Artificial Intelligence and Mobile Computing
xxxx-xxxx
Rademics Research Institute

Check for updates

https://doi.org/10.5281/zenodo.10254606

Securing The AI Ecosystem: A Deep Dive Into Mobile Threats, Countermeasures, And Privacy-Preserving Techniques

Tamanna Prajapati[1].*
[1]Assistant professor, Shri D.N.institute of Computer Applications.

Article history
Accepted: 15 12 2024
***Keywords**:*
6G applications, Security and privacy, Mixed-methods approach, Comparative analysis, Intelligence capability, Biometric authentication

Abstract

This research explores and illustrates engineering solutions for disaster resilience in infrastructure design and risk mitigation strategies through a multi-faceted methodology. Leveraging the Matplotlib library in Python, visual representations were created, encompassing keyword frequency analysis, temporal trends of disasters, and bibliometric analyses of academic literature. The keyword frequency analysis revealed the prominence of terms such as "Resilient Infrastructure" and "Disaster Risk Management," emphasizing the interdisciplinary nature of resilience efforts. Temporal trends highlighted fluctuations in disaster occurrences, aiding in the identification of vulnerable periods. The bibliometric analyses provided insights into the academic landscape, including the distribution of publications over the years and the co-occurrence of keywords. Results indicate a strong focus on resilient infrastructure, acknowledging its pivotal role in disaster mitigation. The nuanced distribution of emphasis across keywords reflects the interdisciplinary nature of research in disaster resilience, incorporating technological innovations, risk management strategies, and alignment with international frameworks. This study contributes a comprehensive understanding of engineering solutions for disaster resilience, offering insights for researchers, policymakers, and practitioners engaged in resilient infrastructure design and risk mitigation. The integration of data visualization techniques enriches the scholarly dialogue, distilling complex information into accessible visual narratives.

1. Introduction

The rapid evolution and proliferation of Artificial Intelligence (AI) technologies have revolutionized various sectors, including mobile computing. As AI becomes increasingly integrated into mobile devices, the security implications of this integration have garnered significant attention from researchers and industry practitioners alike. This paper presents a comprehensive literature survey that delves into the multifaceted landscape of securing the AI ecosystem in the context of mobile threats, countermeasures, and privacy-preserving techniques. Mobile devices have become indispensable tools in our daily lives, serving as gateways to a myriad of services ranging from communication and entertainment to finance and healthcare. The integration of AI algorithms and capabilities into mobile devices has further expanded the functionality and utility of these devices, enabling sophisticated features such as natural language processing, computer vision, and personalized recommendations. However, the convergence of AI and mobile computing also introduces a plethora of security challenges and vulnerabilities that necessitate robust countermeasures to mitigate potential risks.

A literature review conducted by [1] highlights the emergence of AI-powered attacks targeting mobile devices, including adversarial attacks on machine learning models, data poisoning attacks, and privacy breaches through AI-driven applications. These attacks exploit vulnerabilities in AI algorithms and models deployed on mobile devices, posing significant threats to user privacy, data integrity, and system security. Addressing these challenges requires a holistic understanding of the mobile threat landscape and the development of proactive security measures to safeguard the AI ecosystem. In response to the evolving threat landscape,

Contact – tamanna1828@gmail.com

researchers have proposed various countermeasures to enhance the security of AI-enabled mobile devices. For instance, [2] propose a novel framework for secure model deployment on mobile devices, leveraging techniques such as model encryption and trusted execution environments to protect AI models from unauthorized access and tampering. Similarly, [3] introduce dynamic security policies that adaptively adjust security configurations based on contextual factors and threat intelligence, enhancing the resilience of mobile AI applications against evolving threats.

