**Intrusion Deletion System in IoMT: Survey**

**Abstract:**

The [Internet of Medical Things](https://www.sciencedirect.com/topics/computer-science/internet-of-medical-things) (IoMT) has revolutionized the [healthcare industry](https://www.sciencedirect.com/topics/computer-science/healthcare-industry) by enabling [physiological data](https://www.sciencedirect.com/topics/computer-science/physiological-data) collection using sensors, which are transmitted to remote servers for continuous analysis by physicians and healthcare professionals. This technology offers numerous benefits, including early disease detection and automatic medication for patients with chronic illnesses. However, IoMT technology also presents significant security risks, such as violating patient privacy or exposing sensitive data to [interception attacks](https://www.sciencedirect.com/topics/computer-science/interception-attack) due to [wireless communication](https://www.sciencedirect.com/topics/computer-science/wireless-communication), which could be fatal for the patient. Additionally, traditional security measures, such as cryptography, are challenging to implement in medical equipment due to the heterogeneous communication and their limited computation, storage, and energy capacity. These protection methods are also ineffective against new and zero-day attacks. It is essential to adopt robust security measures to ensure data integrity, confidentiality, and availability during data collection, transmission, storage, and processing. Intrusion detection systems (IDSs) are therefore widely used along with other security mechanisms such as firewall and access control in IoMT systems. Many research ideas have been proposed pertaining to the IDS using machine learning (ML) techniques, deep learning (DL) techniques, Fuzzy, and swarm and evolutionary algorithms (SWEVO). The paper presents applications of IDS with challenges and potential future research directions. The study presented, can serve as a pedestal for research communities and novice researchers in the field of network security for understanding and developing efficient IDS models.

## Intrusion Detection Systems (IDS) Background

The process of the monitoring, detection and identification of malicious activity on network or computer system is called intrusion detection [14]. A generic IDS consists of three components, which are the monitoring, the detection and the response. The monitoring component analyzes the traffic flow behavior. The detecting component detects any suspect behaviors and notifies the reacting element of any occurrences detected. The response component triggers an alert or informs the network manager. Depending on its working principles and analysis methods, An IDS can be based on signatures, anomalies or specifications. while it can be categorized as network-based, host-based, or hybrid IDS depending on the target location, as shown in Fig. 1 [2].

Signature-based systems, also known as misuse detection methods, detect previously known attacks by comparing their signatures to the data being analyzed [15]. They are effective in contexts where most attack patterns are already known. Their main limitation is the need for regular signature database updates, as well as the inability to detect zero-day attacks and unknown threats [16]. In contrast, anomaly-based IDSs use sophisticated decision techniques like ML to detect threats based on the characteristics of the traffic flow. They monitor the usage behavior deviation from the normal functionality [17]. One advantage of using anomaly-based schemes is the ability to be effective in detecting both unknown and zero-day attacks, but they can generate high false-positive outcomes. [18]. On the contrary, specification-based (hybrid systems), for identifying attacks, are using a combination of the two variants mentioned earlier in this section, it employs a halfway technique between signature-based IDS, in which pre-defined rules are used to identify known attacks, as well as anomaly-based IDS, in which the normal behavior can be set to discover any unusual activity, even unknown, unlike signature-based IDS [19]. In specification-based IDS, the developers manually set the constraints and characteristics that depict normal operation behavior, in contrast to anomaly-based IDS, which are generated automatically. Therefore, the algorithm of intrusion detection can identify suspicious activity by discovering the deviation between the two patterns [20]. Approaches detection based on specification and signature need low overhead in comparison to the anomaly-based methods. However, due to computational power limitations and the large numbers of interconnected devices, a conventional IDS based on anomalies is not effective in the IoMT [2].

In addition, IDS are categorized into two classes based on their deployment, namely network-based IDSs and host-based IDSs [21]. In the host-based IDSs, the detector system is deployed and installed within a particular host for monitoring the behaviors of a specific system, including analysis of inbound and outbound traffic, system calls, file system access details, and so on [16]. These systems can only monitor the network passing through the host on which they are implemented. The detection of botnets and malware are the two main types of host-based IDS [22], Threats in other parts of the system are undetectable. Network-based IDSs are strategically placed inside a network, such as at the gateway node or in a decentralized way, to identify any threat on the network's hosts. Because network-based IDS are monitoring all traffic passing over the network, they must analyze traffic quickly and drop as few traffic data packet as possible[16].

IDSs are also classified into two categories: active and passive. Active IDS also known as IPS (Intrusion Prevention System) [23]. IPS is designed to monitor activities at the system or network level to identify attacks and deliver corrective actions in real time without requiring an administrator's intervention. On the other side, passive IDSs can only detect attacks. It alerts the administrator if any attack is detected and cannot perform any corrective action by itself. By default, the majority of IDSs are passive [16].

