Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 22 February 2025

Hand-in Date: 8 March 2025

Hand-in Method: Online Submission via E-Learning.

Assignment Report: A LITERATURE REVIEW REPORT ON INTERNET OF THINGS (IOT) SECURITY AND ROUTING PROTOCOLS

Student ID: 251002398

Student Name: Abdel Hafez Alassar

Contents

Abstract 2

Summary of Research Papers 2

Critical Analysis 4

Connections and Conflicts 5

Synthesis Matrix for Literature Review: 7

References 9

Abstract

The increasing adoption of the Internet of Things (IoT) has introduced security vulnerabilities, particularly in routing protocols, which are critical for network performance and security. This paper reviews six recent research studies focusing on intrusion detection, machine learning-based threat detection, and secure routing mechanisms in IoT networks. The studies analyse various security threats, including version number attacks, botnet attacks, and energy-efficient intrusion detection strategies. Key findings highlight the efficiency of AI-driven models, machine learning approaches, and ensemble intrusion detection systems in identifying and mitigating threats. However, challenges such as computational overhead, energy constraints, and real-world applicability remain significant concerns. This review emphasizes the need for continuous innovation in securing IoT networks and optimizing routing protocols

Summary of Research Papers

Paper 1: AI-DRIVEN SECURE INTRUSION DETECTION FOR INTERNET OF THINGS (IOT) NETWORKS(Ejeofobiri et al., 2024)

This study explores AI-powered intrusion detection systems (IDS) designed for IoT environments. By leveraging machine learning techniques, the proposed system enhances real-time anomaly detection. The paper categorizes existing IDS approaches into supervised, unsupervised, and reinforcement learning models. Key findings indicate that AI-driven IDS significantly improve detection accuracy but face challenges related to computational efficiency and energy constraints in IoT devices.

Paper 2: A MACHINE LEARNING-BASED INTRUSION DETECTION FOR DETECTING INTERNET OF THINGS NETWORK ATTACKS(Saheed et al., 2022)

This research introduces a machine learning-based IDS using the UNSW-NB15 dataset. The study employs principal component analysis (PCA) for feature selection and utilizes multiple ML algorithms, including CatBoost and XGBoost. The results show a 99.9% accuracy in attack detection. The paper highlights challenges such as high false positives and scalability concerns in real-time applications.

Paper 3: DETECTING VERSION NUMBER ATTACKS IN LOW POWER AND LOSSY NETWORKS FOR INTERNET OF THINGS ROUTING: REVIEW AND TAXONOMY (Alfriehat et al., 2024)

This paper focuses on securing Routing Protocol for Low-Power and Lossy Networks (RPL) by addressing version number attacks (VNA). The study categorizes existing detection and mitigation approaches, evaluating their efficiency. Key findings indicate that RPL networks remain highly susceptible to VNAs, necessitating improved security frameworks. The paper identifies the need for hybrid security solutions integrating both anomaly detection and lightweight cryptographic techniques.

Paper 4: EVALUATION AND SELECTION MODELS FOR ENSEMBLE INTRUSION DETECTION SYSTEMS IN IOT(Alghamdi &Bellaiche, 2022)

This study presents an ensemble-based approach to intrusion detection, combining multiple ML classifiers for enhanced accuracy. The researchers evaluate different IDS models based on integrated evaluation metrics (IEM). The proposed system demonstrates improved accuracy (99.45%) and scalability. However, the study acknowledges limitations such as increased computational complexity and the need for real-world dataset validation.

Paper 5: MACHINE LEARNING-BASED ATTACKS DETECTION AND COUNTERMEASURES IN IOT(Zagrouba&Alhajri, 2021)

This research investigates ML-based detection strategies for IoT botnet attacks, with a focus on distributed denial-of-service (DDoS) mitigation. The study employs random forest classifiers and anomaly detection techniques, achieving a 99.99% accuracy rate. The findings emphasize the importance of low-power security solutions suitable for constrained IoT devices.

Paper 6: A REVIEW OF PERFORMANCE, ENERGY, AND PRIVACY OF INTRUSION DETECTION SYSTEMS FOR IOT(Arshad et al., 2020)

This paper provides a comparative analysis of intrusion detection methods in IoT, focusing on trade-offs between performance, energy consumption, and privacy concerns. The study highlights the challenges of balancing detection accuracy with resource efficiency. Key insights suggest the need for adaptive IDS models that can optimize security without compromising energy efficiency.

Critical Analysis

The reviewed studies provide a comprehensive perspective on IoT security, focusing on intrusion detection, attack prevention, and secure routing protocols. While they present valuable contributions, several strengths and limitations emerge upon critical evaluation.

