Real-Time DDOS Attack Detection and Mitigation Framework for Internet of Medical Things Network: A Comprehensive Review

[1]Joshua J. Tom, [2]Wilfred Adigwe, [3]Chioma L. Aworonye, [4]Ifeanyi J. Odegwo

[1]Senior Lecturer, [2]Senior Lecturer, [3]Lecturer I, [4] Senior Lecturer
[1]Department of Computer Science, Achievers University Owo, Nigeria
[2] Department of Computer Science, Delta State University of Science and Technology, Ozoro, Nigeria.
[3] Department of Computer Science, Novena University Ogume, Nigeria.
[4] Department of Data Science and Analytics, Southern Delta University, Ozoro, Nigeria.

[1]tom.jj@achievers.edu.ng, [2]adigwew@dsust.edu.ng, [3] chayoma@novenauniversity.edu.ng, [4] odegwoij@dsust.edu.ng

***Abstract*— The Internet of Medical Things (IoMT) has revolutionized healthcare through the use of interconnected medical and wearable devices, among other internet technologies, to monitor and analyze patients' health real time data. IoMT has made remote patient monitoring possible and enhanced the quality of healthcare provision. Nonetheless, the heightened use of round-the-clock network connectivity exposes IoMT networks to threats e.g. distributed denial of service (DDoS) attacks. Disruptions caused by DDoS attacks can have severe consequences on IoMT-based hospital services and delivery, including compromised patient safety and hacked hospital systems. This paper presents a survey of the state-of-the-art DDoS attack detection and mitigation solutions in IoMT environments, along with the challenges therein. We propose a conceptual framework based on deep learning using LSTM-Autoencoders to effectively model the sequential and time-dependent network traffic data and efficient reconstruction of normal traffic patterns for DDoS detection respectively. We also propose to deploy Particle Swarm Optimization (PSO) to enable efficient parameter optimization and effective feature selection. Finally, we highlight some potential future research directions toward ensuring that IoMT systems are secure and resilient.**

***Index Terms*— DDoS Attack, IoMTs Network, LSTM-Autoencoder, Particle Swarm Optimization, Real-time Network Monitoring, Anomaly Detection, DDoS Detection System.**

I. INTRODUCTION

The rapid development in Internet of Medical Things (IoMT) technology and the proliferation of IoMT devices have revolutionized healthcare delivery through the simple integration of medical devices, wearables, hospital infrastructure, and cloud platforms. IoMT provides immediate monitoring of patients, remote diagnosis, customized treatment, and improved operational efficiency, hence enhanced patient outcomes and reduced healthcare costs [1]. The integration of networked medical devices and sensors in healthcare settings generates gigantic amounts of sensitive health information, which are processed and analyzed for timely clinical decision-making. In spite of this interconnectedness, there are very serious cybersecurity concerns involved. The severity of healthcare service renders IoMT networks a high-value object for cyberattacks, particularly DDoS attacks. These attacks aim to overwhelm network resources, discontinue service availability of sensitive health information [2]. For IoMT, such attacks can have disastrous consequences, including delayed diagnosis, patient safety violations, and business paralysis of healthcare institutions. Despite the expanding threat profile, existing security measures tend to fall short of effective and real time detection and mitigation of these attacks, especially because of the IoMT devices resource limitation and the instantaneous need for low-latency response [3]. Traditional security tools e.g. intrusion detection schemes based on attack signature are not well-equipped to handle complex attack patterns and high-speed network traffics typical of IoMT contexts [4]. Besides, the heterogeneity and scarcity of medical devices necessitate adaptive, light, and customized security systems that can operate efficiently in real time. Advances in deep machine learning have opened up new opportunities in intrusion detection and have presented the promise for more adaptive and accurate detection mechanisms. Recurrent neural network-based methods [5, 6], convolutional neural network-based methods [7, 8], and autoencoder-based methods [9, 10] have evidenced encouraging results in detecting complex attack patterns in network traffic data. Of these, Autoencoders learn to model normal network traffic patterns using unlabeled network traffic and attack data, which enable identification of unknown attack signatures in real-time. Autoencoders reconstruct normal traffic with low error, a capability that allows them to identify deviations in real-time [11]. With this, any high reconstruction error signals potential anomalies including DDoS. Long Short-Term Memory (LSTM) networks can efficiently learn model's sequential and varied length network data with temporal dependencies especially as DDoS attacks are characterized by temporal behaviors including sudden spikes in traffic, sustained high volumes, or patterned request bursts [12]. This positions a model to distinguish between benign network fluctuations and malicious activity. These make the pair most suited for real-time network traffic anomaly detection. Moreover, optimization methods such as Particle Swarm Optimization (PSO) have also been employed leveraging the algorithm's global search ability, which can improve the performance of deep learning models by fine-tuning parameters, selection of features, and removal of false positives [13].

Despite the availability of these technologies, development of end-to-end, real-time DDoS detection and mitigation platforms specific to IoMT environments remains an open problem. Current methods typically fall short of the integration level needed for deployment in resource-constrained healthcare settings or prove inefficient in addressing the inherent operational needs of IoMT. This review aims to provide a comprehensive overview of current research activity, techniques, and methodologies geared towards real-time DDoS attack detection and countermeasures in IoMT networks. We critically analyze state-of-the-art methods for detecting DDoS, identify their strengths and weaknesses, and note open research issues. Additionally, we determine important trends that are emerging and propose directions for developing resilient, efficient, and adaptive security solutions that fit the requirements of IoMT ecosystems. Finally, this review intends to warn researchers, practitioners, and policymakers about effective means of securing healthcare infrastructures against unfolding cyber threats.

In this paper, we reviewed articles published from 2015 up to and including those scheduled for publication in 2026 in reputable journals including IEEE, Google Scholar, ScienceDirect, and Springer by crafting relevant keywords such as "Deep Learning DDoS mitigation", "DDoS attack detection using deep learning", "Real-Time Network Monitoring", "Anomaly Detection in IoMT", "Security Framework for IoMT", and "IoMT Data Protection ".

This comprehensive review identified the following research gap for DDoS detection and mitigation in IoMTs networks upon analysis of recent and relevant literatures.

(i) The majority of the existing DDoS detection methods are designed for traditional networks and may fail to account for the unique traffic behavior, protocols, and device heterogeneity in IoMT environments [14].

(ii) It is nontrivial to develop low-latency and high-accuracy detection mechanisms that are suitable for resource-constrained IoMT devices [15]. There is a shortage of scalable solutions that can operate effectively in real-time without overloading the device or network resources

(iii) Most research focuses either on detection or mitigation separately. There is a need to build unified frameworks that can detect and mitigate DDoS attacks in real-time [16] in IoMT networks in an integrated fashion.

(iv) While machine learning (ML)-based approaches hold promise for detecting attacks, applying them on IoMT devices with limited processing power and energy [17] is largely uncharted territory.

(v) Many studies target volumetric DDoS attacks only without considering more sophisticated or adaptive types of attacks [18] e.g., application-layer or hybrid DDoS attacks targeting IoMT devices.

(vi) There is no comprehensive, publicly available dataset simulating real-world IoMT traffic and attack patterns, hindering the development and benchmarking of detection systems [19].

The main contribution here is that this review paper stresses the need for adaptive, specialized, and effective detection mechanisms that can address the particular constraints and security risks of IoMT networks. By so doing, it attempts to bridge the gaps identified above by suggesting a conceptual LSTM-Autoencoder-based deep learning paradigm powered by PSO for the detection and mitigation of DDoS in the healthcare environment.