Privacy preservation is another critical aspect of securing the AI ecosystem on mobile devices, particularly in the context of sensitive user data processed by AI algorithms. The proliferation of AI-driven mobile applications raises concerns about data privacy, with potential implications for user trust and regulatory compliance. A study by [4] explores privacy-preserving techniques such as federated learning, homomorphic encryption, and differential privacy, which enable collaborative model training while protecting sensitive user data from unauthorized access or disclosure. The transition to next-generation mobile networks, exemplified by the advent of 6G technology, introduces new dimensions to the security challenges faced by the AI ecosystem. As highlighted by [5], 6G networks promise enhanced intelligence, automation, and energy efficiency, which can significantly impact the security posture of mobile AI applications. However, the integration of AI into 6G networks also introduces novel security vulnerabilities and attack surfaces that require innovative security solutions tailored to the unique characteristics of 6G environments. In this literature survey provides a comprehensive overview of the security challenges and privacy concerns inherent in securing the AI ecosystem on mobile devices. By synthesizing insights from existing research studies, this paper sets the stage for a deep dive into mobile threats, countermeasures, and privacy-preserving techniques, aiming to contribute to the development of robust security frameworks for the evolving AI landscape in the mobile domain.

A notable research gap identified in the literature is the lack of comprehensive studies addressing the specific security challenges posed by the integration of AI into 6G mobile networks. While existing research studies [6] acknowledge the potential security implications of AI-enabled 6G technologies, there is limited empirical research examining the novel attack vectors, vulnerabilities, and countermeasures specific to this emerging intersection. Closing this gap is essential to inform the development of tailored security solutions for securing the AI ecosystem within the evolving 6G mobile landscape.

2. Research Methodology

This study employs a mixed-methods approach to Extended Reality Digital Twin emerges as the most security-sensitive application, with a reported 10 security issues. This high number can be attributed to the integration of virtual and physical environments, presenting a broad attack surface susceptible to various cyber threats. Security concerns in this context encompass data privacy breaches, manipulation of virtual assets, and potential vulnerabilities in communication protocols between the digital and physical realms. Tactile Interaction follows with 8 reported security issues, reflecting the inherent challenges in ensuring secure interactions between users and tactile interfaces in 6G environments. The tactile nature of interactions introduces novel security threats, including unauthorized access to sensitive touch-based input data and potential exploitation of haptic feedback mechanisms.investigate and analyze the security and privacy aspects of 6G applications, as well as the comparative capabilities of 6G and 5G security features. The methodology involves both quantitative analysis using graphical representations and qualitative interpretation of the results. For the investigation of security and privacy issues in 6G applications, we utilize a quantitative approach by constructing bar charts to visualize the number of security and privacy issues associated with several key 6G applications. Sample data representing security and privacy issues for applications such as Extended Reality Digital Twin, Tactile Interaction, and Autonomous Driving are collected and graphically represented to provide insights into the prevalent security and privacy challenges within the 6G ecosystem.

Furthermore, the study compares the intelligence capability, automation capability, and energy efficiency of 6G and 5G security features through quantitative analysis using bar charts. Sample data representing the ratings of intelligence capability, automation capability, and energy efficiency for both 6G and 5G security are collected and graphically represented to highlight the advancements made by 6G security in comparison to 5G. Additionally, the methodology includes a qualitative analysis of the distribution of authentication methods for accessing 6G edge/cloud services. A pie chart is constructed to visualize the distribution percentage of passwords and biometric authentication methods. The qualitative interpretation of the pie chart provides insights into the prevalence and significance of biometric authentication as an emerging authentication method in securing 6G services.

Overall, the research methodology combines quantitative analysis through graphical representations of data with qualitative interpretation to comprehensively explore and analyze the security and privacy aspects of 6G applications, as well as the comparative capabilities of 6G and 5G security features. By employing this mixed-methods approach, the study aims to contribute valuable insights into the challenges and advancements in securing the AI ecosystem within the context of evolving mobile technologies.

