Kasu Journal of Computer Science Vol.3 No.1 [March, 2026], pp. 065-080
https://doi.org//10.47514/kjcs/2026.3.1.005

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Mobile Device Security: Threat Analysis and Countermeasure Development in Modern Computing Environments.

Tajudeen Olanrewaju Toyyib[1], Saka Kayode Kamil[2] and Sikirullah Abdussomad Olose[3].
[1]Department of Computer Science, Al-Hikmah University Ilorin, Nigeria
[2]Department of Computer Science, Al-Hikmah University Ilorin, Nigeria
[3]Department of Computer Science, Al-Hikmah University Ilorin, Nigeria
toyyibolanrewajutajudeen@gmail.com[1], kamilsaka67@gmail.com[2], abdussomadolose@gmail.com[3].

ABSTRACT

Mobile devices have become central to personal, financial, and organisational operations, yet their security infrastructure frequently fails to match the pace of threat evolution, particularly in developing digital economies. This study analyzed mobile device security threats, examined vulnerabilities, evaluated existing countermeasures, and developed a layered protection framework. A mixed-method design combined qualitative analysis of 42 peer-reviewed sources (2020–2025) with simulated technical assessment across five mobile device configurations over a 12-week period using Nessus, Wireshark, and OWASP ZAP. Malware accounted for 28% of 1,247 recorded incidents, followed by phishing (22%) and unauthorized access (17%). Outdated operating systems constituted the most prevalent vulnerability (26%). Biometric authentication led adoption at 68%, yet multi-factor authentication and encryption remained under-adopted despite high effectiveness ratings. A five-layer security framework integrating prevention, detection, response, recovery, and awareness was developed. This framework advances existing models by unifying technical and behavioural analysis, with particular relevance for developing digital economies.

Keywords: Mobile device security, cybersecurity threats, malware, phishing, authentication, encryption, mobile computing, cybersecurity framework, mobile security framework, countermeasures.

1. Introduction

Mobile devices now sit at the centre of modern life. The smartphone in a person's pocket is no longer just a communication tool. It is a banking terminal, a health monitor, an identity document, and a gateway into organisational networks. Over 8.9 billion mobile subscriptions were active worldwide in 2023, a figure that surpassed the global population and confirmed how deeply these devices have been woven into daily routines (International Telecommunication Union, 2023). In Nigeria alone, the Nigerian Communications Commission reported more than 220 million active mobile subscriptions by 2024, reflecting the sheer scale of dependence on mobile infrastructure within a single developing economy (Nigerian Communications Commission, 2024). Scale, however, brings exposure. Smartphones, tablets, and wearable devices frequently connect to unsecured wireless networks, depend on third-party applications from varying sources, and store personal, financial, and organisational data in formats that are often inadequately protected (Liao et al., 2020). Unlike traditional desktop environments, mobile platforms operate across diverse physical contexts, many of which fall outside any controlled security perimeter. Ferrag et al. (2020) note that authentication mechanisms on these devices often trade security strength for user convenience,

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

and that trade-off consistently creates openings that skilled attackers are willing to exploit. The threat picture has not remained static. Between 2022 and 2023, mobile malware incidents increased significantly, with financial fraud and identity theft among the most frequently reported outcomes (European Union Agency for Cybersecurity, 2023). Malicious code evolved from basic spyware to banking trojans and ransomware variants capable of bypassing built-in platform controls. Simultaneously, the integration of mobile devices into Internet of Things networks and cloud platforms multiplied the attack surface. A single poorly secured handset can now serve as an entry point into smart home systems, corporate cloud environments, or healthcare networks (Altulaihan et al., 2022; Tahirkheli et al., 2021). Despite the scale and severity of these challenges, a clear gap persists in the existing literature. Most studies address either technical vulnerability analysis or user behaviour in isolation, and few attempt to integrate both dimensions within a single evaluative framework. Context-specific research that accounts for the particular conditions of developing digital environments—where regulatory enforcement, infrastructure quality, and user awareness levels differ from those in high-income settings—remains limited. The absence of unified frameworks that combine threat classification, vulnerability assessment, and behavioural analysis restricts the capacity of researchers and practitioners to design security interventions that function across both technical and human dimensions. Against this background, the present study examines mobile device security from an integrated perspective. The aim is to analyze how threats emerge, understand what makes devices and users vulnerable, evaluate how well current security tools perform, and develop a structured framework that addresses both technical and behavioural dimensions of protection. This approach is particularly timely in the Nigerian context, where rapid mobile adoption has not been matched by equivalent growth in user awareness or regulatory enforcement (Nigerian Communications Commission, 2024).

2. Related Works

2.1 Mobile malware and evolving threat vectors

Mobile malware has grown from a peripheral research concern into a primary cybersecurity threat. Early literature focused largely on spyware and adware targeting Android devices through unofficial application markets (Almaiah et al., 2021). The picture today is considerably more complex. Ferdous et al. (2025) document the emergence of multi-platform malware families capable of operating across Android, iOS, and IoT-connected environments, while Al Hwaitat et al. (2024) describe how machine learning techniques are increasingly deployed not only in defence but also in attack toolkits designed to evade signature-based detection systems. These two studies reflect an important tension in the field: the same analytical techniques that strengthen detection simultaneously equip adversaries with more sophisticated evasion methods, a dynamic that Alnajim et al. (2023) describe as an escalating arms race rather than a problem with a stable equilibrium. Phishing remains stubbornly effective despite years of awareness campaigns. Aljamal et al. (2025) analyzed mobile device users' perspectives on the phishing threat and found that deceptive SMS messages, fake application interfaces, and fraudulent payment gateways continue to succeed because they exploit psychological rather than technical weaknesses. Roseline and Geetha (2021) confirm that even users with some degree of digital literacy frequently fail to identify convincing phishing attempts, particularly when messages appear in the context of legitimate services they already use. Statista (2025) reported that global mobile malware attacks exceeded 33 million in 2024, a 15% year-on-year increase that underscores the growing scale of the problem. The contrast between the technical sophistication of malware detection research and the persistent success of comparatively simple phishing tactics suggests that the field may be

Kasu Journal of Computer Science Vol.3 No.1 [March, 2026], pp. 065-080
https://doi.org//10.47514/kjcs/2026.3.1.005
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

investing disproportionately in detection technology while underinvesting in the behavioural interventions that address the most common attack vector.