The main objectives of this review research are:

(i) To perform a comprehensive survey of the state-of-the-art DDoS attack detection and mitigation solutions in IoMT environments.

(ii) To evaluate the effectiveness of different approaches deployed in detecting and mitigating DDoS attacks in medical IoT environments.

(iii) To propose a conceptual and novel deep learning-based framework using LSTM-Autoencoders coupled with PSO for DDoS detection and mitigation

The rest of the paper is organized as follows: Section 2 discusses IoMTs devices and networks, DDos attacks and attack variants, DDoS detection techniques, and threat intelligence and DDoS mitigation techniques. Section 3 presents a review of existing research on DDoS attacks in IoMTs environments and current state of DDoS attacks. Section 4 covers the methodology used in conducting the literature review process. In section 5, the research discussion and the findings of are presented while the proposed conceptual and novel deep learning-based framework for detecting and mitigating DDoS attacks in IoMT is presented in section 6. Finally, the conclusion is present in section 7.

II. IoMT Security and Defense

Internet of Things (IoT) is the most important technology of the twenty first century and is the forerunner of the IoMT technology. IoMT brings the IoT technology to the world of healthcare by shifting from a device-centric architecture, characteristic of the IoT technology, to a modern connected architecture with a focus on patient-centric monitoring with the effect that hospitals are able to scale their capabilities and expand monitoring to unlimited number of patients without disrupting the real-time mission critical nature of patient monitoring. Figure 1 shows a typical network of IoT network.

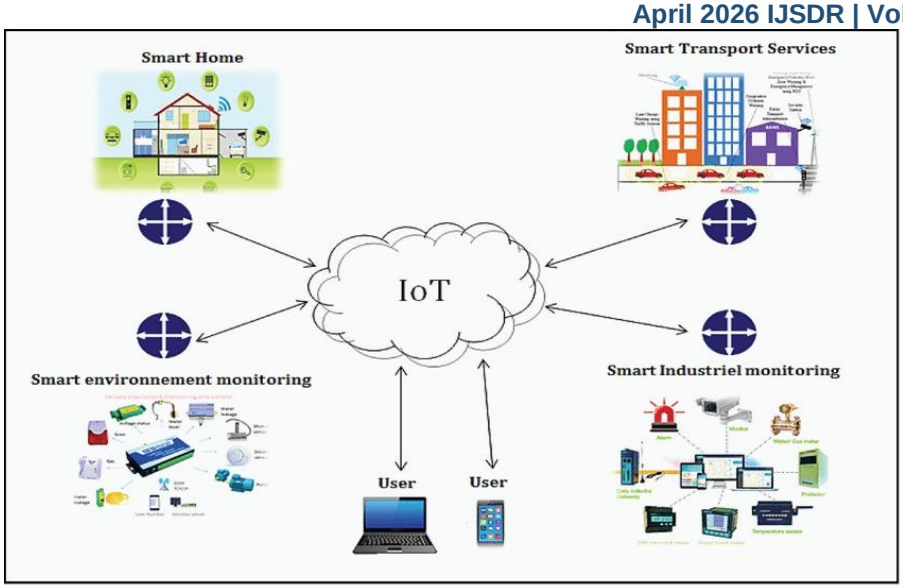

Figure 1: A General IoT Network Architecture (Adapted from: [20])

IoMT Devices and Networks

The revolution in the health sector is brought about by the integration of IoMT devices and software applications through network connectivity. This innovation offers personalized healthcare services, streamlined clinical workflows and remote patient monitoring bringing improvements in patients' healthcare delivery. IoMT devices can remotely collect, analyze, and transmit a patient's medical data in real-time. IoMT network is a network of smart medical devices including systems for remote patient monitoring, heart rate monitors, implantable devices, wearable sensors, wearable ECG devices, connected diagnostic tools, and insulin pumps. The devices in the network may also consists of implantable devices such as pacemakers used to regulate heart activities and neurostimulators used for remotely managing neurological conditions and tailored therapy adjustments. Figure 2 depicts a IoMT network with smart medical devices, patients, medical personnel, and hospital systems connected in a network.

Figure 2: IoMTs Network Structure (Adapted from: [21])

DDos Attacks

Health data is almost the most sensitive information since it is a life-centric artifact, requiring robust security to safeguard patient privacy and ensure uninterrupted access [22]. Attacks that target the availability of such data, like Distributed Denial of Service (DDoS) or ransomware, are severely critical because they can interfere with life-saving care services, delay life-saving treatments, and compromise patient safety.

The uniqueness of the "medical" component of the IoMT paradigm is the imperative of patient safety [23]. This is because there is a need to carefully balance both harm and healing in a way that the initial objective of deploying IoMT technology to improve healthcare delivery is not jeopardized.

DDoS is the most common form of cyberattack that may be launched against a system such as IoMT-based hospital systems. A typical DDoS attack against a IoMT-based network is shown in Figure 3. Motivations for DDoS attacks against such system include the attacker's intent to disrupt healthcare services by incapacitating the patient monitoring system in the IoMT network denying healthcare providers

access to patient data to frustrate timely diagnosis and treatment. This can be part of a ransomware scheme where payment is demanded by the attacker in exchange for a seize-fire or restoring normalcy. DDoS can also be deployed as a weapon of cyber warfare against a nation state by targeting the country's critical medical infrastructure with malicious intent to destabilize public health services as a sabotage during conflicts [24]. Disgruntled employees with enormous technical skills may unleash DDoS attack on an organization to settle personal grievances [25]. Attackers may deploy DDoS attack to distract their victims while aiming to compromise other segments of the network either to steal sensitive patient information or stealthily install a malware in the system. Hacktivists can also launch DDoS as a protect against certain government policies hence attackers can target IoMT-based health facilities to cause unavailability of these health services providing and enabling systems.

DDoS attacks on IoMT network take different forms. Attackers may overload the network by flooding it with excessive network traffic causing availability issues by making medical devices, hospital systems, and servers inaccessible. Critical medical infrastructure may also be targeted where the attacker is interested in disrupting important IoMT components like emergency response subsystem, patient monitoring subsystem, and the platforms handling data exchanges. Attackers can also recruit a large number of compromised systems (zombies) to form a botnet [26], which is used to generate massive volume of network traffic. This form of DDoS attack is particularly difficult to mitigate for several reasons including the botnet's scale and distributed nature, a bot's legitimately looking traffic, recruitment of IoT devices with exploitable weak security and outdated firmware, difficulty in blocking attack from source due to the use of spoofed IP addresses and dynamically changing the command and control (C&C) server which makes it easy to evade static blacklist. Another challenge in combating DDoS is its multi-vector attack possibility as attackers can combine volume, protocol, and application layer-based attack types resulting a single, complex DDoS attack and hence difficult to detect and mitigate [27].

2.3 DDoS Attack Classification

In the recent past, the vulnerability of the IoMT network to DDoS attacks has become quite worrisome due to the IoMT's critical importance in modern day health services delivery. Failure to adequately address the menace can result in the IoMT-based health infrastructure's security and reliability being compromised. The development of effective real-time DDoS detection and mitigation strategies for IoMT networks [28], can be facilitated through a thorough understanding of the classes into which DDoS attacks are categorized. Such classification system enables researchers and practitioners to design efficient mitigation solutions targeted at specific DDoS variants. Incident responders can also identify particular DDoS attack instances and respond quickly to curtail the attack. DDoS attacks can be classified based on attack vector, attack method, attack source, attack duration, and other classifications. Figure 3 shows a comprehensive classification of DDoS attacks.