One of the major strengths of the reviewed studies is the introduction of innovative security mechanisms. Many of the papers propose novel techniques, such as AI-driven intrusion detection systems and ensemble machine learning-based intrusion detection systems (IDS), which enhance cybersecurity through automation and predictive modeling. Additionally, the

research employing machine learning techniques reports impressive detection rates, demonstrating the efficiency of AI and ML in identifying cyber threats. These studies also provide comprehensive analyses of routing attacks, particularly in RPL-based networks, offering valuable insights for future countermeasures. Another significant contribution is the focus on energy efficiency, as some studies highlight the trade-off between energy consumption and security in IoT intrusion detection, recognizing the importance of designing lightweight yet effective security solutions. Scalability and adaptability also stand out as key strengths, as some papers discuss IDS models that can be deployed across different IoT environments, accommodating various network sizes and architectures.

Despite these strengths, several limitations remain. A primary concern is the lack of real-world deployment, as most studies rely on simulations or predefined datasets rather than actual IoT implementations, raising questions about their practical applicability. Moreover, the high computational costs of AI and ML-based intrusion detection methods pose challenges for resource-constrained IoT devices. Another limitation is the limited consideration of hybrid attacks, as the reviewed studies primarily focus on specific attack types rather than addressing evolving cyber threats that combine multiple attack vectors. Additionally, scalability concerns exist in large-scale networks, where ensemble learning models may improve accuracy but at the expense of increased computational and memory demands. Finally, while AI and ML techniques enhance security, their reliance on static datasets limits their adaptability to new attack patterns, highlighting the need for continuous learning mechanisms to address evolving threats.

Connections and Conflicts

The analyzed research works demonstrate significant thematic links through their collective emphasis on protecting IoT networks by utilizing artificial intelligence and machine learning

techniques alongside sophisticated routing protocols. The reviewed papers uniformly focus on intrusion detection systems to examine solutions for detecting and addressing cybersecurity threats in IoT networks. Multiple research papers demonstrate how machine learning helps automate security functions while decreasing human involvement in intrusion detection tasks. Multiple studies examine the vulnerabilities present in low-power and lossy networks (LLNs) while suggesting enhancements to the Routing Protocol for Low-power and Lossy Networks (RPL) as part of their focus on routing security. The issue of energy efficiency is a prominent topic because multiple papers investigate how security performance interacts with the power limitations of IoT devices.

The research connections exist but they also highlight differing perspectives within the studies. The main disagreement revolves around which is superior for intrusion detection: centralized approaches or distributed methods. Multiple research papers support centralized machine learning models for network protection while other studies recommend using decentralized and lightweight IDS systems to serve resource-limited IoT settings. The field of detection methodologies experiences a fundamental disagreement because certain studies support signature-based intrusion detection systems while others promote artificial intelligence-driven anomaly detection approaches. Some research highlights the importance of lightweight security solutions for IoT devices with limited computational resources yet other research supports the development of complex multi-layered security structures despite their higher complexity and overhead.

The tension between scalable solutions and accurate threat detection emerges as a significant challenge because ensemble models and deep learning techniques deliver superior accuracy yet face difficulties in real-time application because of their high computational requirements. Some research areas concentrate on theoretical evaluations of security models whereas others

execute empirical experiments which results in inconsistencies during real-world applicability assessments.

Synthesis Matrix for Literature Review:

Study	Authors	Year	Research Design	Key Findings/Results	Methodology	Limitations
AI-Driven Secure Intrusion Detection for Internet of Things (IOT) Networks	Ejeofobiri et al.	2024	Experimental & Theoretical Analysis	AI-driven IDS enhances real-time anomaly detection but faces energy constraints.	AI-based intrusion detection using supervised and unsupervised learning models	High computational overhead, limited real-world deployment
A machine learning-based intrusion detection for detecting internet of things network attacks	Saheed et al.	2022	Experimental	Machine learning classifiers improve attack detection accuracy to 99.9%.	Feature selection using PCA, classification with CatBoost and XGBoost	High false positives, scalability concerns
Detecting Version Number Attacks in Low Power and Lossy Networks for Internet of Things Routing: Review and Taxonomy	Alfriehat et al.	2024	Review & Taxonomy	RPL networks are vulnerable to VNAs; hybrid security models needed.	Classification of existing RPL attack mitigation techniques	Lack of practical implementation and real-time validation
Evaluation and Selection Models for Ensemble Intrusion Detection Systems in IoT	Alghamdi &Bellaiche	2022	Experimental	Ensemble-based IDS enhances accuracy to 99.45% and scalability.	Multi-classifier ensemble evaluation using IEM	High computational complexity, real-world validation needed
Machine Learning based Attacks Detection and Countermeasures in IoT	Zagrouba&Alhajri	2021	Experimental	ML-based models detect botnet and DDoS attacks with 99.99% accuracy.	Random forest classifiers, anomaly detection methods	Real-time constraints, model adaptability concerns

A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT	Arshad et al.	2020	Review & Comparative Analysis	IDS solutions trade off between energy efficiency, detection performance, and privacy.	Comparative study of various IDS frameworks	Need for adaptive IDS models balancing efficiency and security

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

Alfriehat, 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