



Review of Lightweight Cryptography for Mobile Phone Security Against Modern Cyber Threats

¹Nandini Sharma, ²Dr. Naveen Kumar Singh

¹Research Scholar, ²Professor

^{1/2}Computer Science & Engineering, Dept. of Engineering & Technology, HRIT, Ghaziabad

¹nandininov05@gmail.com, ²focanaveen@hrituniversity.edu.in

<https://doi.org/10.64882/ijrt.v14.i3.1804>

ABSTRACT

Mobile phones have become the primary computing platform for personal and financial data, yet they operate under strict constraints of battery life, memory, and processing power that limit the practicality of conventional cryptographic standards such as AES and RSA. This paper presents a review of the literature on lightweight cryptography (LWC) as a mechanism for securing mobile phones against modern cyber threats, including malware, network interception, and behavioural exploitation. Drawing on twenty-five peer-reviewed sources published between 2015 and 2024, the review examines the design principles of lightweight cryptographic algorithms, the evolving mobile malware landscape, the standardisation efforts led by the National Institute of Standards and Technology (NIST), and the existing frameworks proposed for constrained-device security. The review finds that while lightweight cryptographic algorithms have matured considerably in terms of theoretical security and implementation efficiency, comparatively few studies evaluate these algorithms within complete, real-device mobile security frameworks that explicitly address contemporary malware threats. The paper concludes by identifying this integration gap and proposing directions for future research, including real-device benchmarking, threat-model-driven framework design, and the co-design of cryptographic and detection-based defences.

Keywords: Lightweight cryptography; mobile phone security; cyber threats; malware detection; authenticated encryption; NIST standardisation.

1. INTRODUCTION

1.1 Background of Mobile Phone Security

Mobile phones have evolved from simple communication devices into general-purpose computing platforms that store banking credentials, personal identification, health information, and enterprise data. This transformation has made smartphones an attractive target for cybercriminals, and the resource limitations inherent to mobile hardware, including constrained battery capacity, limited processing power, and restricted memory, mean that security mechanisms designed for desktop or server environments are often poorly suited to mobile deployment (Dhanda et al., 2020). Conventional cryptographic standards such as the Advanced Encryption Standard (AES) and RSA remain mathematically secure, but their computational overhead can degrade device performance and battery life when applied continuously across the volume of data a modern smartphone process (Suryateja & Rao,



2024). This tension between security strength and resource efficiency forms the central motivation for lightweight cryptography research.

The scale of this challenge is amplified by the sheer diversity of the mobile device ecosystem, which spans budget handsets with modest processors to flagship devices with considerable computational headroom, meaning that any proposed security mechanism must remain effective across a wide spectrum of hardware capability. Amrita et al. (2024) note that this heterogeneity has driven researchers to favour cryptographic designs that scale gracefully across processor architectures rather than assuming a single, high-performance computing environment, a consideration that distinguishes mobile-oriented cryptographic research from cryptography designed purely for server or cloud infrastructure.

1.2 The Modern Cyber Threat Landscape for Mobile Devices

The threats facing mobile devices have grown substantially in scale and sophistication over the past decade. Qamar et al. (2019) categorise mobile malware according to infection vector and payload behaviour, noting a marked shift toward data exfiltration and banking-credential theft as dominant attack objectives. Garg and Baliyan (2021) similarly document how the Android permission model and inter-component communication architecture have been repeatedly exploited to grant malicious applications disproportionate access to sensitive data. These findings collectively demonstrate that mobile phones face a persistent and evolving risk profile that extends beyond traditional malware to include network-based interception and platform-level architectural weaknesses.

This evolving risk profile is further compounded by the increasing use of obfuscation and evasion techniques by malware authors, which limit the effectiveness of purely signature-based detection tools. Razgallah et al. (2021) observe that malicious applications increasingly exploit legitimate system permissions and background services to carry out data harvesting activities without triggering conventional security alerts, meaning that reliance on detection alone leaves a residual window of vulnerability during which sensitive data may be exposed. This residual risk directly motivates the case for strong, efficient encryption as a complementary, preventive layer of defence, rather than viewing detection and encryption as substitutable security controls.

