Intrusion detection system in lightweight devices: issues and challenges

Nuruddeen Musa Shanono, Zulkiflee Muslim, Nur Azman Abu, Siti Rahayu Selamat, Haniza Nahar
Information Security Forensics and Computer Networking, Center for Advanced Computing Technology (C-ACT), Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Article Info

Article history:

Received Dec 18, 2023
Revised Aug 29, 2024
Accepted Sep 28, 2024

Keywords:

Cyber attack
Internet of things devices
Intrusion detection system
Lightweight devices
Security
Systematic literature review

ABSTRACT

Intrusion detection system (IDS) is a crucial component in ensuring the security of computer networks. It helps in identifying and responding to unauthorized access attempts or malicious activities within a network. The focus of this systematic review is on IDS specifically designed for lightweight devices. This systematic review aims to provide an abstract understanding of the current state of IDSs for lightweight devices. It involves a comprehensive analysis of existing research papers, evaluating the methodologies, techniques, and performance metrics used in these IDS solutions. The goal of the systematic review is to provide a critical assessment and analysis of the literature on IDS in lightweight devices, closing the research gap in this field. The review analyzed and evaluated 55 studies out of 678 initially identified. The findings of the study are presented in the paper, which includes insights into the state-of-the-art proposals in the field, challenges and limitations of existing solutions, and recommendations for future research directions. The outcome of this paper can help the advancement of IDS for lightweight devices.

Corresponding Author:

Zulkiflee Muslim
Information Security Forensics and Computer Networking, Center for Advanced Computing Technology
Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka
Hang Tuah Jaya, 76100 Durian Tunggal Melaka, Melaka, Malaysia
Email: zulkiflee@utem.edu.my

1. INTRODUCTION

Throughout the course of human history, communication methods have undergone significant evolution, progressing from primitive forms such as smoke signals and drums to more sophisticated means including the Pony Express, carrier pigeons, telegraphs, telephones, and subsequently, cell phones, culminating in the ubiquitous presence of the internet in contemporary society. The advent of the internet has revolutionized the dissemination and accessibility of data and information. However, the absence of robust security protocols poses a considerable risk of data breaches and theft. Particularly underscored during the COVID-19 pandemic, the internet assumes paramount importance in facilitating connectivity and technological solutions to navigate the challenges of the new normal. Indeed, the internet has become indispensable for myriad activities in today's global landscape. Leveraging the internet of things (IoT) has become imperative, particularly in the context of remote work arrangements, wherein virtual meetings, conferences, and seminars have supplanted traditional in-person interactions. In certain regions, the shift towards remote work is not merely an option but a directive necessitating adaptation to a home-based work environment.

The solution to the menace of malicious users is taking a proactive stance against them by deploying security appliances that will protect our networks from them. Traditionally, firewalls have been the primary security device used in business and home environments. It didn't take long before it was realized that a firewall alone cannot protect the system from threats [1]. Increasing security threats make intrusion detection an absolute must for all networks. Information requires security from attackers [2], [3]. Cryptographic security is insufficient as it can only protect the network from outside attacks. Still, we need a second line of defense, such as the intrusion detection system (IDS) [4]. Since lightweight devices are connected to the internet, attackers can easily gain access to the device. This is where an IDS comes into play. Ideal IDS provides 100% effectiveness in the fight against possible vulnerabilities. Therefore, the importance of IDS is undeniable [5], [6]. Figure 1 shows a network configuration that aims to provide a secure and efficient environment for various devices and services. The firewall protects the network from unauthorized access, while the IDS server monitors for potential threats. Lightweight devices and LAN devices can access the network and its resources, including the server farm, under the protection of the firewall and IDS.

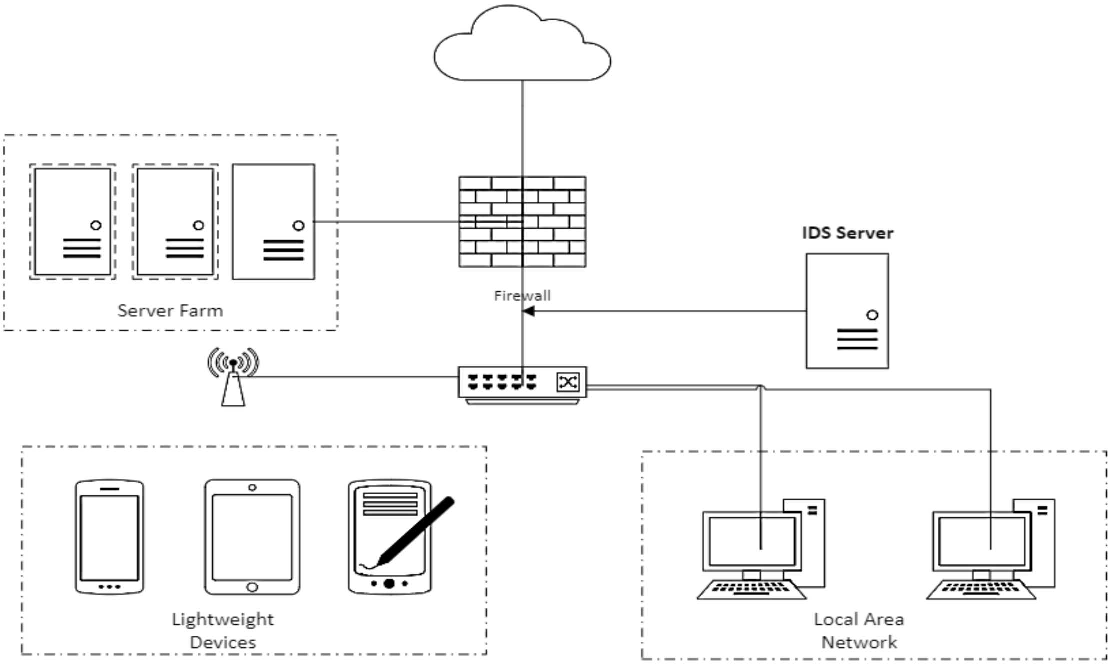

Figure 1. IDS

Recently, lightweight devices especially mobile phones play a vital role in our daily activities ranging from shopping, banking, communication, working, entertainment, education and many more. Studies demonstrate that the knowledge of activities of daily living (ADL) for example, strolling and running can be mined based on data collected by on body sensors. Especially with the advancement of mobile technology, the ADL of smartphone user can be precisely mined depending on readings of the sensor deployed in mobile phones.

With the help of mobile apps, they become more intelligent, user-friendly, and capable of making complex tasks easier. Those app can collect a whole lot of data about us, such as name and email address, location history, personal contacts, photos and videos, purchases, health and fitness data, financial information, browsing and search history, your IP address, and other sensitive data. Those data collected about us can be shared or sold to third parties, usually without you even knowing. Most of these lightweight devices are usually designed to be portable on purpose to be nonintrusive in user's daily lives resources [7]. The hardware inside lightweight devices has several limitations because of the low processing power and limited storage capacity. The growing threats to security make an IDS an absolute necessity for all networks [8]-[10]. IDSs are systems developed to monitor the network or network devices for hostile attacks originating from both external sources and internal sources and then report their findings [11]. The IDS usually checks against a list of known attacks to determine whether the network is under attack or not, it does so by checking a database for common attack signatures, patterns, traffic, or behavior [12].

By 2025, the total number of devices connected to the global IoT is expected to reach 30.9 billion units, a significant increase from 13.8 billion units in 2021. One of the most significant current discussions about lightweight device is its popularity because it is light, small, and convenient to use and carry and has dressing characteristics [13]. Lightweight devices, due to their limited computational power and constrained resources, pose distinct challenges for implementing effective IDSs [14]. These devices are often deployed in sensitive environments, such as healthcare, industrial automation, and smart homes, where security is paramount. In this context, IDSs play a crucial role in safeguarding sensitive data and ensuring the integrity of these systems [15].

