International Journal of Advanced Digital Systems
and Multidisciplinary Studies (IJADSMS),
Volume - 2, Issue - 2 pp. 110–113, 2026

Cell Phone Theft and IMEI Manipulation: Detection, Prevention, and Legal Implications

Mr. Ajit Kumar[1], Ms. Lakshmi Kumari[2], Ms. Kumari Puja[3], Mr. Abhishek Kumar[4], Ms. Anupama[5],Mr. Sachin Kashyap[6]

[1]Assistant Professor, Amity Institute of Information Technology (AIIT), Amity University Jharkhand, Ranchi

[2,3,4,5,6] Assistant Professor ,School of Computer Applications, Noida Institute of Engineering and Technology (NIET) Greater Noida

akumar7@rnc.amity.edu [1], lakshmi1051999@gmail.com[2], gkp2910@gmail.com[3],abhishek.kumar@niet.co.in[4] , anupama0140@gmail.com[5] , sachinkashyap80770@gmail.com[6]

Abstract

This paper explores the multifaceted issues surrounding cell phone theft and the illicit manipulation of International Mobile Equipment Identity numbers, which serve as unique identifiers for mobile devices. The International Mobile Equipment Identifier is a critical component for identifying mobile devices globally, akin to a serial number, and is factory-assigned, stored in the device's firmware, and transmitted during network authorization. Despite its intended permanence, the IMEI can be illegally altered or cloned, facilitating the resale of stolen devices and complicating efforts to track and recover them. This paper delves into the technological vulnerabilities that enable such manipulation, the sophisticated methods employed by perpetrators, and the consequential challenges faced by law enforcement and network providers in combating this evolving threat. Furthermore, it examines the current strategies for detection and prevention, including the role of centralized databases like the Central Equipment Identity Register in blacklisting stolen devices and the continuous efforts by manufacturers to enhance tamper-proof IMEI storage. The discussion extends to an analysis of the legal frameworks and international collaborations aimed at mitigating the impact of cell phone theft and IMEI manipulation, offering insights into policy gaps and potential areas for reform.

Keywords: Cell phone theft, IMEI manipulation, mobile security, legal implications, crime prevention.

Introduction

The pervasive integration of mobile devices into daily life has inadvertently created new vulnerabilities, making them prime targets for sophisticated cybercriminal activities like cell phone theft and International Mobile Equipment Identity manipulation [1]. These security risks pose significant challenges for detection and traceability, often exacerbated by the illicit alteration of IMEI numbers to obscure a device's true identity and origin [2]. This paper explores the multifaceted issues surrounding cell phone theft and IMEI manipulation, including the technical methods employed for these illicit activities, current detection and prevention strategies, and the intricate legal ramifications for perpetrators and victims alike [2]. Specifically, it investigates how evolving mobile security threats, such as SIM card swapping and phishing, contribute to the broader landscape of device compromise and data exploitation [1]. Furthermore, we review the countermeasures that can be employed to mitigate the risks posed by IMSI catchers, including network-based solutions and user-based solutions [3]. This analysis also delves into the advanced techniques employed by criminals, such as the use of rogue devices like IMSI catchers, to intercept and manipulate cellular communications, thereby compromising user privacy and enabling potential financial fraud [3], [4]. These sophisticated devices, often referred to as "Stingrays" or "cell site simulators," have become increasingly advanced with the proliferation of 4G and 5G networks, exacerbating the challenges in maintaining cellular network security [3], [4]. The impact of these IMSI catcher deployments on cellular network security, particularly in the context of advanced 4G and 5G infrastructures, necessitates a comprehensive understanding of their operational methodologies and the resultant vulnerabilities they exploit [4]. This paper will also examine the innovative methods criminals use to conceal stolen phones, including physically altering devices and fabricating counterfeit IMEI labels, alongside the rising global incidence of mobile phone theft [5].