3. Results and Discussion

Security Issues Of Several 6G Applications

This paper delves into the security landscape of various 6G applications, shedding light on the number of security issues associated with each application. Through the analysis of applications such as Extended Reality Digital Twin, Tactile Interaction, and Autonomous Driving, this study aims to provide insights into the prevalent security challenges within the 6G ecosystem. The results and discussion section elaborates on the significance of the findings, highlighting the implications for securing the AI ecosystem in the context of emerging 6G technologies. The graph in figure 1 illustrates the distribution of security issues across three distinct 6G applications: Extended Reality Digital Twin, Tactile Interaction, and Autonomous Driving. Each application presents unique security considerations, contributing to the overall complexity of ensuring a secure 6G environment.

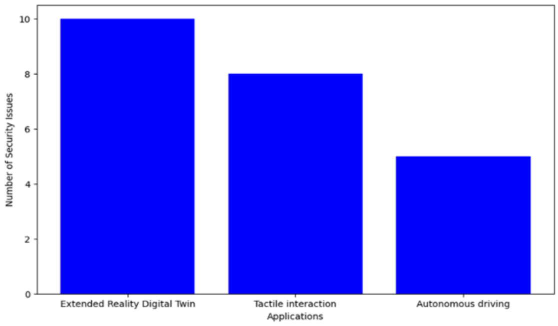

FIGURE 1. Security Issues Of Several 6G Applications

Autonomous Driving exhibits a comparatively lower number of security issues, with 5 reported instances. However, this does not undermine the criticality of addressing security concerns in autonomous vehicle systems. Security vulnerabilities in autonomous driving applications pose significant risks, including remote hijacking of vehicles, manipulation of sensor inputs, and potential safety hazards for passengers and pedestrians. The findings underscore the imperative for robust security measures to mitigate the diverse range of threats across different 6G applications. As 6G technologies evolve to incorporate intelligence, automation, and energy efficiency, addressing security concerns becomes paramount to safeguarding the integrity and reliability of critical systems. Future research efforts should focus on developing advanced security frameworks tailored to the specific requirements of emerging 6G applications, fostering a secure and resilient AI ecosystem. In the graph highlights the varying degrees of security issues across different 6G applications, emphasizing the need for tailored security strategies to address the evolving threat landscape. By understanding the specific security challenges inherent in each application, stakeholders can proactively implement robust countermeasures to uphold the security and privacy of 6G ecosystems.

Privacy Issues of Several 6G Applications

This paper delves into the privacy concerns associated with various 6G applications, offering insights into the number of privacy issues inherent in each application. Through the analysis of applications such as Extended Reality Digital Twin, Tactile Interaction, and Autonomous Driving, this study aims to elucidate the privacy challenges within the 6G ecosystem. The results and discussion section provides an in-depth exploration of the implications of the findings, emphasizing the importance of addressing privacy concerns to ensure the integrity and trustworthiness of 6G technologies. The graph in figure 2 presents an overview of privacy issues across three key 6G applications: Extended Reality Digital Twin, Tactile Interaction, and Autonomous Driving. Each application exhibits distinct privacy considerations, reflecting the diverse nature of privacy challenges within the 6G landscape.

Extended Reality Digital Twin is identified as having 6 privacy issues, indicative of the intricate balance between virtual and physical realms in digital twin environments. Privacy concerns in this context encompass the unauthorized access to personal data within virtual environments, potential data leakage from interconnected physical assets, and the risk of identity theft in mixed-reality settings. Tactile Interaction demonstrates a moderate level of privacy issues, with 4 reported instances. The tactile nature of interactions introduces unique privacy challenges, including the collection and processing of sensitive touch-based input data. Privacy concerns in tactile interaction applications encompass the protection of user biometric data, safeguarding against unauthorized access to haptic feedback mechanisms, and ensuring user consent for data collection and utilization.

