)," 2024.
15. S. Axelsson, "The Base-Rate Fallacy and Its Implications for Intrusion Detection," *ACM CCS*, 1999.