# Internet of Things Security Improvement

Subjects: Computer Science, Software Engineering

Contributor: Latifah Almalki , Amany Alnahdi , Tahani Albalawi

The growing popularity and extensive use of IoT devices have also introduced new security challenges. IoT devices often lack proper security measures, rendering them vulnerable to attacks. These attacks can range from simple network-based attacks to more sophisticated ones that target the physical devices themselves. The security of the IoT ecosystem is a complex and interdisciplinary domain that combines cybersecurity with various engineering fields, such as mechanical and electrical engineering. It goes beyond protecting data, servers, network infrastructure, and information. It also involves the supervision and management of physical systems connected through the Internet, whether in a centralized or distributed manner.

IoT security Internet of Things

## 1. Introduction

The Internet of Things (IoT) has experienced rapid growth and is increasingly pervasive in various domains, including healthcare, transportation, manufacturing, and smart homes. This expansion highlights the urgent need to address the security challenges associated with managing the large amount of data generated by IoT devices [1][2]. As the number of connected devices increases, so do the security risks. IoT devices often have vulnerabilities that can be exploited by malicious actors, resulting in privacy breaches, data leaks, device tampering, or even physical harm. Investigating and addressing these security risks is crucial to safeguarding the integrity, confidentiality, and availability of IoT systems. Understanding the roles, responsibilities, and interdependencies of these stakeholders is essential for effective decision making, resource allocation, and risk mitigation strategies. This article’s focus on stakeholder categorization contributes to enhancing the understanding of stakeholder dynamics in IoT security management.

The management of IoT security and clustering stakeholders face several bottlenecks [3][4][5][6], including scalability challenges, heterogeneity and interoperability issues, privacy and data protection concerns, collaboration and communication gaps, adaptability to dynamic IoT environments, and optimizing security measures for resource-constrained IoT devices. To overcome these challenges, it is essential to engage in multidisciplinary research efforts and make advancements in security protocols [5], privacy-enhancing technologies [5], standardization [6][7], collaborative frameworks [7][8], and resource-management techniques [5]. By effectively addressing these bottlenecks, the field of IoT security and stakeholder management can make substantial progress in achieving secure and sustainable IoT deployments.

## 2. IoT Security Improvement

The IoT is a rapidly expanding technology with the potential to transform numerous facets of our daily lives. IoT devices are equipped with sensors and communication capabilities, allowing them to collect and transmit data over the Internet. These devices have utility across a range of applications, including smart residences, industrial automation, and transportation networks [9].

However, the growing popularity and extensive use of IoT devices have also introduced new security challenges. IoT devices often lack proper security measures, rendering them vulnerable to attacks [10][11]. These attacks can range from simple network-based attacks to more sophisticated ones that target the physical devices themselves [11].

The security of the IoT ecosystem is a complex and interdisciplinary domain that combines cybersecurity with various engineering fields, such as mechanical and electrical engineering [12][13]. It goes beyond protecting data, servers, network infrastructure, and information. It also involves the supervision and management of physical systems connected through the Internet, whether in a centralized or distributed manner [14][15].

## 2.1. Taxonomy

Different categories of attacks can significantly impact the security of IoT devices and the information they collect and transmit [16]. It is essential for both organizations and individuals to have knowledge about these attack types and implement appropriate measures to protect against them. A classification of IoT attacks is illustrated in **Figure 1**.