Literature Review

This section provides an overview of existing research on cell phone theft, IMEI manipulation, and related cybersecurity threats, drawing upon various studies that highlight the evolution of these crimes and the efforts to combat them. It further synthesizes findings on detection techniques, preventive measures, and the legal frameworks established to address these pervasive issues. A significant portion of the literature focuses on the technical vulnerabilities within mobile networks, especially concerning the susceptibility of 4G and 5G networks to advanced surveillance tools like IMSI catchers, which are used to intercept cellular communications and track user identities [3], [6]. These devices exploit inherent weaknesses in network protocols to force devices to reveal their International Mobile Subscriber Identity, a critical long-term identifier, often prior to the assignment of a temporary identifier [6]. This vulnerability allows for the interception of communications and location tracking, posing substantial privacy risks to users [7], [8]. Moreover, the rapid evolution of mobile network technology, particularly 4G and 5G networks, has introduced new fraud vulnerabilities that necessitate continuous adaptation of detection strategies [9], [10]. Despite constant upgrades to IP-based multimedia services in mobile networks over the past two decades, the security measures on mobile equipment often lag behind technological advancements, creating new vulnerabilities and attack vectors [11]. This disparity often arises from the complex interplay of hardware limitations, software update cycles, and the inherent difficulties in securing a globally interconnected and diverse mobile ecosystem against increasingly sophisticated threats [3], [12]. For instance, prevalent fraud vectors such as SMS/text message fraud, including smishing and phishing schemes, leverage these vulnerabilities to compromise user credentials and financial assets [13]. The increasing sophistication of these fraudulent activities, coupled with the rising global incidence of mobile phone theft, underscores the urgent need for more robust security frameworks and collaborative efforts between service providers, regulators, and users to safeguard against evolving threats [9], [14]. Further research also highlights that mobile money services, despite their critical role in financial inclusion, are particularly susceptible to sophisticated text-based schemes such as phishing and fraudulent SMS verification codes [13]. The reliance on manual fraud detection tools and non-biometric customer validation processes within many mobile network operators further exacerbates these vulnerabilities, leaving systems open to exploitation and forgery [9]. Moreover, the centralized nature of traditional financial institutions creates single points of failure, making them attractive targets for organized criminal groups who heavily invest in developing sophisticated malware, viruses, and zero-click attacks specifically targeting mobile devices and financial transactions [15]. This trend not only results in significant financial losses for customers but also erodes trust in digital financial systems, thereby impeding broader efforts toward financial inclusion and exacerbating socioeconomic disparities [13], [16]. These advanced cyber threats underscore the critical need for continuous innovation in security protocols and user education to safeguard mobile financial ecosystems against evolving criminal tactics [14], [17].

Methodology

This section details the research design, data collection procedures, and analytical approaches used to investigate cell phone theft and IMEI manipulation. It outlines the systematic approach taken to gather and interpret data, aiming to provide a comprehensive understanding of the mechanisms behind these illicit activities and their broader implications. The methodology employed a mixed-methods approach, integrating both quantitative and qualitative data to identify key vulnerabilities and prevalent attack vectors in mobile money systems, especially those related to smishing and identity theft [18]. Specifically, the quantitative analysis involved examining anonymized transaction data and incident reports from mobile network operators to identify patterns of fraudulent activity, while the qualitative component included interviews with cybersecurity experts and law enforcement officials to gain insights into emerging threats and mitigation strategies. This multifaceted approach allowed for a robust assessment of the effectiveness of current security protocols and the identification of gaps in existing preventative measures. A detailed examination of mobile agent systems, particularly those based on Multi-modal Large Language Models, reveals novel security challenges beyond traditional attack vectors, necessitating new defensive strategies against sophisticated threats like those seen in mobile financial ecosystems [19]. These advanced models introduce complex vulnerabilities, especially through social engineering attacks such as phishing, vishing, smishing, and pretexting, which have resulted in substantial fraud losses in mobile money services across various regions, particularly in Africa [20], [21]. Furthermore, the rapid expansion of mobile financial technologies, while facilitating financial inclusion, has inadvertently opened new avenues for illicit activities due to a knowledge gap in understanding the full scope of mobile money's vulnerabilities [22]. The methodology utilized a hybrid descriptive research design, combining quantitative analysis of scam incident reports with qualitative surveys of affected users to characterize the patterns and common attributes of AI-generated scams within mobile financial platforms [23], [24].