1.3 The Need for Lightweight Cryptography

Lightweight cryptography has emerged as a response to the specific constraints of mobile and embedded devices, offering cryptographic primitives engineered explicitly to balance security strength against implementation cost (Amrita et al., 2024). Unlike conventional cryptography, which assumes abundant computational resources, lightweight cryptographic design prioritises compact code size, low energy consumption, and efficient hardware implementation without unduly compromising security margins (Rana et al., 2022). This design philosophy has been substantially advanced by the National Institute of Standards and Technology (NIST), whose multi-year standardisation process has provided a common evaluation framework against which candidate algorithms can be assessed (Turan et al., 2021).



The importance of this standardisation effort should not be understated: prior to the emergence of a common evaluation methodology, lightweight cryptographic proposals were frequently assessed using inconsistent benchmarks, making it difficult for practitioners to compare competing algorithms on equal terms. Karthik and Rengarajan (2024) argue that the resulting convergence toward standardisation-compliant algorithms has strengthened practitioner confidence in lightweight cryptography as a viable alternative to conventional cryptographic standards, particularly for applications, such as mobile phone security, where the constraints of the deployment environment make conventional cryptography a genuinely costly proposition rather than merely a theoretical inconvenience.

1.4 Objectives and Scope of the Review

This review paper aims to synthesise the existing literature on lightweight cryptography as it relates specifically to mobile phone security, with three primary objectives. First, to examine the algorithmic and standardisation developments that have shaped the field of lightweight cryptography. Second, to characterise the modern cyber threat landscape facing mobile devices, drawing on the malware detection and security assessment literature. Third, to critically evaluate the extent to which existing cryptography-based frameworks address these threats in an integrated, mobile-specific manner. The scope of the review is limited to peer-reviewed sources published between 2015 and 2024, focusing on studies directly relevant to lightweight cryptographic algorithm design, mobile malware characterisation, and constrained-device security frameworks.

By combining these two historically separate strands of research, cryptographic algorithm design and mobile threat characterisation, within a single review, this paper seeks to provide a more integrated foundation for practitioners and researchers seeking to design mobile security solutions that are both cryptographically sound and empirically responsive to real-world threat conditions. The remainder of this paper is organised as follows: Section 4 presents the literature review across four thematic subheadings, supported by three comparative tables; Section 5 outlines the research methodology adopted in conducting this review; Section 6 presents the conclusions drawn from the reviewed literature; and Section 7 proposes directions for future research.

2. LITERATURE REVIEW

2.1 Lightweight Cryptographic Algorithms and Design Principles

A substantial body of literature has examined the design principles underlying lightweight cryptographic algorithms. Suryateja and Rao (2024) provide a broad survey of lightweight cryptographic algorithms for the Internet of Things (IoT), organising algorithms into block ciphers, stream ciphers, hash functions, and authenticated encryption schemes, and conclude that no single design dominates across the competing objectives of security, implementation cost, and performance. Dhanda et al. (2020) similarly trace the historical development of lightweight primitives, arguing that energy efficiency and side-channel resistance have grown steadily in importance as design criteria. Rana et al. (2022) extend this analysis with a systematic comparison of block cipher, stream cipher, and hash-based approaches across metrics including gate equivalent count, throughput, and energy consumption, concluding



that authenticated encryption with associated data (AEAD) has become the preferred construction for constrained device communication because it combines confidentiality, integrity, and authenticity within a single efficient primitive.

Specific algorithmic contributions have advanced this field considerably. Banik et al. (2020) present GIFT-COFB, an authenticated encryption scheme combining a compact block cipher with an efficient feedback mode, demonstrating strong performance on both hardware and software platforms. Dobraunig et al. (2021) present Ascon v1.2, a sponge-based authenticated encryption and hashing family that has since been adopted as the outcome of the NIST standardisation process, achieving compact hardware footprints alongside efficient software implementations. Beierle et al. (2020) introduce ForkSkinny, a tweakable block cipher with forward-secure properties built upon the SKINNY design, illustrating the diversity of structural approaches capable of achieving lightweight security. Daemen et al. (2020) examine protections against statistical ineffective fault attacks, demonstrating that algorithmic security alone is insufficient without careful attention to implementation-level side-channel resistance, a consideration of particular relevance to mobile phones given their exposure to physical access by potential adversaries.

Dutta et al. (2019) characterise the Internet of Things as an “Internet of insecure things,” arguing that the rapid proliferation of connected devices has consistently outpaced adequate security deployment, positioning lightweight cryptography as the most promising avenue for closing this gap. Gunathilake et al. (2021) similarly review recent advances in lightweight cryptography, highlighting the emergence of permutation-based sponge constructions as a particularly efficient pattern for combined hashing and encryption functionality.