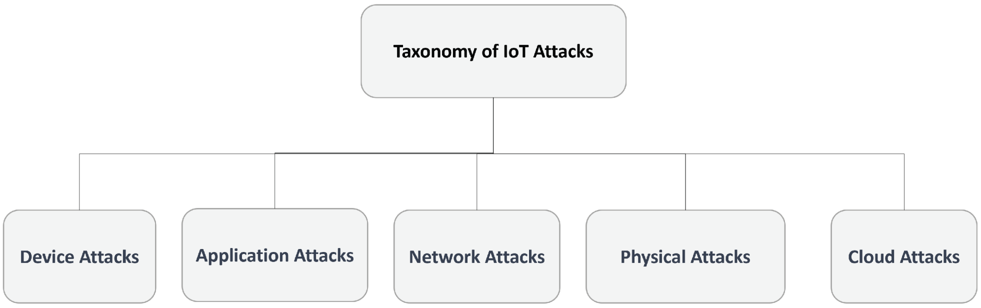

**Figure 1.** Taxonomy of IoT attacks based on different features.

### 2.1.1. Device Attacks in IoT

Security threats targeted toward specific devices or types of devices exploit vulnerabilities in the hardware or software of the device, potentially causing harm to the device itself or the network it is connected to [17]. These device-specific attacks involve exploiting known vulnerabilities in the device’s operating system, firmware, or hardware, compromising the device through phishing attacks, or even physically tampering with the device [18][19]. As the number of IoT devices continues to grow, it has become crucial for manufacturers to prioritize device security, and users must also take proactive measures to protect their devices [20][21]. This can include keeping software up to date, using strong passwords, and exercising caution when connecting to untrusted networks.

### 2.1.2. Application Attacks in IoT

Security threats that target the applications and software running on IoT devices exploit vulnerabilities within the applications, including issues within the code or the way the application interacts with other systems [22][23]. Examples of application attacks in the IoT include cross-site scripting [24], SQL injection [18], and buffer overflow attacks [25]. These attacks can compromise the security of the device and potentially grant attackers access to sensitive data or control over the device. To prevent application attacks in the IoT, it is crucial for developers to adhere to secure coding practices, and users should ensure their devices are updated with the latest security patches and software versions. Additionally, employing encryption and authentication technologies can help protect against application attacks in the IoT.

### 2.1.3. Network Attacks in IoT

Security threats that target the network infrastructure used by IoT devices exploit vulnerabilities within the network itself, potentially compromising the security and functionality of connected devices. Examples of network attacks in the IoT include man-in-the-middle attacks [26], denial-of-service (DoS) attacks [27], and unauthorized access attacks [28]. These attacks can enable attackers to intercept and manipulate data transmitted over the network or disrupt the network, affecting the availability and reliability of connected devices. To prevent network attacks in the IoT, organizations should implement secure network design and deployment practices, such as using secure protocols, firewalls, and access controls. Additionally, regularly monitoring network activity and promptly addressing any security incidents can help mitigate the risk of network attacks in the IoT.

### 2.1.4. Physical Attacks in IoT

Physical attacks in the context of IoT refer to security threats that involve the physical manipulation of a device [18]. These attacks can range from simple tampering to more sophisticated and malicious activities, including theft or destruction of the device [29][30]. Physical attacks can be particularly detrimental in critical infrastructure systems used in sectors such as healthcare, transportation, or energy production [31]. To prevent physical attacks, it is crucial for manufacturers to prioritize security in the design of their devices, and for users to secure their devices in physically inaccessible locations to unauthorized individuals. Additionally, implementing measures such as secure enclosures, tamper-evident seals, or biometric authentication can help mitigate the risk of physical attacks.

### 2.1.5. Cloud Attacks in IoT

Security threats targeting IoT devices' cloud infrastructure and services exploit vulnerabilities in the cloud platform, its applications, or the communication between the cloud and IoT devices [32]. Examples of cloud attacks in IoT include cloud data breaches, server misconfigurations, and unauthorized access to cloud resources [32][33]. These attacks can compromise sensitive data stored in the cloud, disrupt the functioning of connected IoT devices, or grant attackers unauthorized access to cloud resources. To prevent cloud attacks in IoT, organizations should adopt secure cloud deployments and management practices, such as implementing encryption, access controls, and monitoring tools. Regularly updating and patching cloud platforms and applications can also help mitigate the risk of cloud attacks in the context of IoT.

## 2.2. Impact of Attacks

The impact of attacks in the field of IoT security can be substantial, resulting in various consequences, such as financial losses, reputational damage, physical harm, and loss of critical information. Having an understanding of these impacts is crucial for organizations and individuals to prioritize security measures and mitigate the risks associated with IoT attacks. This section discuss the impact of attacks in three specific areas: side-channel attacks (SCA), post-quantum cryptography (PQC), and standardization efforts.

### 2.2.1. SCAs

SCAs pose a significant threat to IoT security, as they exploit unintended side-channel leakages to extract sensitive information. These attacks can have severe consequences, including the unauthorized disclosure of cryptographic keys and confidential data, thereby compromising the overall security of IoT systems [34]. To mitigate the impact of SCAs, several countermeasures have been developed [35][36][37], such as error detection and correction techniques, redundancy mechanisms, secure implementation practices, and masking techniques that introduce random noise to power traces or resist power analysis.