Lightweight devices are equipped of tiny embedded systems called sensors. These sensors gather information from the environment, receive and process it and communicate with the end user. Sensors are being utilized around us for many purposes and benefits i.e., military target tracking and surveillance, biomedical health monitoring, detection of catastrophic events, hazardous environment exploration and seismic sensing, in medical clinics to screen and gather the patient information, and structural sensing [16]. This paper delves into the intricacies of intrusion detection in lightweight devices, discussing the challenges involved, existing solutions, and future possibilities for enhancing security in these devices.

Lightweight devices are becoming ubiquitous, and an increasing number of applications are being developed for these devices. Sen and Ramamritham [17] identify that many of these applications deal with significant amounts of data and involve complex joins and aggregate operations which necessitate a local database management system on the device. Lightweight devices are extremely vulnerable and attractive to attackers for their highly heterogeneous components, naive security configurations and weak encryption verification. This is a challenge as these devices are constrained by limited stable storage and main memory [18], [19]. The key contributions of this paper are outlined:

- This paper delves into the intricacies of intrusion detection in lightweight devices.
- The identification of challenges involved and existing solutions.
- The future possibilities for enhancing security in these devices.

Multiple concepts (avoid, for example, ‘and’, ‘of’). Be sparing with abbreviations: only abbreviations firmly established in the field may be eligible. These keywords will be used for indexing purposes. Indexing and abstracting services depend on the accuracy of the title, extracting from it keywords useful in cross-referencing and computer searching. An improperly titled paper may never reach the audience for which it was intended, so be specific.

The current research studies (review and survey) are covered in this section. The significance and necessity of this scoping review will be demonstrated. Kim *et al.* [20] has demonstrated that a blockchain is emerging as a solution to solve the problem in the IoT network by storing blocks to each device. However, lightweight devices cannot store all the blockchain due to their low storage capacity. Therefore, they proposed a storage compression consensus (SCC) algorithm which compresses a blockchain in each device to ensure the storage capacity. Similarly, Dittmann and Jelitto [21] introduced a blockchain proxy as a service for lightweight IoT devices to offload communication with a blockchain while retaining full control of all transactions committed to the shared ledger.

In a different study, Chen *et al.* [22] proposed a lightweight and real-time key establishment scheme for wearable devices by leveraging the integrated accelerometer. Specifically, they introduced a novel way for users to initialize a shared key using random shakes or movements on their wearable devices. As highlighted by [23], they addressed the problem of securing the exchange of information in IoT networks towards overcoming confidentiality issues with low resources and small latency. They also presented a new efficient, flexible, lightweight, and secure cipher algorithm for IoT applications.

Höglund *et al.* [24] developed an automated certificate enrollment protocol light enough for highly constrained devices, which provides end-to-end security between certificate authorities (CA) and the recipient IoT devices. Furthermore, Le-Tuan *et al.* [25] introduced a lightweight resource description framework (RDF) engine, which comprises of RDF storage and SPARQL (standard query language and protocol) processor, for lightweight edge devices, called RDF4Led. RDF4Led follows the reduce instruction set computer (RISC) design philosophy. The design comprises a flash-aware storage structure, an indexing scheme and a low-memory-footprint join algorithm which improves scalability as well as robustness over competing solutions.

Malluhi *et al.* [26] proposed a decentralized CP-ABE scheme that can deal well with the problem of security of user, and additionally possesses some nice properties meeting the requirement for lightweight-device applications, such as fast decryption, constant-size of secret key, optimized cipher text size and fine-grained access control. Al-Maitah *et al.* [27] proposed a selective memory balancing (SMB) technique for improving the performance of residential lightweight devices. Langiu *et al.* [28] presented UpKit, a portable and lightweight software update framework for constrained IoT devices encompassing all phases of the update process from the generation and signature of a new firmware to the transmission of the latter to an IoT device, its verification and installation. Arshad *et al.* [29] proposed an intrusion detection framework for the energy-constrained lightweight devices which form the foundation of an industrial internet of things (IIoT) ecosystem. In view of the ad hoc nature of such systems as well as emerging complex threats such as botnets, they assessed the feasibility of collaboration between the host (IoT devices) and the edge devices for effective intrusion detection whilst minimizing energy consumption and communication overhead.

2. METHOD

A systematic review provides a transparent method to analyze, synthesize and evaluate existing literature. The systematic literature review (SLR) identified the need for a systematic review to evaluate the use of IDS in the lightweight devices. In addition, it also identifies the strengths and weaknesses of existing methods. To the best of our knowledge, no review paper has been published that provides a critical assessment and analysis of the literature on IDS in lightweight devices. Therefore, the goal of this paper is to close the research gap. In the systematic literature review, the techniques demonstrated in [30] is used to accomplish the planning, conducting, and reporting process. Figure 2 shows the steps required in systematic review. It identifies the need for a systematic review to assess the use of IDS in lightweight devices. It also determined the weaknesses and strengths of the existing methods. The existing systematic review process consists of several steps that must be carried out systematically, which includes the development of review protocols, conducting systematic reviews, analyzing, visualizing, and presenting the results, and discussing recommendations.

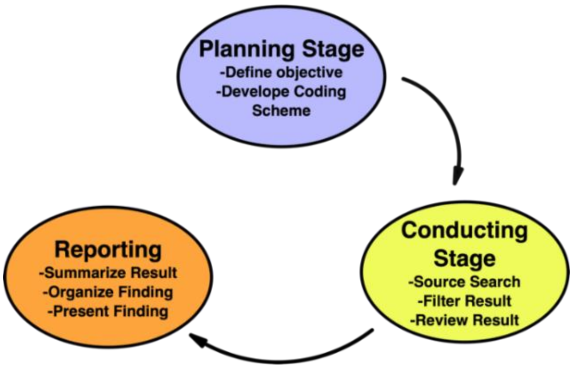

Figure 2. Research method.

2.1. Research questions.

The overall objective of this SLR is to gain insight into studies based on lightweight devices. This study outlines and answers four vital research questions (RQs). These key RQs will enable us to categorize and comprehend the current research in lightweight devices and identify the limitations and future research directions in the field. The key RQs are given below.

- RQ1: what are the demographic characteristics of the selected studies?
- RQ2: what is the research focus of the selected studies?
- RQ3: what are the contributions proposed by the selected studies, and how they can be categorized?
- RQ4: what is the state-of-the-art proposal in the field of study?

2.2. Data source

The papers used in this study were retrieved from two electronic databases (Scopus and Springer Link). This database is the primary data source for finding potentially relevant studies. However, Google Scholar was excluded due to the low precision and the overlap of the results from other data sources adopted in the study. As a result, all relevant articles in Google Scholar have been captured by the other sources.

2.3. Search strategy and study selection.

The search string represents synonyms and alternative spellings using the Boolean OR and Boolean AND. Therefore, four keywords were chosen: “intrusion detection system”, “security technique”, “lightweight devices”, and “IoT devices”. The following search terms are used to select the main studies (“security techniques” OR “security methods” OR “physical security techniques”) AND (“lightweight devices” OR “IoT devices”).

The purpose of the study selection process is to identify related articles most relevant to this SLR research target. This process has been carefully studied to improve the reliability of the selection process and minimize the bias error. Therefore, if an article appears in multiple sources, only one is considered based on our search order. Figure 3 illustrates the process for selecting studies for systematic review.

