

INTERNET OF THINGS (IOT) SECURITY AND ROUTING PROTOCOLS

Lecturer: Dr. Mohammed Anbar

Student ID: 251002398

Student Name: Abdel Hafez Adeeb Alassar

TABLE OF CONTENTS

ABSTRACT.....	1
CHAPTER 1	3
1.0 INTRODUCTION.....	3
1.1 BACKGROUND.....	5
1.2 PROBLEM STATEMENT	7
1.3 RESEARCH OBJECTIVES	8
1.4 RESEARCH SCOPE	9
CHAPTER 2	11
2.0 LITERATURE REVIEW.....	11
2.1 IMPORTANT THINKING	13
2.2 CONNECTIONS AND CONFLICTS	14
CHAPTER 3	15
3.0 RESEARCH METHODOLOGY	15
3.1 Expected Outcomes.....	17
3.3 GANTT CHART.....	18
REFERENCES	19

ABSTRACT

Linking different devices and allowing real-time data sharing across several sectors including healthcare, smart agriculture, industrial automation, and smart cities, the exponential growth of the Internet of Things (IoT) has fundamentally changed digital ecosystems. Still, this never experienced interconnectivity brings with it a many layered spectrum of privacy and security weaknesses, especially in the field of routing protocols and intrusion detection systems. Protocols like the Routing Protocol for Low Power and Lossy Networks (RPL) enable data routing in IoT environments, which are defined by resource constrained nodes working within low power and lossy networks (LLNs). Although RPL is becoming more and more popular, it is intrinsically vulnerable to advanced cyberattacks like version number manipulation, rank attacks, sinkhole intrusions, and selective forwarding, all of which seriously compromise data integrity, availability, and confidentiality. Moreover, traditional signature-based and rule-based security solutions lack the adaptability and intelligence needed to identify developing threats; hence, sophisticated Artificial Intelligence (AI) and Machine Learning (ML) techniques must be incorporated.

The research gives a thorough study of AI driven security frameworks inside IoT settings, homing in on the convergence of secure routing techniques and intrusion detection systems (IDS). Starting with a thorough systematic literature review to find current issues and research gaps, the study uses a demanding mixed methods research design. Data quality is gathered by semi structured interviews with field experts, protocol designers, and cyber security practitioners along with in-depth case studies to probe real-world application practices. Structured surveys aimed at a worldwide group of IoT developers and cybersecurity specialists help to gather quantitative insights. Threat perception, efficiency of

existing IDS methods, computational practicality, energy usage, and scalability issues are among the criteria evaluated by these studies.

The gathered empirical data guides the creation of a new, flexible, and light artificial intelligence powered cyber defence system. Optimized routing protocols are combined with supervised and ensemble learning models—such as Random Forest, CatBoost, and XGBoost—to improve real-time threat detection and secure data transmission in limited IoT environments. Performance metrics including detection accuracy, packet delivery ratio, latency, energy consumption, and false positive rates are evaluated using tools like Cooja and NS3 in simulation-based validation. Expert assessment and pilot use provide additional confirmation of the robustness, versatility, and practical usefulness of the framework.

Addressing important gaps in intrusion detection and routing security, this study helps to advance the theoretical and practical aspects of internet of things cybersecurity. Its AI-driven design is energy-efficient, context savvy, and validated, able to help in difficult cyber threats in changing IoT surroundings. The results have important strategic applications for how next generation security systems are developed and rolled out to fit the limitations and operational needs of modern IoT networks.

Keywords: Internet of Things (IoT), Intrusion Detection System (IDS), Routing Protocol for Low-Power and Lossy Networks (RPL), Cybersecurity, Artificial Intelligence (AI), Machine Learning (ML), Secure Routing, Energy Efficiency, Anomaly Detection, Low-Power Networks, Ensemble Learning, Mixed-Methods Research, Simulation-Based Validation, Adaptive Security Framework.

CHAPTER 1

1.0 INTRODUCTION

The Internet of Things (IoT) has changed conventional computing concepts by means of its arrival and quick spread allows ubiquitous, instant connectivity among digital systems, sensors, devices, and physical objects. Across many sectors including healthcare, manufacturing, transportation, agriculture, energy, and smart cities, this change of paradigm allows for fast communication, automation, and data-driven decision-making. The complexity and volume of data travelling across these networks have exploded with billions of gadgets connected via the internet and equipped with sensors and actuators, therefore presenting not just new chances but also unique cybersecurity challenges.

