International Journal of Emerging Trends in Information & Knowledge Management
https://www.eurekajournals.com/knowledge.html
ISSN: 2581-3579
Special Issue: "Transcending Tech Ed Nexus: Advancing Education through Technological Integration" - 12th June-2024

A Review of Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HeIoT): Mitigation Attacks, Techniques, Deployment Strategy, and Challenges

Kalpana Chittor S[1], Dr. Melita Luke[2]

[1]Assistant Professor, Sri Krishna Degree College, Kathreguppe, Bangalore.
and Research Scholar, CMR University, OMBR Campus, Bangalore.
[2]Assoc Prof. Dept. of CS, CMR University, OMBR Campus, Bangalore.

Abstract

A new area of study called heterogeneous internet of things (HetIoT) has the potential to significantly alter both how we currently understand basic computer science concepts and how we live in the future. HetIoT is being used in an expanding variety of fields, including advanced manufacturing, smart manufacturing, smart cities, intelligent transportation, environmental monitoring, and security systems. HetIoT will thus enrich our lives and offer a variety of useful services in the future by relying on strong application fields. In this review paper, we give an overview of intelligent IDS for HeIoT and talk about the key elements of its design, such as the sensing layers, networking layers, cloud architecture, and HeIoT architectural applications. We cover the present research on intelligent IDS for HeIoT and talk about the many methods used by researchers, including deep reinforcement learning, deep learning, supervised learning, unsupervised learning, and reinforcement learning. We also look at the difficulties in installing IDS for HeIoT, such as resource limitations, scalability, and heterogeneity, and we investigate unresolved issues and knowledge gaps in this area. The contributions of this study provide insights into the creation of intelligent IDS for HeIoT, highlighting the difficulties and unsolved issues in this area, and offering suggestions for future research.

Keywords: Intelligent intrusion detection system, Heterogeneous Internet of Things, Security threats, Machine learning, Reinforcement learning, Deployment strategies, Network security.

Introduction

IoT stands for the Internet of Things, which is the connecting of different equipment and gadgets with a distinct digital identity, such as smart sensors, smart devices, and industrial systems. IoT provides efficient transfer of data from smart devices with precise position information utilizing

wired or wireless networks and a variety of communication tags. Using proper information security measures, a central server keeps an eye on and manages the objects, offering customized real-time online monitoring, security management, and service functions [4, 5]. Researchers have created a number of IoT-related hardware and software platforms throughout the years, and these platforms are now widely used in daily life and business [6]. These applications have embraced HetIoT with various network architectures, such as WSN, Wi-Fi, MCN (3G/4G/LTE/5G), WMN, & Vehicular Network, that use RFID, sensors, and smart terminals to receive thorough sensing information whenever and wherever they are needed [7]. The gadgets are capable of securely establishing a connection to cloud servers over the internet or through satellite, and they may send data and urgent events to a remote monitoring center in real-time for processing [8]. To accomplish intelligent object control, the central server processes and examines the data in an intelligent manner.

A security system called an Intelligent Intrusion Detection System (IDS) employs a number of strategies, including machine learning and deep learning techniques, to identify and reduce security threats. An IDS is created to identify unauthorized access, malicious activity, and intrusions in a network of devices with various hardware, software, and communication protocols in the context of the Heterogeneous Internet of Things (HeIoT). HeIoT settings are vulnerable to a number of security risks, including denial of service attacks, unauthorized access, and data leaks. By identifying and responding to potential security breaches, an intelligent IDS for HeIoT can assist in reducing these risks. However, the deployment strategy and the capacity to quickly identify and stop potential attacks determine how effective an IDS for HeIoT will be.

Motivation

The background of the study in this review paper is the increasing use of Heterogeneous Internet of Things (HeIoT) systems, which are characterized by a large number of heterogeneous devices with different communication protocols and capabilities. These systems are used in various applications, such as healthcare, smart homes, smart cities, and industrial control systems. However, the use of HeIoT systems presents several security threats due to the large number of devices, which makes it difficult to ensure adequate security measures for each device. Traditional Intrusion Detection Systems (IDS) are inadequate for detecting and preventing attacks in HeIoT environments due to their limited capabilities in dealing with the heterogeneity and complexity of these systems. To address these security challenges, the development of intelligent IDS for HeIoT has become essential. These systems use advanced machine learning techniques, such as reinforcement learning, supervised learning, unsupervised learning, deep reinforcement learning, and deep learning, to detect and prevent attacks in HeIoT environments.