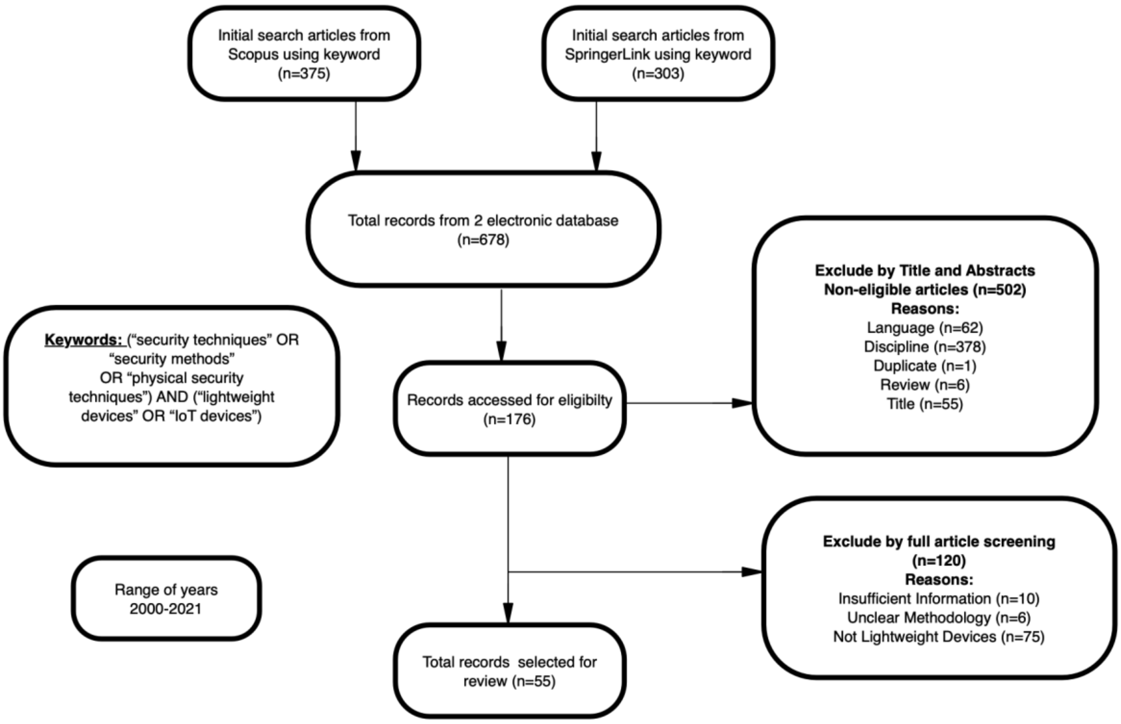
Initial search articles from Scopus using keyword (n=375)
Initial search articles from SpringerLink using keyword (n=303)
Total records from 2 electronic database (n=678)
Exclude by Title and Abstracts Non-eligible articles (n=502) Reasons: Language (n=62) Discipline (n=378) Duplicate (n=1) Review (n=6) Title (n=55)
Keywords: ("security techniques" OR "security methods" OR "physical security techniques") AND ("lightweight devices" OR "IoT devices")
Records accessed for eligibilty (n=176)
Exclude by full article screening (n=120) Reasons: Insufficient Information (n=10) Unclear Methodology (n=6) Not Lightweight Devices (n=75)
Range of years 2000-2021
Total records selected for review (n=55)

Figure 3. Flowchart

2.4. Data extraction

Research on this study analysis has been extracted from the Scopus and Springer Link electronic databases. These studies are identified by research work published between 2000 and 2021 by using a combination of search keywords. This search has produced much research and then filtered using inclusion and exclusion criteria as shown in Table 1. The data extraction technique eliminates unreliable and nonpeer-reviewed articles and any duplicates. Studies with unclear methodology and articles in languages other than English were excluded from the review. A total of 678 articles identified using this search strategy were individually selected for final research. As a result of the final selection, 55 articles were assessed.

Table 1. Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Articles published from 2000-2021	Articles outside the scope of security technique in LWD
Articles written in English language	Non-English papers
Studies published in LWD/IoT field	Non-peer reviewed and non-full text articles review studies
Articles discussing issues in LWD	Duplicates articles

2.5. Overview of selected studies

Table 2 provides an overview of various research papers in IoT security, including machine learning algorithms for cyber attacks, profiling lightweight devices, detecting cyber attacks in power control systems, and detecting malicious activities in home area networks. Some papers focus on real-world experiments, while others are limited to simulations. The proposed methodologies show high accuracy rates, enhanced security and stability, and improved efficiency compared to other algorithms. However, some approaches lack real-life deployment and scalability evaluation.

Table 2 provides a comprehensive overview of the current state of IoT security research, and the various techniques being explored to address the challenges in this domain, for examples, lack of scalable solutions for IoT security as the number of connected devices continues to grow. More research is needed to develop security approaches that can effectively handle the increasing scale of IoT systems. Also, there's a need for more robust and efficient encryption algorithms to secure IoT data. Existing algorithms may not be sufficient to protect against evolving security threats in IoT environments.

Furthermore, there are challenges in securing shared lightweight devices where multiple users or applications may access the same device. Developing access control mechanisms and secure data-sharing protocols is an important research area. Moreover, there are opportunities for improving anomaly detection in IoT systems to identify and mitigate security threats. More advanced machine learning and data analysis techniques could be explored to enhance the accuracy and responsiveness of anomaly detection. Thus, there is a need for more efficient key management and distribution mechanisms in IoT environments to support secure communication and data protection. Developing lightweight and decentralized key management solutions is an important research gap.

Table 2. Enhancement focus of selected studies

Study	High accuracy	Lower resource consumption	Enhanced security	Improved performance?	Evaluation metric?
[31]	No	No	No	Yes	No
[32]	No	Yes	No	No	No
[33]	No	Yes	Yes	No	No
[34]	Yes	No	No	No	Yes
[35]	Yes	Yes	No	No	No
[36]	Yes	No	Yes	Yes	No
[37]	No	Yes	Yes	Yes	No
[38]	No	Yes	No	No	No
[39]	No	No	Yes	Yes	No
[40]	Yes	No	Yes	Yes	Yes
[41]	Yes	No	No	Yes	Yes
[42]	No	Yes	No	No	No
[43]	Yes	Yes	No	No	No
[44]	No	No	Yes	Yes	No
[45]	No	Yes	Yes	Yes	No
[46]	Yes	Yes	Yes	Yes	No
[47]	No	No	Yes	No	No
[48]	No	No	Yes	No	No
[49]	Yes	No	Yes	No	No
[50]	No	Yes	No	Yes	No
[51]	Yes	No	Yes	Yes	No
[52]	Yes	Yes	No	Yes	No
[53]	No	Yes	No	No	No
[54]	No	Yes	No	Yes	No
[55]	No	Yes	No	No	No
[56]	No	Yes	No	No	No
[57]	Yes	No	No	No	No
[58]	Yes	No	Yes	Yes	No
[59]	No	Yes	Yes	Yes	No
[60]	No	Yes	No	No	No
[61]	Yes	Yes	No	No	No
[62]	No	No	No	Yes	No
[63]	Yes	No	No	Yes	No
[64]	No	No	Yes	Yes	No
[65]	No	Yes	Yes	Yes	No
[66]	Yes	No	Yes	Yes	No
[67]	Yes	No	Yes	No	No
[68]	No	Yes	No	Yes	No
[69]	No	No	Yes	Yes	No
[70]	Yes	Yes	Yes	Yes	No
[71]	No	No	Yes	No	No
[72]	No	No	Yes	Yes	No
[73]	No	Yes	Yes	Yes	No
[74]	No	No	Yes	Yes	No
[75]	No	No	Yes	Yes	No
[76]	No	Yes	Yes	No	No
[77]	Yes	No	Yes	No	No
[78]	No	Yes	No	No	No
[79]	No	No	No	Yes	No
[80]	Yes	No	Yes	Yes	No
[81]	No	No	Yes	Yes	No
[82]	No	No	Yes	Yes	No
[83]	No	No	Yes	Yes	No
[84]	Yes	Yes	Yes	No	No
[85]	No	Yes	No	No	No

There's also a challenge in ensuring the privacy of IoT data, especially in scenarios where sensitive information is collected and shared. Therefore, exploring privacy-preserving techniques and data anonymization methods could be valuable research topics. There's an opportunity for improving the integration of LWD security with other emerging technologies, such as edge computing and blockchain, to create more comprehensive and resilient security solutions for IoT systems.