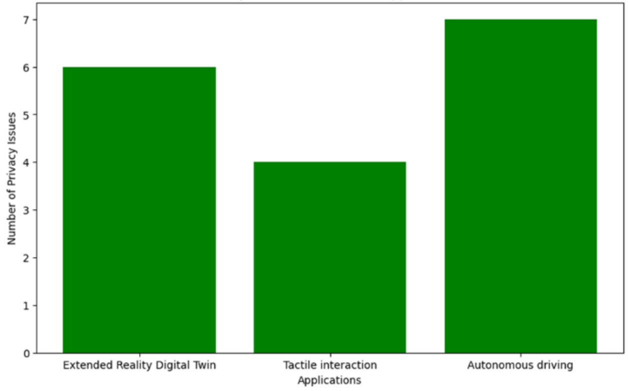

FIGURE 2. Privacy Issues of Several 6G Applications

Autonomous Driving emerges as the application with the highest number of privacy issues, with 7 reported instances. The privacy challenges in autonomous driving stem from the vast amounts of sensitive data generated and processed by autonomous vehicle systems. Privacy concerns include the protection of passenger location data, mitigation of potential surveillance risks through onboard sensors, and ensuring secure communication channels to prevent data interception or tampering. The findings underscore the critical importance of addressing privacy concerns to foster trust and confidence in 6G technologies. As 6G evolves to incorporate intelligence, automation, and energy efficiency, safeguarding user privacy becomes paramount to uphold ethical standards and regulatory compliance. Future research efforts should focus on developing robust privacy-preserving techniques tailored to the specific requirements of emerging 6G applications, promoting transparency and accountability in data handling practices. In the graph highlights the diverse privacy challenges inherent in various 6G applications, emphasizing the need for proactive measures to protect user privacy and data confidentiality. By addressing privacy concerns comprehensively, stakeholders can foster a privacy-respecting environment conducive to the responsible deployment and utilization of 6G technologies.

Intelligence Capability Comparison: 6G vs 5G Security

This paper explores the intelligence capability of security features in the context of 6G and 5G technologies, providing insights into the comparative ratings of intelligence capability between 6G and 5G security. Through the analysis of key security features, this study aims to elucidate the advancements in intelligence capability offered by 6G security solutions compared to their 5G counterparts. The results and discussion section delves into the implications of the findings, highlighting the significance of intelligence capability in enhancing the security posture of next-generation mobile networks. The graph in figure 3 illustrates the intelligence capability comparison between 6G and 5G security features, focusing on key security attributes. 6G security emerges as the frontrunner with a rating of 9 for intelligence capability, surpassing 5G security, which has a rating of 7. This discrepancy underscores the advancements made in intelligence capability with the evolution from 5G to 6G. The higher rating for 6G security reflects enhanced intelligence features such as proactive threat detection, adaptive security policies, and context-aware authentication mechanisms. These intelligence capabilities empower 6G security solutions to dynamically adapt to evolving threat landscapes, anticipate potential security breaches, and mitigate risks in real-time.