Operating mostly on lightweight communication protocols and decentralized architectures, IoT networks run in extremely dynamic and resource constrained surroundings. Because of its scalability and fit for limited devices, the Routing Protocol for Low Power and Lossy Networks (RPL) has been widely accepted standard for IoT routing. RPL and other routing algorithms nonetheless face many risks including version number attacks, rank attacks, sinkhole attacks, and selective forwarding. These assaults endanger system integrity and user privacy, disturb data flows, and compromise network dependability.

Adding to these limitations is the growing complexity of cyber criminals who use changing attack vectors to take advantage of the architectural and functional constraints of IOT ecosystems. These new dangers call for the use of intelligent, automatic, and flexible security systems since traditional rule-based and signature-based ones have proved useless. In answer, scientists have looked at Artificial Intelligence (AI) and Machine Learning (ML) to improve the resiliency and security of Internet-of-Things (IoT) networks.

Anomaly detection algorithms and AI-driven Intrusion Detection Systems (IDS) have shown great promise in increasing threat detection accuracy, lowering false positives, and automating incident response. Successful application of machine learning algorithms, including supervised, unsupervised, and ensemble learning, have been made to detect botnet operations, distributed denial-of-service (DDoS) attacks, and network behavioural anomalies. Furthermore, IDS systems have been enhanced by including cutting-edge feature selection techniques such as Principal Component Analysis (PCA) and classification models such as Random Forest, CatBoost, and XGBoost to raise detection performance.

Notwithstanding these developments, several thorny issues remain. Because of their demand for great computational power, artificial intelligence-based security systems are not especially appropriate for energy-constrained IOT devices. Furthermore, hampering the efficiency and acceptance of current approaches is the dependence on static datasets, the high rate of false positives, limited ability to adapt to new dangers, and the absence of real-world validation. Moreover, underexplored is the integration of security means with routing protocols, which leads to gaps in network protection all but throughout.

Using artificial intelligence and machine language tools, this study looks at the intersection of IoT security and routing protocol optimization to tackle these issues. It suggests building an intelligent, lightweight, and flexible AI-driven framework that combines intrusions detection with safe routing techniques. While guaranteeing real-time threat detection and safe data transmission, the research seeks to improve the general resiliency, scalability, and energy efficiency of Internet of Things networks.

The study combines simulation-based framework development, systematic literature review, qualitative interviews with field experts, and quantitative survey-based analysis. By interacting with interested parties, validating the framework in controlled and simulated

environments, and benchmarking performance against current solutions, this research seeks to provide ethical, scalable, and practical cybersecurity answers custom-fit for IoT networks.

By so doing, this study offers practical ideas for policy makers, developers, and practitioners wishing to implement strong and intelligent security systems in progressively more complicated IoT environments and also adds to the scholarly debate on AI in cybersecurity.

1.1 BACKGROUND

The explosion of the Internet of Things (IoT) has changed the scene of digital interconnectivity by allowing billions of varied devices spanning diverse industries including healthcare, industrial automation, transportation, agriculture, and intelligent cities to communicate and trade data almost automatically. This interdependent system enables unprecedented degree of automation, real-time monitoring, and efficient operations. But the quick growth of IoT also brings a difficult range of security and privacy problems—especially within the sphere of network routing and intrusion detection—about. Often working in resource-constrained, low-power, and lossy network (LLN) settings, internet of things devices are exposed to many vulnerabilities.

The Routing Protocol for Low-Power and Lossy Networks (RPL), specially created for restricted situations, most of all controls routing in IoT networks. Notwithstanding its appropriateness, RPL is naturally sensitive to several routing attacks such as Version Number Attacks (VNA), Rank Attacks, Sinkhole Attacks, and Selective Forwarding. These assaults let nefarious nodes interrupt routing paths, intercept sensitive information, and start Denial Of Service (DoS) attacks by means of protocol's structural vulnerabilities. As a result, the integrity, availability, and confidentiality of data travelling Internet of Things networks are

seriously compromised, therefore reducing user trust and slowing the usage of mission-critical Internet of Things technologies.