3. RESULTS AND DISCUSSION

This section is divided into 2 parts. The first part presents the research results of this study. Part 2 focuses on some of the key issues identified with possible recommendations and direction for future work.

3.1. Result

The objective of this paper is to analyze the security techniques of lightweight devices in the current trend. Out of thousands of studies from our initial search from the electronic databases, 55 studies were selected from 678 studies (excluding studies that did not meet the inclusion/exclusion criteria) to examine study similarity. The studies are then analyzed and evaluated. The findings of our study are as follows.

Figure 4 shows the similarities of the benefits obtained from these studies. From the chart, the advantages of lightweight device security techniques in the current trend are enhanced performance, reduced cost, enhanced security, and environment flexibility. An advantage that most of the article repeated was enhanced performance and enhanced security. While these methods offer benefits like increased security and improved network performance, they also face challenges such as scalability issues and the need for further research to address specific attack scenarios.

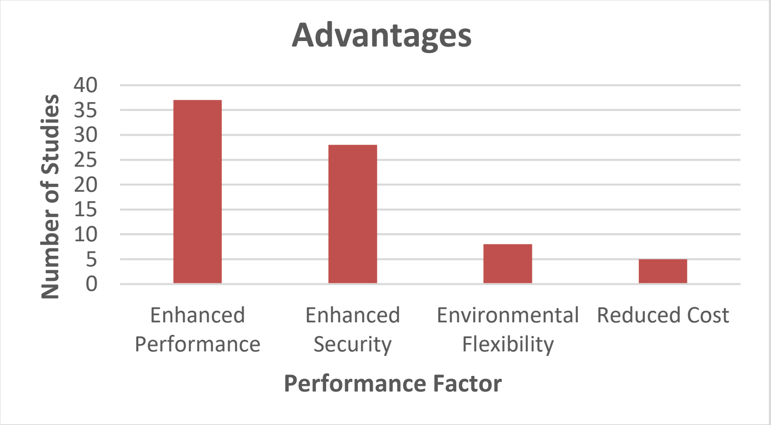

Figure 4. Advantages

Figure 5 visualized the shortcomings of lightweight device security techniques in the current trend, which are, capacity limitations (eg., power, storage, and memory), threat vulnerabilities (eg., lacks important security features), and complex computation (eg., consumes time or difficulty in configuring). The most common disadvantages are limited capacities and exposed to threat. This can make it difficult to ensure data protection, trust, confidentiality, authentication, and system-wide access control.

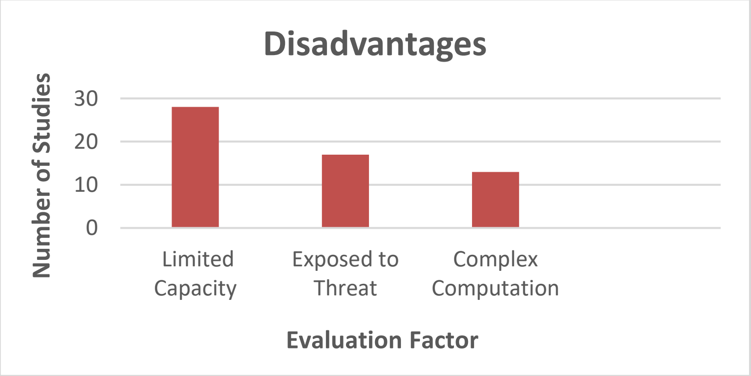

Figure 5. Disadvantages

Figure 6 shows how the test was conducted for security techniques of lightweight devices. In the current trend, which are, testbed and simulation. Out of the 56 studies analyzed, 28 used Testbed likewise in simulation.

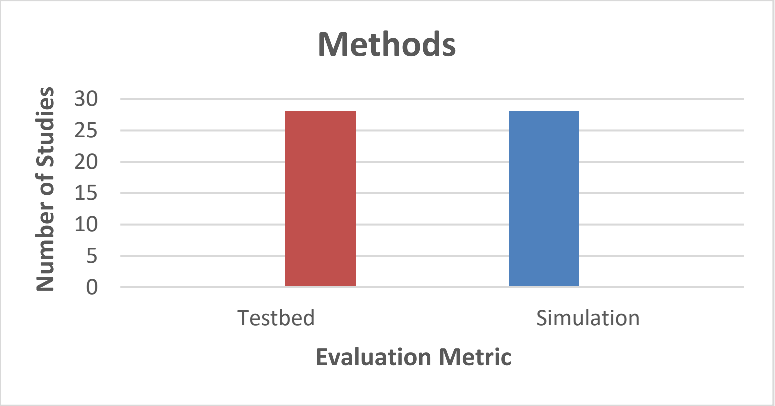

Figure 6. Methods

3.2. Challenges in lightweight device intrusion detection

As the landscape of IoT security continues to evolve, the development of effective lightweight intrusion detection systems (LIDS) and robust encryption algorithms will be essential in safeguarding IoT ecosystems from emerging security challenges. Furthermore, there are challenges in securing shared lightweight devices where multiple users or applications may access the same device. Developing access control mechanisms and secure data-sharing protocols is an important research area. Securing lightweight devices presents unique challenges due to their inherent limitations. These devices, often characterized by minimal processing power, memory, and battery life, require IDS that are both effective and resource efficient. Let’s delve deeper into these key hurdles:

- Resource constraints: lightweight devices typically lack the robust processing power and memory found in traditional computers. This translates to limitations in running complex algorithms or storing large datasets, both crucial elements for comprehensive intrusion detection. An IDS for these devices need to be lightweight and consume minimal resources to avoid impacting the device’s primary functionality.
- Heterogeneity: the diverse nature of lightweight devices adds another layer of complexity. With a multitude of forms, operating systems, and functionalities. A single, universal IDS solution becomes impractical. Instead, customization becomes essential, tailoring the IDS to the specific needs and capabilities of each device type and its intended application.
- Communication constraints: many lightweight devices prioritize low-power operation and may not have continuous network connectivity. This creates challenges for both transmitting intrusion alerts to a central monitoring system and receiving updates for the IDS databases themselves. The chosen IDS need to be adaptable to intermittent communication, ensuring critical alerts are delivered even with limited network availability.
- Real-time requirements: certain lightweight devices, particularly those critical for safety and security like medical implants or autonomous vehicles, demand real-time intrusion detection. In these scenarios, even a slight delay in identifying a threat can have serious consequences. The IDS need to be optimized for minimal latency, guaranteeing a swift response to any potential intrusion attempt.

By acknowledging these challenges, developers can create robust and efficient IDSs specifically designed for the unique requirements of resource-constrained devices.

