A Comparative Analysis for Designing Security Mechanism for Resource-Constrained Internet of Things Devices

Sristi Vashisth, Anjali Goyal

Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh, India

Corresponding author: Sristi Vashisth, Email: srishtivashisht1509@gmail.com

In today's digital age, the rise of Internet of Things (IoT) devices has remarkably transformed technological interactions, offering unprecedented convenience and efficiency across various domains. However, this rapid increase in IoT adoption has also introduced significant network security challenges, as these interconnected devices offer a broader surface vulnerable to cyber threats. Intrusion Detection Systems (IDS) aim to monitor network traffic, identify suspicious patterns, and promptly respond to potential security breaches. This paper provides a comprehensive review of various machine learning algorithms employed in IDS specifically designed for IoT devices. Our primary objective is to critically evaluate the efficiency, strengths, and limitations of these algorithms in detecting and countering threats within the unique constraints of IoT ecosystems. This review encompasses a thorough analysis of emerging ML technologies, including but not limited to Decision Trees, Support Vector Machines, Random Forests, Neural Networks, and Deep Learning models.

Keywords: Network Security, Machine Learning, Intrusion Detection

in: *Advancements in Communication and Systems*. Ed. by Ashish Kumar Tripathi and Vivek Shrivastava. Computing and Intelligent Systems, SCRS, India., 2023, pp. 21–35. DOI: https://doi.org/10.56155/978-81-955020-7-3-3

1 Introduction

The Internet of Things (IoT) has become a pivotal force in enhancing collaboration and communication in recent years. Its widespread adoption has introduced unparalleled convenience to our daily lives, a stark contrast to previous decades. The significance of IoT spans both private and public sectors, with many organizations capitalizing on its capabilities to improve online services for their users. While IoT brings numerous advantages, the decentralized and distributed nature of its devices, coupled with their inherent self-organizing and self-healing features, makes them susceptible to cyber threats. To address these vulnerabilities, Intrusion Detection Systems (IDS) is going to be one of the essential tools, adept at detecting policy violations and network anomalies. To ensure the security of critical systems, a variety of techniques are employed within IDS frameworks. Devices termed as ”resource-constrained” typically exhibit limited computational capabilities, which includes restricted memory, processing power, or energy resources. Such limitations can impede their performance, especially when tasked with running intricate applications. A vast majority of IoT devices, such as smart sensors and wearables, are resource-constrained, often characterized by limited battery life, minimal RAM, and lesser processing power in comparison to traditional computers or smartphones.

As far as we aware, no subsisting survey in the current literature addresses this specific topic. Thus, this paper stands as the pioneering comprehensive survey on real-time Intrusion Detection Systems, incorporating insights from the most pertinent academic sources for this detailed study. However, IoT environments present unique challenges for IDS deployment. Given the diverse nature of IoT devices, from smart thermostats to industrial control systems, a one-size-fits-all approach to security is impractical. Many IoT devices operate under resource constraints, limiting their ability to run sophisticated security algorithms. Moreover, the decentralized and distributed nature of IoT networks complicates the task of monitoring and responding to threats. Recognizing these challenges, the research community has been fervently exploring innovative solutions to bolster IoT security. The main aim of this paper is to provide an extensive overview of these efforts, shedding light on emerging techniques and their efficacy. Through a meticulous survey, we delve into cutting-edge approaches tailored for IoT, emphasizing their potential to safeguard our increasingly connected world, By understanding the landscape of IoT security, stakeholders – from device manufacturers to end-users – can make informed decisions, ensuring that as we embrace the benefits of IoT, we do so with due diligence to its inherent risks.