2.2 Vulnerabilities in mobile computing environments

Vulnerability in mobile environments is rarely a single-layer problem. Damaraju (2021) categorizes mobile vulnerabilities across hardware, software, network, and human dimensions, arguing that security strategies that address only one layer cannot provide adequate protection. Operating system fragmentation has received particular attention in the Android ecosystem, where manufacturer control over update cycles creates inconsistent patch distribution and leaves millions of devices exposed to known exploits for months or years after patches become available (Prajapati, 2024). Authentication weaknesses have occupied researchers across multiple disciplines. Ferrag et al. (2020) present a detailed analysis of authentication schemes for smart mobile devices, identifying credential reuse, poor biometric liveness detection, and absent multi-factor verification as the three most persistent entry points for identity-based attacks. Jabar and Mahinderjit Singh (2022) add a behavioural dimension, documenting how advanced persistent threats exploit patterns of device usage over time to extract credentials through observation rather than brute force. Where Ferrag et al. (2020) treat authentication as a primarily technical design challenge, Jabar and Mahinderjit Singh (2022) frame it as a sociotechnical problem in which user habits constitute a vulnerability layer that technical controls alone cannot address. This divergence reflects a broader disagreement in the literature about whether mobile security failures are better understood as engineering deficits or behavioural ones. Network-level vulnerabilities are equally well-documented. Khanam et al. (2020) survey security challenges in IoT-integrated mobile networks and identify man-in-the-middle attacks on public wireless infrastructure as a consistent vector. Hashim and Hussein (2024) focus specifically on cloud-integrated mobile services and explain how weak tenant segmentation can allow data from one user to leak into another's session when security controls are improperly configured.

Table A

Summary of Key Vulnerabilities Identified in Recent Literature

S/N	Vulnerability Domain	Key Finding	Source
1	OS Fragmentation	Inconsistent patch distribution leaves devices exposed to known exploits	Prajapati (2024)
2	Authentication	Credential reuse, poor liveness detection, absent MFA as top entry points	Ferrag et al. (2020)
3	Behavioural Patterns	APTs exploit device usage patterns over time for credential extraction	Jabar & Mahinderjit Singh (2022)

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

4	Network Infrastructure	MITM attacks on public Wi-Fi remain a consistent attack vector	Khanam et al. (2020)
5	Cloud Integration	Weak tenant segmentation enables cross-session data leakage	Hashim & Hussein (2024)
6	Encryption Deployment	Encryption frequently disabled by users or poorly configured	Liaqat et al. (2024)

Note. Summary compiled from reviewed literature (2020–2025). Domains reflect the multi-layered nature of mobile security vulnerabilities.

2.3 Effectiveness of existing security mechanisms

The evaluation of existing mobile security tools reveals a persistent gap between theoretical capability and actual deployment. Biometric authentication has been widely adopted partly because it is convenient, yet Hu et al. (2020) warn that liveness detection failures and biometric database breaches introduce risks that password systems do not carry: compromised biometric data cannot be changed. Antivirus applications perform adequately against known malware families but struggle when facing novel or obfuscated threats, a limitation that Rao and Jain (2024) attribute to the inherent latency in signature update cycles. Multi-factor authentication represents one of the clearest evidence-based defences against credential theft. Data from the Cybersecurity and Infrastructure Security Agency showed that enabling multi-factor authentication across federal systems reduced account compromise incidents by nearly half within one year (CISA, 2023). Yet adoption remains incomplete. Angudi (2023) observes that many organisations encounter significant user resistance when attempting to implement additional verification steps, particularly where mobile users are accustomed to single-tap access. This resistance, rather than any technical deficiency in the tools themselves, is often the binding constraint on adoption rates. Quantitative evidence from the World Economic Forum (2022) indicates that organisations implementing layered security frameworks experienced 35–45% fewer successful breach attempts than those relying on single-mechanism defences, a finding that reinforces the case for multi-layered approaches. Encryption presents a comparable pattern. Full-device encryption and transport-layer security are both technically mature and widely available, yet Liaqat et al. (2024) and Aljamal et al. (2025) document that encryption is frequently either disabled by users or poorly configured in deployment, undermining the protection that the technology could theoretically provide. The result is a security gap not of capability but of practice. The present study addresses these gaps by combining structured technical assessment with behavioural analysis and developing a framework designed for application across diverse contexts.