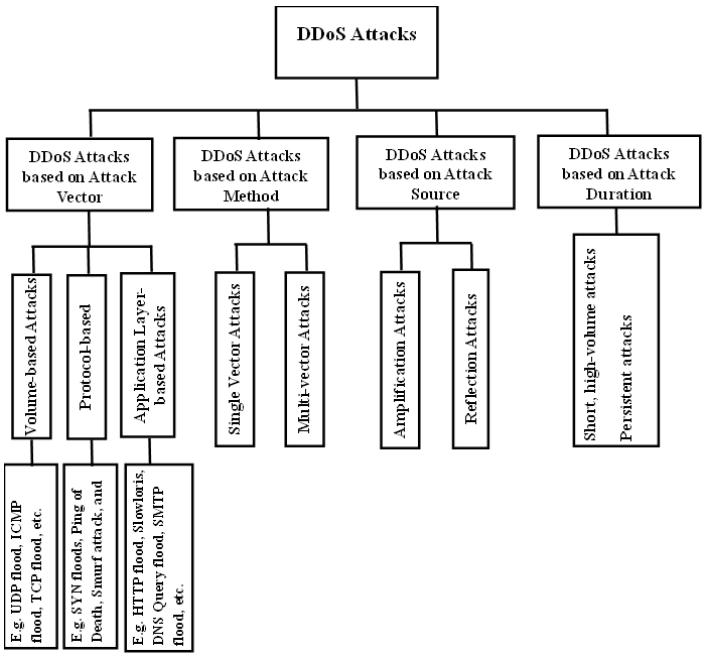

Figure 3: Comprehensive DDoS Attack Taxonomy

In this work, only the most commonly known class of DDoS attack types based on attack vector are described. The taxonomy of the attack vector-based DDoS attacks includes volume-based attacks, protocol-based attacks, and application layer-based DDoS attack [29]. The volume-based attacks are designed to overwhelm the capacity of the victim by saturating it with high volume of traffic with the intent to disrupt services and compromise availability. As shown in fig. 4, attackers with control over a vast number of compromised computers (bots or zombies) formed into a huge network of bots (botnets) can remotely control these botnets to launch attacks on target systems. For example, servers, networks, and databases can be overwhelmed with requests, network traffic, and query calls respectively. The magnitude of these attacks is measured according to the bandwidth consumed (Gbps). This high-volume traffic can incapacitate servers, networks and network devices, or any security defenses including firewalls to differentiate legitimate requests from malicious traffic by exhausting the server's processing power, network bandwidth, network device memory and the firewall's ability to filter network traffic and stop malicious data packets from accessing the network. Volume-based DDoS attacks are the most prevalent of this class of attacks, accounting for more than 75% of DDoS attacks [30]. Examples of volume-based attacks include ICMP floods, DNS reflection floods, UDP floods,

ping floods, SYN floods attacks, etc. apart from using botnets, attackers also deploy amplification techniques to carry out volume-based DDoS attacks. The techniques include DNS, Network Time Protocol (NTP), Simple Service Discovery Protocol (SSDP) amplifications, etc. These attacks use spoofed source IP addresses to conceal or hide attackers' identity when directing traffic to victims. Amplification attacks are aimed at maximizing the impact of the attacks on the victims while minimizing the attackers' resources such as bandwidth usage. These attacks exploit vulnerabilities in most network protocols stemming from the protocols' design which allows them to respond with larger responses relative to small amounts of queries or requests received [31].

Protocol based DDoS attacks leverage the weaknesses in the network and transport layers of the network protocol stack to overwhelm a target [32], exhausting server or intermediate equipment resources like firewalls and load balancers. Common vulnerabilities in the network layer are IP Spoofing, IP fragmentation, route injection and route leaks, and IPv4 address exhaustion. These attacks exploit weaknesses in protocols to exhaust particular resource such servers, firewalls or load balancers. Attackers exploit weaknesses in the network communication protocols including SSDP, NTP, TCP, HTTP, DNS, SNMP, etc. to overwhelm and disrupt a target system's services. Such attacks are aimed at exhausting firewalls, routers, and servers by sending malformed requests or exhausting server connection tables with relatively low volume of traffic. Like high volume traffic directed at a server, sending relatively low volume of traffic can also be problematic and have several implications [33]. Low volume attacks can be very effective if it targets specific vulnerabilities such as memory leaks and logic flows, e.g. sending small and maliciously crafted requests to exploit buffer overflow or application bugs. Persistent low-volume traffic has the tendency to gradually deplete server resources such as CPU, connections to database, and memory leading to degraded performance or outright services denial. Low volume traffic is as dangerous as high-volume traffic as it less likely to be detected by a traditional IDS thereby aiding and abetting detection evasion and attack persistence. The magnitude of protocol-based DDoS attacks is measured in packets per second (pps), bandwidth usage (bps), etc.

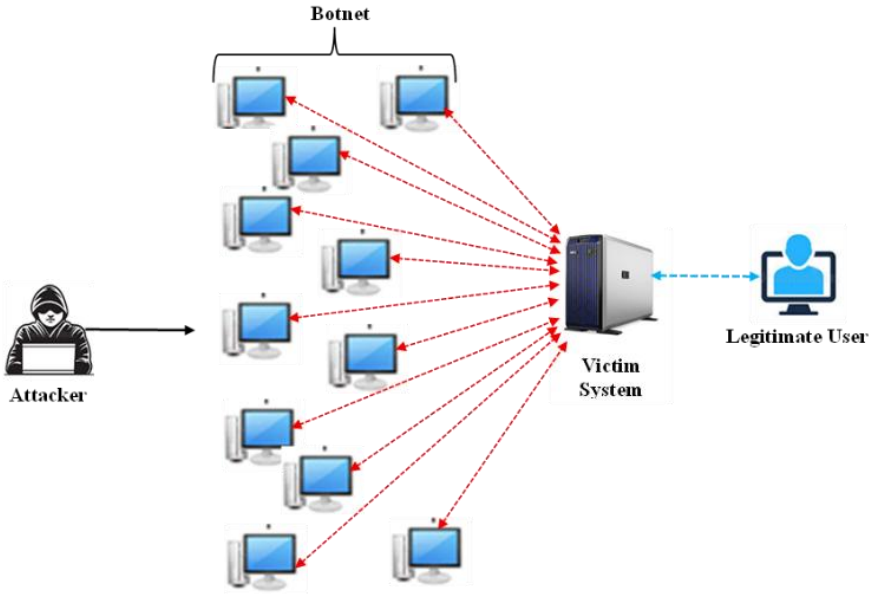

Figure 4: Volume-based Attack to Breach Server Availability to a Legitimate User

On the other hand, application- based DDoS attacks target vulnerabilities in applications with the aim to make applications to crash. Other DDoS attack types target is on disrupting infrastructure but application-based DDoS attacks are focused on disrupting resources at the application layer of layer 7 of the network stack [34]. Applications targeted DDoS can cause overloading of the CPU and memory exhaustion affecting the server and applications running on it. For example, processes like adding items to a shopping cart, checkout items in the cart could be abused with many concurrent requests. This is capable of overwhelming the application's limits or the host computer's resources. While other DDoS attack types focus on disrupting infrastructure, application centered attacks target particular vulnerabilities in applications thwart computational operations or use SQL injections to disrupt databases [35]. Hackers exploit vulnerabilities in software applications to steal data, take down networks, disrupt businesses, and extort funds from companies and organizations. The impact of application-based DDoS can be measured in many different ways including the request rate (rps) indicating how an attacker floods the application with requests, the number of unique users or IPs involved, the total data transferred per second (bps), etc. Figure 5 depicts an application-based DDoS attack.