2 Preliminaries

2.1 Security Overview in IoT devices

Nowadays deployment of IoT devices is increasing rapidly which makes use of many Machine Learning techniques so that an effective solution can be obtained. Many strategies have been proposed to improve protection or information security. As the use of IoT increases, there are more chances of attack on the network. In IoT devices, there are wireless edge devices which are used to store sensitive and critical information and by targeting these devices one can easily misuse IoT services. Many attackers try to capture or sneak the personal information of the target user [4]. There are many techniques which are being used for securing IoT environment. Lot of data has exploded nowadays from deploying the Internet of Things (IoT) [11]-[13]. It is a requirement of strong authentication and authorization techniques or being incroporated for systematized access of the requisite parameters. Data that is being transmitted between IoT devices, gateways and cloud servers should be in encoded form. IoT devices rely on wireless communication So a necessity of a strong Intrusion detection system that prevents the security breaching of IoT networks. Nowadays many technologies have been used for securing networks in IoT devices. Many researchers are applying traditional methods for classifying traffic in an IoT environment and also flows of traffic addressing and coming to smart devices.

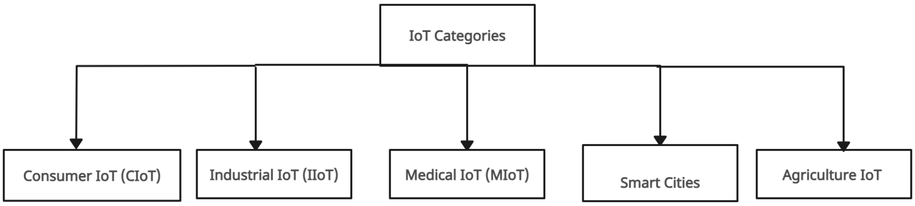

Figure 1: IoT Categories

2.2 Intrusion Detection System

Intrusion Detection Systems (IDS) can be broadly categorized into four types:

1. **Signature-based IDS**: This system stores patterns or sequences of known attack types on a network. If a matching pattern is detected, an alarm is triggered.

2. **Anomaly-based IDS**: Initially, it records the standard behavior of a system. Any deviation from this behavior is compared to a set threshold. If the deviation exceeds the threshold, an alarm is triggered. While capable of detecting undefined attacks, this method requires significant computational resources and memory.

3. **Hybrid IDS**: A amalgam of signature and anomaly-based IDS, this system aims to minimize the computational costs of the anomaly-based IDS and the data storage requirements of the signature-based IDS. It also addresses the false positive alarms typical of anomaly-based systems.

4. **Specification-based IDS**: This system operates based on predefined operations. It compares these operations to the current operations to detect any discrepancies.

Although extensive research has been conducted on IDS, it's challenging to detect every type of attack. Thus, the primary focus is often on detecting attacks based on routing protocol attacks.

Effective network security management typically involves three strategies: detection, prevention, and mitigation. Detecting intrusions helps identify network vulnerabilities. IDS play a crucial role in classifying real-time, unlabeled attacks. They monitor system behavior, triggering alerts upon detecting intrusions. Given the absence of standardized communication protocols and limited resources in IoT environments, ensuring comprehensive security for IoT devices is challenging. While lightweight security protocols exist, they often fail to provide adequate protection against potent threats targeting IoT devices.

3 Background Studies – A Thorough Investigation

Although numerous studies have addressed Intrusion Detection Systems, especially those relying on specific temporary storage mechanisms, I found no systematic survey directly focusing on intrusion detection techniques for IoT devices.

This section reviews papers that have conducted broader surveys on IDS. Pecori et al. [6] discussed the application of traditional methods for classifying traffic in IoT environments and traffic flows directed towards smart devices. They constructed a comprehensive dataset of IoT traffic flows from four networks and used it to test a deep learning model's efficiency, which consists of multiple hidden layers. The results were then compared with other effective machine learning algorithms to demonstrate the deep learning model's efficacy in both binary and multinomial classification techniques.

Alsoufi et al. [7] reviewed the application of deep learning techniques for securing IoT environments. They presented a systematic literature review analyzing existing research. While some architectures were based on signature identification (limited in detecting unknown attacks), others incorporated anomaly-based architectures capable of identifying zero-day attacks. Seven deep learning techniques used in IoT security were reviewed, demonstrating their effectiveness in safeguarding IoT environments. The study revealed that supervised machine learning techniques outperform semi-supervised and unsupervised approaches. They also highlighted the impact of learning methods and data types on deep learning techniques' performance, providing insights for enhancing new models for anomaly intrusion detection analysis and prediction.