Paper Organization

The paper is organized into several sections. The introduction provides background information and the motivation for the study. The second section discusses the architecture components of HeIoT. The third section is a literature survey, which reviews existing research on intelligent IDS for HeIoT. The fourth section focuses on intelligent intrusion detection systems for heterogeneous IoT, discussing mitigation attacks, techniques, and deployment strategy. The fifth

section explores open problems and challenges in the domain of HeIoT. Finally, the conclusion and future directions section summarizes the review paper and provides directions for further research. The paper is well organized and structured, making it easy to navigate and understand.

Contributions of Survey

The contributions of the survey are providing an overview of an intelligent intrusion detection system for Heterogeneous Internet of Things (HeIoT) and its architecture components. Reviewing existing research studies on HeIoT and the various approaches adopted by researchers to tackle security threats. Discussing intelligent approaches such as reinforcement learning (RL), supervised learning (SL), unsupervised learning (UL), deep reinforcement learning (DRL), and deep learning (DL) for Heterogeneous IoT. Highlighting the issues and challenges in the domain of HeIoT, providing further directions for researchers. Presenting deployment strategies for an intelligent IDS for HeIoT to ensure its effectiveness.

Architecture Components Of Heiot

Architecture Components

The suggested four-layered structure of HetIoT's architecture consists of four layers: the applications layer, the cloud computing layer, the networking layer, and the sensing layer. This architecture was developed to handle the complex nature of the Internet of Things and its multiple heterogeneous networks. Figure 1 shows the four-layered structure, with each layer having unique functions and scalability.

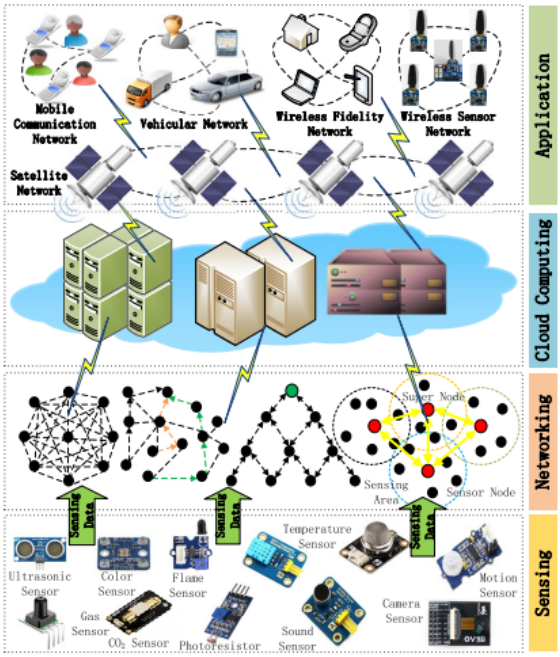

Figure 1: Four-layer Heterogeneous Internet of Things [6]

Several sensors are used in the sensing layer's data collection, which is then efficiently transferred to cloud servers through heterogeneous networking units made up of various network topologies. Because to developments in sensor hardware design and network topology

optimization, HetIoT has many uses in both industry and daily life. We examine the specifics of each layer of the suggested HetIoT architecture in the sections that follow.

Sensing Layers

The HetIoT architecture's sensing layer uses a variety of sensors to collect important sensing data that the cloud server may store and use. Environmental sensors, colour sensors, flame sensors, motion sensors, cameras, and other types are among these sensors. To transport the sensing data in the monitoring region, many sensors are placed there and set up in a self-organizing, multi-hop topology. The sensor nodes, sink nodes, and management nodes that make up the sensor network system typically send the sensing data in a multi-hop fashion through the sink nodes. With management nodes, users can release monitoring tasks and control the sensor network. Certain nodes are more prone to failure owing to environmental factors and energy depletion as HetIoT networks get bigger and more complicated. Changes in network topology brought on by these problems may impair network connectivity and coverage. In order to increase network robustness, researchers have created a number of algorithms and techniques, including the heuristic algorithm DPSO [7], GRASP mechanism [8,], and WCM protocol based on cognitive learning [9]. For best performance and data forwarding, a network topology must be effective. In order to create a network topology that is effective, superfluous wireless communication links must be eliminated by managing energy usage and choosing backbone nodes. These tactics lessen the possibility of failure while assisting in ensuring network coverage and connectivity. Future HetIoT architectures will also depend on various types of sensors, which could be subject to intrusion and malicious assaults. Node location information is a serious security risk since it is particularly vulnerable to exploitation. Smart sensor nodes can be installed to increase protection against attacks and reduce the danger of intrusion, which will improve the security and safety of HetIoT.

