International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 October 2023*

Real-Time Threat Assessment through Machine Learning intended for Enhancing Security Measures in Mobile App

Dr. Padma Mishra
Asst.Professor, MCA, Thakur Institute of Management, Studies, Career Development and Research (TIMSCDR) ,Mumbai, India
mishrapadma1988@gmail.com

Dr. Vinita Gaikwad
Director, MCA, Thakur Institute of Management Studies,Career Development and Research (TIMSCDR), Mumbai, India
vinitagaikwad2@gmail.com

Dr. Rama Bansode
Assistant Professor, MCA., Modern College of Engineering, Pune, India
rama.bansode@moderncoe.edu.in

Mr.Shirshendu Maitra
Assistant Professor, MCA, Thakur Institute of Management, Studies, Career Development and Research (TIMSCDR)
Mumbai,India
slm2007@gmail.com

***Abstract*—** The ubiquitous presence of mobile operating systems like Android and iOS has fuelled the development of feature-rich applications, accommodating the diverse needs of users, including the management of personal data such as location and contacts. However, the expansive app ecosystem has also become a target for malicious actors seeking to exploit sensitive user information. Current approaches, such as permissions-based security models, provide only partial insights into app behaviors, leaving users vulnerable to privacy breaches.

In response to this challenge, we present Threat Check, an automated framework designed for continuous threat assessment of mobile applications. Unlike conventional methods that rely on user intervention and contextual understanding, threat Check leverages a one-time initialization process, where users specify trusted applications and rank permission groups based on relevance. Subsequently, threat Check dynamically assesses the threat level of installed applications by monitoring their runtime behaviors and interactions with system services, comparing them against established baselines.

Through its real-time threat rankings facilitated by threat Prior, threat Check empowers users to make informed decisions about app safety, providing ongoing insights into application behaviors and potential privacy violations. By automating threat assessment and enhancing user awareness, threat Check offers a proactive solution to mobile application security, enabling users to mitigate threats effectively and protect their personal data in an ever-evolving threat landscape.

Keywords*—Mobile application security; Threat Check; Permissions-based security; Privacy breaches ; Automated threat assessment; Real-time threat rankings; Personal data security*

I. INTRODUCTION

In recent years, the proliferation of mobile operating systems, notably Android and iOS, has revolutionized the way individuals interact with technology, facilitating access to a myriad of feature-rich applications that cater to diverse user needs. These applications, ranging from productivity tools to social networking platforms, often require access to sensitive user information such as location, contacts, and personal preferences to provide tailored experiences. [1][2] However, the exponential growth of the mobile app ecosystem has also introduced significant security

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 October 2023*

challenges, as it has become a lucrative target for malicious actors seeking to exploit vulnerabilities and access users' private data. Traditionally, mobile platforms like Android have employed permissions-based security models to help users understand the level of access requested by applications at the time of installation. While these permissions provide some insight into an application's intended use of resources, they often fall short in comprehensively assessing the potential threats associated with app behaviours. Consequently, users may inadvertently grant permissions to applications that abuse their sensitive data, leading to privacy breaches and other security incidents.[3]To address these shortcomings, there is a growing need for automated frameworks that can continuously monitor mobile applications and assess their threat levels in real-time. By leveraging advanced machine learning algorithms and runtime analysis techniques, such frameworks can provide users with timely insights into app behaviours and empower them to make informed decisions about app safety. Additionally, these frameworks can play a crucial role in mitigating security threats by alerting users to potential privacy violations and facilitating proactive measures to protect their personal data. In this context, we introduce Threat Check, an automated framework designed for continuous threat assessment of mobile applications.[4] By dynamically analysing app behaviours and interactions with system services, Threat Check aims to provide users with real-time threat rankings, enabling them to make proactive decisions about app installation and usage. Through its user-centric design and focus on privacy protection, Threat Check represents a significant step forward in enhancing mobile application security and empowering users to safeguard their personal data in an increasingly connected world.