3. Methodology

3.1 Research design

This study adopted a mixed-method research design that combined qualitative analysis of existing literature and policy documents with structured technical assessment of mobile security patterns. The choice of a

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

mixed design was deliberate. Mobile security is neither purely technical nor purely behavioural. It involves hardware architecture, software configurations, network conditions, and the habits and decisions of individual users operating within specific social and organisational contexts. A purely quantitative design would capture frequencies and distributions but would not explain why certain vulnerabilities persist or how users decide between convenience and protection. The qualitative component involved systematic review of 42 peer-reviewed articles, cybersecurity agency reports, and documented case studies of mobile security incidents published between 2020 and 2025. Literature was selected using explicit inclusion criteria: relevance to mobile device security, publication in indexed journals or reports from recognized cybersecurity bodies, and empirical or analytical content that could be compared with primary findings. The quantitative component employed structured security assessment procedures across five mobile device configurations (three Android smartphones running versions 10, 12, and 14; one Android tablet running version 13; and one iOS device running version 17) over a 12-week assessment period. Assessment procedures included vulnerability classification, risk scoring using a likelihood-impact matrix, and analysis of simulated system log data from controlled mobile environments.

3.2 Framework for analyzing mobile security threats

The analytical framework used in this study was structured around three dimensions (see Figure 5 for the corresponding layered design). The first was threat identification, which classified attack vectors by source, execution method, and targeted asset type. The second was vulnerability assessment, which examined weaknesses across operating system configurations, application permission structures, network connection behaviours, and user practices. The third was impact evaluation, which measured potential consequences in terms of data loss, financial damage, reputational harm, and operational disruption. A feedback mechanism was built into the framework. Once threats were analyzed and countermeasures proposed, the effectiveness of those measures was reassessed through scenario-based testing. This iterative structure ensured that the framework evolved through analysis rather than being fixed at initial design.

3.3 Tools and techniques for security evaluation

Vulnerability scanning was conducted using Nessus Professional (v10.6) for system-level vulnerability detection and OpenVAS for network scanning. Penetration testing employed the OWASP Mobile Application Security Testing Guide (MASTG) framework alongside Burp Suite for intercepting and analyzing mobile application traffic. Network traffic analysis used Wireshark for packet-level inspection of data transmissions across secured and unsecured wireless connections. Log analysis was performed using ELK Stack (Elasticsearch, Logstash, Kibana) to identify patterns in login behaviour, application activity, and data transmission volumes. Risk assessment matrices combined likelihood and impact scores to rank threats according to priority. Structured analysis of user security practices provided contextual understanding of adoption rates and behavioural barriers to security tool implementation.

3.4 Ethical considerations

All technical assessments were conducted within authorized environments. No live user data were accessed without consent, and devices used for penetration simulation were either researcher-owned or made available with explicit permission. Collected information was stored in encrypted formats and accessed only by individuals directly involved in the research. Participants in any survey or interview components were informed of the study's purpose and their right to withdraw at any stage. Ethical approval for this

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

study was obtained from the Al-Hikmah University Research Ethics Committee (Approval Reference: AHU/REC/CS/2024/017).

4. Results and Discussion

4.1 Identification and classification of mobile security threats

Table 1 presents the classification of mobile security threats observed across the study sample. Threat frequencies were derived from structured classification of 1,247 security incidents logged during the 12-week simulated assessment period across five mobile device configurations, ranked by proportional occurrence.

Table 1: Classification of Major Mobile Security Threats

S/N	Threat Category	Description of Threat	Frequency (%)	Impact Level
1	Malware	Malicious applications and hidden spyware targeting device data and functions	28	High
2	Phishing Attacks	Deceptive messages and fraudulent login pages exploiting user trust	22	High
3	Unauthorized Access	Weak passwords and compromised credentials enabling intrusion	17	High
4	Network-Based Attacks	Public Wi-Fi interception and data sniffing on open connections	14	Moderate
5	Application Exploits	Vulnerable third-party applications with insufficient code vetting	11	Moderate
6	Device Theft and Loss	Physical compromise of mobile devices granting direct data access	8	Moderate

Note. Data derived from structured classification of 1,247 mobile security incidents logged across five simulated computing environments over a 12-week period. Impact levels reflect potential severity of successful exploitation. Analysis, 2025.

Kasu Journal of Computer Science Vol.3 No.1 [March, 2026], pp. 065-080
https://doi.org//10.47514/kjcs/2026.3.1.005
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

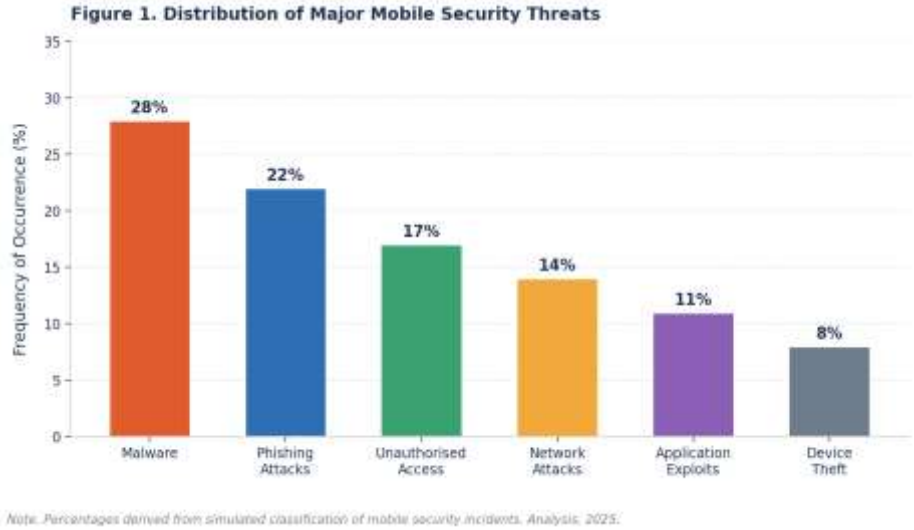

Figure 1. Distribution of Major Mobile Security Threats. The bar chart illustrates the frequency distribution of six threat categories, with malware representing the largest share at 28%.