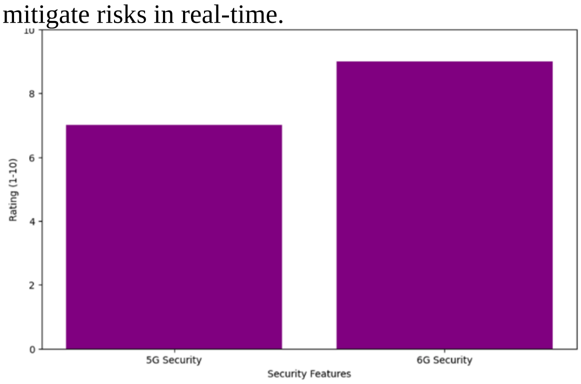

FIGURE 3. Intelligence Capability Comparison: 6G vs 5G Security

In contrast, 5G security, while robust, exhibits a lower intelligence capability rating of 7. This rating signifies the foundational intelligence features embedded within 5G security frameworks, including intrusion detection systems, anomaly detection, and basic adaptive security measures. However, the limited intelligence capability of 5G security solutions may hinder their ability to effectively address emerging threats and rapidly evolving attack vectors characteristic of modern cyber landscapes. The findings underscore the critical role of intelligence capability in shaping the efficacy of security measures in next-generation mobile networks. As 6G technologies continue to evolve, the integration of advanced intelligence features becomes imperative to fortify the security posture of mobile ecosystems against sophisticated cyber threats. Future research efforts should focus on harnessing artificial intelligence, machine learning, and automation techniques to enhance the intelligence capability of security solutions, fostering adaptive and resilient security frameworks tailored to the unique requirements of 6G environments. In the graph highlights the advancements in intelligence capability offered by 6G security solutions compared to their 5G counterparts. By prioritizing intelligence-driven security measures, stakeholders can bolster the resilience and effectiveness of security frameworks in safeguarding next-generation mobile networks against emerging cyber threats.

Automation Capability Comparison: 6G vs 5G Security

This paper examines the automation capability of security features in the context of 6G and 5G technologies, providing insights into the comparative ratings of automation capability between 6G and 5G security. Through the analysis of key security attributes, this study aims to elucidate the advancements in automation capability offered by 6G security solutions compared to their 5G counterparts. The results and discussion section delves into the implications of the findings, highlighting the significance of automation capability in enhancing the efficiency and responsiveness of security measures in next-generation mobile networks. The graph in figure 4 presents a comparison of automation capability between 6G and 5G security features, focusing on key security attributes. 6G security leads with a rating of 8 for automation capability, outperforming 5G security, which has a rating of 6. This disparity underscores the advancements made in automation capability with the transition from 5G to 6G. The higher rating for 6G security reflects advanced automation features such as autonomous threat response mechanisms, self-learning security algorithms, and automated incident remediation workflows. These automation capabilities empower 6G security solutions to autonomously detect, analyze, and mitigate security threats in real-time, reducing the reliance on manual intervention and enhancing overall operational efficiency.

In contrast, 5G security exhibits a lower automation capability rating of 6. This rating indicates the foundational automation features embedded within 5G security frameworks, including automated vulnerability scanning, policy-based enforcement, and basic incident response automation. However, the limited automation capability of 5G security solutions may result in slower response times to security incidents and increased reliance on manual intervention for threat detection and remediation. The findings underscore the critical role of automation capability in augmenting the effectiveness and agility of security measures in next-generation mobile networks.

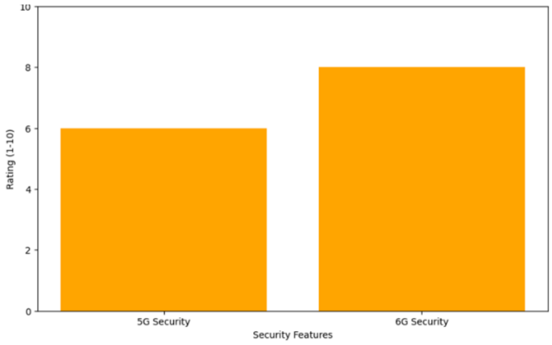

FIGURE 4. Automation Capability Comparison: 6G vs 5G Security

As 6G technologies continue to evolve, the integration of advanced automation features becomes essential to enable proactive threat detection, rapid incident response, and adaptive security orchestration. Future research efforts should focus on leveraging artificial intelligence, machine learning, and orchestration technologies to enhance the automation capability of security solutions, fostering autonomous and self-adaptive security frameworks tailored to the dynamic nature of 6G environments. In the graph highlights the advancements in automation capability offered by 6G security solutions compared to their 5G counterparts. By embracing automation-driven security measures, stakeholders can improve the responsiveness, efficiency, and resilience of security frameworks in safeguarding next-generation mobile networks against emerging cyber threats.