Recent studies have emphasized including Internet of Things (IoT) security frameworks Artificial Intelligence (AI) and Machine Learning (ML) tools as a way to reduce these dangers. Rising in popularity thanks to their dynamic threat identification, adaptive learning, and decreased dependence on set rule sets are AI-driven Intrusion Detection Systems (IDS). Research including Ejeofobiri et al. 2024) and alongside Saheed et al. In accurately identifying a range of threats including botnet and DDoS attacks, 2022 have shown the effectiveness of supervised and ensemble-based machine learning models like CatBoost, XGBoost, and Random Forest. Zagrouba and Alhajri (2021) also stressed the usefulness of small models customized for power-efficient environments, whereas Arshad et al. 2020) gave a comparative study on trade-off between detection accuracy, energy consumption, and user privacy.

Notwithstanding substantial headway, several technical and operational constraints continue to restrict the application of AI and ML-based solutions in actual Internet of Things configurations. Poor scalability, heavy energy use, and high computational complexity—along with limited practical value in limited circumstances—impede the application of these models. Moreover, many suggested approaches are created and validated using artificial or simulation-based data sets, therefore restricting their applicability to actual network circumstances. Furthermore, of note is a research gap in dealing hybrid attacks combining several vectors as well as building adaptive IDS able to change with developing threats. Centralized against decentralized IDS structures is another contentious issue since each method has unique benefits and drawbacks in scalability, response time, and resource allocation.

Routing protocol security is another important aspect needed to preserve a steady and dependable communication framework in IoT networks. Alfrichat et al. 3 Alghamdi and Bellaiche (2022) and (2024) point out major flaws in present routing methods and suggest systems for incorporating cryptographic approaches with anomaly detection. Particularly in extensive, varied network settings, nevertheless, the difficulties of computational overhead, latency, and real-time adaptability continue to be raised.

This study therefore seeks to close the current divides by thoroughly assessing modern AI-based intrusion detection and secure routing methods in IoT networks. It will lead in the creation of an original, flexible, and energy-efficient AI-driven cybersecurity platform. This architecture will be tailored particularly to work well in IoT environments constrained in resources, therefore guaranteeing real-time detection, resilience against many different attack mechanisms, and easy integration with current routing networks. By resolving the dual problems of intrusion detection and secure routing, this research aims to improve the dependability, scalability, and integrity of Internet of Things environments in both academic and commercial applications.

1.2 PROBLEM STATEMENT

Since cyber threats are constantly changing, there is a great danger to digital infrastructure that calls for sophisticated detection and response systems. Traditional cybersecurity techniques including rule-based systems and signature-based threat detection have difficulty dealing with new developments including zero-day exploits, insider attacks, and advanced phishing tactics. Recent developments in Artificial Intelligence (AI) and Machine Learning (ML) have shown better threat detection using anomaly detection, behavioural analysis, and

real-time response automation. Notwithstanding these improvements, existing AI-driven cybersecurity solutions have many significant drawbacks, such as high false positive rates, hostile vulnerabilities, computational overhead, and ethical concerns.

Especially in Internet of Things (IoT) settings and insider threat cases, the literature emphasizes the accuracy of deep learning models; including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs); in identifying cyber dangers. Still, these techniques demand significant computational power, therefore restricting their use in resource-limited settings. Natural Language Processing (NLP)based threat detection has also shown promise in reducing phishing attacks, but bias in AI training data and model opacity are still significant problems. Moreover, adversarial machine learning approaches enable threat agents to go around AI security systems, therefore compromising the strength of current cyber security models.

Even with these developments, there is a crucial lack in linking artificial intelligence cyber security systems with current security infrastructure to improve real time threat answer, increase computer efficiency, and guarantee moral openness. Effective real-world applications would call for research to create adaptive, explainable, and computationally efficient A driven security systems that can effectively fight cyber risks while also handling adversarial robustness, ethical issues, and deployment problems.

1.3 RESEARCH OBJECTIVES

This study's main goal is to create an improved AI-based cyber security architecture that improves ethical openness, response automation, and threat detection. The particular objectives are:

- To assess artificial intelligence-based cyber security systems in terms of their capacity to find and stop changing internet threats together with their benefits, constraints, and operational issues.
- To assess the performance of many machine learning approaches; such supervised learning, unsupervised learning, and reinforcement learning; in internet security scenarios.
- To create an AI-powered cybersecurity system that improves live threat identification and meshes effortlessly with current security systems.
- Given artificial intelligence-driven threat detection models, research the moral, openness, and adversarial risks thereof and suggest approaches to improve AI explainability and governance.
- To maximize AI-driven cybersecurity solutions to lower computational overhead and increase scalability, particularly in IoT and cloud settings.