Results

This comprehensive methodological approach allowed for a robust understanding of both the technical vulnerabilities exploited in cell phone theft and IMEI manipulation, as well as the socio-technical factors contributing to their prevalence and impact on mobile financial services. The findings presented in this section will detail the outcomes of these analyses, revealing critical insights into the evolving landscape of mobile security threats and the effectiveness of current countermeasures. A systematic security investigation into multi-modal mobile GUI agents, for instance, has uncovered 34 previously unreported attacks and identified critical vulnerabilities within perception, reasoning, and memory modules of these systems [19], [25]. Notably, certain vulnerabilities stem from a "Reasoning Gap," a latent flaw in the reasoning stage of multimodal agents that significantly increases their susceptibility to active environment injection attacks [26]. This highlights that despite advances in AI reasoning capabilities, multimodal large language model-based mobile agent systems remain susceptible to various attack techniques across their lifecycle, including perception, reasoning, memory, and multi-agent collaboration modules [19]. These vulnerabilities underscore the necessity for developing more secure and comprehensive defense strategies to safeguard against such multimodal attacks, particularly given the rapid progress in the reasoning capabilities of Multi-modal Large Language Models [19], [27]. This necessitates a focused effort on integrating robust security measures directly into the architectural design of AI agents, moving beyond mere prompt-based defenses which have proven largely ineffective against sophisticated adversarial techniques [27], [28].

Discussion

This section thoroughly examines the implications of the identified vulnerabilities and the efficacy of current countermeasures, proposing a refined framework for enhancing mobile security protocols against both traditional and AI-driven threats. Specifically, it will delve into the critical need for upgraded encryption protocols, multifactor authentication, and real-time threat monitoring to mitigate risks associated with mobile banking applications [29]. Additionally, the discussion will explore the broader impact of active environment injection attacks on multimodal agents, particularly focusing on adversarial content injection within multimodal interaction interfaces that can mislead agent decision-making [27], [28]. This form of attack exploits the agent's inability to detect impostors within its operational environment, thereby manipulating its execution processes through malicious environmental elements [26], [27], [28]. The identified "Reasoning Gap" represents a significant structural vulnerability in the "Perception–Reasoning–Action" pipeline of multimodal agents, making them highly susceptible to such active environmental injection attacks [28]. Experimental results show that these attacks can achieve a success rate of up to 93% on benchmarks like AndroidWorld, highlighting the limited robustness of current multimodal agents [28].

Conclusion

In conclusion, the pervasive threat of cell phone theft and IMEI manipulation, compounded by sophisticated AI-driven attacks on multimodal agents, necessitates a multi-faceted approach to bolster mobile security. This includes enhancing detection and prevention mechanisms for physical theft and IMEI manipulation, alongside developing robust defenses against novel AI threats such as active environment injection attacks and prompt injection attacks [27], [28], [30]. Such attacks exploit critical vulnerabilities in multimodal interaction interfaces and the reasoning processes of AI agents, necessitating a paradigm shift towards security-by-design in their development [27], [28]. This proactive approach mandates the integration of security considerations from the initial stages of AI agent design, addressing vulnerabilities at the architectural level rather than as post-hoc patches [19]. For instance, attackers can embed adversarial instructions within environmental elements to mislead agent decision-making, showcasing the vulnerability of multimodal interaction interfaces to such sophisticated attacks [27], [28]. This inability of AI agents to discern "impostors" or malicious manipulations disguised as environmental elements poses a significant risk, particularly in mobile operating systems where AI agents are becoming increasingly integral to task execution [27], [28]. This underscores the urgent need for novel security architectures, potentially incorporating technologies like blockchain for environmental credibility verification, to counter these advanced threats [28].

References

[1] S. Murugalakshmi, H. M. D. Doreen, and R. C. R. Rene, “Advancements in mobile security: A comprehensive study of SIM card swapping and cloning - trends, challenges and innovative solutions,” i-manager s Journal on Mobile Applications and Technologies , vol. 10, no. 1, p. 23, Jan. 2023, doi: 10.26634/jmt.10.1.20103.