3.3. Discussion

Most of the research on lightweight devices (LWD) focused on how to minimize energy consumption and accuracy of data, however, there are very few on how to improve the security [15], [27]. Security has always been and perhaps will always be a challenge. But the challenge is even greater when working within the resource constraints devices. Lightweight devices are practically in all aspect of our lives due to number of gadgets we are surrounded with. These devices are often available in different sizes and levels of complexity. Traditionally, power consumption has always been a limiting factor in these devices. This key factor is also an important challenge that requires ongoing research in the field of lightweight device. Cybercriminals are always on prowl, devising all sort of ways to steal our data. This is why data ought to be encrypted upon capture by the LWD device, thereby providing extra and more significant level of security. Thus, preventing threat such as cyberbullying. By encrypting data, you are giving additional layer of protection that secures your data from vulnerabilities that might occur further down the communication chain. Security is no longer optional because users need to know and believe that their data is protected. The cost of security breaches can be significant if the vulnerability is used to compromise the security of our networks or devices. The internet is the most powerful technology known to mankind, without it, our world, ability to work, keep in touch, and share information, would be radically different. This gives us a sense of urgency. Since lightweight devices are connected to the internet, attackers can easily gain access to the device. This is where the IDS come into play. Ideal IDS provide 100% efficiency against the possible vulnerabilities. Therefore, the significance of IDSs is undeniable.

The main challenges to the effectiveness and interpretation of this systematic review are the poor quality of the research process, the lack of regular and transparent behavior and reporting, and random errors. This includes the risk of an overall assessment of the quality of the evidence. The extent to which studies are designed and implemented is reasonable but does not rule out systematic bias in many published studies. In this way, the likelihood of overestimating the benefits and underestimating the harm is increased. Much emphasis was placed on assessing the methodological quality of the selected literature as far as possible and excluding articles of low methodological quality. This is important because the quality of a systematic review depends on the relevance and quality of the studies included in the literature review.

Furthermore, some studies lack systematic and transparent conduct and reporting. This may affect the quality of the review results for the work. Careful attention has been taken in selecting articles for the review to reduce the chances of making use of such kind of work. This will mitigate the impact of this threat. Evaluation of evidence quality is an important tool for systematic reviews and impacts the effectiveness of the work. It helps to initiate the integration of evidence and the transparency of findings. The studies involved in the study may include bias in the results or conclusions, as this may affect the effectiveness of the study. In addition, some of the studies used or selected have not fully explained the specific information that could be extracted. It is important to extract the data systematically. However, if one does not have the necessary information about the extracted content, it may affect the effectiveness of systematic reviews.

The future of IDS in LWDs lies in its ability to correlate and analyze data from other sources beyond the ones the device or network has interacted with in the past at record speed. it’s ability to examine data from other sources in different place would play a vital role in increasing its efficiency. The integration of edge computing capabilities in lightweight devices can enhance the ability to process data locally, therefore, reducing the need for constant data transmission and minimizing latency in intrusion detection. As machine learning techniques continue to evolve, there’s potential for more accurate and resource efficient intrusion detection in lightweight devices. Customized models can be trained to adapt to the unique characteristics of each device. Collaborative intelligence devices in IoT ecosystems can benefit from shared intelligence and centralized management systems, which can provide real-time updates and threat information, thereby enhancing security across the network. Lastly, the development of standardized protocols for intrusion detection in lightweight devices can simplify implementation, improve interoperability, and facilitate the exchange of threat intelligence. one should prioritise mobile cybersecurity measures, including robust antivirus software, regular updates, user education, and vigilance against social engineering tactics to safeguard their mobile devices and sensitive data. It also advised that individuals should check the permissions of apps that they use and think carefully before permitting an app, especially when it comes to high-risk permissions such as accessibility services.

3.4. Recommendation

Several approaches have been proposed and implemented to address intrusion detection in lightweight devices. These solutions are typically tailored to meet the specific challenges posed by these devices. While it is true that LIDS have gained attention in the context of IoT security, there are several criticisms and challenges associated with their implementation. One of the primary concerns with LIDS is the trade-off between detection accuracy and resource consumption. Lightweight IoT devices often have limited computational resources and energy constraints, and implementing robust intrusion detection mechanisms could further strain these resources. As a result, the effectiveness of LIDS in accurately detecting and mitigating security threats may be compromised.

Moreover, anomaly detection techniques, which are commonly used in LIDS for IoT security, are known to generate a significant number of false positives. This could lead to a high rate of false alarms, resulting in alert fatigue for system administrators and potentially causing them to overlook genuine security incidents. Additionally, while lightweight cryptographic techniques are explored for securing IoT data, there are concerns about the adequacy of these methods in providing strong security. Lightweight cryptographic algorithms may not offer the same level of protection as their traditional counterparts, leaving IoT systems vulnerable to sophisticated security attacks. Furthermore, the dynamic nature of IoT networks and the diversity of devices and applications pose a significant challenge for LIDS. Adapting intrusion detection mechanisms to the constantly evolving IoT environment is a complex task, and there is a risk that LIDS may lag in effectively addressing new and emerging security threats. In conclusion, while LIDS offer potential benefits for IoT security, it is important to carefully consider the trade-offs and limitations associated with their implementation, particularly in the context of resource constrained IoT devices and the evolving nature of security threats.

4. CONCLUSION

In conclusion, the development of LIDS has garnered significant attention in addressing the specific security constraints and requirements of lightweight IoT devices. However, it is crucial to carefully consider the trade-offs and limitations associated with their implementation, particularly in the context of resource constrained IoT devices and the evolving nature of security threats. As the landscape of IoT security continues to evolve, the development of effective LIDS and robust encryption algorithms will be essential in safeguarding IoT ecosystems from emerging security challenges. Furthermore, addressing the challenges in securing shared lightweight devices, improving anomaly detection, efficient key management, and distribution mechanisms, ensuring the privacy of IoT data, and integrating LWD security with other emerging technologies are vital research areas that require further exploration and development. By focusing on these research areas, the IoT community can work towards developing more comprehensive and resilient security solutions for IoT systems, ultimately enhancing the overall security posture of lightweight devices in IoT environments.

ACKNOWLEDGEMENTS

The author would like to thank the Research Group of Information Security Forensics and Computer Networking, Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka. The author also would like to express gratitude to the Center for Research and Innovation Management (CRIM) UTeM for the continuous support of this work. This work has been supported by Universiti Teknikal Malaysia Melaka.

REFERENCES

[1] C. Kiennert, Z. Ismail, H. Debar, and J. Leneutre, “A survey on game-theoretic approaches for intrusion detection and response optimization,” *ACM Computing Surveys (CSUR)*, vol. 51, no. 5, 2018, doi: 10.1145/3232848.

[2] Y. Al-Hadhrami and F. K. Hussain, “Real time dataset generation framework for intrusion detection systems in IoT,” *Future Generation Computer Systems*, vol. 108, pp. 414–423, 2020, doi: 10.1016/j.future.2020.02.051.

[3] N. Mohd, A. Singh, and H. S. Bhadauria, “A Novel SVM Based IDS for Distributed Denial of Sleep Strike in Wireless Sensor Networks,” *Wireless Personal Communications*, no. 0123456789, 2019, doi: 10.1007/s11277-019-06969-9.

[4] N. M. Shanono, N. A. Abu, and W. Mohamed, “Intrusion Detection System Architecture : Issues and Challenges,” *Technology Reports of Kansai University*, vol. 62, no. 7, 2020.

[5] V. Jyothsna, “A Review of Anomaly based IntrusionDetection Systems,” *International Journal of Computer Applications*, vol. 28, no. 7, pp. 975–8887, 2011.

[6] C. Day, “Intrusion prevention and detection systems,” *Managing Information Security: Second Edition*, pp. 119–142, 2013, doi: 10.1016/B978-0-12-416688-2.00005-2.

[7] A. Y. Poschmann, “Lightweight cryptography,” Ph.D. dissertation, Faculty of Electrical Engineering and Information Technology Ruhr-University Bochum, Germany, 2009.

[8] S. J. Roberts, “The Necessity of Information Security in the Vulnerable Pharmaceutical Industry,” *Journal of Information Security*, vol. 05, no. 04, pp. 147–153, 2014, doi: 10.4236/jis.2014.54014.