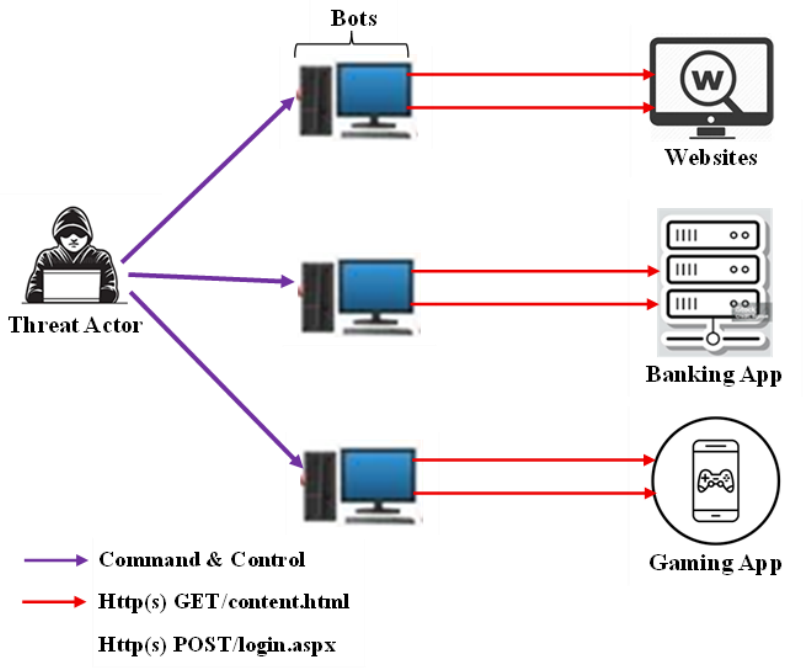

Figure 5: Application-based DDoS attack Orchestration

DDoS Detection Techniques

In this section, we describe some of the techniques employed by security experts and researchers for detection of DDoS attacks in networks to guard against attacks aiming to cause breach of security services including confidentiality, integrity, nonrepudiation, and availability. These detection mechanisms include but not limited to traffic analysis and monitoring, anomaly-based detection, signature-based, rate limiting and throttling, source IP filtering and blocklisting, etc.

Network Traffic Monitoring and Analysis

Traffic monitoring and analysis encompasses continuously keeping an eye on the incoming network traffic using metrics such as packet rates, sizes, traffic volume, traffic patterns, packet rates, connection counts, CPU and memory usage, error rates and traffic sources. This information is used for analysis it to detect abnormal patterns or anomalies that may signify a DDoS attack [36]. DDoS monitoring focuses on incoming traffic, watching out for unfamiliar patterns or spikes that might indicate a DDoS attack, which floods fake traffic to overwhelm networks and devices making services completely unavailable to legitimate users. In monitoring DDoS attacks, certain techniques tools and are used to detect attacks including networking monitoring tools like Zabbix, Nagios, and SolarWinds, network traffic analyzers, SIEM tools e.g. Splunk, and flow-based tools like NetFlow. Many researchers such as have proposed traffic analysis and monitoring-based DDoS detection mechanisms [37] in recent times. Though traffic analysis is effective in detecting certain variants of DDoS attacks, its potential limitation is struggling to distinguish legitimate spikes from actual attacks.

[38] presented a broad multi-layered framework combining deception, cloud-based ML, a hierarchical multi-controller architecture for effective DDoS detection in SD-IoT networks, and P4 switches for real-time traffic analysis and monitoring. [39] proposed a real-time traffic monitoring and analysis framework for DDoS attacks leveraging cooperation from edge server-device, where each device monitors the incoming traffic data in real-time through the model and presents suspicious data to the edge server for analysis.

Anomaly Detection

Anomaly based DDoS detection technique, also called behavior-based technique is a method that stipulates a standard for normal network behavior, or unusual patterns, that could signify a network threat [40]. The technique creates profiles of acceptable network activity and then issues alerts on any significant deviations from normal behavior as specified by the profiles. These profiles are the normal hosts, users, network connections, and applications behaviors. The profiles are established through monitoring network characteristics over a period of time and used in order to classify network traffic into benign behavior or malicious activity. This is effective for detecting unknown attacks with no pre-existing attack signatures. Anomalies detected by anomaly-based detection systems are categorized into point anomalies [41] which are individual data instances that deviate from the normal, contextual anomalies [42] which are abnormal only within a specific context, and collective anomalies [43] involving groups of data instances behaving anomalously relative to the entire dataset.

In evolving or dynamic environments, anomaly-based detection technique faces some challenges. In non-static environments, maintenance of accurate profiles is difficult or impractical due to constant changes in network behaviors, which leads to increase in false positive rates with the potential to affect organization's business operations. Also, defining baseline conditions for 'normal' user and network activity is difficult due to operational and policy dynamics that may cause unpredictable spikes in network activity, equally causing high false positive rates that adversely affect business operations.

Anomaly-based threat detection employs different types of models including statistical methods, ML, and deep learning models. Statistical-based anomaly detection technique [44] is made up of two methods namely parametric and non-parametric methods. The former includes methods such as Gaussian-based models and regression techniques. These methods are based on the assumption that normal network data follow a common probability distribution. They use parameters like mean and variance to classify anomalies by

setting thresholds on anomaly scores to encapsulate data features and classify anomalies based on interquartile range and range values. [45] presented a defense strategy to detect and mitigate spoof flooding DDoS attacks by proposing a solution based on a statistical measure known as Interquartile Range (IQR) and implemented in the SND controller. Non-parametric methods do not need any previous knowledge of the data distribution. For example, non-parametric methods like histograms estimate data occurrence probabilities by frequency counting, while kernel density estimators detect anomalies as data points in low-probability areas of the predicted probability distribution function. Rule-based statistical detection, another non-parametric method, flags values outside acceptable the set lower and upper data limits as anomalies.

Machine learning (ML) methods for implementing anomaly-based detection consists of supervised, semi-supervised, and unsupervised learning methods [46]. In supervised learning methods, labeled datasets are needed for both normal and anomalous classes. Classification algorithms such as one-class Support Vector Machines (SVM), random forest (RF), etc. are used to build models for predictive models. The Semi-supervised methods are used to train a model on labeled normal data only and detect anomalies in unlabeled test data. However, in unsupervised methods no labeled data is required, instead unlabeled dataset is used where clustering or outlier analysis is often used to detect anomalies based on deviations from learned patterns. [47] presented a detection framework leveraging the flow-based ICMPv6 traffic representations and the kernel-based ML algorithms to improve the accuracy of detection. The framework integrated three ML models including SVM, logistic regression, and random forest with nine different kernel functions to achieve a robust and adaptive detection mechanism. These approaches can use handcrafted feature engineering, relying on expert knowledge, or data-driven, automated features extraction from raw data for efficient threat detection.

Deep learning models including neural networks e.g. autoencoders, RNN e.g. LSTM and Convolutional LSTM, and generative models e.g. Generative Adversarial Networks (GANs) and Variational Autoencoders are often deployed in learning feature representations or anomaly scores from complex, high-dimensional, and temporal data.