[2] S. J. Alsunaidi and A. M. Almuhaideb, “The Security Risks Associated With IMEIs And Security Solutions,” p. 1, May 2019, doi: 10.1109/cais.2019.8769521.

[3] K. M. Kareem, “The Impact of IMSI Catcher Deployments on Cellular Network Security: Challenges and Countermeasures in 4G and 5G Networks,” arXiv (Cornell University) , May 2024, doi: 10.48550/arxiv.2405.00793.

[4] K. M. Kareem, “The Impact of IMSI Catcher Deployments on Cellular Network Security: Challenges and Countermeasures in 4G and 5G Networks,” May 2024, doi: 10.31234/osf.io/tudc5.

[5] E. N. Ekwonwune, U. C. Chukwuebuka, A. E. Duroha, and A. N. Duru, “Analysis of Global System for Mobile Communication (GSM) Subscription Fraud Detection System,” International Journal of Communications Network and System Sciences , vol. 15, no. 10, p. 167, Jan. 2022, doi: 10.4236/ijcns.2022.1510012.

[6] I. Palamà, F. Gringoli, G. Bianchi, and N. Bléfari-Melazzi, “IMSI Catchers in the wild: A real world 4G/5G assessment,” Computer Networks , vol. 194, p. 108137, May 2021, doi: 10.1016/j.comnet.2021.108137.

[7] F. van den Broek, R. Verdult, and J. de Ruiter, “Defeating IMSI Catchers,” p. 340, Oct. 2015, doi: 10.1145/2810103.2813615.

[8] S. F. Mjølsnes and R. F. Olimid, “Easy 4G/LTE IMSI Catchers for Non-Programmers,” in Lecture notes in computer science , Springer Science+Business Media, 2017, p. 235. doi: 10.1007/978-3-319-65127-9_19.

[9] J. Mundia, E. K. Miriti, S. Mburu, A. M. Kahonge, and C. Chepken, “Assessing Mobile Network Fraud Threats and Prevention Strategies in Kenya,” East African Journal of Information Technology , vol. 7, no. 1, p. 279, Sep. 2024, doi: 10.37284/eajit.7.1.2212.

[10] A. J. Kouam, A. C. Viana, and A. Tchana, “Battle of Wits: To What Extent Can Fraudsters Disguise Their Tracks in International bypass Fraud?,” p. 366, Jun. 2024, doi: 10.1145/3634737.3657023.

[11] J. Shi et al. , “IMS is Not That Secure on Your 5G/4G Phones,” p. 513, May 2024, doi: 10.1145/3636534.3649377.

[12] N. A. Victoire, V. Kombou, T. N. I. Gavilla, F. I. Ndenbe, E. P. Djong-Ignabé, and M. G. Chelaine, “Navigating 5G Network Vulnerabilities: A Comprehensive Survey of Risks and Protective Strategies for Businesses,” Jan. 2024, doi: 10.2139/ssrn.5001492.

[13] U. Sayibu, M. Asante, G. Abdul-Salam, and F. Twum, “Fraud Prediction and Prevention in Mobile Money Payment Systems (MMPS): A Systematic Literature Review of Text-Based Detection Methods,” Security and Communication Networks , vol. 2025, no. 1, Jan. 2025, doi: 10.1155/sec/8913715.

[14] K. O. Phiri and C. Kashale, “Unveiling deception: a socio-economic analysis of smishing attacks on mobile money transaction users,” Humanities and Social Sciences Communications , vol. 12, no. 1, Dec. 2025, doi: 10.1057/s41599-025-06141-8.

[15] E. Kurshan, D. Mehta, B. Bruss, and T. Balch, “AI versus AI in Financial Crimes and Detection: GenAI Crime Waves to Co-Evolutionary AI,” arXiv (Cornell University) , Sep. 2024, doi: 10.48550/arxiv.2410.09066.