These sponge-based and permutation-driven designs share a common design advantage: a single underlying permutation can be reused across multiple cryptographic functions, including encryption, decryption, and message authentication, thereby reducing the total code footprint that must be implemented and audited on a constrained device. This shared-primitive approach has become increasingly influential across the surveyed algorithmic literature, with Dobraunig et al. (2021) explicitly noting that the Ascon construction’s sponge-based design allows it to support hashing and authenticated encryption within a single, compact implementation, directly benefiting mobile applications that must minimise both storage footprint and the surface area exposed to potential implementation vulnerabilities.

2.2 The Mobile Malware and Cyber Threat Landscape

The mobile malware detection literature provides essential context for understanding the threats that lightweight cryptography must ultimately help mitigate. Alzaylaee et al. (2020) introduce DL-Droid, a deep learning-based Android malware detection system evaluated on real devices, demonstrating that dynamic analysis performed on genuine hardware yields substantially higher detection accuracy than emulator-based testing. Bai et al. (2020) propose FAMD, a fast multifeature detection framework combining static and dynamic features to achieve rapid classification with reduced computational overhead, a design philosophy that mirrors the objectives of lightweight cryptography itself. Feng et al. (2020) develop a two-



layer deep learning method based on network traffic analysis, illustrating that malicious behaviour can often be identified through communication patterns even when the malicious payload evades on-device analysis.

More recent contributions continue to refine detection approaches while addressing practical deployment challenges. Costa and Moia (2023) propose a lightweight, multi-stage Android malware detection approach using non-invasive machine learning techniques explicitly designed to minimise computational and battery overhead. Sharma and Kaul (2024) review machine learning techniques for malware detection and note that hybrid static-dynamic approaches consistently outperform purely static or dynamic methods. Manzil and Naik (2024) provide an extensive taxonomy of detection approaches, concluding that the field would benefit from greater standardisation in evaluation methodology. Alzaylaee et al. (2024) extend this line of enquiry with a comprehensive survey of deep learning algorithms applied to malware detection, cataloguing architectures and noting that the computational cost of many models remains prohibitive for on-device deployment.

Beyond individual detection techniques, systematic reviews have sought to consolidate the fragmented Android security literature. Garg and Baliyan (2021) conduct a wide-ranging assessment of Android security, identifying a persistent research gap concerning the integration of cryptographic protections with behavioural detection mechanisms. Razgallah et al. (2021) similarly survey malware detection techniques and observe that despite considerable academic progress, real-world detection rates remain inconsistent, particularly against threats that exploit legitimate system permissions.

A recurring conclusion across this body of literature is that detection accuracy, however high, cannot be assumed to reach one hundred percent in practical deployment, meaning that some proportion of malicious applications will inevitably evade detection for some period of time. Manzil and Naik (2024) note that this residual detection gap has, if anything, widened in recent years as malware authors adopt increasingly sophisticated evasion and dormancy techniques designed specifically to delay detection until sensitive data has already been harvested. This observation reinforces the argument that cryptographic protection of sensitive data must be treated as a foundational, preventive control rather than a secondary consideration layered on top of detection-based defences, since the practical harm arising from any period of undetected compromise is determined substantially by the strength of the encryption protecting the data an attacker might otherwise access.

2.3 NIST Standardisation and Comparative Algorithm Development

The NIST lightweight cryptography standardisation process has substantially shaped the direction of applied research in this field. Turan et al. (2021) document the second round of this process, detailing evaluation criteria including security margin, implementation efficiency, and side-channel resistance. Turan et al. (2023) subsequently publish the final status report, documenting the selection of the Ascon family as the standardised lightweight authenticated encryption and hashing algorithm. This standardisation effort has provided a unifying reference point against which subsequent algorithm proposals and comparative surveys are measured, as reflected in the work of Karthik and Rengarajan (2024), who survey

lightweight cryptography solutions for IoT security and note a discernible shift toward standardisation-compliant algorithms in recently published frameworks.

Thakor et al. (2021) provide an extensively cited comparative review of lightweight cryptography algorithms for resource-constrained devices, benchmarking block ciphers, stream ciphers, and hash functions across implementation metrics, and conclude that hybrid approaches combining multiple lightweight primitives may offer superior overall trade-offs compared to reliance on a single algorithm. Kumar et al. (2024) extend this discussion to encompass lightweight key management, authentication, and privacy-preserving protocols, arguing that a comprehensive mobile security framework must integrate these complementary mechanisms rather than treating encryption as a standalone solution.