Furthermore, Kannari et al. [8] have introduced a novel approach to performing classification in a resource-constrained environment. The motive is to develop a technique that is used to facilitate the classification process, a crucial learning algorithm, inside a resource-constrained IoT environment. Their approach is to select prototypes and deploy those data points or prototypes over IoT nodes. They have selected a prototype in such a way that it represents the whole dataset and will be able to classify the new incoming data appropriately. The originality lies in the manner in which the data points have been selected for a cluster. They consider not only the location of the datapoints within the same cluster but also the datapoints in a neighbouring cluster. The efficiency of this approach is validated using quality data sets and compare the same how the classification technique is used in the resource-constrained IoT environments. They have also deployed this technique in the real world over an Arduino Uno-based IoT node and explored the efficiency of this technique.

Moreover, Shone et al. [9] have an extended deep-learning model for tracing down intrusions.IDs based on networking play a pivotal role in safe guarding computer networks. However, there are many concerns related to network security, as these concerns directly relate to the increasing levels of human interaction and the decrease in detection accuracy. They have proposed their classification model based on deep learning, which they have constructed by using NDAEs. They have implemented their proposed model for classifying in a graphics processing unit (GPU), which is implemented in tensor flow, and they have computed the same using datasets from KDD Cup '99 and NSL-KDD datasets. They also demonstrate the improvements over the existing approaches and how effective it is to use them in NIDs.

Raddy et al. [10] have proposed a multiclass random forest technique for anomaly detection in resource-constrained IoT environments that is also very effective on streaming data. They have stated that the ensemble random forest technique is based on a multiclass algorithm and is very effective in handling streams of data, including the preprocessing stage. They have used Principal Component Analysis (PCA) to reduce the data dimension in the pre-processing stage. They have also stated that for handling streaming characteristics, a sliding window mechanism can also be used, which creates a sequence of blocks of data from streaming data so that processing can be done systematically. Ensemble multiclass random forest is as effective as random forest in identifying anomalies, but it has lower predictive and storage complexities as compared to other techniques that are used for anomaly detection in resource-constrained environments. They have also evaluated their approach with standard datasets and shown the performance of their proposed system with the help of different technologies such as the Area Under the Receiver Operating Characteristic Curve (AUC-ROC), which is very much capable of working with streaming and high-dimensional data. They have also done a hardware real-world implementation of the multiclass random forest technique and proved that this technique can also be used in practice in resource-constrained IoT environments.

Pasikhani et al. [14] have established the use of those networks with less power and networks which are lossy in nature (LLNs), which consist many nodes. Those nodes are characterized by constrained memory, energy resources, and computation power. These LLNs are often deployed in unattended and hostile conditions, and taking care of them is more challenging. They are prone to routing threats as these LLN devices are extensively interconnected. They have proposed an Adversarial Reinforcement Learning architecture to create an efficient IDS for developing data environments. To generate robust and efficient IDS detectors, they have integrated incremental machine learning and ARL. They demonstrate how this approach, which holds the concepts of drift adaptation and detection, can handle avertible changes so that IDS can detect attacks. They have considered the range of the most extensive routing attack. They have used grey-Box and Black-Box ML-Based challenges to disrupt 6LOWPAN, which are addressed and distinguished.

Further more Wani et al. [15] have put forward an intrusion detection architecture that is based on SDN. IoT devices are heterogeneous in nature. There are no defined standards and protocols for communication in IoT devices, and the IoT environment has a limited number of resources. For IoT devices, validating the security is not an easy task. There are many powerful threats in IoT devices, and light-weight protocols which are responsible to provide security to a network are incompetent to provide ideal security. For networking, SDN has a programming-based approach that splits data planes. This IDS is used for deep learning classifiers for anomaly detection in an IoT environment. Execution has been completed in the parallel environment. The result of the model has been computed using different approaches, and then comparisons have been performed with different methods.