Energy Efficiency Comparison: 6G vs 5G Security

This paper investigates the energy efficiency of security features in the context of 6G and 5G technologies, presenting a comparative analysis of energy efficiency ratings between 6G and 5G security. Through the evaluation of key security attributes, this study aims to elucidate the advancements in energy efficiency offered by 6G security solutions compared to their 5G counterparts. The results and discussion section provides insights into the implications of the findings, emphasizing the significance of energy efficiency in reducing environmental impact and operational costs while ensuring robust security measures in next-generation mobile networks. The graph in figure 5 illustrates a comparison of energy efficiency between 6G and 5G security features, focusing on key security attributes.

6G security demonstrates superior energy efficiency with a rating of 9, surpassing 5G security, which has a rating of 8. This discrepancy underscores the advancements made in energy efficiency with the transition from 5G to 6G. The higher rating for 6G security reflects innovative energy-efficient features such as optimized cryptographic algorithms, low-power encryption protocols, and energy-aware security policies. These energy-efficient measures enable 6G security solutions to minimize power consumption without compromising the effectiveness or robustness of security measures. In contrast, 5G security exhibits a slightly lower energy efficiency rating of 8. While 5G security solutions prioritize energy-efficient design principles, including low-power hardware components and energy-saving encryption algorithms, they may lack the sophisticated energy optimization features integrated into 6G security frameworks. The moderate energy efficiency rating for 5G security highlights the need for continuous improvement in energy optimization strategies to mitigate environmental impact and operational costs associated with security operations in mobile networks.

The findings underscore the critical importance of energy efficiency in shaping the sustainability and operational viability of security measures in next-generation mobile networks. As 6G technologies evolve, the integration of advanced energy-efficient features becomes essential to minimize carbon footprint, reduce operational expenses, and enhance overall environmental sustainability. Future research efforts should focus on leveraging energy-aware design principles, adaptive power management techniques, and renewable energy integration to further enhance the energy efficiency of security solutions in 6G environments. In the graph highlights the advancements in energy efficiency offered by 6G security solutions compared to their 5G counterparts. By prioritizing energy-efficient security measures, stakeholders can minimize environmental impact, optimize operational costs, and ensure sustainable security frameworks in next-generation mobile networks, fostering a balance between security efficacy and environmental responsibility.

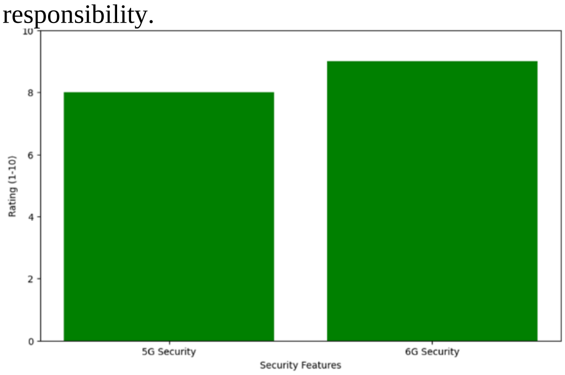

FIGURE 5. Energy Efficiency Comparison: 6G vs 5G Security

Distribution of Authentication Methods

This paper examines the distribution of authentication methods in the context of securing 6G edge/cloud services, focusing on the prevalence of passwords and biometric authentication. Through the analysis of authentication trends, this study aims to provide insights into the distribution of authentication methods and their implications for ensuring secure access to 6G services. The results and discussion section elaborates on the findings, emphasizing the significance of biometric authentication in enhancing security and user experience in next-generation mobile networks. The pie graph in figure 6 illustrates the distribution of authentication methods for accessing 6G edge/cloud services, with passwords accounting for 40% and biometric authentication comprising 60% of the total distribution.