The practical significance of the NIST standardisation process extends beyond the selection of a single winning algorithm; it has also established a shared vocabulary of evaluation criteria, including gate equivalent count, throughput per unit energy, and resistance to fault and side-channel attacks, that subsequent comparative surveys, such as those conducted by Thakor et al. (2021) and Kumar et al. (2024), have adopted as a common benchmarking framework. This shared methodology has, in turn, made it substantially easier for practitioners to compare candidate algorithms across studies conducted by different research groups, addressing a methodological fragmentation that characterised earlier lightweight cryptography research prior to the standardisation effort.

2.4 Comparative Summary of Reviewed Studies

The following tables summarise key aspects of the reviewed literature to support the comparative analysis presented above.

Table 1: Comparison of Selected Lightweight Cryptographic Algorithms

Algorithm	Structural Type	Primary Function	Key Reference
GIFT-COFB	Block cipher with feedback mode	Authenticated encryption	Banik et al. (2020)
Ascon v1.2	Sponge-based permutation	Authenticated encryption and hashing	Dobraunig et al. (2021)
ForkSkinny	Tweakable block cipher	Forward-secure authenticated encryption	Beierle et al. (2020)

Table 2: Comparison of Selected Android Malware Detection Approaches

Study	Technique	Analysis Type	Key Contribution
Alzaylaee et al. (2020)	Deep learning (DL-Droid)	Dynamic, real-device	Demonstrated superior accuracy of real-device over emulator-based testing
Bai et al. (2020)	Multifeature classification (FAMD)	Static and dynamic	Fast, low-overhead detection framework
Feng et al. (2020)	Two-layer deep learning	Network traffic analysis	Detected malicious behaviour via communication patterns



Costa and Moia (2023)	Non-invasive machine learning	Multi-stage, lightweight	Minimised computational and battery overhead
-----------------------	-------------------------------	--------------------------	--

Table 3: Summary of Research Gaps Identified in the Reviewed Literature

Focus Area	Gap Identified	Supporting Studies
Algorithm–device fit	Limited focus on general-purpose smartphones relative to IoT sensors	Dhanda et al. (2020); Rana et al. (2022)
Evaluation methodology	Reliance on simulation over real-device benchmarking	Kumar et al. (2024); Thakor et al. (2021)
Threat integration	Limited alignment between cryptographic frameworks and empirical malware threat models	Qamar et al. (2019); Razgallah et al. (2021)
Detection–encryption synergy	Limited co-design of cryptographic and detection mechanisms	Manzil and Naik (2024); Costa and Moia (2023)

3. RESEARCH METHODOLOGY

This review adopts a narrative literature review methodology, selected because the aim of the study is to synthesise and critically evaluate conceptual and technical developments across two related but historically distinct research domains, lightweight cryptography and mobile malware security, rather than to conduct a fully systematic, protocol-driven review of a narrowly defined research question. lightweight cryptographic algorithm design, mobile malware characterisation and detection, or the standardisation and comparative evaluation of constrained-device security mechanisms.

Sources were identified through a structured search of academic databases, including IEEE Xplore, ScienceDirect, SpringerLink, and the IACR Cryptology ePrint Archive, using search terms combining “lightweight cryptography,” “mobile security,” “malware detection,” and “NIST standardisation.” peer-reviewed or formally issued standardisation status, and substantive relevance to at least one of the three thematic pillars of the review, namely cryptographic algorithm design, mobile threat characterisation, or framework-level security evaluation. Sources outside these criteria, including purely theoretical mathematics papers unrelated to implementation, were excluded.

The analytical approach applied to the selected literature involved three stages. First, each source was categorised according to its primary thematic contribution, algorithmic, threat-characterisation, or framework-level, to enable structured comparison within Section 4. Second, recurring themes and points of consensus or disagreement across sources were identified through iterative reading and cross-referencing, informing the comparative tables presented above. Third, the reviewed literature was critically evaluated to identify methodological patterns, including the balance between simulation-based and real-device evaluation, and to surface the research gap that motivates the future work directions proposed in Section 7. This methodology, while not a fully systematic review in the formal sense, provides a structured and transparent basis for the conclusions drawn in this paper, consistent with established practice in technology-focused narrative literature reviews.