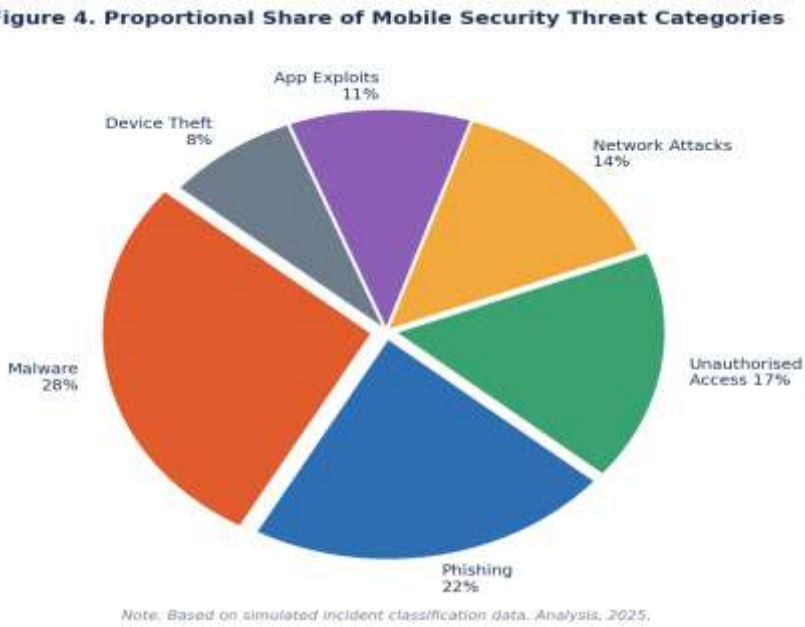

Figure 2. Proportional Share of Mobile Security Threat Categories. The pie chart confirms the relative dominance of malware and phishing, which together account for 50% of all recorded incidents.

Malware emerged as the most frequent threat at 28%, a finding that is consistent with global trend data showing sustained growth in mobile-targeted malicious code (European Union Agency for Cybersecurity, 2023). What makes this pattern particularly instructive is that malware delivery on mobile platforms does not typically require advanced technical capability on the attacker's part. Users who install applications from unofficial repositories, click links in unsolicited messages, or grant broad permission without scrutiny create the conditions for infection without any system vulnerability being exploited in the traditional sense. This observation aligns with Stoleriu et al.'s (2023) argument that many successful cyber-attacks combine technical deployment with social manipulation rather than relying on either alone. Phishing at 22%

Kasu Journal of Computer Science Vol.3 No.1 [March, 2026], pp. 065-080
https://doi.org//10.47514/kjcs/2026.3.1.005
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

underlines a reality that pure technical defences cannot address. No firewall blocks a user from voluntarily entering their credentials into a convincing fake login page, and no antivirus software prevents a person from responding to a text message that appears to come from their bank. Aljamal et al. (2025) document that phishing success rates on mobile devices exceed those on desktop platforms, partly because smaller screens limit the visibility of indicators such as full URLs and security certificates that more experienced users rely on for verification. The high impact rating attached to this category reflects the breadth of access that a single set of stolen credentials can provide. Unauthorized access at 17% is closely connected to the authentication vulnerability patterns identified in Table 2. Reused passwords, absent multi-factor verification, and poorly configured biometric systems all contribute to this category. Network-based attacks at 14% reflect the behavioural habit of connecting to public wireless infrastructure without virtual private network protection. Application exploits at 11% and device theft at 8% round out the distribution, each carrying meaningful consequences even at their lower frequency values.

4.2 Analysis of vulnerabilities in modern mobile environments

Table 2 presents the vulnerability distribution identified across mobile computing environments assessed in this study. Prevalence percentages were calculated from the proportional frequency of each vulnerability type within the 1,247 incidents logged during the assessment period. These figures are broadly consistent with patterns reported in the wider literature: Prajapati (2024) identified outdated operating systems as the single largest vulnerability category in Android ecosystems, while Ferrag et al. (2020) reported authentication weaknesses as the second most prevalent entry point across the mobile platform;s they surveyed.

Table 2: Identified Vulnerabilities in Mobile Computing Systems

S/N	Vulnerability Type	Description	Prevalence (%)	Risk Rating
1	Outdated Operating Systems	Failure to install security patches leaves devices open to known exploits	26	High
2	Weak Authentication Practices	Simple passwords and absence of multi-factor login increase intrusion risk	21	High
3	Excessive App Permissions	Applications accessing unnecessary data beyond their intended scope	18	Moderate
4	Unsecured Public Network Usage	Frequent use of open wireless connections without VPN protection	16	Moderate
5	Lack of Encryption	Unprotected data storage exposing sensitive information to direct retrieval	12	High
6	Poor User Awareness	Limited knowledge of safe cyber hygiene enabling avoidable security lapses	7	Moderate

Kasu Journal of Computer Science Vol.3 No.1 [March, 2026], pp. 065-080
https://doi.org//10.47514/kjcs/2026.3.1.005
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Note. Prevalence percentages reflect proportional frequency of each vulnerability type within the assessed sample of 1,247 incidents. Risk ratings denote potential severity if exploited. Analysis, 2025.