[9] M. Bajwa, “Wireless Network Security Threats and Mitigation—A Survey,” *Open Journal of Business and Management*, vol. 02, no. 04, pp. 292–297, 2014, doi: 10.4236/ojbm.2014.24034.

[10] A. Mohajer, M. H. Hajimobini, A. Mirzaei, and E. Noori, “Trusted-CDS Based Intrusion Detection System in Wireless Sensor Network (TC-IDS),” *OAlib*, vol. 01, no. 07, pp. 1–10, 2014, doi: 10.4236/oalib.1100848.

[11] “Network based Intrusion Detection System using the SPSS Method,” *REST Journal on Data Analytics and Artificial Intelligence*, vol. 2, no. 1, pp. 82–92, Mar. 2023, doi: 10.46632/jdaai/2/1/13.

[12] K. Nalavade and B. Meshram, “Layered Security Framework for Intrusion Prevention,” *IJCSNS International Journal of Computer Science and Network Security*, vol. 11, no. 6, pp. 253–259, 2011.

[13] J. Keteku, G. O. Dameh, S. A. Mante, T. K. Mensah, S. L. Amartey, and J.-B. Diekuu, “Detection and Prevention of Malware in Android Mobile Devices: A Literature Review,” *International Journal of Intelligence Science*, vol. 14, no. 04, pp. 71–93, 2024, doi: 10.4236/ijis.2024.144005.

[14] M. Jouhari and M. Guizani, “Lightweight CNN-BiLSTM based Intrusion Detection Systems for Resource-Constrained IoT Devices,” *2024 International Wireless Communications and Mobile Computing (IWCMC)*, Ayia Napa, Cyprus, 2024, pp. 1558-1563, doi: 10.1109/IWCMC61514.2024.10592352.

[15] W. Feng, Y. Qin, S. Zhao, and D. Feng, “AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS,” *Computer Networks*, vol. 134, pp. 167–182, 2018, doi: 10.1016/j.comnet.2018.01.039.

[16] M. Välimäki, K. Hipp, J. Chen, X. Huang, J. Guo, and M. S. Wong, “Sensor technology to monitor health, well-being and movement among healthcare personnel at workplace: A systematic scoping review protocol,” *BMJ Publishing Group*, Nov. 11, 2021, doi: 10.1136/bmjopen-2021-054408.

[17] R. Sen and K. Ramamritham, “Efficient data management on lightweight computing devices,” *21st International Conference on Data Engineering (ICDE'05)*, Tokyo, Japan, 2005, pp. 419-420, doi: 10.1109/ICDE.2005.58.

[18] O. Mbae, D. Mwathi, and E. Too, "Secure Cloud Based Approach for Mobile Devices User Data," *OAlib*, vol. 09, no. 09, pp. 1–20, 2022, doi: 10.4236/oalib.1109264.

[19] S. I. Nilima, M. K. Bhuyan, M. Kamruzzaman, J. Akter, R. Hasan, and F. T. Johora, "Optimizing Resource Management for IoT Devices in Constrained Environments," *Journal of Computer and Communications*, vol. 12, no. 08, pp. 81–98, 2024, doi: 10.4236/jcc.2024.128005.

[20] T. Kim, J. Noh, and S. Cho, "SCC: Storage Compression Consensus for Blockchain in Lightweight IoT Network," *2019 IEEE International Conference on Consumer Electronics, ICCE 2019*, pp. 1–4, 2019, doi: 10.1109/ICCE.2019.8662032.

[21] G. Dittmann and J. Jelitto, "A blockchain proxy for lightweight iot devices," *Proceedings - 2019 Crypto Valley Conference on Blockchain Technology, CVCBT 2019*, pp. 82–85, 2019, doi: 10.1109/CVCBT.2019.00015.

[22] Z. Chen, W. Ren, Y. Ren, and K. R. Choo, "wearable embedded devices by gestures or motions LiReK : A Lightweight and Real-time Key Establishment Scheme for Wearable Embedded Devices by Gestures or Motions," *Future Generation Computer Systems*, 2017, doi: 10.1016/j.future.2017.10.008.

[23] H. Noura, A. Chehab, and R. Couturier, "Lightweight Dynamic Key-Dependent and Flexible Cipher Scheme for IoT Devices," *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–8, 2019, doi: 10.1109/WCNC.2019.8885976.

[24] J. Höglund, S. Lindemer, M. Furuhed, and S. Raza, "PKI4IoT: Towards public key infrastructure for the Internet of Things," *Computers & Security*, vol. 89, 2020, doi: 10.1016/j.cose.2019.101658.

[25] A. Le-Tuan, M. Wylot, C. Hayes, and D. Le-Phuoc, "RDF4LED: An RDF engine for lightweight edge devices," *ACM International Conference Proceeding Series*, 2018, doi: 10.1145/3277593.3277600.

[26] Q. M. Malluhi, A. Shikfa, V. D. Tran, and V. C. Trinh, "Decentralized ciphertext-policy attribute-based encryption schemes for lightweight devices," *Computer Communications*, vol. 145, no. June, pp. 113–125, 2019, doi: 10.1016/j.comcom.2019.06.008.

[27] M. Al-Maitah, A. A. AlZubi, and A. Alarifi, "An optimal storage utilization technique for IoT devices using sequential machine learning," *Computer Networks*, vol. 152, pp. 98–105, 2019, doi: 10.1016/j.comnet.2019.01.025.

[28] A. Langiu, C. A. Boano, M. Schub, and K. Romer, "UpKit: An open-source, portable, and lightweight update framework for constrained IoT devices," *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, Dallas, TX, USA, 2019, pp. 2101-2112, doi: 10.1109/ICDCS.2019.00207.

[29] J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, "An intrusion detection framework for energy constrained IoT devices," *Mechanical Systems and Signal Processing*, vol. 136, p. 106436, 2020, doi: 10.1016/j.ymssp.2019.106436.

[30] Y. Xiao and M. Watson, "Guidance on Conducting a Systematic Literature Review," *Journal of Planning Education and Research*, vol. 39, no. 1, doi: 10.1177/0739456X17723971.

[31] Y. C. Tok, C. Wang, and S. Chattopadhyay, "STITCHER: Correlating digital forensic evidence on internet-of-things devices," *Forensic Science International: Digital Investigation*, vol. 35, p. 301071, 2020, doi: 10.1016/j.fsidi.2020.301071.

[32] A. H. Sodhro, S. Pirbhulal, M. Muzammal, and L. Zongwei, "Towards Blockchain-Enabled Security Technique for Industrial Internet of Things Based Decentralized Applications," *Journal of Grid Computing*, 2020, doi: 10.1007/s10723-020-09527-x.

[33] M. Zhang, J. Zheng, Q. Huang, and M. Kadoch, "Green communication for MIMO SWIPT-powered 5G Internet of Things with full-duplex relay base on secure transmission and energy collection constraints," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, 2020, doi: 10.1186/s13638-020-01732-2.

[34] M. Al-Akhras, M. Alawairdhi, A. Alawairdhi, and S. Atawneh, "Using Machine Learning To Build A Classification Model For Iot Networks To Detect Attack Signatures," *International Journal of Computer Networks and Communications*, vol. 12, no. 6, pp. 99–116, 2020, doi: 10.5121/ijcnc.2020.12607.

[35] C. A. de Souza, C. B. Westphall, R. B. Machado, J. B. M. Sobral, and G. dos S. Vieira, "Hybrid approach to intrusion detection in fog-based IoT environments," *Computer Networks*, vol. 180, 2020, doi: 10.1016/j.comnet.2020.107417.

[36] J. Lee, S. Choi, D. Kim, Y. Choi, and W. Sun, "A novel hardware security architecture for IoT Device: PD-CRP (PUF database and challenge-response pair) bloom filter on memristor-based PUF," *Applied Sciences (Switzerland)*, vol. 10, no. 19, 2020, doi: 10.3390/APP10196692.