Networking Layers

The networking layer is essential in the HetIoT design for creating a topology that will effectively convey data from the source node to the destination node. To provide high data transmission capacity for the nodes, various networking models—including star networks, tree networks, scale-free networks, and hybrid networks—are described. Via sink nodes, super nodes, and other relay units, these networking models enable data transmission to the cloud server. These relay units also assist in node management by offering effective topology construction methods. However, HetIoT's use of diverse routing protocols also has certain drawbacks in terms of power usage, data speed, and vulnerability to malicious attacks. To make networking models more resilient and able to endure a specific number of node failures, self-organizing routing protocols have been developed. HetIoT will eventually need a large data transmission capacity in order to send massive data to the cloud server. Energy-saving techniques are used in difficult environments with restricted power supplies to increase the lifespan of HetIoT. By lowering the energy consumption of the nodes, these protocols aid in energy optimization and increase the lifespan of HetIoT.

Cloud Architecture

Large-scale HetIoT systems are now able to process and manage enormous amounts of data with efficiency because to the development of cloud computing technology. The cloud computing layer will be essential in receiving and processing data from other layers in the future HetIoT architecture [10]. Cloud servers' robust analytical computing capabilities enable them to do more than just store data; they also enable them to base choices on the findings of analyses. Because they can react swiftly depending on event-aware techniques, they are especially well suited for emergency applications. A growing demand for better decision-making procedures that can effectively use cloud computing is being driven by the heterogeneity of data in HetIoT. Due to its sophisticated data analytical features, cloud computing is better able to handle heterogeneity in IoT than middleware. The delivery of high-quality services for numerous applications is made possible by the ability of middleware to hide the differences between distinct operating systems and network protocols. Unfortunately, the majority of widely used middleware services employ proprietary protocols, which might complicate interoperability. Incompatible protocols in subsystems may also cause time delays and memory overhead for middleware services. In contrast, the cloud server's high level of flexibility and adaptability allows it to function as an abstract layer that may smoothly facilitate communication between diverse systems. HetIoT systems can increase their overall efficiency and efficacy by utilizing cloud computing, making it possible to handle and process complicated data more efficiently.

HeIoT Architecture Applications

Future HetIoT is anticipated to support a wide range of applications in its applications layer, including MCN, vehicular networks, Wi-Fi, and WSN. Using platforms like WeChat, Skype, and Line, MCN applications enable users to interact with each other utilising smart mobile devices whenever and wherever they want. Intelligent transportation systems use vehicular networks to detect traffic emergencies. These networks connect people, cars, and other intelligent mobile devices. By employing the cloud computing layer, they can forecast traffic patterns based on real-time traffic data. Wi-Fi networks are widely utilized in smart homes, smart cities, and healthcare systems and can support a variety of network communication protocols. Smart gadgets that are connected to Wi-Fi networks can be managed by people. Environmental characteristics like temperature, humidity, sound, light, smoke, and gas are all monitored by WSNs. They have been used in a variety of contexts, including forecasting debris flows and detecting forest fires. Applications must have a friendly user interface in order for HetIoT to be usable and available to people in their daily lives. Moreover, HetIoT uses secure smart terminal devices that can transmit data via satellite to the cloud server layer. The system will function at its best thanks to the cloud servers' ability to remotely control devices depending on the findings of analytical data analysis. HetIoT applications will fundamentally alter how we connect with our environment and improve people's life overall.

Literature Survey

With the deployment of devices and sensors in numerous applications, including smart homes, healthcare, and transportation systems, the Internet of Things (IoT) is quickly becoming

pervasive. Yet, IoT systems are susceptible to a variety of security risks due to the heterogeneity of the devices, protocols, and communication technologies they use. IoT systems in particular are vulnerable to assaults that could jeopardize their confidentiality, availability, and integrity.

[11] provides a thorough analysis of IoT privacy and trust challenges. The varied standards and communication stacks involved with IoT technologies make it impossible to instantly use traditional security countermeasures because they are relatively different from one another. A flexible architecture is desired to address risks in a dynamic environment where scalability challenges develop as a result of the large number of networked devices. The authors distinguished unresolved concerns and proposed future research paths while presenting and discussing key research challenges and popular solutions in IoT security. IoT challenges are also covered in [12], where the authors present industrial IoT, examine pertinent security and privacy issues, and then offer workable solutions that result in an all-encompassing security framework. [13] summarizes the security risks and privacy issues associated with IoT in more detail. In [14], there are attempts to draw a connection between information, privacy, and trust.