1.4 RESEARCH SCOPE

The research concentrates on building a strong and energy-efficient framework that combines secure routing protocols with advanced intrusion detection systems (IDS) to improve the security of Internet of Things (IoT) networks. With the goal of finding performance restrictions, computational problems, and practical deployment problems, the scope of this study includes a thorough analysis of current AI-driven intrusion detection methods and routing protocols employed in Internet of Things contexts.

The research will especially investigate the use of supervised, unsupervised, and ensemble-based machine learning models in identifying several IoT-specific threats including botnet

attacks, Distributed Denial of Service (DDoS) attacks, version number manipulation, and data forwarding attacks. Particularly in low-power and lossy network (LLN) environments, it will also analyse the strengths and drawbacks of traditional routing techniques, particularly RPL, in responding to these dangers.

In addition to theoretical and simulation-based analyses, the research will use case studies, expert evaluations, and testbed experiments where possible to include real-world validation. Suggested solutions' energy efficiency, scalability, and adaptability will be closely examined in real-time Internet of Things environments. The practicality of using AI-based security systems on resource-constrained devices, ethical issues, and privacy issues will be analysed.

While the scope will be rather narrow on hardware-based encryption methods or physical-layer security models, it will instead focus on software-driven, intelligent security strategies that might be deployed across a varied spectrum of IoT networks. The anticipated result is a verified, scalable, lightweight framework able to identify changing threats, optimize routing paths, and maintain energy efficiency while also increasing the general resilience of IoT networks.

CHAPTER 2

2.0 LITERATURE REVIEW

The fast growth of the Internet of Things (IoT) has added new dimensions to digital connectivity, opening both creative chances and serious security risks. The intrinsically distributed, resource-limited, and varied character of IoT networks has made them vulnerable to a variety of advanced cyber-attacks, especially at the network layer and inside routing protocols. Drawing on six recent academic publications, this literature review combines results of studies on several different aspects of intrusion detection systems (IDS), machine learning (ML)based threat detection, and safe routing techniques customized for IoT settings.

Ejeofobiri, C. K., Victor-Igun, O. O., & Okoye, C. (2024) suggest a hybrid AI-driven intrusion detection model especially developed for IoT networks. The research divides IDS methods into supervised, unsupervised, and reinforcement learning paradigms and underlines their real-time anomaly identification performance. Although the technique is constrained by high computational demands and energy inefficiency—two main restrictions in IoT surroundings defined by limited processing power and battery capacity— it produces strengthened detection abilities, especially in recognizing hitherto unknown threats.

Saheed et al. Trained on the UNSWNB15 dataset, 2022 advance the conversation by means of machine learning approaches including CatBoost and XGBoost. Including Principal Component Analysis (PCA) for dimensionality reduction in their study increases classification accuracy to a remarkable 99.9%. Their model's scalability in Realtime environments is, nonetheless, in doubt since the overhead linked with controlling broadscale deployments and high false-positive rates are rather high. This uncovers a fundamental difficulty in transforming high-performing simulation-based models into practical, scalable uses.

Alrfi eather et al. (2024) Investigating Version Number Attacks (VNA) aimed at the Routing Protocol for Low-Power and Lossy Networks (RPL), one should focus on routing level vulnerabilities. Their research calls for hybrid solutions combining anomaly detection and low-weight cryptography methods and offers a thorough classification of current mitigation measures. Notwithstanding the elaborate classification, the document points out the lack of real-world validation and stresses the need for more adaptive, scalable, and resilient routing security architectures able to evolve with network conditions.

Using Integrated Evaluation Metrics (IEM), Alghamdi and Bellaiche (2022) suggest an ensemble-based IDS powered by several machine learning classifiers. Their findings reveal improved adaptability over many different IoT network setups and nearly perfect detection accuracy—that is, 99.45%. Still, the raised computational complexity linked with ensemble learning techniques begs questions about their viability in settings with very restricted memory and energy availability. The research highlights a repeating trade-off in IoT security studies: resource consumption against performance accuracy.

Using anomaly detection techniques and random forest classifiers, Zagrouba and Alhajri (2021) explore the identification of Distributed Denial of Service (DDoS) attacks with botnet purposes. Their approach provides strong defense against volumetric strikes since it achieves a near perfect detection rate of 99.99%. But the absence of a dynamic learning mechanism reduces the model's adaptability to changing threat environments. The research also highlights the inability of the model to distinguish between hybrid assault channels, thereby indicating a more general restriction in modern intrusion detection work.