A limitation of this methodology, acknowledged transparently, is that the narrative review approach does not apply the exhaustive, protocol-driven search and inclusion procedures characteristic of formal systematic reviews conducted according to established reporting guidelines. This choice was made deliberately, given that the objective of the present study is conceptual synthesis and critical evaluation across two related but distinct research domains rather than an exhaustive quantitative meta-analysis of a single, narrowly defined research question. Nonetheless, the twenty-five sources selected span a broad range of publication venues, including IEEE Access, Computers & Security, the IACR Cryptology ePrint Archive, and official NIST interagency reports, providing reasonable confidence that the major themes and developments within both the lightweight cryptography and mobile malware detection literatures have been adequately represented within this review.

4. CONCLUSION

This review has examined the literature on lightweight cryptography as a mechanism for securing mobile phones against modern cyber threats, drawing on twenty-five sources spanning cryptographic algorithm design, mobile malware characterisation, and standardisation efforts. The review demonstrates that lightweight cryptography has matured substantially as a technical discipline, driven in large part by the NIST standardisation process and the resulting Ascon family of algorithms, which offer strong security margins alongside compact implementation footprints suitable for resource-constrained mobile hardware. At the same time, the mobile malware detection literature demonstrates that the threat landscape facing mobile devices continues to evolve in sophistication, with detection-based defences alone proving insufficient to eliminate risk. The review identifies a persistent gap between these two mature bodies of literature: relatively few studies evaluate lightweight cryptographic algorithms within complete, real-device mobile security frameworks that are explicitly designed and benchmarked against contemporary, empirically characterised malware threats. Addressing this gap represents an important direction for future research and practical framework development.

More broadly, this review suggests that the future of mobile phone security is likely to depend not on the further refinement of cryptographic algorithms or detection systems in isolation, both of which have already reached a considerable degree of individual maturity, but on the deliberate, empirically grounded integration of these two research strands into unified, evaluated security frameworks. Achieving this integration will require closer collaboration between the cryptographic engineering and mobile security research communities, whose evaluation methodologies and publication venues have historically remained largely separate, as reflected in the distinct thematic clusters identified across the literature reviewed in this paper.

5. FUTURE WORK

Building on the gaps identified in this review, several directions for future research are proposed. First, future studies should prioritise the implementation and benchmarking of lightweight cryptographic frameworks on genuine mobile hardware under realistic operating conditions, including variable battery state and network quality, rather than relying



predominantly on simulation. Second, future frameworks should be explicitly designed and evaluated against empirically derived mobile threat models, drawing on the malware taxonomies and detection literature reviewed in this paper, to ensure that cryptographic strength translates into measurable, real-world risk reduction. Third, further research is needed into the co-design of lightweight cryptographic mechanisms and machine learning-based detection systems, examining whether shared resource budgeting between these complementary defensive layers can improve overall security outcomes without imposing unacceptable performance or battery costs. Finally, future work should examine the usability implications of lightweight cryptographic frameworks, including the frequency and burden of key management and authentication processes, since security mechanisms that are not adopted in practice cannot deliver their intended protective benefit.

In addition to these four directions, future research would benefit from developing standardised, publicly available benchmarking datasets and testbeds specifically designed for evaluating mobile cryptographic frameworks under adversarial conditions, analogous to the standardised evaluation criteria already established for algorithm-level comparison through the NIST process. Such a testbed would allow researchers to compare proposed frameworks on a like-for-like basis, addressing the methodological fragmentation identified in Section 4.4 and enabling more cumulative, comparable progress across the field than has been possible to date.

REFERENCES

1. Alzaylaee, M. K., Yerima, S. Y., & Sezer, S. (2020). DL-Droid: Deep learning based Android malware detection using real devices. *Computers & Security*, 89, 101663. <https://doi.org/10.1016/j.cose.2019.101663>
2. Alzaylaee, M. K., Yerima, S. Y., & Sezer, S. (2024). Detecting Android malware using deep learning algorithms: A survey. *Computers and Electrical Engineering*, 119, 109544. <https://doi.org/10.1016/j.compeleceng.2024.109544>
3. Amrita, Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight cryptography for Internet of Things: A review. *EAI Endorsed Transactions on Internet of Things*, 10(1). <https://doi.org/10.4108/eetiot.5565>
4. Bai, H., Xie, N., Di, X., & Ye, Q. (2020). FAMd: A fast multifeature Android malware detection framework, design, and implementation. *IEEE Access*, 8, 194729–194740. <https://doi.org/10.1109/ACCESS.2020.3033026>
5. Banik, S., Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M., Peyrin, T., Sasaki, Y., Sim, S. M., & Todo, Y. (2020). GIFT-COFB. *IACR Cryptology ePrint Archive*, 2020/738.
6. Beierle, C., Leander, G., Moradi, A., & Rasoolzadeh, S. (2020). ForkSkinny: A tweakable block cipher with forward-secure properties. *IACR Transactions on Symmetric Cryptology*, 2020(1), 1–36.
7. Costa, L. da, & Moia, V. (2023). A lightweight and multi-stage approach for Android malware detection using non-invasive machine learning techniques. *IEEE Access*, 11, 73127–73144. <https://doi.org/10.1109/ACCESS.2023.3296606>