Rehman et al. [16] have addressed the hindrance of IDS for IoT devices having a lack of resources, which are centralized in nature. They have basically proposed two methods, distributed and semi-distributed, which are used to combine those features that perform well. Those features also help in exploiting the potential of fog-edge analysis of coordinates. They have developed parallel machine learning models to divide the computation task. In the case where the semi-distributed method is used, they have applied collateral machine learning classifiers for selecting features in parallel, which is subsequent to single multilayer classification coordinating on the fog side. while in distribution technique, both single multilayer perceptron they perform the selection of features as well as classification tasks in an individual manner by subsequent machine learning models, and the output will be combined by fog-edge coordinates for making the final decision. Then they have drawn a conclusion based on numerical values, demonstrated teh performance of the model in terms of accuracy, and also compared it with the centralized approach of Deep Feature Extraction and Selection (DFIS).

Verma and Ranga [17] have investigated the probability of using the classification algorithm of machine learning to protect IoT devices from DoS attacks. They have carried out studies on different classification algorithms for the advancement of the architecture which is used to detect the anomaly. They have made use of popular sets of data such as CIDDS-001, NSL-KDD, and UNSW-NB15 for standardizing classifiers. They have employed the Nemenyi and Friedman tests to determine the difference between the classifiers. They have also made use of Raspberry Pi hardware to evaluate the classifier's response time on IoT hardware. Their main motive is to motivate researchers to develop IDS to enhance IoT security using ensemble learning techniques and to suggest appropriate methods to analyse the performance of classifiers.

Guezzaz et al.[18] have reviewed the hybrid IDS for securing edge-based IoT devices. As there is a vast development in the field of cloud technology and the network of the Internet of Things (IoT). like telecommunication, Industry IoT (IIoT) healthcare systems, and so on. The most challenging task is to protect these emerging technologies. The security issue of IIoT represents the main provocation for actors in industry and researchers. So to protect the IoT environment, an integrated approach to intrusion detection is introduced to improve the network security of IIoT devices.They have also concluded that their approach to integrating IDS has many advantages over recent models. There is an ACC of 99.10 a false alarm rate (FAR) of 2.7 percent, and a DR of 98.2 percent on the dataset NSL-KDD, and on the BOT-IOT dataset, an ACC of 98.2 percent, a FAR of 2.9 percent, and a DR of 97.6 percent, which is comparatively better than existing Machine Learning approaches.

Furthermore, Muraleedharan and Janet [19], have brought forward a deep learning model for classification to make use of flow of data to determine DoS attacks on HTTP. They have used the CICIDS 2017 dataset to evaluate their proposed work. In their work, they are dealing with DoS attacks. The accuracy of the classifier obtained is 99.61 percent.

In their proposed work, Singhla et al. [20] investigated the capability of algorithms. This approach is used to enable features that are used to tranfer knowledge from a model which is well-trained to a target model with a small amount of new training data. They compare the outcome of the Network Intrusion Detection architecture (NIDS) which is upgraded using the Transfer Learning (TL) algorithm, with a NIDS which is trained from the scratch. They have also concluded that those models which are based on TL techniques have high performance to identify those attacks which are not in records when training data is not sufficient.