Arshad et al. and Asharini et al. By examining the interaction between performance, energy consumption, and privacy throughout different IDS frameworks, 2020 provide a macrolevel view. Their comparative analysis underlines the immediate need of adaptive models that find

a perfect balance of energy efficiency and detection capability. Particularly in contexts where data sensitivity is of first importance, they stress the need of including privacy-preserving techniques. For scientists looking to create IDS that are safe, effective, and privacy-aware, this presents a multidimensional optimization difficulty.

2.1 IMPORTANT THINKING

Taken together, the considerable development achieved in using AI and ML to improve IoT security is underlined by the cumulative body of research. Substantial improvements in detection accuracy, scalability, and automation have been evidenced by advanced classifiers, ensemble learning methods, and adaptive IDS models as in other Time Machine notes here. Furthermore, offering quantifiable insights into model accuracy, several studies also provide tough performance appraisals from standardized datasets.

Notwithstanding these developments, several drawbacks endure. One recurring theme among the examined papers is the dependency on simulated or benchmark data, which might not accurately represent the intricacy of actual IoT environments. Furthermore, acting as major obstacles to actual deployment are great computational and memory demands, particularly in limited devices. Many models neglect hybrid attacks that merge several strategies and techniques and lack real-time learning capabilities.

There is also a recurring tension between centralized and decentralized IDS architectures. Centralized models tend to offer higher detection rates but suffer from latency and single points of failure, while decentralized models provide robustness and scalability at the cost of reduced detection accuracy. Moreover, ethical and privacy considerations are often

underexplored, raising concerns about data misuse and the opacity of AI-driven decision-making processes.

2.2 CONNECTIONS AND CONFLICTS

The studies converge on several key themes, particularly the need for adaptive, energy-efficient, and scalable IDS frameworks that can operate reliably in dynamic IoT environments. They also uniformly recognize the vulnerabilities of RPL and the importance of securing routing protocols against targeted attacks such as VNAs and sinkhole attacks.

However, methodological divergences are evident. Some researchers prioritize the use of ensemble and supervised learning techniques for higher accuracy, while others advocate for anomaly-based and lightweight models that prioritize resource efficiency. These differences reflect broader debates in the field regarding the prioritization of detection accuracy versus system overhead and real-time applicability.

In sum, the reviewed literature provides a critical foundation for this research, which seeks to bridge existing gaps by developing a novel AI-driven framework that integrates secure routing with adaptive intrusion detection capabilities. The framework aims to balance performance, energy efficiency, scalability, and ethical transparency, offering a practical solution for next-generation IoT security challenges.

CHAPTER 3

3.0 RESEARCH METHODOLOGY

In this study, we use a well-rounded research approach that blends both qualitative and quantitative methods. This helps us take a deeper and more complete look at how artificial intelligence can improve IoT security and make routing protocols more efficient. This integrated approach allows for a multi-layered analysis of current techniques, their practical implications, and the development of an advanced AI-driven security framework specifically designed for constrained IoT environments.

Phase 1: Systematic Literature Review

The research begins with an in-depth systematic literature review aimed at synthesizing findings from scholarly articles, peer-reviewed journals, technical standards, and white papers. This phase identifies key AI and ML methods applied to intrusion detection and routing in IoT, their comparative efficiencies, and limitations in deployment. A synthesis matrix is used to categorize research design, findings, methodologies, and limitations across studies. The literature review not only informs subsequent phases but also provides critical insight into existing research gaps and potential areas for innovation.

Phase 2: Qualitative Inquiry via Expert Interviews and Case Studies

The qualitative phase employs purposive and snowball sampling to recruit a diverse panel of experts, including IoT security architects, AI system engineers, protocol developers, and cybersecurity policymakers. Data will be collected through in-depth semi-structured interviews focused on practical implementation experiences, challenges with energy efficiency, real-time detection, model transparency, and integration with existing infrastructures. Concurrently, detailed case studies will examine organizations that have

implemented AI-based IDS and RPL security enhancements. Thematic coding and grounded theory will guide the analysis of interview and case study data to reveal context-specific insights and strategic design considerations.