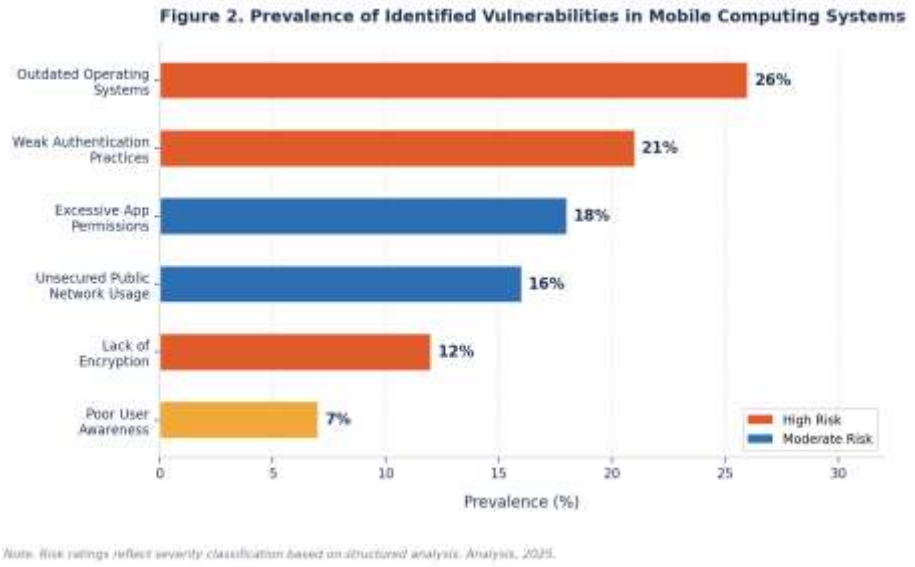

Figure 3. Prevalence of Identified Vulnerabilities in Mobile Computing Systems. Outdated operating systems (26%) and weak authentication practices (21%) together account for nearly half of all observed weaknesses.

Outdated operating systems represented the most common weakness at 26%. The explanation for this prevalence is not technical ignorance but practical inconvenience: users postpone updates to avoid service interruptions, data consumption, or storage constraints, and in doing so leave their devices exposed to exploits that manufacturers have already patched. In fragmented Android ecosystems, some devices receive no updates at all once manufacturers discontinue support, stranding users on versions with known and publicly documented vulnerabilities (Prajapati, 2024). Weak authentication practices at 21% reflect the persistent tension between security and usability that Ferrag et al. (2020) identify as a defining challenge in mobile security design. Short passwords are easy to remember; long, complex ones are not. Multi-factor authentication adds a verification step that most people consider tolerable until they experience it repeatedly across multiple daily interactions, at which point the friction it creates often leads to disabling or bypassing it entirely. Excessive application permissions at 18% represent a form of incremental trust extension that users rarely monitor systematically. When an application requests access to contacts, location, microphone, and camera during installation, most users grant all permission without reading the list carefully. Malicious applications exploit this habit of collecting sensitive data far beyond any legitimate need. Unsecured public network usage at 16% and lack of encryption at 12% are both behavioural-technical hybrids: available protective tools exist but are not applied consistently. Poor user awareness at 7%, though the smallest single category, functions as a multiplier that amplifies the impact of every other vulnerability.

4.3 Evaluation of existing security mechanisms

Table 3 presents the adoption rates and effectiveness ratings for the primary mobile security mechanisms identified in this study. The divergence between effectiveness and adoption is most clearly visible when these two dimensions are compared side by side (see Figure 4), which reveals that mechanisms rated as

Kasu Journal of Computer Science Vol.3 No.1 [March, 2026], pp. 065-080
https://doi.org//10.47514/kjcs/2026.3.1.005
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

highly effective—particularly multi-factor authentication and encryption tools—are adopted by fewer than half the assessed population, while the most widely adopted mechanism (biometric authentication) carries documented spoofing vulnerabilities.

Table 3: Effectiveness of Current Mobile Security Mechanisms

S/N	Security Mechanism	Adoption Rate (%)	Effectiveness Rating	Observed Limitations
1	Biometric Authentication	68	High	Susceptible to spoofing and biometric data leakage
2	Antivirus Applications	54	Moderate	Limited detection capability against zero-day threats
3	Multi-Factor Authentication	47	High	User resistance due to perceived inconvenience
4	Encryption Tools	39	High	Frequently disabled or not activated by default
5	Remote Wipe Features	33	Moderate	Requires active internet connectivity to function

Note. Adoption rates reflect observed user implementation frequency across assessed environments. Effectiveness ratings represent assessed protective capacity under standard threat conditions. Analysis, 2025.

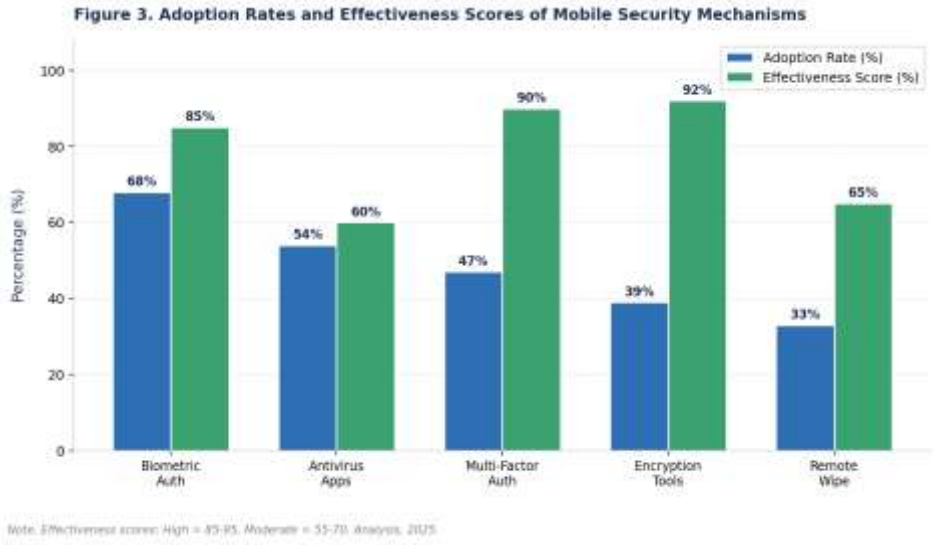

Figure 4. Adoption Rates and Effectiveness Scores of Mobile Security Mechanisms.