Signature-based Detection Method

Signature-based DDoS attack detection methodology stands out when detecting threats whose attack signatures are known by matching these attack signatures [48]. Signature-based detection can also be referred to as Knowledge-based detection or Misuse detection [49]. [50] proposed a signature-based intrusion detection system combined with data mining technique to improve detection accuracy by implementing a feature selection methodology. In the selection process, the score of each feature is calculated to determine the most relevant features to recognize threat patterns based on the threat signature. Traditional intrusion detection systems (IDS) that employ signature-based detection technique often struggle to detect new cyber threats. [51] presented a lightweight signature-based plug-and-play detection system against multichannel man-in-the-middle (MC-MitM) attacks, which can easily with Wi-Fi-based IoT with no need to modify existing network settings.

Rate Throttling and Limiting Techniques

Rate limiting and throttling are network traffic management mechanisms that ensure that a system, or network is not overwhelmed with excessive load or network traffic allowing faster network traffic and reducing delays [52]. Rate limiting and throttling are important detection and mitigation mechanisms for DDoS detection and mitigation by controlling the flow of traffic to a system or through a network to provide resources availability for legitimate users.

Rate limiting and throttling are important concepts used in controlling unintended spikes network traffic to keep network services stable and available [53]. Techniques used for implementing rate limiting and throttling include token bucket, sliding window, leaky bucket, and fixed window techniques. Other methods include those based on implementation methods including IP-based, server-based, and geography-based limiting methods [54]. Fixed window algorithm is a simple yet efficient algorithm that defines a time window by dividing time into a discrete and non-overlapping interval called windows whereby a maximum request limit is set for each window. The algorithm's security implication is that a uniformed output rate is maintained, levelling out network traffic peaks and disallowing flooding-based attacks to overwhelm the system with prohibitive volume packet bursts. [55] designed an adaptive sliding window-based scheme to detect potential threat behavior using Generative Adversarial Network (GAN) achieving a high detection accuracy and lower false positive rate. [56] presented a mathematical model to address table overflow attacks and performed mitigation of this attack using a token bucket algorithm. Table overflow attacks are perpetrated against switches, which could result in memory exhaustion. [57] designed a synergetic DoS (SDoS) attack capable of causing hiding damages to a router and thereafter proposed a self-proving mechanism based on leaky buckets as a countermeasure.

Source IP Filtering and Blocklisting

Source IP filtering is one of the many security measures deployable for controlling access to network and network resources based on the IP address of the origin of a data packet [58]. IP blocklisting is a mechanism to deny access to a specific block or predefined list of IP addresses designated as malicious or untrusted [59]. These mechanisms are implemented in a firewall or other security tool using rules in which systems can either allow or deny traffic from specific IPs or origins helping to reduce risk of threats like DDoS, spam, malware, and brute-force attacks. Although domain blocklists contributes immensely in denying malicious domains unauthorized access to reach targeted users, state-of-the-arts blocklists are merely reactive and are generally sluggish in reacting to attacks, by which time it is too late to prevent damage to the network infrastructure. This is due to blocklist and reputation systems over reliance on website contents and user interactions to identify website maliciousness. In response to this, [60] investigated the prospect of a proactive prediction of malicious domains from a given list of domains and observed that malicious domains normally reuse existing infrastructure which have been used in an earlier attack. Based on this reflection, the authors discriminately browse the internet for passive DNS data aiming to identify malicious domains in given list of domains.

III. RELATED WORKS

A number of research works had been carried out that proposed deployment of different threat detection methods for detecting DDoS attacks in IoT/IoMT. This review considers various specialized threat detection methods such as anomaly-based, signature-based, flow-based analysis, ML models, rule or heuristic-based detections methods, and hybrid approaches to DDoS detection designed to cater for the distinctive properties of the IoT/IoMT networks including need for detection of threats in real-time, resource limitedness, and the criticality of the health data in terms of privacy and security. Based on these, we analyzed some existing works with respect to the year of publication, adopted methodology, dataset used, model accuracy, and limitations.

In curbing VANET's vulnerability to DDoS attacks, [61] presented an innovative approach to combat DDoS attacks in VANET networks. The authors proposed a SDN controller framework leveraging BiLSTM Attention network and Dung Beetle Optimization (DBO), a metaheuristic optimization algorithm. This is designed to improve DDoS detection accuracy, increase convergence speed, and tune parameters efficiently. Their results suggest the developed model could enhance real-time traffic monitoring to a significant extent and attack mitigation in next-generation intelligent transportation systems. However, combining BiLSTM attention network with DBO is impractical and unrealistic on resource-constraint devices such as those in IoMTs networks as a result of significant computational and implementation challenges including increased computational overhead and resource-intensive operations.

A compelling approach for detecting DDoS attack in SDN was presented by [62]. The authors proposed a hybrid deep learning methodology that leveraged the efficient spatial feature extraction characteristic of CNN and ability to capture temporary dependencies of LSTM to address the critical need for a comprehensive detection mechanism beyond a single DDoS attack variant. The scheme's reported accuracy of 99.9% underlines its effectiveness in real-world deployment. The strengths of this model lie in the feature selection process, which selects the top eight features from the InSDN dataset and the deployment of cross-entropy on the control plane of the SDN, which provides a good metric for anomaly detection. While the proposed approach is capable of enhancing detection accuracy and effective selection of feature, the model is limited by its reliance on dataset representativeness and its resource-strenuous computations.

With the prevalent and sophisticated nature of DDoS attacks on IoT ecosystem, [63] presented a novel approach for detecting and mitigating DDoS attack integrating state-of-the-art ML algorithms. Their approach utilizes a blockchain-based edge computing technique designed for the IoT environments. With the decentralized and tamper resistant characteristics of the blockchain technology, the trust and integrity required in IoT networks are addressed by means of secure data collection and processing. With the extensive benchmarking through evaluation of multiple ML algorithms on the CICDDoS2019 dataset, the work provided valuable insights into the performance capabilities of the different models. based on these evaluations, the study identified the LightGBM algorithm to be an efficient and good option for real time DDoS detection. However, Blockchain-based solutions are generally at a disadvantage especially due its tamper-proof and decentralized nature which usher in serious latency issues.

The impacts of Agriculture 4.0 have been felt through enhanced productivity through especially the IoT technology, which enables real-time data gathering including crop health, soil quality, and monitoring farming equipment functionality. This, on the other hand, poses DDoS threats to cause non-availability and non-reliability of critical infrastructure. To address this concern by mitigating DDoS attack, [64] proposed a hybrid IDS that combines a deep-Autoencoder (dAE) and a a scheme for Spatial Clustering of Applications based on hierarchical density with noise. The former is for binary classification while the latter is for multiclass clustering. This approach demonstrates effective detection and classification capabilities attaining an accuracy of 98% on CIC-DDoS2019 dataset. Though the combination of dAE ensure effective detection of anomalies couple with HDBSCAN's ability to classify threats into multiple classes, combining these two is computationally intensive for small and resource-constraint IoT devices deployed in Agriculture 4.0. Secondly, though the model performs well when evaluated on the CIC-DDoS2019 dataset, its effectiveness on the changing real-world agricultural environments remains undeterminable and uncertain.

Given the proliferation of interconnected devices, [65] presented an approach to address the critical issue of DDoS attacks in IoT sensor network. To achieve this, the authors proposed a framework to detect DDoS using feature pruning with optimal deep learning (HFPODL-DDoSCD). The framework followed a multilayered approach with the first layer involving a Z-score normalization to standardize input data and stabilize the model. The model also deployed the Siberian tiger optimization for feature extraction. This ensures that the model's computational complexity is reduced without losing pertinent data. The last layer combined bi-directional temporal convolutional networks (BiTCN) and bi-directional gated recurrent units (BiGRU) for efficient capturing of network traffic data's temporal dependencies and complex patterns. To further optimize the model, the authors used the artificial protozoa optimizer (APO) for hyperparameter tuning leading to high detection accuracy. However, the complex model architecture introduces serious computational overheads especially considering the resource-constrained devices on the IoT network.