A solution to this issue is the Intelligent Intrusion Detection System (IDS) for Heterogeneous Internet of Things (HeIoT). IDS is created and implemented as a line of defense with other security tools set up for the network's foundation. IDS's ability to vary its security measures based on the demands and needs of the underlying network architecture is one of its architectural advantages [15]. Moreover, machine learning (ML) techniques that employ the learning dialectic can be used to create an improved IDS. An IDS is a software/hardware system created to identify potential threats to the system's resources and to warn the user if any odd activity is found. Yet, with the development of remote access and advanced networking technologies, the frequency and severity of data breaches and incursions have increased, harming the network and its resources over the long run.

A number of security tools, including firewalls and access control systems, are employed as a deterrent to filter network traffic passing via host systems. These techniques are set up to act as the first line of defense by applying restrictions to network packets and allowing network communications [16]. Although firewalls, access control mechanisms, and intrusion detection systems are all essential to network security, they are all unique in terms of their operating principles, methods for identifying patterns, and responses to unlawful entry [17]. IDS is different from firewall and access control techniques in that both of these check the outside of the systems and network for threats and breaches in order to prevent them from hurting the network and systems. Firewalls prevent breaches by blocking hostile network packets and restricting their access; however, these defenses do not detect breaches that originate inside the underlying network. IDS, on the other hand, keeps track of network activity, analyses network packets, and sends out an alarm if any malicious activity is found. IDS also monitors network flow coming into and leaving the systems by sniffing network communications, using heuristics, and patterns of known threats. If any anomaly is discovered, security operators are alerted [16].

Analyzing a significant volume of audit and file logs produced by various network interactions is one of the most important responsibilities for safeguarding computer and network systems. Also, one of the difficult duties is to recognize patterns in audit and file logs because doing so can help

network administrators identify intrusions by extracting impressions from the logs [18]. In order to ensure the security and integrity of network and system resources, it is necessary to create a coherent and effective security mechanism, such as an IDS, given the significance of network security and the explosion in networking technologies and devices [19]. Yet, because the network data that IDS collects and analyses is heterogeneous and dynamic in nature, a comprehensible representation is needed in order to create constructive and effective IDS. Dealing with heterogeneous and dynamic data with various network characteristics and display has an impact on network security. Many organizational and infrastructure requirements must be taken into account for the development of an effective intrusion detection and classification system, including good storage capability, a simplified infrastructure, and accurate packet flow analysis [20].

Intelligent Intrusion Detection Systems For Heterogeneous Iot

HetIoT's main purpose is to collect sensing data from smart terminals dispersed around various habitats, such as forests, mountains, volcanoes, and other inhospitable places where it is difficult to recharge devices [21]. Given the current state of energy technology, energy-saving strategies in the IoT have consequently become a major study topic [22]- [24]. It is critical to protect the information adequately because as HetIoT expands, more private and significant data is exchanged. Many communication safety procedures have been proposed to protect private data, whereas intrusion detection systems can identify forgeries, altered information, and routing attacks [25], [26], and [27]. The next section will examine intelligent strategies for HetIoT, such as deep reinforcement learning (DRL) and deep learning (DL), as well as supervised learning (SL), unsupervised learning (UL), and reinforcement learning (RL).

RL is a type of machine learning technique that involves an agent learning to take actions in an environment to maximize a reward signal. In the context of intrusion detection in HetIoT systems, RL can be used to train an agent to take actions to detect and mitigate attacks. The agent receives feedback in the form of a reward signal, which is positive when an attack is detected and negative when a false positive occurs. The RL agent then learns to take actions that maximize the expected reward signal. SL is a type of machine learning technique that involves training a model using labeled data. In the context of intrusion detection in HetIoT systems, SL can be used to train a model to classify network traffic as either normal or malicious based on labeled data. The labeled data consists of examples of both normal and malicious network traffic, and the model learns to distinguish between the two based on features extracted from the network traffic. UL is a type of machine learning technique that involves training a model using unlabeled data. In the context of intrusion detection in HetIoT systems, UL can be used to train a model to detect anomalies in network traffic based on patterns in the data. The model learns to identify patterns that are different from those in normal network traffic, which can indicate the presence of an attack [28]. DRL is a type of machine learning technique that combines RL with deep learning. In the context of intrusion detection in HetIoT systems, DRL can be used to train a deep neural network to take actions to detect and mitigate attacks. The neural network receives feedback in the form of a reward signal, and the weights of the network are updated using backpropagation to maximize the expected reward signal [29]. DL is a type of machine learning technique that involves training deep neural networks with multiple layers. In the context of intrusion detection

in HetIoT systems, DL can be used to train a neural network to classify network traffic as either normal or malicious based on features extracted from the network traffic. The deep neural network can learn complex patterns in the data that are difficult to capture using traditional machine learning techniques [30-31].