II. STUDY OF PROBLEM

The pervasive use of smartphones and apps among young people underscores the critical importance of data security in today's digital landscape. As technology advances and internet connectivity becomes ubiquitous, the threat of data breaches and cyber attacks looms large.[7] Personal and financial information, once compromised, can have far-reaching consequences, underscoring the need for proactive measures to safeguard data.[8] While app developers may request permissions or registration for ostensibly benign reasons such as analytics, users must remain vigilant about the information they share. Instances of data breaches at tech giants like Facebook and Yahoo serve as stark reminders of the potential dangers posed by lax data security measures.[9] The leak of millions of users' information in these breaches highlights the severity of the issue and the widespread impact of such incidents.[14][15] In light of increasingly sophisticated cyber threats, both individuals and organizations must prioritize data security.[16] By adopting proactive measures and adhering to best practices, such as implementing robust encryption protocols and regularly updating security measures, stakeholders can mitigate the threat of data breaches and protect sensitive information from falling into the wrong hands.[5]

In conclusion, in today's digital age, data security is not merely a concern but a fundamental necessity. The continued proliferation of technology underscores the urgency of addressing data security threats and fortifying defenses against cyber-attacks.[By remaining vigilant and proactive, individuals and organizations can ensure the safe storage and use of valuable information in an increasingly interconnected world.[6]

III. AIM

The aim of this research paper is to introduce Threat Check, an automated framework designed for continuous threat assessment of mobile applications.[10] By leveraging advanced machine learning algorithms and runtime analysis techniques, Threat Check aims to provide users with real-time insights into app behaviors and empower them to make informed decisions about app safety. The primary objectives include:

1. Develop an automated framework for monitoring and assessing the threat levels of mobile applications in real-time.
2. Utilize advanced machine learning algorithms to analyze app behaviors and interactions with system services.
3. Provide users with timely threat rankings of installed applications to enable proactive decision-making.
4. Empower users to mitigate security threats by alerting them to potential privacy violations and facilitating proactive measures to protect their personal data.
5. Enhance user awareness and understanding of mobile application security issues, particularly related to privacy breaches and data vulnerabilities.
6. Contribute to the ongoing efforts to improve mobile application security and privacy protection in the face of evolving threats and challenges.[11]

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 October 2023*

IV. PROPOSED FRAMEWORK FOR ENHANCING SECURITY MEASURES S IN MOBILE APP

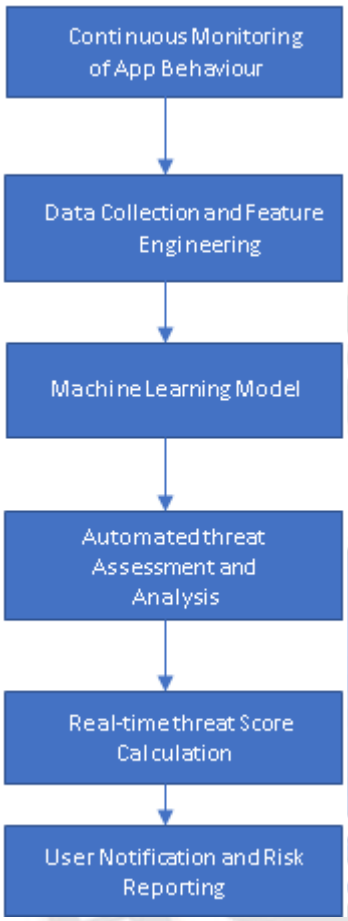

Fig 1: Diagram Outlines The Flow Of The Machine Learning Framework For Proactive Mobile Application Security

a. Continuous Monitoring of App Behaviour: The framework continuously monitors the behavior of installed mobile applications.
b. Data Collection and Feature Engineering: Data collected from app behavior is processed and engineered into features suitable for machine learning algorithms.
c. Machine Learning Model: Various machine learning algorithms such as anomaly detection, classification, and regression are employed to analyze the engineered features and assess the threat level of each application. [13]
d. Automated Threat Assessment and Analysis: The machine learning model automates the process of threat assessment and analysis, identifying potential security threats based on the input data.
e. Real-time Threat Score Calculation: Based on the results of the threat assessment, the framework calculates a real-time threat score for each application. [17]
f. User Notification and Threat Reporting: Users are notified of any identified security threats and provided with detailed reports, enabling them to take proactive measures to mitigate threats effectively. [18] [19]

V. CONCLUSION

In conclusion, the Threat Check framework significantly enhances mobile application security by providing continuous, real-time threat assessment through advanced machine learning algorithms and runtime analysis techniques. By monitoring app behaviors and interactions with system services, Threat Check offers users timely insights and threat rankings, empowering them to make informed decisions about app safety and take proactive measures to protect their personal data. This innovative approach not only addresses the limitations of traditional permissions-based models but also strengthens user awareness and privacy protection in an increasingly interconnected digital world.

References

[1] Khan, H.U., Sohail, M., Nazir, S. et al. Role of authentication factors in Fin-tech mobile transaction security. J Big Data 10, 138 (2023). https://doi.org/10.1186/s40537-023-00807-3.