4 Discussion and Comparison

The transformative power of the Internet of Things (IoT) in reshaping our modern world is undeniable, but with its ubiquity comes an intricate web of security challenges. As this review has highlighted, the stakes are high. From individual homes to expansive public sectors, the consequences of unaddressed security vulnerabilities span from personal data breaches to large-scale infrastructural failures. As we peer into the horizon of the IoT's future, a multi-pronged approach to its security emerges as essential. Quantum-resistant algorithms and homomorphic encryption might bolster the security of data transmission and storage, rendering IoT devices resilient against even state-of-the-art cyber threats. Concurrently, machine learning and artificial intelligence stand poised to revolutionise threat detection by offering adaptive and real-time responses to emerging dangers. Beyond the technical realm, there's an imminent need for global standardisation in IoT security. A universal benchmark, backed by stringent policy regulations, can ensure that manufacturers across the globe adhere to best practises, safeguarding users from potential threats. As technologies such as blockchain gain traction, their decentralised nature promises a new era of tamper-proof and trustworthy IoT networks. However, technology alone isn't the panacea; the human element remains crucial. Educating end-users—often the weakest link in security chains—about the nuances of IoT security, from the perils of default configurations to the merits of regular updates, is paramount. This holistic approach to security is further enriched by fostering collaborative research initiatives that bridge academia, industry, and governmental bodies, leading to comprehensive solutions that are swiftly implemented. In sum, as we navigate towards an increasingly interconnected future, our commitment to IoT security must be unwavering. By embracing these prospective avenues, we can hope to strike a harmonious balance where the vast potentials of the IoT are tapped without the shadow of security compromises looming large.n resource-constrained environments, the discussion surrounding Intrusion Detection Systems (IDS) for Internet of Things (IoT) becomes paramount due to the vulnerability of IoT devices to cyber threats. One of the primary challenges lies in deploying IDS in IoT devices with limited computing power and memory. To address this, lightweight and efficient algorithms are being explored to ensure real-time threat detection while conserving energy consumption to prolong the operational life of the devices.

Given the paramount importance of securing IoT devices, discussions frequently address the need for security updates and patch management to effectively counter vulnerabilities. Specific attacks, such as sensor spoofing and replay attacks, undergo thorough analysis to bolster the resilience of IDS in these contexts. Furthermore, the potential of edge computing in providing distributed IDS solutions is explored as a means to reduce dependence on centralized cloud-based systems, which could enhance response times and bolster network efficiency.

5 Research Gaps

1. **Efficiency and Scalability**: Most IoT environments include a massive number of devices. Research can traverse adaptable and effective.IDS solution that can handle the increasing volume of IoT devices related to cloud-based platforms without compromising performance.

2. **Detection in Real-Time**: Achieving real-time encroachment detection is important for IoT orders, especially when considering critical applications like healthcare or industrial control. Research can focus on developing real-

Table 1: A Comparative Analysis of Relevant Anomaly-based IDS Techniques

References	Objective	Technique Employed	Result	Advantage	Disadvantage
Pecori et al. [6]	Exploration of traditional methods for classifying IoT traffic	Deep learning model compared with established machine learning algorithms	Comprehensive dataset analysis from four networks	Self-adaptive; low false alarm rate	High delay; not all anomalies are triggered by malicious IDS
Alsoufi et al. [7]	Examination of deep learning techniques for IoT security	Review of seven deep learning techniques for intrusion detection in IoT	Insight into anomaly-based IDS and comparative analysis of techniques	Flexibility; low complexity; low false positive rate	Review-based; potential oversight of certain techniques
Kannari et al. [8]	Introduction of classification in resource-constrained environments	Classification using CNN and innovative networking techniques	Successful data classification	Accuracy; adaptability; robustness	High resource consumption; increased storage cost
Shone et al. [9]	Proposal of a deep learning model for NIDS operations	Novel deep learning technique for intrusion detection	High accuracy, recall, precision, and reduced training time	Low false alarm rate; scalability	High computational cost; lengthy training time
Raddy et al. [10]	Introduction of a multiclass random forest technique for IoT anomaly detection	Multiclass random forest technique for anomaly detection in IoT	Real-world hardware implementation showcasing practical applicability	Real-time; high detection accuracy	High resource consumption during training
Pasikhani et al. [14]	Exploration of Low-power and lossy networks (LLNs) with numerous nodes	Grey-Box and Black-Box ML-Based challenges to disrupt 6LOWPAN	Achieved high accuracy, recall, precision against black-box and grey-box testing	Accuracy; adaptability	Inability to detect all anomalies; high detection time
Wani et al. [15]	Proposal of SDN-based IDS for heterogeneous IoT devices	Deep learning classifier for anomaly-based detection techniques	Detection of intrusions in IoT network systems	Ease of computation; high accuracy	Limited to specific attacks
Verma and Ranga [17]	Investigation of machine learning's role in protecting IoT from DoS attacks	Nemenyi and Friedman tests to differentiate among classifiers	Performance analysis of seven machine learning algorithms	Adaptability; feasibility	Prolonged processing time
Guezzaz et al. [18]	Review of hybrid IDS for edge-based IIoT device security	Use of K-NN and PCA for data analysis and classification	Achieved high accuracy and low false alarm rate on NSL-KDD and BOT_IOT datasets	Low false alarm rate; high accuracy	Delayed detection time
Muraleedharan and Janet [19]	Proposal of a deep classification model for detecting DoS attacks on HTTP	Dataset UNSW-NB15 used; ensemble-based machine learning techniques considered	Model outperformed existing works in accuracy	Accuracy; robustness	Lower detection accuracy in some scenarios
Singhla et al. [20]	Introduction of a transfer learning model for intrusion detection	Deep Neural Network for experiments	Improved classification accuracy with smaller deep neural networks using transfer learning	Feasibility; reduced computation	Complex implementation