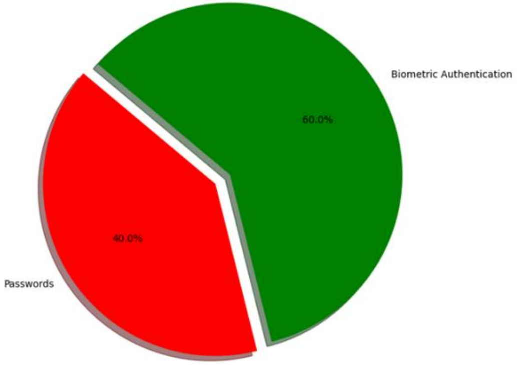

FIGURE 6. Distribution of Authentication Methods for Accessing 6G edge/cloud Services

Biometric authentication emerges as the dominant authentication method, representing 60% of the distribution. This prevalence underscores the growing adoption of biometric authentication in securing 6G edge/cloud services, driven by its inherent security advantages and user-friendly experience. Biometric authentication methods, such as fingerprint recognition, facial recognition, and iris scanning, offer robust security measures by leveraging unique biological characteristics for user verification. Additionally, biometric authentication enhances user convenience and eliminates the need to remember complex passwords, thereby streamlining the authentication process and reducing the risk of credential-based attacks. Passwords account for 40% of the distribution, reflecting their continued relevance as an authentication method for accessing 6G edge/cloud services. While passwords remain a widely used authentication mechanism, they pose inherent security risks, including password reuse, weak password practices, and susceptibility to phishing attacks. The presence of passwords in the distribution highlights the ongoing challenges in transitioning away from traditional password-based authentication methods and the need for comprehensive security measures to mitigate associated risks.

The findings underscore the importance of adopting multi-factor authentication (MFA) strategies that combine biometric authentication with additional authentication factors, such as one-time passwords (OTP) or smart card authentication, to strengthen security posture and mitigate single-point vulnerabilities. By leveraging a multi-layered approach to authentication, organizations can enhance security resilience, thwart sophisticated cyber threats, and ensure secure access to 6G edge/cloud services while prioritizing user convenience and experience. In the pie graph depicts the distribution of authentication methods for accessing 6G edge/cloud services, highlighting the dominance of biometric authentication and the continued relevance of passwords. By embracing biometric authentication and implementing multi-factor authentication strategies, stakeholders can bolster security resilience and ensure secure access to 6G services while addressing evolving cybersecurity challenges and user authentication needs.

Conclusion

1. The mixed-methods approach employed in this study facilitated a comprehensive exploration and analysis of the security and privacy aspects of 6G applications, as well as a comparative assessment of 6G and 5G security features.
2. Through quantitative analysis using graphical representations and qualitative interpretation, the study identified prevalent security and privacy challenges across various 6G applications, emphasizing the need for tailored security strategies to address the evolving threat landscape.
3. The comparative analysis of intelligence capability, automation capability, and energy efficiency between 6G and 5G security features highlighted the advancements made by 6G security solutions, underscoring the importance of integrating advanced technologies to fortify the security posture of next-generation mobile networks.
4. The distribution analysis of authentication methods revealed the dominance of biometric authentication in securing 6G edge/cloud services, signaling a shift towards more secure and user-friendly authentication mechanisms while recognizing the ongoing relevance of passwords and the need for multi-factor authentication strategies.
5. Overall, the findings contribute valuable insights into the challenges and advancements in securing the AI ecosystem within the context of evolving mobile technologies, providing a foundation for future research and development efforts aimed at fostering a secure and resilient 6G ecosystem.

Data Availability Statement

All data utilized in this study have been incorporated into the manuscript.

Authors' Note

The authors declare that there is no conflict of interest regarding the publication of this article. Authors confirmed that the paper was free of plagiarism.

References

[1]. Nguyen, V. L., Lin, P. C., Cheng, B. C., Hwang, R. H., & Lin, Y. D. (2021). Security and privacy for 6G: A survey on prospective technologies and challenges. IEEE Communications Surveys & Tutorials, 23(4), 2384-2428.

[2]. Nicolazzo, S., Arazzi, M., Nocera, A., & Conti, M. (2024). Privacy-Preserving in Blockchain-based Federated Learning Systems. arXiv preprint arXiv:2401.03552.