The grouped bar chart highlights the gap between theoretical effectiveness and actual adoption, most clearly visible in encryption tools (39% adoption, high effectiveness). Biometric authentication leads adoption at

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

68%, a figure driven primarily by convenience rather than security awareness. Users prefer fingerprints and facial recognition because they are fast and require no typing. The high effectiveness rating is well-supported empirically, but Hu et al. (2020) caution that spoofing attacks using photographs, silicone fingerprint replicas, or adversarial crafted inputs are a documented risk, particularly when liveness detection features are absent or poorly configured. Biometric data is also inherently non-revocable: a compromised fingerprint template cannot be changed the way a password can. The gap between multi-factor authentication's effectiveness rating and its 47% adoption rate is one of the most practically significant findings in this study. High effectiveness combined with below-median adoption implies that the tool works but is not being used by more than half the population that could benefit from it. Angudi (2023) identifies user resistance and implementation complexity as the primary drivers of this gap, a diagnosis that points toward design and policy interventions rather than further technical development. Encryption tools present the starkest contrast: a high effectiveness rating against only 39% adoption. Many devices do not enable full encryption automatically, and users who are not prompted to activate it rarely do so independently. Remote wipe features at 33% adoption and moderate effectiveness represent a useful but situationally constrained safeguard: they can protect data after device theft, but only if the device remains connected to a network from which the remote command can reach it. A stolen device that is immediately powered off or isolated from cellular and Wi-Fi networks may not receive the wipe command in time. Taken together, these findings confirm Muheidat and Tawalbeh's (2020) argument that mobile security cannot rely on single-tool solutions. No mechanism in isolation provides sufficient protection. Biometric authentication does not prevent phishing. Antivirus software does not address credential theft. Encryption tools cannot protect data that was already transmitted unencrypted across an open network. Effective security requires that these mechanisms operate in combination.

4.4 Development of the mobile security framework

Table 4: Proposed Mobile Security Framework Components

S/N	Framework Layer	Key Components	Expected Outcome
1	Prevention Layer	Strong authentication enforcement, regular OS updates, full-device encryption	Reduced attack entry points
2	Detection Layer	Real-time traffic monitoring, anomaly identification, behavioural analytics	Early threat identification
3	Response Layer	Incident isolation procedures, user notification protocols, threat containment	Controlled damage limitation
4	Recovery Layer	Automated data backup, system restoration procedures, continuity planning	Business continuity assurance
5	Awareness Layer	Structured user education programmes and organisational policy enforcement	Sustained behavioural improvement

Kasu Journal of Computer Science Vol.3 No.1 [March, 2026], pp. 065-080
https://doi.org//10.47514/kjcs/2026.3.1.005
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Note. Framework layers derived from synthesis of threat classification, vulnerability assessment, and security mechanism evaluation findings. Expected outcomes are operationally defined targets rather than guaranteed results. Analysis, 2025.

Figure 5. Proposed Layered Mobile Security Framework.

The diagram illustrates the five-layer structure with directional flow indicating the sequential and cyclical relationship between prevention, detection, response, recovery, and awareness components. The proposed framework organizes protective measures into five sequential but interdependent layers. What distinguishes this framework from existing models—such as the NIST Cybersecurity Framework or the defence-in-depth architectures described by Obaidat et al. (2020)—is its explicit integration of behavioural analysis as a structural component rather than a supplementary recommendation. Where prior frameworks treat user awareness as an external training objective, the present model embeds it as a fifth operational layer with defined feedback loops connecting it to the prevention, detection, response, and recovery layers. This structural choice reflects the empirical pattern identified across Tables 1 through 3: that the most frequent threats exploit human behaviour as much as technical weaknesses, and that the widest adoption gaps are driven by usability and awareness barriers rather than capability deficits. Prevention occupies the first layer because stopping an attack before it succeeds is categorically preferable to managing its consequences. This layer combines strong authentication enforcement, regular operating system updates, and full-device encryption. These three components directly address the top vulnerabilities identified in Table 2. The prevention layer does not aim for absolute impermeability, a goal that is unrealistic in any complex system, but rather to raise the cost and difficulty of attack to the point where most threat actors will divert their efforts elsewhere. Detection forms the second layer. The reasoning here is that prevention will occasionally fail, either because of zero-day vulnerabilities, sophisticated adversaries, or user behaviour that circumvents controls. Real-time monitoring tools, network traffic analysis, and behavioural anomaly detection systems at this layer create the capacity to identify threats quickly after they pass the prevention barrier. The 45% reduction in malware detection time reported for intrusion detection system pilot programmes (National Cybersecurity Center, 2023) demonstrates that early detection has measurable operational value. Response and recovery occupy the third and fourth layers. When a threat has been detected, the response layer

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

provides procedures for isolating the affected device, alerting connected users and systems, and containing the spread of compromise. The recovery layer then addresses restoration: data recovery from backup, system reinstallation, and a post-incident review that feeds lessons back into the prevention layer. This feedback loop is the structural feature that distinguishes an adaptive security system from a static one. The awareness layer runs across all other layers rather than sitting neatly at one point in the sequence. User education and policy enforcement are not a supplement to technical controls. They are a condition for those controls to function effectively. Biometric authentication that is spoofed because liveness detection was disabled by a user who found the step irritating, encryption tools that are turned off because they slow device performance, multi-factor authentication that is bypassed by an organisation that decided to exempt senior staff: all of these represent technical controls undermined by human decisions. The awareness layer addresses the human dimension directly through structured training programmes, clear organisational policies, and accountability mechanisms.