The combination of Differential Power Analysis (DPA) and Differential Fault Analysis (DFA) attacks poses a significant threat to cryptographic implementations. Attacks that exploit unintended side-channel leakages, such as power consumption, electromagnetic radiation, or timing information, can extract sensitive information from cryptographic implementations [38]. To mitigate the risks associated with these combined attacks, countermeasures such as Threshold Implementations (TI) circuits and error detection schemes are crucial. TI circuits provide built-in security features and tamper-resistant designs, while error detection schemes incorporate redundancy and error-checking mechanisms [39]. These measures enhance the resilience of cryptographic systems and protect against the compromise of sensitive information through fault and power analysis [38][40]. By implementing these countermeasures, the security of cryptographic implementations can be effectively enhanced against combined DPA and DFA attacks.

Field-Programmable Gate Arrays (FPGAs) play a crucial role in implementing cryptographic algorithms for IoT devices. However, the physical characteristics of FPGAs, such as power consumption, electromagnetic radiation, and timing information, can unintentionally leak information about the internal operations and secret keys of the implemented algorithms [41]. SCAs, including power analysis attacks and fault attacks, take advantage of these leakages to extract sensitive information from FPGA-based implementations. Power analysis attacks analyze power consumption patterns to infer secret keys [42], while fault attacks manipulate the FPGA to induce faults and analyze resulting behavior variations [43].

To enhance the security of FPGA-based implementations against SCAs, researchers have been working on countermeasures, including those targeting post-quantum cryptographic algorithms such as Ring-Learning with

Errors (Ring-LWEs) [44][45]. These countermeasures aim to mitigate side-channel leakages and protect sensitive information processed by FPGAs. Furthermore, specific fault detection techniques for FPGA platforms have been developed to detect and mitigate the impact of faults in cryptographic algorithms such as Ring-LWEs [46].

### 2.2.2. PQCs

With the rise of quantum computing, there is a growing concern that traditional cryptographic algorithms, such as Elliptic Curve Cryptography and Rivest–Shamir–Adleman, may be vulnerable to being broken by quantum computers [47][48]. Post-Quantum Cryptography (PQC) aims to address this challenge by providing cryptographic algorithms that are resistant to attacks by quantum computers [6]. The adoption of PQC has implications for security applications across various domains, including IoT [49]. The impact of PQC implementation on IoT security is twofold [6][50][51]. Firstly, the adoption of PQC algorithms requires significant changes in cryptographic protocols and infrastructure. This transition may introduce challenges, such as increased computational and storage requirements for IoT devices, which could potentially affect their performance and resource constraints. Secondly, ensuring compatibility between legacy IoT systems and PQC algorithms is crucial to ensure a seamless transition without compromising security. Efforts are currently underway to standardize PQC algorithms and protocols, aiming to achieve interoperability and widespread adoption. Standardization of PQC is essential in establishing a secure foundation for future IoT deployments, as it enables the development of robust cryptographic systems capable of withstanding attacks from quantum computers.

In the context of embedded systems, including IoT devices, it is crucial to have specific implementations of PQC algorithms that are optimized for ARM Cortex M4 and Cortex-A processors. These processors are widely used in embedded systems due to their low power consumption and cost effectiveness [52][53][54].

Several previous papers have focused on the development and analysis of PQC implementations on ARM processors, specifically the Cortex-M4 and Cortex-A processors. For example, refs. [55][56][57] discusses the implementation of Curve448 and Ed448 algorithms on the Cortex-M4 processor. In [6][58], the focus is on the implementation of the SIKE (Supersingular Isogeny Key Encapsulation) algorithm on the Cortex-M4 processor, with the latest version being SIKE Round 3 [58][59]. Furthermore, ref. [60] explores the implementation of the Kyber post-quantum cryptographic algorithm on 64-Bit ARM Cortex-A processors. Kyber is a lattice-based PQC algorithm.

Fault detection and diagnosis techniques are of paramount importance in ensuring the reliability, integrity, and security of cryptographic algorithms such as the Pomaranch cipher [61], Grostl hash [62], Midori cipher [63], and RECTANGLE cipher [63]. These techniques play a vital role in identifying and mitigating faults that can compromise the functionality and resilience of cryptographic systems. By promptly detecting and addressing faults, these techniques help maintain the effectiveness and robustness of cryptographic algorithms, thus safeguarding sensitive information and providing protection against potential attacks.