Combining anomaly detection based on entropy with ML for efficient DDoS attack detection, [66] proposed a framework consisting of multiple phases to detect and mitigate DDoS attacks in SDN-based fog-enabled IoT networks. The framework deployed dynamic thresholding to cater for real-time network fluctuations and an attribute selection algorithm to provide robust classification of DDoS threats.

The failure of the traditional techniques to ensure security of networks against DDoS has contributed to the problems of real time medical monitoring and services provision in IoMT networks. To address this, [67] proposed a scheme based on IoMT for the detection and classification network anomalies composed of a dual-layer and innovative approach to ensure data confidentiality through detecting and preventing of DDoS attacks in IoMTs environments. This was achieved by integrating deep learning, advanced encryption, and optimization techniques. The deployment of Optimal Feistel Block Cipher (OFBC) optimized by using Hybrid Grey-Wolf Optimizer combined with Particle Swarm Optimizer (HGWO-PSO) provided security of sensitive medical data. The use of ResNet50 deep learning model provided efficient detection and prevention of DDoS attacks. They claim that the solution outperforms existing approaches and demonstrates a vital combination of techniques aimed at protecting IoMTs networks. However, the authors seem to misconstrued COVID-19 as a DDoS attack. Based on this review, the focus of their work is to detect COVID-19 in the medical data rather than detection of DDoS.

Despite the transformation of healthcare sector through IoMTs technology, the vulnerability of IoMTs to DDoS due to its resource-constrained and heterogeneity properties remains a nightmare. [68] presented a new and refined design of a hybrid AIDS for IoMT networks. The design utilized outlier and novelty detection algorithms to detect common and new types of attacks. The refined model combined ML algorithms such as one-class SVM, local outlier factor, gaussian kernel density estimation, minimum covariance determinant, isolation forest algorithms, etc. Though the work reported promising results in terms of performance, these ML algorithms may show some level of sensitivity to hyperparameter choices and data quality often requiring careful tunning for anomaly detection. Secondly, the performance of some of the ML model here may degrade when applied to large datasets affecting both scalability and computational efficiency.

To address the challenges associated with DDoS attacks at the application layer, [34] presented an effective and adaptable approach to detect different DDoS attacks at the application layer of the network protocol stack. The proposed detection mechanism utilized random forest, gaussian mixture models (GMM) and a human expert in DDoS attacks identification. The model prioritizes high quality data selection through use of multiple datasets including CICIDS2017 and CICDDoS2019 datasets and ensure adaptability to time-dependent changes in data distributions by deploying the GMM. Combining RF, GMM, and human expert in DDoS attack detection take advantage of ML accuracy with expert insight. This enhances accuracy of threat detection, reduce false positives, and ensure adaptive responses to sophisticated DDoS attack patterns. However, this combination may result in increased complexity, computational overhead, and dependence on expert decision, which impedes real-time detection speed and disable model's scalability in evolving DDoS attack situations.

[69] proposed a multilayer perceptron-based (MLP) framework for intrusion detection in the smart healthcare field. The authors aimed at protecting medical devices and IoMT networks from DDoS attacks. They used NSL-KDD and UNSW-NB15 datasets to evaluate their security framework. The work is novel as it focuses on practical deployment based on real-world need in the healthcare arena. Employing MLP is strategic as it is suitable in the handling of complex data patterns in the network traffic. The use of the datasets named above lends credence to the evaluation of the model by the authors, which allows it to be benchmarked with other detection mechanisms with similar focus. However, relying solely on MLP algorithm can limit the model's diversity as other ML algorithms such as CNN, RNNs, ensemble models, etc. could have offered superior performance. Also, like other deep learning (DL) algorithms, the model does not provide explainability, since these DL are considered as black boxes offering no interpretability. Table 1 presents a summary of existing approaches for DDoS detection review in this paper on the basis of year of publication, the area of focus, methodology used, datasets, contribution to DDoS detection field and the limitations of the approaches.

Table 1: Summary of Existing Approaches for Detection of DDoS Attacks Reviewed

Reference	Year	Focus	Adopted Methodology	Deployed Dataset	Key Contributions	Limitations
[61]	2025	VANETs	BiLSTM Attention network with Dung Beetle Optimization	UNSW_NB15 and Litnet20	ensemble deep learning model with spatial feature extraction and temporal dependency learning	increased computational overhead and resource-intensive operations
[62]	2025	SDN	Hybrid ML-based with LSTM, CNN networks	InSDN dataset	integration of CNN and LSTM architectures, leveraging their complementary strengths	Real-time detection not realizable in resource-constrained device due to model complexity
[63]	2025	IoT	ML techniques with edge computing based on blockchain	CICDDoS2019	The combination of Blockchain technology with ML at the network edge	Blockchain-based solutions are impractical for resource-limited devices. its tamper-proof and decentralized nature bring latency issues.
[64]	2025	IoT-based Agriculture 4.0	deep-Autoencoder (dAE) and Hierarchical Density-Based Spatial Clustering	CIC-DoS2019 dataset	a hybrid IDS combining deep-Autoencoder and spatial clustering based on hierarchical density	computationally intensive for small and resource-constraint IoT devices
[65]	2025	IoT	Feature Pruning with Optimal Deep Learning	IoT/IIoT dataset, Bot-IoT dataset, MQTTset dataset, and	Harnessing feature pruning with optimal deep learning	Reliance on predefined dataset

				TON_IoT dataset		
[66]	2025	SDN-based fog-enabled IoTnetworks	entropy-based anomaly detection with ML	BoT-IoT dataset	integration of entropy-based detection, ML, and adaptive thresholding within a fog-enabled SDN environment	Computational overheads, dependence on labelled data, and inability capture sensitive deviations in network behavior
[67]	2024	IoMT networks	integrated deep learning, advanced encryption, and optimization techniques	NSL-KDD dataset	deployment of an Optimal Feistel Block Cipher (OFBC) for securing sensitive medical data	No real-world clinical validation. Model practical applicability, scalability, and robustness in actual healthcare settings is not guaranteed
[68]	2025	IoMTs networks	Anomaly-based IDS using ML algorithms: OCSVM, LOF, G-KDE), MCD, IsoForest, PW-KDE, and B-GMM	NSL-KDD, IoT/IoMT security testbed-based generated dataset	ML-based Novelty detection and Outlier detection algorithms	sensitivity to hyperparameter choices and data quality often requiring careful tunning for anomaly detection
[34]	2023	Application layer of the network stack	Combined random forest, GMM and human expert in DDoS	CICIDS2017 and CICDDoS2019	Use of adaptive ML-based approach to detection of DDoS attacks	availability and quality of training data, as well as its ability to generalize to emerging or sophisticated application-layer DDoS attack patterns
[69]	2024	smart healthcare networks	multilayer perceptron	NSL-KDD and UNSW-NB15 datasets	develop a framework based on MLP to detect DDoS in healthcare networks	Limited model diversity and absence of explainability
Our study	2026	IoMTs	LSTM-Autoencoder with PSO	CIC-DDoS2019, TCP-SYNC SDN, and CICIoMT2024 datasets	adaptive, specialized, and effective detection mechanisms that can address the particular constraints and security risks of IoMT networks	the framework's effectiveness in practical scenarios remains to be validated through empirical testing and real-time implementation

IV. Discussions and Findings

In this paper, we examined the existing setting of DDoS attack detection and mitigation schemes within the IoMT environment, emphasizing the life-threatening importance of protecting IoMTs infrastructure against DDoS-based disruptions. We examined and considered existing research, to identify predominant challenges, and introduced a conceptualized framework that seeks to utilize Long Short-Term Memory (LSTM) Autoencoders coalesced with Particle Swarm Optimization (PSO) for better DDoS detection performance. LSTM model is known for its efficiency in capturing temporal dependencies in sequential data characteristic of network traffic over time. Autoencoders provide excellent compression and reconstruction of input data, learning a representation of normal network behavior when trained on benign network traffic. PSO is adopted in the conceptualized framework to automatically fine tune key parameters and selection of relevant features for enhanced DDoS detection accuracy.