Mitigation Attacks

Systems for detecting and thwarting various HeIoT assaults are known as intrusion detection systems. Denial of Service (DoS), Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), and replay attacks are a few of the attacks that intelligent IDS can counteract. To identify and counteract these threats, the IDS employs a variety of methods including rule-based systems, deep learning, and machine learning. Attacks that cause a denial of service (DoS) have terrible consequences for IoT applications [32]. The accessibility of IoT services and devices is crucial in IoT applications. DoS attacks obstruct the IoT services' regular operations by rendering them unavailable. DDoS attacks [33] are typically conducted simultaneously by several coordinated attackers, making it challenging to identify them before the services are rendered unavailable. IDS for IoT i.e., SCADA is described in length in [34], which also briefly touches on the development of IDS approaches. Being vulnerable to a denial-of-service attack, 6LoWPAN-based IoT frequently faces disastrous circumstances. For 6LoWPAN-based IoT, the authors in [35] presented a DoS detection architecture. The cost of communication between elements of the suggested architecture and overhead is not assessed by the authors. It also has a single point of failure because it has a centralized architecture. You can find broadcast protocol variants, such as the DoS-tolerant TESLA for IoT, in [36]. For example, in [37], the authors presented two sensor-based secure communication protocols for IoT-based healthcare systems. The scientific community has also offered protocols for protecting privacy in IoT. The most recent research on the IoT key management protocol can be found in [38]. In addition, the protocol provides lightweight node authentication, quick rek eying, and effective defense against replay attacks.

Techniques for Heterogeneous IoT

Intelligent IDS for HeIoT employ a variety of methods to identify and stop attacks. Anomaly detection, signature-based detection, and behavior-based detection are a few of the methods employed. Monitoring device and sensor activity in order to spot any variation from typical behavior is known as anomaly detection. The process of signature-based detection entails contrasting network traffic with a database of acknowledged attack signatures. The goal of behavior-based detection is to identify any anomalous activity by learning how sensors and equipment behave. This work [39] introduces RADS, a rule-based anomaly detection system that monitors and quickly identifies Sybil attacks in massive WSNs. The suggested expert system's fundamental component is an ultra-wideband (UWB) ranging-based detection algorithm that functions in a distributed way and doesn't require communication or information sharing between sensor nodes to carry out the responsibilities of anomaly detection. Analytical evidence is provided for the viability of the suggested technique, and a thorough numerical and mathematical evaluation of RADS's effectiveness in revealing Sybil attacks is also provided. The findings

obtained show that RADS accomplishes good detection accuracy and a low false alarm rate, designating it as a promising ADS candidate for this type of wireless networks.

In HetIoT systems, anomaly detection is a common method for detecting intrusions. This method entails keeping an eye on the behavior of gadgets and sensors and looking for any variation from that behavior. Several techniques, such as clustering-based algorithms, support vector machines (SVMs), and neural networks, have been proposed by researchers for anomaly detection. [40] suggests a network traffic anomaly detection algorithm for HetIoT systems that makes use of a clustering-based strategy. The process of signature-based detection entails contrasting network traffic with a database of acknowledged attack signatures. This method works well for catching known attacks, but it might miss brand-new or undiscovered ones. For signature-based detection, researchers have put forth a number of different strategies, such as rule-based and machine learning-based systems. [41] provide a rule-based intrusion detection solution for HetIoT systems that employs known attack signatures to identify intrusions. The goal of behavior-based detection is to identify any anomalous activity by learning how sensors and equipment behave. Although this method is efficient at finding both known and unidentified attacks, it may occasionally provide false positive results. For behavior-based detection, researchers have proposed a variety of machine learning-based algorithms, including decision trees, random forests, and deep learning-based methods. The authors suggest a decision-tree-based behavior-based intrusion detection system for HetIoT systems that distinguishes between legitimate and malicious network traffic. In general, these methods are combined to create HetIoT system intelligent intrusion detection systems. By limiting false positives and false negatives, an intrusion detection system must be able to identify both known and unknown attacks.