Phase 3: Quantitative Survey-Based Analysis

The third phase involves the design and administration of a comprehensive survey targeted at cybersecurity professionals, researchers, and IoT practitioners globally. The survey will collect data on a range of variables, including perceived threat levels, IDS accuracy, energy consumption patterns, deployment feasibility, and adaptive routing success. Likert-scale items, categorical questions, and scenario-based responses will be analyzed using SPSS and R. Descriptive and inferential statistical techniques such as chi-square tests, multivariate regression, and factor analysis will be used to identify statistically significant patterns and validate qualitative findings.

Phase 4: Simulation-Based Framework Development

Building on previous phases, a novel AI-driven framework integrating intrusion detection and secure routing protocols will be developed. The framework will incorporate lightweight AI algorithms optimized for edge processing, anomaly detection, and secure RPL extensions. Framework development will utilize simulation tools such as Cooja (for Contiki OS) and NS-3 to model routing behaviours, attack vectors, and IDS responses in LLN environments. Performance metrics will include packet delivery ratio, energy consumption, throughput, latency, detection accuracy, false positive/negative rates, and memory footprint.

Phase 5: Validation and Pilot Testing

The proposed framework will undergo extensive validation through expert reviews, lab-based emulation using IoT development boards (e.g., Raspberry Pi, ESP32), and testbed deployment where feasible. Expert validation will follow the Delphi method to ensure iterative refinement and consensus. Pilot testing in controlled environments will assess real-world feasibility, scalability, and adaptability. Evaluation results will be benchmarked against existing solutions using standardized testing scenarios.

Ethical Considerations

This research will adhere strictly to ethical standards. Participants in interviews and surveys will be fully informed about the study's purpose, assured of confidentiality, and required to provide informed consent. Ethical approval will be secured from institutional review boards. Data handling will comply with data protection regulations such as GDPR.

Limitations

This study acknowledges potential limitations such as restricted access to real-time threat datasets, reliance on simulation environments, limited scalability testing across large heterogeneous networks, and the generalizability of case study findings. Triangulation, sensitivity analysis, and iterative expert consultation will be employed to minimize these limitations and enhance research credibility.

3.1 Expected Outcomes

The research is expected to result in a validated, lightweight, and adaptive AI-driven cybersecurity framework tailored for IoT environments. The framework will address real-time intrusion detection, secure and efficient routing, energy optimization, and adversarial

robustness. It aims to serve as a scalable model for practical deployment in real-world IoT infrastructures and a reference architecture for future research and development initiatives in AI-powered IoT security.

3.3 GANTT CHART



Task	Start Date	Duration (Days)
Literature Review	1/1/2025	15
Formulate Research Questions	1/16/2025	15
Develop Methodology	2/1/2025	15
Data Collection	2/16/2025	25
Data Analysis	3/15/2025	10
Framework Development	3/25/2025	7
Drafting Thesis	4/1/2025	10
Revisions	4/15/2025	5
Final Submission	4/25/2025	4
Presentation Preparation	4/30/2025	3

REFERENCES

- Zagrouba, R., &Alhajri, R. (2021). Machine learning based attacks detection and countermeasures in IoT. *International Journal of Communication Networks and Information Security*, 13(2), 158-167. <https://core.ac.uk/download/pdf/539893726.pdf>
- Alfrieht, N., Anbar, M., Karuppayah, S., Rihan, S. D. A., Alabsi, B. A., & Momani, A. M. (2024). Detecting version number attacks in low power and lossy networks for internet of things routing: review and taxonomy. *IEEE Access*. <https://ieeexplore.ieee.org/abstract/document/10443394/>
- Ejeofobiri, C. K., Victor-Igun, O. O., & Okoye, C. (2024). AI-Driven Secure Intrusion Detection for Internet of Things (IOT) Networks. *Asian Journal of Mathematics and Computer Research*, 31(4), 40-55. <https://hal.science/hal-04826235/>
- Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., &Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, 61(12), 9395-9409. <https://www.sciencedirect.com/science/article/pii/S1110016822001570>
- Alghamdi, R., &Bellaiche, M. (2022). Evaluation and selection models for ensemble intrusion detection systems in IoT. *IoT*, 3(2), 285-314. <https://www.mdpi.com/2624-831X/3/2/17>
- Arshad, J., Azad, M. A., Amad, R., Salah, K., Alazab, M., & Iqbal, R. (2020). A review of performance, energy and privacy of intrusion detection systems for IoT. *Electronics*, 9(4), 629. <https://www.mdpi.com/2079-9292/9/4/629>