Most intrusion detection systems have a basic common design that contains: (1) a data collecting module that gathers data which may contain proof of an intrusion, (2) an analyze module that identifies threats after handling this data, and (3) a process to report an intrusion [13]. As shown in Fig. 2. In data collection subsystem, input data from each component of the IoMT systems can be collected and analyzed to find the behavior pattern of the interaction, and thus detect the malicious behaviors at an early stage. The analytics module could be deployed with various methods and techniques, although, approaches based on ML and DL are more appropriate and dominating for the data examination in order to learn the benign and abnormal behaviors resulting from the interaction of IoMT systems and devices in IoMT environments. In addition, ML/DL techniques are able to predict novel attacks, that are often significantly different than previous attacks, as ML/DL methods are capable of intelligently predicting the future unknown threats by learning from the available legitimate samples [24].

**Related Work:**

1. **Machine Learning Techniques for Ids in IoMT**

Over the last decades, Machine Learning algorithms have been widely employed in several application domains like speech recognition, bioinformatics, spam detection, intrusion detection, etc. [41]. ML methods are used for constructing the computational model in a cost-effective way. In addition, they improve efficiency and reliability. ML constructs the models by processing the data automatically, accurately and rapidly. It enables access to the massive amounts of data collected from sensors and the extraction of information required from the data collected [42]. Given the significance and complexity of an IDS, a variety of machine learning techniques and algorithms are used to offer practical IDS methods with high rate of true negatives and low false positive rates [25].

Machine learning techniques are commonly categorized into two classes, Known as Unsupervised Learning and Supervised Learning. Various machine algorithms have been developed in recent years. Popularly used algorithms include SVM (Support Vector Machine), RF (Random Forest), DT (Decision Tree), ANN (Artificial Neural Network) and EL (Ensemble Learning) [4] [17] [43]. Many researchers are interested in working on IoMT security issues using ML models due to recent advances made in ML technology. Table II provides a brief summary of the research work done to propose IDS for IoMT using numerous ML-based methods.

**Current ML-based Ids in IoMT**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ref/Year** | **Description** | **Algorithms** | **Attacks addressed** | **Dataset** | **Accuracy rate** | **Limitations** |
| 2021 | A neural network-based system for detecting and disabling suspect devices in the IoT-enabled healthcare systems | Neural network | Detect and isolate suspect devices. | Real data. | 99.4% | CPU usage and memory are not taken into account. |
| 2021 | An ensemble Learning (EL) algorithm based IDS that uses fog-cloud technology to mitigate cyberattacks in IoMT networks. | DT, NB, RF and XGboost | Cyberattacks in IoMT environment. | ToN-IoT | 96.35% | CPU usage, battery and memory are not taken into account. |
| 2021 | An IDS based on ML methods which can distinguish between normal and attack traffic. | KNN, RF, ANN, J48, SVM, and Decision Table. | MitM and Dos attacks. | Generated dataset. | 97.67% | FPR, memory, and CPU utilization are not taken into account. |

## Deep Learning Techniques for Ids in IoMT

With the drastic growth in the data complexity and volume of network traffic, IDS based on conventional ML with a shallow architecture is inappropriate for the IoT context involving billions of IoT devices [27]. Deep Learning appears to be one of the most appropriate and powerful methods to be implemented to various IoT security measures in this context [44]. In addition, DL is able to automatically model complicated features sets from the samples data. A further advantage of Deep Learning based approaches is their capacity to enable deep binding in IoT based networks [45]. This allows for automatic interventions among IoT -based systems without human intervention to execute collaborative assigned functions.

DL could be utilized within generative mode by unsupervised learning including AE (Autoencoder) and DBN (Deep Belief Network), discriminative mode employing supervised learning, for example CNN (Convolutional Neural Network) and RNN (Recurrent Neural Network), or a hybrid mode which combines both approaches, such as Generative Adversarial Network (GAN) and Ensemble of DL Networks (EDLNs).

The recent advancements in DL technology have piqued the interest of many researchers in working on the IoT security issues utilizing DL models. Table III below provides a concise summary of recent research works conducted in order to propose IDS for IoMT using various DL-based techniques.

**Current DL-based Ids in IoMT**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ref/Year** | **Description** | **Algorithms** | **Attacks addressed** | **Dataset** | **Accuracy rate** | **Limitations** |
| 2021  A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). | A hybrid architecture SDN model (CNN-LSTM) driven by DL for malware detection in the IoMT | CNN  LSTM | Malware attacks | IoT Malware Dataset | 99.83% | High CPU and memory overhead.  Not real-time. |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. **Fuzzy Logic Techniques for IDS in IoMT**
2. **swarm and evolutionary algorithms Techniques for IDS in IoMT**

**References:**