### 2.2.3. Standardization Efforts

Standardization plays a critical role in enhancing IoT security by providing consistent frameworks, protocols, and guidelines for implementing secure systems. The aim of standardization efforts is to establish best practices and promote interoperability, enabling different IoT devices, platforms, and services to seamlessly work together while ensuring security. By defining common security requirements, protocols, and encryption algorithms, standardization efforts help prevent vulnerabilities and ensure the adoption of robust security mechanisms in the IoT ecosystem [10]. Standardization also provides guidelines for secure communication, authentication, access control, and data protection, thereby mitigating the risks associated with IoT attacks [7].

The NIST (National Institute of Standards and Technology) is a U.S. federal agency with the responsibility of promoting and maintaining standards in various fields, including cryptography [64]. In the domain of lightweight cryptography, NIST has actively participted in the standardization process to identify and promote cryptographic algorithms suitable for resource-constrained devices, such as those used in IoT devices and embedded systems. NIST’s efforts in lightweight standardization aim to evaluate and select cryptographic algorithms that offer strong security while requiring minimal computational resources [63]. These algorithms are designed to meet the specific constraints of resource-constrained devices, including low power consumption, limited memory, and processing capabilities [65].

To address the evolving technologies and challenges in IoT security, standardization efforts must encompass areas such as SCAs and PQC, and the specific requirements of embedded systems such as ARM Cortex M4 and Cortex-A implementations. The development and adoption of comprehensive security standards that cover these aspects are crucial for establishing a strong security foundation for IoT devices and systems. By understanding the impact of attacks in the areas of SCAs, PQC, and standardization, stakeholders can effectively develop countermeasures and ensure the security and resilience of IoT ecosystems. This understanding allows for the proactive enhancement of the security posture of IoT systems, protection of sensitive information, and mitigation of risks associated with emerging threats.

**Table 1** summarizes various attack types in the field of cybersecurity and provides information on their impact and corresponding countermeasures. The table highlights different categories of attacks, including device attacks, application attacks, network attacks, physical attacks, cloud attacks, SCAs, DFA and Differential Power Analysis (DPA) attacks, and PQC attacks. For each attack category, the table includes specific attack types, the potential impact on security, and recommended countermeasures to mitigate the risks.

**Table 1.** Summary of attack types, impact, and countermeasures in cybersecurity.

| Type | Attack | Impact | Countermeasures |
|---|---|---|---|
| Device Attacks [17][18][19][20][21] | Exploiting vulnerabilities in device hardware or software, phishing attacks, physical tampering | Harm to device or network, unauthorized access, data compromise | Regular software updates, strong passwords, cautious network connections |

| Type | Attack | Impact | Countermeasures |
|---|---|---|---|
| Application Attacks [18][22][23][24][25] | Code vulnerabilities, cross-site scripting, SQL injection, buffer overflow attacks | Compromised device security, data access/control by attackers | Secure coding practices, software patching, encryption, authentication |
| Network Attacks [26][27][28] | Man-in-the-middle attacks, DoS attacks, unauthorized access attacks | Data interception/manipulation, network disruptions, compromised device functionality | Secure network design, protocols, firewalls, access controls, monitoring |
| Physical Attacks [18][29][30][31] | Tampering, theft, destruction of devices | Device compromise, data loss, disruption in critical infrastructure systems | Secure device design, physical security measures, enclosures, authentication |
| Cloud Attacks [32][33] | Cloud data breaches, server misconfigurations, unauthorized access | Data compromise, device disruptions, unauthorized cloud resource access | Secure cloud deployment, encryption, access controls, monitoring, patching |
| SCA [35][36][37] | Active and passive SCAs, fault attacks, power analysis attacks | Compromise of sensitive information, cryptographic implementations | Error detection/correction, redundancy, secure implementation, masking techniques |
| DFA and DPA Attacks [38][39][40] | DFA and DPA attacks | Compromise of sensitive information through fault or power analysis | Countermeasures specific to DFA and DPA, such as tamper-resistant designs, error detection, secure implementation |
| PQC Attacks [6][47][48][49][50][51] | Attacks targeting PQC algorithms and implementations | Compromise of encrypted data, undermining security against quantum computers | Development of PQC algorithms, standardization, secure implementation, compatibility considerations |

## References

1. Yao, X.; Farha, F.; Li, R.; Psychoula, I.; Chen, L.; Ning, H. Security and privacy issues of physical objects in the IoT: Challenges and opportunities. Digit. Commun. Netw. 2021, 7, 373–384.
2. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet Things 2020, 11, 100227.
3. Angel, N.A.; Ravindran, D.; Vincent, P.D.R.; Srinivasan, K.; Hu, Y.C. Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. Sensors 2021, 22, 196.
4. Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A survey of security in cloud, edge, and fog computing. Sensors 2022, 22, 927.

5. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 2019, 7, 82721–82743.
6. Schöffel, M.; Lauer, F.; Rheinländer, C.C.; Wehn, N. Secure IoT in the era of quantum computers—Where are the bottlenecks? Sensors 2022, 22, 2484.
7. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A review of security standards and frameworks for IoT-based smart environments. IEEE Access 2021, 9, 121975–121995.
8. Melo, M.; Aquino, G. FaTEMa: A Framework for Multi-Layer Fault Tolerance in IoT Systems. Sensors 2021, 21, 7181.
9. Ramson, S.J.; Vishnu, S.; Shanmugam, M. Applications of internet of things (iot)—An overview. In Proceedings of the 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 5–6 March 2020; pp. 92–95.
10. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and security: Challenges and solutions. Appl. Sci. 2020, 10, 4102.
11. Pal, S.; Hitchens, M.; Rabehaja, T.; Mukhopadhyay, S. Security requirements for the internet of things: A systematic approach. Sensors 2020, 20, 5897.
12. Sidhu, S.; Mohd, B.J.; Hayajneh, T. Hardware security in IoT devices with emphasis on hardware trojans. J. Sens. Actuator Netw. 2019, 8, 42.
13. Bansal, S.; Kumar, D. IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. Int. J. Wirel. Inf. Netw. 2020, 27, 340–364.
14. Ding, D.; Han, Q.L.; Ge, X.; Wang, J. Secure state estimation and control of cyber-physical systems: A survey. IEEE Trans. Syst. Man Cybern. Syst. 2020, 51, 176–190.
15. Farivar, F.; Haghighi, M.S.; Jolfaei, A.; Alazab, M. Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. IEEE Trans. Ind. Inform. 2019, 16, 2716–2725.
16. Xenofontos, C.; Zografopoulos, I.; Konstantinou, C.; Jolfaei, A.; Khan, M.K.; Choo, K.K.R. Consumer, commercial, and industrial iot (in) security: Attack taxonomy and case studies. IEEE Internet Things J. 2021, 9, 199–221.
17. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Internet of Things: Security and Solutions Survey. Sensors 2022, 22, 7433.
18. Shah, Y.; Sengupta, S. A survey on Classification of Cyber-attacks on IoT and IIoT devices. In Proceedings of the 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 28–31 October 2020; pp. 0406–0413.

19. Gaur, V.; Kumar, R. Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. Arab. J. Sci. Eng. 2022, 47, 1353–1374.
20. Gupta, R.; Phanden, R.K.; Sharma, S.; Srivastava, P.; Chaturvedi, P. Security in manufacturing systems in the age of industry 4.0: Pitfalls and possibilities. In Advances in Industrial and Production Engineering: Select Proceedings of FLAME 2020; Springer: Berlin/Heidelberg, Germany, 2021; pp. 105–113.
21. Eustis, A.G. The Mirai Botnet and the importance of IoT device security. In Proceedings of the 16th International Conference on Information Technology-New Generations (ITNG 2019), Las Vegas, NV, USA, 1–3 April 2019; pp. 85–89.
22. Rajendran, G.; Nivash, R.R.; Parthy, P.P.; Balamurugan, S. Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–6.
23. Vishwakarma, R.; Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun. Syst. 2020, 73, 3–25.
24. Chaudhary, P.; Gupta, B.B.; Singh, A. Securing heterogeneous embedded devices against XSS attack in intelligent IoT system. Comput. Secur. 2022, 118, 102710.
25. Mullen, G.; Meany, L. Assessment of buffer overflow based attacks on an IoT operating system. In Proceedings of the 2019 Global IoT Summit (GIoTS), Chennai, India, 1–3 October 2019; pp. 1–6.
26. Toutsop, O.; Harvey, P.; Kornegay, K. Monitoring and detection time optimization of man in the middle attacks using machine learning. In Proceedings of the 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), Washington DC, DC, USA, 13–15 October 2020; pp. 1–7.
27. Al-Hadhrami, Y.; Hussain, F.K. DDoS attacks in IoT networks: A comprehensive systematic literature review. World Wide Web 2021, 24, 971–1001.
28. Jović, M.; Tijan, E.; Aksentijević, S.; Čišić, D. An overview of security challenges of seaport IoT systems. In Proceedings of the 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May 2019; pp. 1349–1354.
29. Garagad, V.G.; Iyer, N.C.; Wali, H.G. Data integrity: A security threat for internet of things and cyber-physical systems. In Proceedings of the 2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2–4 July 2020; pp. 244–249.
30. Yang, X.; Shu, L.; Liu, Y.; Hancke, G.P.; Ferrag, M.A.; Huang, K. Physical security and safety of iot equipment: A survey of recent advances and opportunities. IEEE Trans. Ind. Inform. 2022, 18, 4319–4330.