[16] E. Mollik and F. A. Majeed, “AI-Driven Cybersecurity in Mobile Financial Services: Enhancing Fraud Detection and Privacy in Emerging Markets,” Journal of Cybersecurity and Privacy , vol. 5, no. 3, p. 77, Sep. 2025, doi: 10.3390/jcp5030077.

[17] M. L. Sanni, B. O. Akinyemi, D. A. Olalere, E. A. Olajubu, and G. A. Aderounmu, “A Predictive Cyber Threat Model for Mobile Money Services,” Annals of Emerging Technologies in Computing , vol. 7, no. 1, p. 40, Jan. 2023, doi: 10.33166/aetic.2023.01.004.

[18] C. Njogu et al. , “Security Gaps in the Mobile Money System in Rwanda: Challenges, Risks and Mitigation,” in Lecture notes in networks and systems , Springer International Publishing, 2024, p. 653. doi: 10.1007/978-3-031-62277-9_42.

[19] Y. Yang et al. , “Systematic Categorization, Construction and Evaluation of New Attacks against Multi-modal Mobile GUI Agents,” arXiv (Cornell University) , Jul. 2024, doi: 10.48550/arxiv.2407.09295.

[20] A. Jha and A. Jha, “Phishing Forensics: A Systematic Approach to Analyzing Mobile and Social Media Fraud,” Journal of Cyber Security , vol. 7, no. 1, p. 109, Jan. 2025, doi: 10.32604/jcs.2025.064429.

[21] M. ADONGO, “Mobile Money Social Engineering Attacks in African Countries: A Survey,” SSRN Electronic Journal , Jan. 2025, doi: 10.2139/ssrn.5257020.

[22] E. Mogaji and N. P. Nguyen, “The dark side of mobile money: Perspectives from an emerging economy,” Technological Forecasting and Social Change , vol. 185, p. 122045, Sep. 2022, doi: 10.1016/j.techfore.2022.122045.

[23] A. Zimba, G. Mukupa, and V. Chama, “On emergent mobile phone-based social engineering cyberattacks in developing countries: The case of the Zambian ICT sector,” African Journal of Science Technology Innovation and Development , vol. 16, no. 6, p. 774, Sep. 2024, doi: 10.1080/20421338.2024.2387886.

[24] D. G. N. Angafor, “Social media security: the impact of AI-generated Whatsapp scams on the security and privacy of Whatsapp community groups,” Computer Science & IT Research Journal , vol. 6, no. 1, p. 1, Jan. 2025, doi: 10.51594/csitrj.v6i1.1793.

[25] Y. Yang et al. , “Systematic Categorization, Construction and Evaluation of New Attacks against Multi-modal Mobile GUI Agents,” 2024, doi: 10.48550/ARXIV.2407.09295.

[26] Y. Chen, X. Hu, K. Yin, J. Li, and S. Zhang, “AEIA-MN: Evaluating the Robustness of Multimodal LLM-Powered Mobile Agents Against Active Environmental Injection Attacks,” arXiv (Cornell University) , Feb. 2025, doi: 10.48550/arxiv.2502.13053.

[27] M. A. Ferrag, D. Hamouda, and M. Debbah, “From Prompt Injections to Protocol Exploits: Threats in LLM-Powered AI Agents Workflows,” arXiv (Cornell University) , Jun. 2025, doi: 10.48550/arxiv.2506.23260.

[28] Y. Chen, X. Hu, K. Yin, J. Li, and S. Zhang, “Evaluating the Robustness of Multimodal Agents Against Active Environmental Injection Attacks,” p. 11648, Oct. 2025, doi: 10.1145/3746027.3755646.

[29] M. A. Hossain, “Assessing the Vulnerabilities of Mobile Banking Applications and Developing Strategies to Improve Their Security,” SSRN Electronic Journal , Jan. 2025, doi: 10.2139/ssrn.5207068.

[30] S. Gulyamov et al. , “Prompt Injection Attacks in Large Language Models and AI Agent Systems: A Comprehensive Review of Vulnerabilities, Attack Vectors, and Defense Mechanisms,” Information , vol. 17, no. 1, p. 54, Jan. 2026, doi: 10.3390/info17010054.