Deployment Strategy

Intelligent IDS for HeIoT can be deployed in different ways depending on the application and the resources available. Some of the deployment strategies include centralized deployment, distributed deployment, and hybrid deployment. In centralized deployment, the IDS is deployed in a central location where it monitors the traffic on the network. In distributed deployment, the IDS is deployed on multiple devices and sensors, and the data is aggregated and analyzed centrally. In hybrid deployment, both centralized and distributed deployment strategies are used. In centralized deployment, the IDS is deployed in a central location where it monitors the traffic on the network. The central location can be a cloud-based server or a dedicated hardware device. All the network traffic from IoT devices is sent to the central location for analysis, and the IDS generates alerts based on the identified threats. One of the significant advantages of centralized deployment is that it is easy to manage and maintain. All the analysis and monitoring are done in a central location, making it easier to maintain and upgrade the system. Additionally, the centralized deployment requires less hardware and software resources on the IoT devices, reducing the deployment costs. Another advantage of centralized deployment is that it provides better visibility and control over the network. Since all the network traffic is routed to the central location, the administrators can have a better understanding of the network's overall security posture. The primary disadvantage of centralized deployment is that it can be a single point of failure. If the central location is compromised, it can affect the entire network's security. Additionally, since all the network traffic is routed to the central location, it can lead to network

congestion and delay in detection and response time. In distributed deployment, the IDS is deployed on multiple devices and sensors, and the data is aggregated and analyzed centrally. This deployment strategy is suitable for large IoT networks with multiple devices, where it is not feasible to send all the network traffic to a central location. One of the significant advantages of distributed deployment is that it provides a more comprehensive and real-time analysis of network traffic. Since the IDS is deployed on multiple devices and sensors, it can monitor the traffic locally and generate alerts based on the identified threats. Another advantage of distributed deployment is that it provides better resilience and redundancy. Since the IDS is deployed on multiple devices, if one device fails, the other devices can still provide network security. Additionally, the distributed deployment reduces the network congestion and delay in detection and response time. The primary disadvantage of distributed deployment is that it can be complex to manage and maintain. Each device and sensor must be configured and managed separately, leading to higher deployment and maintenance costs. Additionally, distributed deployment requires more hardware and software resources on the IoT devices, leading to higher power consumption and limited battery life. In hybrid deployment, both centralized and distributed deployment strategies are used. This deployment strategy is suitable for large IoT networks with multiple devices, where some devices are resource-constrained and cannot handle the IDS's processing load. One of the significant advantages of hybrid deployment is that it provides the best of both centralized and distributed deployment strategies. The resource-constrained devices can send the network traffic to a central location for analysis, while the other devices and sensors can analyze the traffic locally. Another advantage of hybrid deployment is that it provides better scalability and flexibility. As the network grows, additional devices can be added to the distributed deployment, and the centralized deployment can be upgraded to handle the increased network traffic.

Open Problems and Challenges

The existing research on intelligent IDS for HeIoT has identified several open problems and challenges that need to be addressed to improve the security of IoT systems. Here are some of the research gaps that exist in this domain:

Developing Lightweight IDS Techniques: Most IDS techniques require significant computational power to analyze data and detect anomalies, making them unsuitable for IoT devices with limited computational resources. Therefore, developing lightweight IDS techniques that consume less power and can operate on resource-constrained devices is a crucial research gap.

Developing IDS Techniques for Specific IoT Applications: Different IoT applications have different security requirements, and developing IDS techniques that can address specific security concerns for each application is a research gap. For example, healthcare IoT systems require different IDS techniques than smart home IoT systems.

Developing IDS Techniques for New Attacks: As attackers develop new attack methods, IDS techniques need to be updated to detect and mitigate these new attacks. Therefore, developing IDS techniques that can detect new and evolving attacks is a crucial research gap.

Evaluating the Performance of IDS Techniques: To ensure that IDS techniques are effective in detecting and mitigating attacks, their performance needs to be evaluated. Therefore, developing standardized evaluation metrics for IDS techniques is a research gap.

Addressing the Privacy Concerns of IDS: IDS techniques can collect sensitive data from IoT devices, leading to privacy concerns. Therefore, developing IDS techniques that can operate while preserving user privacy is a research gap.

Developing IDS Techniques for Interoperability: As IoT systems are developed using different platforms, developing IDS techniques that can operate across different systems and protocols is a research gap.

Developing IDS Techniques for Edge Computing: As IoT systems move towards edge computing, where data is processed and analyzed closer to the source, developing IDS techniques that can operate in a distributed computing environment is a research gap.

The research gaps in intelligent IDS for HeIoT provide further directions to researchers in this regime to develop lightweight IDS techniques, develop IDS techniques for specific IoT applications, address the privacy concerns of IDS, evaluate the performance of IDS techniques, develop IDS techniques for interoperability, develop IDS techniques for new attacks, and develop IDS techniques for edge computing.