31. González-Granadillo, G.; González-Zarzosa, S.; Diaz, R. Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors 2021, 21, 4759.
32. Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber security in iot-based cloud computing: A comprehensive survey. Electronics 2022, 11, 16.
33. Saini, D.K.; Kumar, K.; Gupta, P. Security issues in IoT and cloud computing service models with suggested solutions. Secur. Commun. Netw. 2022, 2022.
34. Devi, M.; Majumder, A. Side-channel attack in Internet of Things: A survey. In Applications of Internet of Things: Proceedings of ICCCIOT 2020; Springer: Berlin/Heidelberg, Germany, 2021; pp. 213–222.
35. Lo'ai, A.T.; Somani, T.F. More secure Internet of Things using robust encryption algorithms against side channel attacks. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November 2016–2 December 2016; pp. 1–6.
36. Ravi, P.; Poussier, R.; Bhasin, S.; Chattopadhyay, A. On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT: A Performance Evaluation Study over Kyber and Dilithium on the ARM Cortex-M4. In Proceedings of the Security, Privacy, and Applied Cryptography Engineering: 10th International Conference, SPACE 2020, Kolkata, India, 17–21 December 2020; pp. 123–146.
37. Abarzúa, R.; Valencia, C.; López, J. Survey on performance and security problems of countermeasures for passive side-channel attacks on ECC. J. Cryptogr. Eng. 2021, 11, 71–102.
38. Kaur, S.; Singh, B.; Kaur, H. Stratification of hardware attacks: Side channel attacks and fault injection techniques. SN Comput. Sci. 2021, 2, 1–13.
39. Schneider, T.; Moradi, A.; Güneysu, T. ParTI–towards combined hardware countermeasures against side-channel and fault-injection attacks. In Proceedings of the Advances in Cryptology—CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016; pp. 302–332.
40. Dhooghe, S.; Nikova, S.; Rijmen, V. Threshold implementations in the robust probing model. In Proceedings of the ACM Workshop on Theory of Implementation Security Workshop, London, UK, 11 November 2019; pp. 30–37.
41. Magyari, A.; Chen, Y. Review of State-of-the-Art FPGA Applications in IoT Networks. Sensors 2022, 22, 7496.
42. Liptak, C.; Mal-Sarkar, S.; Kumar, S.A. Power Analysis Side Channel Attacks and Countermeasures for the Internet of Things. In Proceedings of the 2022 IEEE Physical Assurance and Inspection of Electronics (PAINE), Huntsville, AL, USA, 25–27 October 2022; pp. 1–7.

43. Gangolli, A.; Mahmoud, Q.H.; Azim, A. A systematic review of fault injection attacks on IOT systems. Electronics 2022, 11, 2023.

44. Ebrahimi, S.; Bayat-Sarmadi, S. Lightweight and fault-resilient implementations of binary ring-LWE for IoT devices. IEEE Internet Things J. 2020, 7, 6970–6978.

45. Imaña, J.L.; He, P.; Bao, T.; Tu, Y.; Xie, J. Efficient hardware arithmetic for inverted binary ring-lwe based post-quantum cryptography. IEEE Trans. Circuits Syst. I Regul. Pap. 2022, 69, 3297–3307.

46. Sarker, A.; Kermani, M.M.; Azarderakhsh, R. Fault detection architectures for inverted binary ring-LWE construction benchmarked on FPGA. IEEE Trans. Circuits Syst. II Express Briefs 2020, 68, 1403–1407.