8. Daemen, J., Dobraunig, C., Eichlseder, M., Gross, H., Mendel, F., & Primas, R. (2020). Protecting against statistical ineffective fault attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020(3), 508–543. <https://doi.org/10.13154/tches.v2020.i3.508-543>
9. Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: A solution to secure IoT. *Wireless Personal Communications*, 112(3), 1947–1980.
10. Dobraunig, C., Eichlseder, M., Mendel, F., & Schl  ffer, M. (2021). Ascon v1.2: Lightweight authenticated encryption and hashing. *Journal of Cryptology*, 34, 33. <https://doi.org/10.1007/s00145-021-09398-9>
11. Dutta, I. K., Ghosh, B., & Bayoumi, M. (2019). Lightweight cryptography for Internet of insecure things: A survey. In *Proceedings of the IEEE International Conference on Consumer Electronics*.
12. Feng, J., Shen, L., Chen, Z., Wang, Y., & Li, H. (2020). A two-layer deep learning method for Android malware detection using network traffic. *IEEE Access*, 8, 125786–125796. <https://doi.org/10.1109/ACCESS.2020.3008081>
13. Garg, S., & Baliyan, N. (2021). Android security assessment: A review, taxonomy and research gap study. *Computers & Security*, 100, 102087. <https://doi.org/10.1016/j.cose.2020.102087>
14. Gunathilake, N. A., Al-Dubai, A., & Buchanan, W. J. (2021). Recent advances and trends in lightweight cryptography for IoT security. In *Proceedings of the IEEE International Conference on Internet of Things and Intelligence System*.
15. Karthik, S., & Rengarajan, A. (2024). Advancing IoT security: A comprehensive survey of lightweight cryptography solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, 13(5). <https://doi.org/10.17148/IJARCCE.2024.13511>
16. Kumar, S., Kumar, D., Dangi, R., Choudhary, G., Dragoni, N., & You, I. (2024). A review of lightweight security and privacy for resource-constrained IoT devices. *Computers, Materials & Continua*, 78(1), 31–63. <https://doi.org/10.32604/cmc.2023.047084>
17. Manzil, H. H. R., & Naik, S. M. (2024). Detection approaches for Android malware: Taxonomy and review analysis. *Expert Systems with Applications*, 238, 122255. <https://doi.org/10.1016/j.eswa.2023.122255>
18. Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*, 97, 887–909. <https://doi.org/10.1016/j.future.2019.03.007>
19. Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, 129, 77–89.
20. Razgallah, A., Khoury, R., Hall  , S., & Khanmohammadi, K. (2021). A survey of malware detection in Android apps: Recommendations and perspectives for future research. *Computer Science Review*, 39, 100358. <https://doi.org/10.1016/j.cosrev.2020.100358>



21. Sharma, M., & Kaul, A. (2024). A review of detecting malware in Android devices based on machine learning techniques. *Expert Systems*, 41(1), e13482. <https://doi.org/10.1111/exsy.13482>
22. Suryateja, P. S., & Rao, K. V. (2024). A survey on lightweight cryptographic algorithms in IoT. *Cybernetics and Information Technologies*, 24(1), 21–34.
23. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access*, 9, 28177–28193. <https://doi.org/10.1109/ACCESS.2021.3052867>
24. Turan, M. S., McKay, K. A., Chang, D., Kang, J., & Kelsey, J. (2021). Status report on the second round of the NIST lightweight cryptography standardization process (NIST Interagency or Internal Report 8369). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8369>
25. Turan, M. S., McKay, K. A., Chang, D., Kang, J., & Kelsey, J. (2023). Status report on the final round of the NIST lightweight cryptography standardization process (NIST Interagency or Internal Report 8454). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8454>