The review of existing methods for DDoS detection reveals a diverse collection of methodologies utilized in detecting DDoS attacks in IoMT networks. These detection methodologies include anomaly-based, signature-based, and hybrid systems. We observed that signature-based methods, though effective when attack vectors are known, lack the requisite adaptability to handle evolving threats in terms of the DDoS variants. This shortcoming is predominantly disadvantageous in the context of IoMT's dynamic nature given the rapidly changing attack patterns. We also found that majority of anomaly-based techniques utilize ML and deep learning algorithms, revealing improved flexibility. However, the high performance recorded by these ML and DL-based mechanisms is frequently marred by computational overhead and high false positive rates due resource-constrained nature of IoMT devices and networks.

Furthermore, majority of existing works on DDoS detection in the literature are dedicated to centralized detection approach with the potential to impede scalability or a mechanism's ability to provide the level of responsiveness in real-time required in critical healthcare systems. Despite the promising efficiency of distributed detection systems, they still face challenges in the area of coordination complexity and privacy concerns when it comes to data sharing among heterogeneous devices.

Regardless of the level of advancements in technology, this review discovered several challenges potentially obstructive to the progress of development of DDoS detection systems in IoMT environments. First and foremost is the problem of data imbalance brought about by the shortage of labeled attack data, which hinders supervised learning models consequently resulting to reduced detection accuracy. Furthermore, the heterogeneous nature of IoMT network traffic cause difficulties during feature engineering and training of the model. Second, IoMT devices are plagued by serious resource limitations in terms devices' limited processing power and energy resources, restricting deployment of performance oriented but complex detection algorithms on these devices. Another challenge is the need for real-time and adaptive attack detection of a modern-day detection mechanism. Preventing service disruptions requires models to poses high-speed deductive abilities, a property that most deep learning models are struggling to keep pace with without optimization. Also, efficient threat detection requires adaptive and robust mechanisms with the ability to learn and evolve with time as attackers persistently develop sophisticated methodologies to evade detection.

Our conceptual framework sets out to fill these gaps identified as challenges by integrating LSTM-Autoencoders with PSO-based optimization algorithm. The LSTM component is responsible for modeling sequential and temporal dependencies fundamental to network traffic data due to its existential suitability for distinguishing between benign and malicious traffic patterns. The autoencoder structure enables unsupervised learning on unlabeled data, allowing the model to effectively reconstruct normal traffic patterns with any deviations signaling potential DDoS attacks. PSO integration in the proposed framework performs two principal functions including optimizing hyperparameters of the model for increased accuracy and improved efficiency, and performing feature engineering to select the most relevant traffic features. These functions together increase resilience in detection, enhance model performance, reduce computational complexity. The implications of the proposed conceptual framework for healthcare security are that such detection frameworks when implemented in IoMT networks is potent enough to significantly strengthen the ruggedness of healthcare systems against DDoS attacks. This can significantly translate to patient safety and medical operations continuity as a result of prompt DDoS detection and rapid mitigation, because hospitals and health professionals are able to maintain uninterrupted access to critical patient data and medical services due to continued system availability.

V. Conceptual Framework for LSTM-Autoencoder based DDoS attacks Detection in IoMT Networks

The findings as discussed in section 4 of this review paper unmistakably showed that the diverse DDoS attack detection techniques have challenges bordering on device constraints limitations, inability to handle adaptive and evolving threats, computational overhead and high false positive rates, deployment of centralized architecture in designing detection systems making the models unscalable and nonresponsive to real-time DDoS attack detection required in critical medical systems. Again, the finding pointed out that most of the existing models are designed for labelled data which does not allow adaptive threat detection. In this section, we present our conceptual model based on LSTM-Autoencoder and PSO algorithm as shown in figure 6 and describe each component deployed in the framework.

LSTM-Autoencoder Model

While our focus in this paper is not particularly on autoencoders and LSTM individual models, we first provide a short description to aid understanding of the LSTM-Autoencoder hybrid. An Autoencoder is a type of neural network designed for dimensionality reduction. This model receives high dimensional data as input and compresses it into a low dimensional data without losing any important features in the data that is relevant for reconstructing the original data from the compressed representation [70]. The autoencoder strives to retain the fundamental features while not focusing on irrelevant details or noise in the dataset. An Autoencoder model basically consists of two components, the encoder and the decoder components as shown in fig. 6.

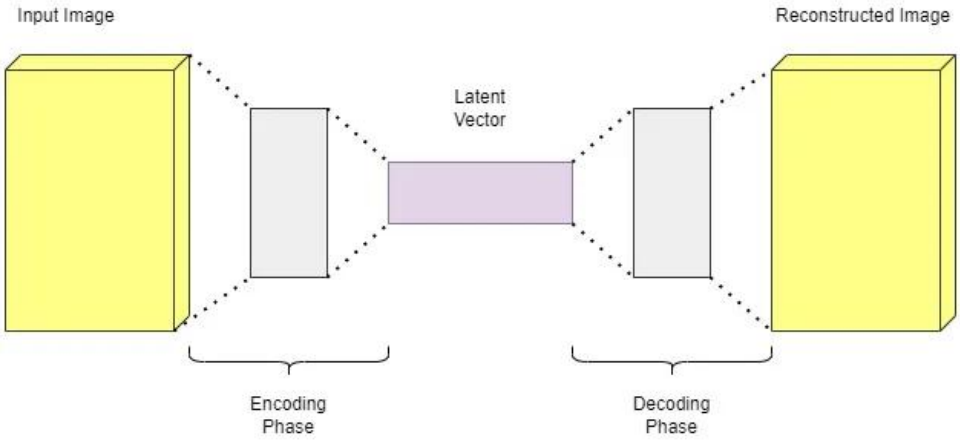

Figure 6: A Basic Autoencoder Architecture (Adapted from: [71])

The former encodes the data into a latent (compressed) representation and the later reconstructs the original data from the latent representation. Autoencoders have use cases in unsupervised learning-based anomaly detection [72], feature extraction [73] and noise reduction [74]. The simplest form of autoencoder is the basic autoencoder. Other types include denoising autoencoder, variational autoencoder, spare autoencoder, convolutional autoencoder, stacked autoencoder, and sequence-to-sequence autoencoder.

LSTM is a recurrent neural network (RNN) with the ability to learn long term dependencies in sequential and temporal data. LSTM utilizes specialized gating mechanisms to control the flow of information in the model, which explains the model's suitability in time series modelling, speech and NLP, and other patterns involving sequential data. the gating mechanisms include the forget gate, which determines information in the model to be discarded, the input gate, that decides what new data to be added to the cell state, cell candidate, responsible for creating values to be added to the cell state given the current input and the previous hidden state, and the out gate, responsible for controlling what information from the cell state will be output as the hidden state. Figure 7 depicts a simple LSTM architecture. There are different variants of LSTM models including Bidirectional LSTM, Stacked LSTM, Basic LSTM, Gated Recurrent Unit (GRU), etc. Each of the above explained models possesses distinct characteristics all of which are specific requirements in achieving the aim of the conceptual model proposed in this paper. This necessitated hybridizing the two models to form the LSTM-Autoencoder (LSTM-AE) architecture.