[2] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, ‘‘Active authentication on mobile devices via stylometry, application usage, Web browsing, and GPS location,’’ IEEE Syst. J., vol. 11, no. 2, pp. 513–521, Jun. 2017.

[3] D. Damopoulos, S. A. Menesidou, G. Kambourakis, M. Papadaki,N. Clarke, and S. Gritzalis, ‘‘Evaluation of anomaly-based IDS for mobile devices using machine learning classifiers,’’ Secur. Commun. Netw., vol. 5, no. 1, pp. 3–14, Jan. 2012.

[4] J. Hall, M. Barbeau, and E. Kranakis, ‘‘Anomaly-based intrusion detection using mobility profiles of public transportation users,’’ in Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun. WiMob, Aug. 2005, pp. 17–24.

[5] S. Subudhi and S. Panigrahi, ‘‘Quarter-sphere support vector machine for fraud detection in mobile telecommunication networks,’’ Procedia Comput. Sci., vol. 48, pp. 353–359, Jan. 2015.

[6] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, ‘‘Cell phone-based biometric identification,’’ in Proc. 4th IEEE Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS), Sep. 2010, pp. 1–7.

[7] C. Nickel, T. Wirtl, and C. Busch, ‘‘Authentication of smartphone users based on the way they walk using k-NN algorithm,’’ in Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process., Jul. 2012, pp. 16–20.

[8] M. Jakobsson, E. Shi, P. Golle, and R. Chow, ‘‘Implicit authentication for mobile devices,’’ in Proc. 4th USENIX Conf. Hot Topics Secur., Aug. 2011, pp. 1–6.

[9] Y. Ashibani and Q. H. Mahmoud, ‘‘A Behavior-based proactive user authentication model utilizing mobile application usage patterns,’’ in Proc. 32nd Can. Conf. Artif. Intell., May 2019, pp. 284–295.

[10] Y. Ashibani and Q. H. Mahmoud, ‘‘A machine learning-based user authentication model using mobile App data,’’ in Proc. Int. Conf. Intell. Fuzzy Syst. (INFUS), Jul. 2019, pp. 408–415.

[11] Y. Ashibani and Q. H. Mahmoud, ‘‘User authentication for smart home networks based on mobile apps usage,’’ in Proc. 28th Int. Conf. Comput. Commun. Netw. (ICCCN), Jul. 2019, pp. 1–6.

[12] F. Li, N. Clarke, M. Papadaki, and P. Dowland, ‘‘Active authentication for mobile devices utilising Behaviour profiling,’’ Int. J. Inf. Secur., vol. 13, no. 3, pp. 229–244, Jun. 2014.

[13] D. Bassu, M. Cochinwala, and A. Jain, ‘‘A new mobile biometric based upon usage context,’’ in Proc. IEEE Int. Conf. Technol. Homeland Secur. (HST), Nov. 2013, pp. 441–446.

[14] U. Mahbub, J. Komulainen, D. Ferreira, and R. Chellappa, ‘‘Continuous authentication of smartphones based on application usage,’’ IEEE Trans. Biometrics, Behav., Identity Sci., vol. 1, no. 3, pp. 165–180, Jul. 2019.

[15] A. A. Alzubaidi, Continuous Authentication of Smartphone Owners Based on App Access Behavior. Colorado Springs, CO, USA: Univ. Colorado, 2018.

[16] Y. Ashibani and Q. H. Mahmoud, ‘‘A user authentication model for IoT networks based on app traffic patterns,’’ in Proc. IEEE 9th Annu. Inf. Technol.,Electron. Mobile Commun. Conf. (IEMCON), Nov. 2018, pp. 632–638.

[17] Y. Ashibani and Q. H. Mahmoud, ‘‘A Behavior profiling model for user authentication in IoT networks based on app usage patterns,’’ in Proc. 44th IEEE Annu. Conf. Ind. Electron. Soc. (IECON), Oct. 2018, pp. 2841–2846.

[18] L. Zhang, B. Tiwana, Z. Qian, Z. Wang, R. P. Dick, Z. M. Mao, and L. Yang,‘‘Accurate online power estimation and automatic battery behavior based power model generation for smartphones,’’ in Proc. 8th IEEE/ACM/IFIP Int. Conf. Hardw./Softw. Codesign Syst. Synth. CODES/ISSS, 2010,pp. 105–114.

[19] Tawalbeh L, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and Security: Challenges and Solutions. Applied Sciences.2020; 0(12):4102.https://doi.org/10.3390/app10124102