47. Zeydan, E.; Turk, Y.; Aksoy, B.; Ozturk, S.B. Recent advances in post-quantum cryptography for networks: A survey. In Proceedings of the 2022 Seventh International Conference On Mobile Furthermore, Secure Services (MobiSecServ), Gainesville, FL, USA, 26–27 February 2022; pp. 1–8.

48. Kirsch, Z.; Chow, M. Quantum Computing: The Risk to Existing Encryption Methods. 2015. Available online: http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf (accessed on 31 May 2023).

49. Septien-Hernandez, J.A.; Arellano-Vazquez, M.; Contreras-Cruz, M.A.; Ramirez-Paredes, J.P. A Comparative study of post-quantum cryptosystems for Internet-of-Things applications. Sensors 2022, 22, 489.

50. Seyhan, K.; Nguyen, T.N.; Akleylek, S.; Cengiz, K. Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: A survey. Clust. Comput. 2022, 25, 1729–1748.

51. Sajimon, P.; Jain, K.; Krishnan, P. Analysis of Post-Quantum Cryptography for Internet of Things. In Proceedings of the 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 25–27 May 2022; pp. 387–394.

52. Park, T.; Seo, H.; Kim, J.; Park, H.; Kim, H. Efficient parallel implementation of matrix multiplication for Lattice-Based cryptography on modern ARM processor. Secur. Commun. Netw. 2018, 2018, 7012056.

53. Asghar, M.N. A review of ARM processor architecture history, progress and applications. J. Appl. Emerg. Sci. 2020, 10, 171.

54. Antony, A.; Sarika, S. A review on IoT operating systems. Int. J. Comput. Appl. 2020, 176, 33–40.

55. Anastasova, M.; Azarderakhsh, R.; Kermani, M.M.; Beshaj, L. Time-Efficient Finite Field Microarchitecture Design for Curve448 and Ed448 on Cortex-M4. In Proceedings of the

Information Security and Cryptology—ICISC 2022: 25th International Conference, ICISC 2022, Seoul, Republic of Korea, 30 November–2 December 2022; pp. 292–314.

56. Bisheh Niasar, M.; Azarderakhsh, R.; Kermani, M.M. Efficient hardware implementations for elliptic curve cryptography over Curve448. In Proceedings of the Progress in Cryptology—INDOCRYPT 2020: 21st International Conference on Cryptology in India, Bangalore, India, 13–16 December 2020; pp. 228–247.
57. Fazzat, A.; Khatoun, R.; Labiod, H.; Dubois, R. A comparative performance study of cryptographic algorithms for connected vehicles. In Proceedings of the 2020 4th Cyber Security in Networking Conference (CSNet), Lausanne, Switzerland, 21–23 October 2020; pp. 1–8.
58. Anastasova, M.; Azarderakhsh, R.; Kermani, M.M. Fast strategies for the implementation of SIKE round 3 on ARM Cortex-M4. IEEE Trans. Circuits Syst. I Regul. Pap. 2021, 68, 4129–4141.
59. Picaut, J.; Can, A.; Fortin, N.; Ardouin, J.; Lagrange, M. Low-cost sensors for urban noise monitoring networks—A literature review. Sensors 2020, 20, 2256.
60. Sanal, P.; Karagoz, E.; Seo, H.; Azarderakhsh, R.; Mozaffari-Kermani, M. Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM Cortex-A processors. In Proceedings of the Security and Privacy in Communication Networks: 17th EAI International Conference, SecureComm 2021, Virtual Event, 6–9 September 2021; pp. 424–440.
61. Mozaffari-Kermani, M.; Azarderakhsh, R.; Aghaie, A. Reliable and error detection architectures of Pomaranch for false-alarm-sensitive cryptographic applications. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 2015, 23, 2804–2812.
62. Abed, S.; Jaffal, R.; Mohd, B.J.; Al-Shayeji, M. An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. Clust. Comput. 2021, 24, 3065–3084.
63. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access 2021, 9, 28177–28193.
64. McKay, K.; Bassham, L.; Sönmez Turan, M.; Mouha, N. Report on Lightweight Cryptography; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
65. Ebrahimi, S.; Bayat-Sarmadi, S.; Mosanaei-Boorani, H. Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in IoT. IEEE Internet Things J. 2019, 6, 5500–5507.