time detection algorithms that efficiently identify and respond interruptions as they happen.

3. **Adaptability to Dynamic Environments**: IoT environments are dynamic, with devices connecting and disconnecting the network frequently. Research can address how IDS can adapt to changes in the IoT network's topology, device configurations, and communication patterns.

4. **Resource Constraints**: IoT devices often have restricted computational resources. Research can traverse inconsequential intrusion detection methods tailored for resource-constrained IoT devices while offloading more complex analyses to the cloud.

5. **Privacy and Security concerns**: Investigate the security and privacy implications of offloading intrusion detection to the cloud. This involves testing potential vulnerabilities in the communication between IoT devices and the cloud-based IDS, in addition to talking privacy concerns related to the data collected for intrusion detection.

6. **Machine Learning for Anomaly Detection**: Explore advanced machine learning techniques for anomaly detection in IoT environments. This involves studying algorithms that can efficiently differentiate between normal IoT device behavior and malicious activities while minimizing false positives.

7. **Attack Surface Analysis**: Research can focus on identifying and analyzing the attack surface of cloud-based IoT environments. Understanding the potential introduction points for attackers can help design more effective intrusion detection strategies.

8. **Integration accompanying Edge Computing**: With the increasing significance of edge computing in IoT, research can explore how IDS can be integrated into edge devices to provide a distributed and more resilient security architecture.

9. **Adversarial Machine Learning**: Investigate potential vulnerabilities of machine learning-based IDS to adversarial attacks. Understanding by virtue of how attackers can maneuver the learning process can help in developing more robust and secure intrusion detection models.

10. **Standardization and Interoperability**: Explore the development of standardized protocols and frameworks for communication between IoT devices and cloud-based IDS. Interoperability is important for the logical unification of different IoT devices into a secure detection ecosystem.

6 Conclusion and Future Research Dimensions

The transformative power of the Internet of Things (IoT) in reshaping our modern world is undeniable, but with its ubiquity comes an intricate web of security challenges. As this review has highlighted, the stakes are high. From individual homes to expansive public sectors, the consequences of unaddressed security vulnerabilities span from personal data breaches to large-scale infrastructural failures. As we peer into the horizon of the IoT's future, a multi-pronged approach to its security emerges as essential. Educating end-users—often the weakest link in security chains—about the nuances of IoT security, from the perils of default configurations to the merits of regular updates, is paramount. This holistic approach to security is further enriched by fostering collaborative research initiatives that bridge academia, industry, and governmental bodies, leading to comprehensive solutions that are swiftly implemented. In sum, as we navigate towards an increasingly interconnected future, our commitment to IoT security must be unwavering. By embracing these prospective avenues, we can hope to strike a harmonious balance where the vast potentials of the IoT are tapped without the shadow of security compromises looming large. Privacy preservation is equally crucial in IoT systems. Implementing privacy-by-design principles and adopting differential privacy techniques can strike a balance between data utility and individual confidentiality, inspiring user trust and confidence in IoT technologies. Considering the resource-constrained nature of IoT devices, innovative lightweight cryptographic solutions are essential for securing communication channels without overwhelming hardware limitations. Integration of anomaly detection mechanisms with traditional intrusion detection systems can provide a comprehensive security approach, enabling the identification of subtle, non-traditional threats that evade conventional methods. Interdisciplinary research involving cybersecurity experts, data scientists, and domain specialists can lead to tailored intrusion detection models that address specific IoT applications, bolstering accuracy and effectiveness

References

[1] Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, M. (2020). Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. Future Generation Computer Systems, 107, 433-442.