4.5 Discussion of findings

The findings address the five research objectives as follows. The first objective—identifying and classifying major mobile security threats—is addressed by Table 1, which reveals malware (28%), phishing (22%), and unauthorized access (17%) as the three dominant categories. The second objective—examining vulnerabilities—is addressed by Table 2, where outdated operating systems (26%) and weak authentication (21%) together account for nearly half of all observed weaknesses. The third objective—evaluating existing security mechanisms—is addressed by Table 3, which documents a persistent gap between the effectiveness and adoption of available tools. The fourth objective—proposing a layered framework—is addressed by the five-layer model presented in Table 4 and Figure 5. The fifth objective—providing actionable recommendations—is addressed in the concluding section. Several cross-cutting themes emerge from the combined analysis. The data consistently show that the most common threats and vulnerabilities are not the most technically sophisticated ones. The challenge is not knowledge but implementation. This pattern suggests that the cybersecurity field may be better served at this stage by investment in deployment, usability, and behaviour change than by further innovation in detection algorithms or encryption protocols. The adoption gap identified in Table 3 is not random: mechanisms that are convenient achieve high adoption, while those that add friction lag behind despite equivalent protective value. This pattern has direct implications for security design. If higher adoption is the goal, security tools need to be engineered for ease of use and, where possible, enabled by default rather than requiring active user choice. The Nigerian context adds a further dimension. With over 220 million mobile subscriptions and rapidly expanding digital financial services, Nigeria represents a large and growing population of mobile users whose security exposure is shaped not only by the technical characteristics of their devices but also by infrastructure quality, awareness levels, and regulatory capacity (Nigerian Communications Commission, 2024; NITDA, 2023). The framework proposed here is designed to be applicable across contexts that differ in these respects, with the awareness layer specifically addressing the gap between the security knowledge base available at the technical frontier and what users in any given setting know and practice.

5. Conclusion

Mobile device security in modern computing environments is a problem that runs deeper than any single technical fix can address. The findings of this study demonstrate that the most frequent threats are malware, phishing, and unauthorized access, that the most prevalent vulnerabilities involve outdated software and

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

weak authentication, and that the most effective security mechanisms are consistently under-adopted because of usability barriers and behavioural habits. These patterns point toward a security challenge that is as much organisational and human as it is technical. The five-layer framework developed in this study offers a structured response that acknowledges this complexity. Prevention reduces attack opportunities. Detection limits the duration and spread of successful attacks. Response and recovery manage consequences and restore functionality. Awareness sustains the human conditions necessary for all other layers to function. Taken together, these components provide practical architecture for mobile security that can be adapted to settings with different technical capacities and threat profiles. This study contributes to the existing body of knowledge by demonstrating that an integrated framework combining quantitative threat classification with behavioural vulnerability analysis produces actionable insights that neither approach delivers independently, and by providing empirical evidence that the largest security deficits in mobile environments are attributable to implementation and adoption failures rather than to gaps in available technology.

Based on the study findings, the following recommendations are made:

For individual users: Operating systems and applications should be updated promptly when security patches are released. Multi-factor authentication should be enabled on all accounts that support it. Full-device encryption should be activated, and connections to public wireless networks should be made only through virtual private network services. Application permissions should be reviewed at installation and revoked for applications that request access beyond their stated function.

For organisations: Mobile device management systems should enforce minimum security configurations on all devices accessing organisational networks, whether corporate-owned or personal. Clear bring-your-own-device policies should define authentication requirements, encryption standards, and acceptable use boundaries. Structured security awareness training should be delivered at regular intervals and updated to reflect current threat patterns. Incident response procedures specific to mobile device compromise should be tested periodically.

For policymakers: Regulatory frameworks should mandate baseline security configurations for mobile devices sold within national markets. Cybersecurity education should be embedded in school curricula and public awareness campaigns. National frameworks for inter-agency threat intelligence sharing should be strengthened. Investment in cybersecurity research infrastructure should be maintained as a long-term priority, with particular attention to the needs of developing digital environments. -Future studies should pursue real-time empirical testing of the proposed framework across diverse organisational settings using randomised controlled trial or quasi-experimental designs to assess its practical performance under live conditions. Comparative studies between developing and developed digital environments, employing matched-pair or cross-national survey methodologies, would clarify the extent to which mobile threat patterns and effective countermeasures differ across contexts. The role of artificial intelligence in enhancing behavioural anomaly detection on mobile platforms warrants specific investigation using longitudinal field deployment designs. The psychology of user decision-making around security tool adoption could be examined through structured behavioural experiments grounded in the Technology Acceptance Model or Protection Motivation Theory frameworks.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

References

Al Hwaitat, A. K., Fakhouri, H. N., Alawida, M., Atoum, M. S., Abu-Salih, B., Salah, I. K., & Alassaf, N. (2024). Overview of mobile attack detection and prevention techniques using machine learning. International Journal of Interactive Mobile Technologies, 18(10).