[37] S. Sujanthi and S. N. Kalyani, "SecDL: QoS-Aware Secure Deep Learning Approach for Dynamic Cluster-Based Routing in WSN Assisted IoT," *Wireless Personal Communications*, vol. 114, no. 3, 2020. doi: 10.1007/s11277-020-07469-x.

[38] H. P. Lin, C. Y. Jung, T. Y. Huang, H. Hendrick, and Z. H. Wang, "NB-IoT Application on Decision Support System of Building Information Management," *Wireless Personal Communications*, vol. 114, no. 1, pp. 711–729, 2020, doi: 10.1007/s11277-020-07389-w.

[39] Y. Liu, K. Xue, P. He, D. S. L. Wei, and M. Guizani, "An Efficient, Accountable, and Privacy-Preserving Access Control Scheme for Internet of Things in a Sharing Economy Environment," in *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6634-6646, July 2020, doi: 10.1109/JIOT.2020.2975140.

[40] N. Guizani and A. Ghafoor, "A network function virtualization system for detecting malware in large IoT based networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1218–1228, 2020, doi: 10.1109/JSAC.2020.2986618.

[41] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020, doi: 10.1016/j.future.2020.02.017.

[42] S. A. Haider, M. N. Adil, and M. J. Zhao, "Optimization of secure wireless communications for IoT networks in the presence of eavesdroppers," *Computer Communications*, vol. 154, no. February, pp. 119–128, 2020, doi: 10.1016/j.comcom.2020.02.027.

[43] V. Morfino and S. Rampone, "Towards near-real-time intrusion detection for IoT devices using supervised learning and apache spark," *Electronics (Switzerland)*, vol. 9, no. 3, 2020, doi: 10.3390/electronics9030444.

[44] F. Tang, Y. Kawamoto, N. Kato, K. Yano, and Y. Suzuki, "Probe Delay Based Adaptive Port Scanning for IoT Devices with Private IP Address behind NAT," in *IEEE Network*, vol. 34, no. 2, pp. 195–201, 2020, doi: 10.1109/MNET.001.1900264.

[45] Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang, and X. Yang, "An attribute-based collaborative access control scheme using blockchain for IoT devices," *Electronics (Switzerland)*, vol. 9, no. 2, 2020, doi: 10.3390/electronics9020285.

[46] M. Amoon, T. Altameem, and A. Altameem, "RRAC: Role based reputed access control method for mitigating malicious impact in intelligent IoT platforms," *Computer Communications*, vol. 151, no. November 2019, pp. 238–246, 2020, doi: 10.1016/j.comcom.2020.01.011.

[47] H. Lei *et al.*, "Safeguarding UAV IoT Communication Systems Against Randomly Located Eavesdroppers," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1230–1244, 2020, doi: 10.1109/JIOT.2019.2953903.

[48] S. Zeadally and M. Tsikerdekis, "Securing Internet of Things (IoT) with machine learning," *International Journal of Communication Systems*, vol. 33, no. 1, pp. 1–16, 2020, doi: 10.1002/dac.4169.

[49] H. Mohammed, S. R. Hasan, and F. Awwad, “Fusion-on-field security and privacy preservation for IoT edge devices: Concurrent defense against multiple types of hardware trojan attacks,” *IEEE Access*, vol. 8, pp. 36847–36862, 2020, doi: 10.1109/ACCESS.2020.2975016.

[50] J. Li *et al.*, “Secrecy Wireless-Powered Sensor Networks for Internet of Things,” *Wireless Communications and Mobile Computing*, vol. 2020, 2020, doi: 10.1155/2020/8859264.

[51] M. A. Khan and K. A. Abuhasel, “An evolutionary multi-hidden Markov model for intelligent threat sensing in industrial internet of things,” *Journal of Supercomputing*, vol. 77, no. 6, pp. 6236–6250, 2021, doi: 10.1007/s11227-020-03513-6.

[52] S. Balamurugan, A. Ayyasamy, and K. S. Joseph, “Enhanced petri nets for traceability of food management using internet of things,” *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 30–43, 2021, doi: 10.1007/s12083-020-00943-0.

[53] D. Xu and H. Zhu, “Secure Transmission for SWIPT IoT Systems With Full-Duplex IoT Devices,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10915–10933, 2019, doi: 10.1109/JIOT.2019.2943377.

[54] Z. Deng, Q. Li, Q. Zhang, L. Yang, and J. Qin, “Beamforming Design for Physical Layer Security in a Two-Way Cognitive Radio IoT Network With SWIPT,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10786–10798, 2019, doi: 10.1109/JIOT.2019.2941873.

[55] A. Alnoman, S. K. Sharma, W. Ejaz, and A. Anpalagan, “Emerging edge computing technologies for distributed IoT systems,” *IEEE Network*, vol. 33, no. 6, pp. 140–147, 2019, doi: 10.1109/MNET.2019.1800543.

[56] A. Bytes, S. Adepu, and J. Zhou, “Towards Semantic Sensitive Feature Profiling of IoT Devices,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8056–8064, 2019, doi: 10.1109/JIOT.2019.2903739.

[57] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, “A Supervised Intrusion Detection System for Smart Home IoT Devices,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, 2019, doi: 10.1109/JIOT.2019.2926365.

[58] X. Ding, Y. Zou, F. Ding, D. Zhang, and G. Zhang, “Opportunistic Relaying Against Eavesdropping for Internet-of-Things: A Security-Reliability Tradeoff Perspective,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8727–8738, 2019, doi: 10.1109/JIOT.2019.2923273.

[59] X. Zheng, X. Hu, J. Zhang, J. Yang, S. Cai, and X. Xiong, “An efficient and low-power design of the SM3 hash algorithm for IoT,” *Electronics (Switzerland)*, vol. 8, no. 9, pp. 1–18, 2019, doi: 10.3390/electronics8091033.

[60] J. M. McGinthy, L. J. Wong, and A. J. Michaels, “Groundwork for Neural Network-Based Specific Emitter Identification Authentication for IoT,” *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6429–6440, 2019, doi: 10.1109/JIOT.2019.2908759.

[61] P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K. K. R. Choo, “A lightweight machine learning-based authentication framework for smart IoT devices,” *Information Sciences*, vol. 484, pp. 255–268, 2019, doi: 10.1016/j.ins.2019.01.073.

[62] W. Ji, J. Xu, H. Qiao, M. Zhou, and B. Liang, “Visual IoT: Enabling Internet of Things Visualization in Smart Cities,” *IEEE Network*, vol. 33, no. 2, pp. 102–110, 2019, doi: 10.1109/MNET.2019.1800258.

[63] L. Xu, J. Chen, M. Liu, and X. Wang, “Active eavesdropping detection based on large-dimensional random matrix theory for massive MIMO-enabled IoT,” *Electronics (Switzerland)*, vol. 8, no. 2, pp. 1–16, 2019, doi: 10.3390/electronics8020146.

[64] D. Wang, X. Zhang, T. Chen, and J. Li, “Discovering Vulnerabilities in COTS IoT Devices through Blackbox Fuzzing Web Management Interface,” *Security and Communication Networks*, vol. 2019, 2019, doi: 10.1155/2019/5076324.

[65] A. Karrothu and J. Norman, “An efficient method for group key management in Internet of Things using machine learning approach,” *Evol Intell*, vol. 14, no. 2, pp. 445–452, 2021, doi: 10.1007/s12065-019-00258-x.

[66] S. Arunkumar, S. Vairavasundaram, K. S. Ravichandran, and L. Ravi, “Riwt and qr factorization based hybrid robust image steganography using block selection algorithm for iot devices,” *Journal of Intelligent and Fuzzy Systems*, vol. 36, no. 5, pp. 4265–4276, 2019, doi: 10.3233/JIFS-169984.