[2] Li, W., Tug, S., Meng, W., & Wang, Y. (2019). Designing collaborative blockchained signature-based intrusion detection in IoT environments. Future Generation Computer Systems, 96, 481-489.

[3] Sheikh, N. U., Rahman, H., Vikram, S., & AlQahtani, H. (2018). A lightweight signature-based IDS for IoT environment. arXiv preprint arXiv:1811.04582.

[4] Rahman, M. A., Asyhari, A. T., Leong, L. S., Satrya, G. B., Tao, M. H., & Zolkipli, M. F. (2020). Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. Sustainable Cities and Society, 61, 102324.

[5] Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. Computer Networks, 160, 165-191.

[6] Pecori, R., Tayebi, A., Vannucci, A., & Veltri, L. (2020, July). IoT Attack detection with deep learning analysis. In 2020 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE.

[7] Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. Applied sciences, 11(18), 8383.

[8] Abd El-Rady, Alla, et al. ”Network Intrusion Detection CNN Model for Realistic Network Attacks Based on Network Traffic Classification.” 2023 40th National Radio Science Conference (NRSC). Vol. 1. IEEE, 2023.

in: *Advancements in Communication and Systems*. Ed. by Ashish Kumar Tripathi and Vivek Shrivastava. Computing and Intelligent Systems, SCRS, India., 2023, pp. 21–35. DOI: https://doi.org/10.56155/978-81-955020-7-3-3

[9] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2(1), 41-50.

[10] Phanindra Reddy Kannari, Noorullah Shariff Chowdary, Rajkumar Laxmikanth Biradar, An anomaly-based intrusion detection system using recursive feature elimination technique for improved attack detection, Theoretical Computer Science, Volume 931, 2022, Pages 56-64.

[11] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. Computer networks, 38(4), 393-422.

[12] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

[13] Wang, F., & Liu, J. (2010). Networked wireless sensor data collection: Issues, challenges, and approaches. IEEE Communications Surveys & Tutorials, 13(4), 673-687.

[14] Pasikhani, A. M., Clark, J. A., & Gope, P. (2022). Adversarial RL-based IDS for evolving data environment in 6LoWPAN. IEEE Transactions on Information Forensics and Security, 17, 3831-3846.

[15] Wani, A., & Khaliq, R. (2021). SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL). CAAI Transactions on Intelligence Technology, 6(3), 281-290.

[16] Rahman, M. A., Asyhari, A. T., Leong, L. S., Satrya, G. B., Tao, M. H., & Zolkipli, M. F. (2020). Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. Sustainable Cities and Society, 61, 102324.

[17] Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 111, 2287-2310.

[18] Guezzaz, A., Azrour, M., Benkirane, S., Mohy-Eddine, M., Attou, H., & Douiba, M. (2022). A lightweight hybrid intrusion detection framework using machine learning for edge-based IIoT security. Int Arab J Inf Technol, 19(5).

[19] Muraleedharan, N., & Janet, B. (2021). A deep learning based HTTP slow DoS classification approach using flow data. ICT Express, 7(2), 210-214.

[20] Singhla, A., Bertino, E., & Verma, D. (2019, June). Overcoming the lack of labeled data: Training intrusion detection models using transfer learning. In 2019 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 69-74). IEEE.

[21] Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. Ad hoc networks, 11(8), 2661-2674.

[22] Saberi, M. K. (2022). Open Access Journals with a view of journals covered in ISI. Iranian Journal of Information Processing and Management, 24(2), 105-122.

[23] Midi, D., Rullo, A., Mudgerikar, A., & Bertino, E. (2017, June). Kalis—A system for knowledge-driven adaptable intrusion detection for the Internet of Things. In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (pp. 656-666). IEEE.