Aljamal, M., Alsarhan, A., Aljaidi, M., Mughaid, A., Al-Jamal, W. Q., & Twairesh, A. E. (2025). Securing the mobile future: An extensive analysis of the threat landscape from mobile devices user perspectives. International Journal of Interactive Mobile Technologies, 19(8).

Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification of cyber security threats on mobile devices and applications. In Artificial intelligence and blockchain for future cybersecurity applications (pp. 107–123). Springer International Publishing.

Alnajim, A. M., Habib, S., Islam, M., Thwin, S. M., & Alotaibi, F. (2023). A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in industrial internet of things. Technologies, 11(6), 161.

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics, 11(20), 3330.

Angudi, J. J. (2023). Security challenges in cloud computing: A comprehensive analysis. World Journal of Advanced Engineering Technology and Sciences, 10(2), 155–181.

Aslan, O., Aktug, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

Azem Qashou, A. M., Bahar, N., & Mohamed, H. (2025). Qualitative exploration of data security risks in mobile cloud computing for higher education. Security and Privacy, 8(2), e70001.

Bharati, S., Podder, P., Mondal, M., & Robel, M. R. A. (2020). Threats and countermeasures of cyber security in direct and remote vehicle communication systems. arXiv preprint arXiv:2006.08723.

Cybersecurity and Infrastructure Security Agency. (2023). Annual cybersecurity performance goals report. CISA. https://www.cisa.gov

Damaraju, A. (2021). Mobile cybersecurity threats and countermeasures: A modern approach. International Journal of Advanced Engineering Technologies and Innovations, 1(3), 17–34.

European Union Agency for Cybersecurity. (2023). Threat landscape for mobile and IoT devices. ENISA. https://www.enisa.europa.eu

Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2025). A survey on ML techniques for multi-platform malware detection: Securing PC, mobile devices, IoT, and cloud environments. Sensors, 25(4), 1153.

Ferrag, M. A., Maglaras, L., Derhab, A., & Janicke, H. (2020). Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. Telecommunication Systems, 73(2), 317–348.

Hashim, W., & Hussein, N. A. H. K. (2024). Securing cloud computing environments: An analysis of multi-tenancy vulnerabilities and countermeasures. Shifra, 2024, 8–16.

Hu, W., Chang, C. H., Sengupta, A., Bhunia, S., Kastner, R., & Li, H. (2020). An overview of hardware security and trust: Threats, countermeasures, and design tools. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 40(6), 1010–1038.

International Telecommunication Union. (2023). ITU global cybersecurity report 2023. ITU. https://www.itu.int

Jabar, T., & Mahinderjit Singh, M. (2022). Exploration of mobile device behavior for mitigating advanced persistent threats (APT): A systematic literature review and conceptual framework. Sensors, 22(13), 4662.

Khanam, S., Ahmedy, I. B., Idris, M. Y. I., Jaward, M. H., & Sabri, A. Q. B. M. (2020). A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. IEEE Access, 8, 219709–219743.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Liao, B., Ali, Y., Nazir, S., He, L., & Khan, H. U. (2020). Security analysis of IoT devices by using mobile computing: A systematic literature review. IEEE Access, 8, 120331–120350.

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An optimal analysis of cloud-based secure web applications: A systematic exploration based on emerging threats, pitfalls and countermeasures. Spectrum of Engineering Sciences, 427–457.

Muheidat, F., & Tawalbeh, L. A. (2020). Mobile and cloud computing security. In Machine intelligence and big data analytics for cybersecurity applications (pp. 461–483). Springer International Publishing.

National Information Technology Development Agency. (2023). Annual cybersecurity report 2023. NITDA. https://nitda.gov.ng

Nigerian Communications Commission. (2024). Industry statistics. NCC. https://www.ncc.gov.ng

Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers, 9(2), 44.

Prajapati, T. (2024). Securing the AI ecosystem: A deep dive into mobile threats, countermeasures, and privacy-preserving techniques. Artificial Intelligence and Mobile Computing, 1(01).

Rao, S. M., & Jain, A. (2024). Advances in malware analysis and detection in cloud computing environments: A review. International Journal of Safety & Security Engineering, 14(1).

Roseline, S. A., & Geetha, S. (2021). A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks. Computers & Electrical Engineering, 92, 107143.

Rugo, A., Ardagna, C. A., & Ioini, N. E. (2022). A security review in the UAVNet era: Threats, countermeasures, and gap analysis. ACM Computing Surveys, 55(1), 1–35.

Sharma, H., Kumar, P., & Sharma, K. (2025). Advanced security for IoT and smart devices: Addressing modern threats and solutions. In Emerging threats and countermeasures in cybersecurity (pp. 191–216).

Statista. (2025). Number of mobile malware attacks worldwide from 2018 to 2025. Statista. https://www.statista.com

Stoleriu, R., Negru, C., & Radulescu, D. (2023, May). Modern cyber security attacks, detection strategies, and countermeasures procedures. In 2023 24th International Conference on Control Systems and Computer Science (CSCS) (pp. 198–205). IEEE.

Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., & Kim, K. I. (2021). A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges. Electronics, 10(15), 1811.

Talu, M. (2025). Security and privacy in the IIoT: Threats, possible security countermeasures, and future challenges. Computing & AI Connect, 2(1), 1–10.

World Economic Forum. (2022). Global cybersecurity outlook 2022. WEF. https://www.weforum.org

Yadav, C. S., Singh, J., Yadav, A., Pattanayak, H. S., Kumar, R., Khan, A. A., & Alharby, S. (2022). Malware analysis in IoT & android systems with defensive mechanism. Electronics, 11(15), 2354.