[67] E. Anthi, S. Ahmad, O. Rana, G. Theodorakopoulos, and P. Burnap, “EclipseIoT: A secure and adaptive hub for the Internet of Things,” *Computers & Security*, vol. 78, pp. 477–490, 2018, doi: 10.1016/j.cose.2018.07.016.

[68] B. J. Mohd and T. Hayajneh, “Lightweight block ciphers for IoT: Energy optimization and survivability techniques,” *IEEE Access*, vol. 6, no. c, pp. 35966–35978, 2018, doi: 10.1109/ACCESS.2018.2848586.

[69] X. Liu, M. Zhao, S. Li, F. Zhang, and W. Trappe, “A security framework for the internet of things in the future internet architecture,” *Future Internet*, vol. 9, no. 3, pp. 1–28, 2017, doi: 10.3390/fi9030027.

[70] A. Saeed, A. L. I. Ahmadinia, A. Javed, and H. Larijani, “Intelligent Intrusion Detection in Low-Power IoTs,” *ACM Transactions on Internet Technology*, vol. 16, no. 4, 2016.

[71] J. Suarez, J. Quevedo, I. Vidal, D. Corujo, J. Garcia-Reinoso, and R. L. Aguiar, “A secure IoT management architecture based on Information-Centric Networking,” *Journal of Network and Computer Applications*, vol. 63, pp. 190–204, 2016, doi: 10.1016/j.jnca.2016.01.016.

[72] Z. Wang, H. Ding, J. Han, and J. Zhao, “Secure and efficient control transfer for IoT devices,” *International Journal of Distributed Sensor Networks*, vol. 2013, 2013, doi: 10.1155/2013/503404.

[73] Q. Qi, X. Chen, C. Zhong, and Z. Zhang, “Physical layer security for massive access in cellular Internet of Things,” *Science China Information Sciences*, vol. 63, no. 2, pp. 1–12, 2020, doi: 10.1007/s11432-019-2650-4.

[74] S. A. Alabady, F. Al-Turjman, and S. Din, “A Novel Security Model for Cooperative Virtual Networks in the IoT Era,” *International Journal of Parallel Programming*, vol. 48, no. 2, pp. 280–295, 2020, doi: 10.1007/s10766-018-0580-z.

[75] N. Alassaf, A. Gutub, S. A. Parah, and M. Al Ghamdi, “Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications,” *Multimedia Tools and Applications*, vol. 78, no. 23, pp. 32633–32657, 2019, doi: 10.1007/s11042-018-6801-z.

[76] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, “A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology,” *Multimedia Tools and Applications*, vol. 79, no. 15–16, pp. 9711–9733, 2020, doi: 10.1007/s11042-019-07835-3.

[77] S. Akhbarifar, H. H. S. Javadi, A. M. Rahmani, and M. Hosseinzadeh, “A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment,” *Personal and Ubiquitous Computing*, 2020, doi: 10.1007/s00779-020-01475-3.

[78] S. Sharma and V. K. Verma, “Security explorations for routing attacks in low power networks on internet of things,” *The Journal of Supercomputing*, vol. 77, pp. 4778–4812, 2021, doi: 10.1007/s11227-020-03471-z.

[79] T. Pasquier, J. Singh, J. Powles, D. Eyers, M. Seltzer, and J. Bacon, “Data provenance to audit compliance with privacy policy in the Internet of Things,” *Personal and Ubiquitous Computing*, vol. 22, no. 2, pp. 333–344, 2018, doi: 10.1007/s00779-017-1067-4.

[80] S. Lee, S. Lee, H. Yoo, S. Kwon, and T. Shon, “Design and implementation of cybersecurity testbed for industrial IoT systems,” *Journal of Supercomputing*, vol. 74, no. 9, pp. 4506–4520, 2018, doi: 10.1007/s11227-017-2219-z.

[81] Y. Duan, J. Li, G. Srivastava, and J. H. Yeh, “Data storage security for the Internet of Things,” *Journal of Supercomputing*, vol. 76, no. 11, pp. 8529–8547, 2020, doi: 10.1007/s11227-020-03148-7.

[82] V. Gupta, S. Khera, and N. Turk, “MQTT protocol employing IOT based home safety system with ABE encryption,” *Multimedia Tools and Applications*, 2020, doi: 10.1007/s11042-020-09750-4.

[83] Y. Jiang, A. Hu, and J. Huang, “A lightweight physical-layer based security strategy for Internet of things,” *Cluster Computing*, vol. 22, pp. 12971–12983, 2019, doi: 10.1007/s10586-018-1820-0.

[84] H. Rathore *et al.*, “Multi-layer security scheme for implantable medical devices,” *Neural Computing and Applications*, vol. 32, no. 9, pp. 4347–4360, 2020, doi: 10.1007/s00521-018-3819-0.

[85] D. Kim, Y. Lee, and S. Lee, “Mobile forensic reference set (MFReS) and mobile forensic investigation for android devices,” *Journal of Supercomputing*, vol. 74, no. 12, pp. 6618–6632, 2018, doi: 10.1007/s11227-017-2205-5.

BIOGRAPHIES OF AUTHORS

Nuruddeen Musa Shanono received his B.Sc. degree in Software Engineering with Multimedia from Limkokwing University of Creative Technolog and B.Sc. Computer Science from Anglia Rusking University in 2013. He received his Masters degree in Software Management from Limkokwing University of Creative Technology in 2015. Currently, he is pursuing Ph.D. in Network Security at Technical University of Malaysia Malacca. His research interests include malware and intrusion detection system. He can be contacted at email: noorshanono@gmail.com or P031810002@student.utem.edu.my.

Zulkiflee Muslim is a senior lecturer at Technical University of Malaysia Malacca (UTeM) since 2002. He obtained his first degree from University of Technology Malaysia (UTM) and his M.Sc. in Data Communication and Software from University of Birmingham City, UK. He also had several professional certifications including CCNAI, CCNAS, CFOT, and IPv6 Network Eng. Certified. His main research interest is related to IT Security, IDS and Feature Selection realm. He has become an active reviewer for several journals which related to network security domain. The main interest is the network security and application of artificial intelligence. He can be contacted at email: zulkiflee@utem.edu.my.

Nur Azman Abu currently works at the Department of Computer System and Communication as Associate Professor in Technical University of Malaysia Malacca. He does research in number theory, applied mathematics and algebra. His current project is ‘random ambience’. His qualifications are: Ph.D. in Cryptography (UTeM), Associate of Science in Computer Science (with distinction) Master of Science in Mathematics (Purdue University, US) Bachelor of Science (Hons) in Statistics (Purdue University). He can be contacted at email: nura@utem.edu.my.

Siti Rahayu Selamat is an Associate Professor at the Universiti Teknikal Malaysia Melaka, Malaysia. She received her Doctor of Philosophy in Computer Science (Digital Forensics). Her research interests include network forensics, cyber terrorism, cyber violence extremism, intrusion detection, network security and penetration testing. She is also a member of the information security, forensics and networking (INSFORNET) research group and is actively researching malware, criminal behaviour, and cyber violence extremism profiling. She can be contacted at email: sitirahayu@utem.edu.my.

Ts. Haniza Nahar a senior lecturer at University of Technical Malaysia Melaka (UTeM). She earned an M.Sc. in ICT for Engineers (distinction) from Coventry University, UK and B.Eng. in Telecommunication from University Malaya. She used to be an engineer and has been qualified for CFOT and IPv6 software engineer. Her postgraduate dissertation has been awarded the best project prize. She can be contacted at email: haniza@utem.edu.my.