Conclusion and Future Directions

In conclusion, the research on intelligent intrusion detection systems for heterogeneous Internet of Things (HeIoT) has identified several promising techniques and strategies for improving the security of IoT systems. However, there are still several challenges and open problems that need to be addressed to make these systems more effective and efficient. To address these challenges and open problems, future research in this area should focus on developing lightweight IDS techniques that can operate on resource-constrained IoT devices, developing IDS techniques for specific IoT applications, addressing the privacy concerns of IDS, evaluating the performance of IDS techniques, developing IDS techniques for interoperability, developing IDS techniques for new attacks, and developing IDS techniques for edge computing. Furthermore, future research should focus on developing integrated security solutions that combine multiple security techniques, including IDS, to provide comprehensive security for IoT systems. These integrated security solutions should also consider the unique security challenges posed by edge computing, where data is processed and analyzed closer to the source. Finally, research in this area should also focus on developing educational and training programs to increase awareness and knowledge of IoT security among developers and users of IoT systems. This will help to ensure that IoT systems are developed and used in a secure and safe manner. Overall, the future of intelligent intrusion detection systems for HeIoT looks promising, and continued research and innovation in this area will be critical to addressing the security challenges of IoT systems and realizing the full potential of the IoT revolution.

References

F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Trans. Netw. Service Manag., vol. 9, no. 2, pp. 169-183, Jun. 2012.

H. Kumarage, I. Khalil, Z. Tari, and A. Zomaya, "Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling," J. Parallel Distrib. Comput., vol. 73, no. 6, pp. 790-806, 2013.

S. K. Fayaz, F. Zarinni, and S. Das, "Ez-channel: A distributed MAC protocol for efficient channelization in wireless networks," Ad Hoc Netw., vol. 31, pp. 34-44, Aug. 2015.

N. Zhao, F. R. Yu, H. Sun, A. Nallanathan, and H. Yin, "A novel interference alignment scheme based on sequential antenna switching in wireless networks," IEEE Trans. Wireless Commun., vol. 12, no. 10, pp. 5008-5021, Oct. 2013.

T. Qiu, R. Qiao, and D. Wu, "EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things," IEEE Trans. Mobile Comput., vol. 17, no. 1, pp. 72-84, Jan. 2018.

Tie Qiu , Senior Member, IEEE, Ning Chen, Keqiu Li, Senior Member, IEEE, Mohammed Atiquzzaman , Senior Member, IEEE, and Wenbing Zhao, Senior Member, IEEE, "How Can Heterogeneous Internet of Things Build Our Future: A Survey", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 20, NO. 3, THIRD QUARTER 2018.

H. Safa, W. El-Hajj, and H. Zoubian, "A robust topology control solution for the sink placement problem in WSNs," J. Netw. Comput. Appl., vol. 39, pp. 70-82, Mar. 2014.

A. C. Santos, C. Duhamel, L. S. Belisário, and L. M. Guedes, "Strategies for designing energy-efficient clusters-based WSN topologies," J. Heuristics, vol. 18, no. 4, pp. 657-675, 2012.

A. El-Mougy and M. Ibnkahla, "A cognitive framework for WSN based on weighted cognitive maps and Q-learning," Ad Hoc Netw., vol. 16, pp. 46-69, May 2014.

M. Jo, T. Maksymyuk, B. Strykhalyuk, and C.-H. Cho, "Device to-device-based heterogeneous radio access network architecture for mobile cloud computing," IEEE Wireless Commune., vol. 22, no. 3, pp. 50-58, Jun. 2015.

S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of, Things: the road ahead," Computer Networks, vol. 76, pp. 146-164, 2015.

T. U. Darmstadt, "Security and privacy challenges in industrial internet of things," in Proceedings of 52nd Annual Design Automation Conference, pp. 1-6, San Francisco, CA, USA, June 2015.

S. J. Kumar and D. R. Patel, "A survey on internet of things: security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, pp. 20-26, 2014.

J. Daubert, W. Alexander, and P. Kikiras, "A view on privacy & trust in IoT," in Proceedings of IOT/CPS-Security Workshop IEEE International Conference on Communications (ICC), London, UK, June 2015.

Thakkar, Ankit and Ritika Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges." In: Archives of Computational Methods in Engineering, pp. 1-33, 2020.

Mishra, Ved Prakash and Balvinder Shukla (2017). "Process mining in intrusion detection-the need of current digital world." In: International Conference on Advanced Informatics for Computing Research. Springer, pp. 238-246.

Thakkar, Ankit and Ritika Lohiya (2020a). "A Review of the Advancement in Intrusion Detection Datasets." In: Procedia Computer Science 167, pp. 636-645.

Rahaman, Mohammad Ashiqur, C´edric Hebert, and J¨urgen Frank (2016). "An attack pattern framework for monitoring enterprise information systems." In: 2016 IEEE 25th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). IEEE, pp. 173-178.