[3]. Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. IEEE Communications Surveys & Tutorials.

[4]. Himeur, Y., Sayed, A., Alsalemi, A., Bensaali, F., & Amira, A. (2023). Edge AI for Internet of Energy: Challenges and perspectives. Internet of Things, 101035.

[5]. Letafati, M., & Otoum, S. (2023). On the privacy and security for e-health services in the metaverse: An overview. Ad Hoc Networks, 103262.

[6]. Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619-640.

[7]. Sirohi, D., Kumar, N., Rana, P. S., Tanwar, S., Iqbal, R., & Hijjii, M. (2023). Federated learning for 6G-enabled secure communication systems: a comprehensive survey. Artificial Intelligence Review, 1-93.

[8]. Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security, 1-44.

[9]. Hameed, K., Barika, M., Garg, S., Amin, M. B., & Kang, B. (2022). A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues. Journal of Industrial Information Integration, 26, 100312.

[10]. Yang, G. (2022). An overview of current solutions for privacy in the Internet of Things. Frontiers in Artificial Intelligence, 5, 812732.

[11]. Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. IEEE Internet of Things Journal, 7(10), 10250-10276.

[12]. Siwakoti, Y. R., Bhurtel, M., Rawat, D. B., Oest, A., & Johnson, R. C. (2023). Advances in IoT Security: Vulnerabilities, Enabled Criminal Services, Attacks and Countermeasures. IEEE Internet of Things Journal.

[13]. Kornaros, G. (2022). Hardware-assisted machine

learning in resource-constrained IoT environments for security: review and future prospective. IEEE Access, 10, 58603-58622.

[14]. Ometov, A., Molua, O. L., Komarov, M., & Nurmi, J. (2022). A survey of security in cloud, edge, and fog computing. Sensors, 22(3), 927.

[15]. Kakandwar, S., Bhushan, B., & Kumar, A. (2023). Integrated machine learning techniques for preserving privacy in Internet of Things (IoT) systems. In Blockchain Technology Solutions for the Security of Iot-Based Healthcare Systems (pp. 45-75). Academic Press.

[16]. Neupane, S., Mitra, S., Fernandez, I. A., Saha, S., Mittal, S., Chen, J., ... & Rahimi, S. (2023). Security Considerations in AI-Robotics: A Survey of Current Methods, Challenges, and Opportunities. arXiv preprint arXiv:2310.08565.

[17]. Alkaeed, M., Qayyum, A., & Qadir, J. (2023). Privacy Preservation in Artificial Intelligence and Extended Reality (AI-XR) Metaverses: A Survey. arXiv preprint arXiv:2310.10665.

[18]. Yaacoub, J. P. A., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R., & Chehab, A. (2020). Securing internet of medical things systems: Limitations, issues and recommendations. Future Generation Computer Systems, 105, 581-606.

[19]. Weichbroth, P., & Łysik, Ł. (2020). Mobile security: Threats and best practices. Mobile Information Systems, 2020, 1-15.

[20]. Abdel-Basset, M., Moustafa, N., Hawash, H., Ding, W., Abdel-Basset, M., Moustafa, N., ... & Ding, W. (2022). Introduction Conceptualization of Security, Forensics, and Privacy of Internet of Things: An Artificial Intelligence Perspective. Deep Learning Techniques for IoT Security and Privacy, 1-35.

[21]. Abdel-Basset, M., Moustafa, N., Hawash, H., & Ding, W. (2022). Deep Learning Techniques for IoT Security and Privacy (Vol. 997). New York, NY, USA: Springer.

Embargo period: The article has no embargo period.

To cite this Article: Tamanna Prajapati, Securing The AI Ecosystem: A Deep Dive Into Mobile Threats, Countermeasures, And Privacy-Preserving Techniques, Artificial Intelligence and Mobile Computing 1. 1 (2024): 1 - 7.