Kim, Kwangjo and Muhamad Erza Aminanto (2017). "Deep learning in intrusion detection perspective: Overview and further challenges." In: 2017 International Workshop on Big Data and Information Security (IWBIS). IEEE, pp. 5-10.

Zhang, Tianye et al. (2017). "A survey of network anomaly visualization." In: Science China Information Sciences 60.12, p. 121101.

N. Zhao, F. R. Yu, H. Sun, A. Nallanathan, and H. Yin, "A novel interference alignment scheme based on sequential antenna switching in wireless networks," IEEE Trans. Wireless Commun., vol. 12, no. 10, pp. 5008-5021, Oct. 2013.

Q. Han, B. Yang, C. Chen, and X. Guan, "Energy-aware and QoS-aware load balancing for HetNets powered by renewable energy," Comput. Netw., vol. 94, pp. 250-262, Jan. 2016.

M. Li, H. Nishiyama, N. Kato, Y. Owada, and K. Hamaguchi, "On the energy-efficient of throughput-based scheme using renewable energy for wireless mesh networks in disaster area," IEEE Trans. Emerg. Topics Comput., vol. 3, no. 3, pp. 420-431, Sep. 2015.

A. Madhja, S. Nikoletseas, and T. P. Raptis, "Hierarchical, collaborative wireless energy transfer in sensor networks with multiple mobile chargers," Comput. Netw., vol. 97, pp. 98-112, Mar. 2016

S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," Ad Hoc Netw., vol. 11, no. 8, pp. 2661-2674, 2013.

A. Mitrokotsa and C. Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection," Ad Hoc Netw., vol. 11, no. 1, pp. 226-237, 2013.

A. Nadeem and M. P. Howarth, "An intrusion detection & adaptive response mechanism for MANETs," Ad Hoc Netw., vol. 13, pp. 368-380, Feb. 2014.

Bostani, Hamid and Mansour Sheikhan (2017). "Modification of supervised OPFbased intrusion detection systems using unsupervised learning and social network concept." In: Pattern Recognition 62, pp. 56-72

Lopez-Martin, Manuel, Belen Carro, and Antonio Sanchez-Esguevillas (2020). "Application of deep reinforcement learning to intrusion detection for supervised problems." In: Expert Systems with Applications 141, p. 112963.

Luijten, Ben, "Deep learning for fast adaptive beamforming." In: ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, pp. 1333-1337

Susilo, Bambang and Riri Fitri Sari (2020). "Intrusion Detection in IoT Networks Using Deep Learning Algorithm." In: Information 11.5, p. 279

C. P. Mayer, "Security and privacy challenges in the internet of things," Electronic Communication of the European Association of Software Science and Technology-ECEASST, vol. 17, pp. 1-12, 2009.

S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning automata-based solution for preventing distributed denial of service in internet of things," in Proceedings of International Conference on Internet of 5ings and 4th International Conference on Cyber, Physical and Social Computing, pp. 114-122, Dalian, China, 2011.

D. Yang, A. Usynin, and J. Hines, "Anomaly-based intrusion detection for SCADA systems," in Proceedings of 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC&HMIT 05), pp. 12-16, 2005.

P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of service detection in 6LoWPAN based internet of things," in Proceedings of International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 600-607, Lyon, France, 2013.

N. Ruan and Y. Hori, "DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of ,ings," in Proceedings of International Conference on Selected Topics in Mobile and Wireless Networking, Avignon, France, 2012.

J.-L. Hou and K.-H. Yeh, "Novel authentication schemes for IoT based healthcare systems," International Journal of Distributed Sensor Networks, vol. 11, no. 11, article 183659, 2015.

S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi, "Key management protocol with implicit certificates for IoT systems," in Proceedings of Workshop on IoT challenges in Mobile and Industrial Systems-IoT-Sys, pp. 37- 42, Florence, Italy, May 2015.

P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Detecting sybil attacks in wireless sensor networks using UWB ranging-based information," Expert Systems with Applications, vol. 42, no. 21, pp. 7560-7572, 2015.

Nusaybah Alghanmi, Reem Alotaibi & Seyed M. Buhari ,"Machine Learning approaches for Anomaly Detection in IoT: An Overview and Future Research Directions Wireless Personal Communications volume 122, pages2309-2324 (2022).

Philokypros P. Ioulianou , Vassilios G. Vassilakis , Ioannis D. Moscholios , Michael D. Logothetis," July 2018 Conference: Information and Communication Technology Forum (ICTF) 2018 At: Graz, Austria, 11-13 July 2018.