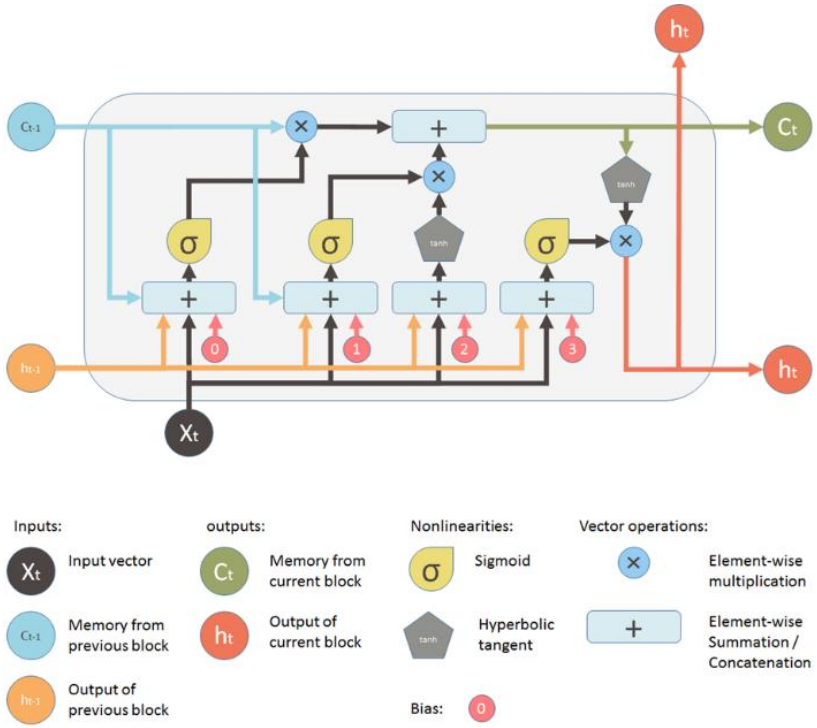

Figure 7: A simple Diagram of a Traditional LSTM Architecture (Adapted from: [77])

5.2 Particle Swarm Optimization Algorithm (PSO)

The process of locating best values for the specific parameters of a given system to achieve all design requirements [75] while bearing in mind the lowest possible cost is referred to as an optimization. PSO one of the computational optimization techniques which is motivated by the behavior of fish schooling or bird flocking in the social context [76]. By creating a complex and emergent pattern of coordinated movements without a central leader, individual members of a schooling of fishes or birds flocking can maintain a certain distance from neighbors and align with their speed and direction. As a population-based and metaheuristic algorithm, the implication of PSO to hyperparameter tunning is its efficient exploratory behavior given a complex, high-dimensional search space. ML and DL models are trained on complex and multidimensional data space with huge number of features, which can be likened to members of fish schooling or birds flocking. PSO uses the concept of social interactions to determine a feature relevance to a particular context enabling optimized features selection (Yadav et al., 2019). The PSO algorithm (represented as a flowchart) is depicted in fig.

8. PSO algorithm is used to optimize the hyperparameters of the LSTM-Autoencoder model, such as the learning rate, batch size, number of epochs, etc. In terms of model selection, the PSO algorithm explores or finds the optimal set of hyperparameters to attain best performance on a validation set by using a number of particles called agents, moving around looking for the optimal solution.

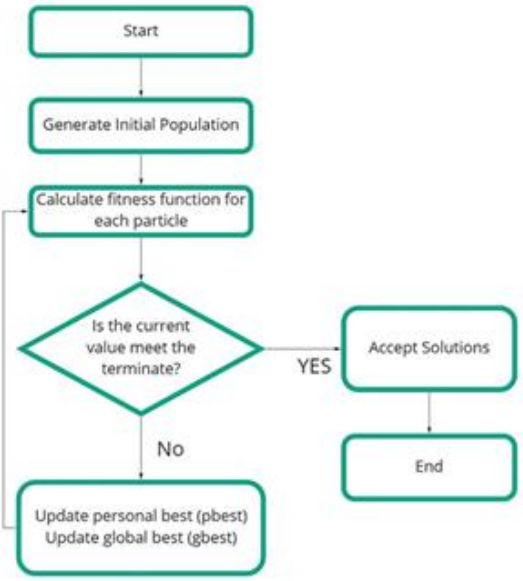

Figure 8: A Flow Diagram of Particle Swarm Optimization (Adapted from: [78])

Proposed LSTM-Autoencoder Model for DDoS Detection

In this section, we present the architecture of the conceptualized system. In this system, the conventional Autoencoder's feedforward layer in the encoder and decoder elements are replaced with LSTM layer such that the autoencoder now consists of an encoder LSTM and a decoder LSTM. Both the LSTM-based encoder and decoder have two layers each having 32 cells each.

Encoder LSTM: The Encoder LSTM component receives the entire high dimensional input sequence and produces fixed-length vector, a hidden state output representing a compressed internal representation of the entire input sequence. The encoder utilizes the memory cells of the LSTM model to preserve the dependencies across multiple data points of the network traffic data and at the same time compressing the high dimensional data to a lower dimension. The final output of the encoder LSTM is an encoded feature vector of the input data fed into the first layer of the encoder LSTM, which then serves as an input to the decoder LSTM component that interprets it as each step in the output sequence is generated. Figure 9 shows the system architecture of the proposed conceptual model.

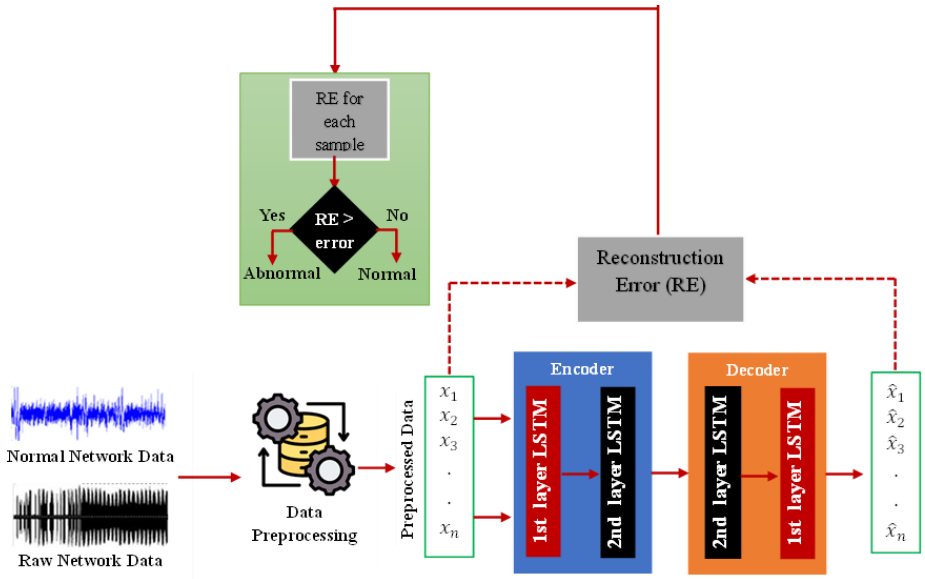

Figure 9: The proposed Conceptual LSTM-Autoencoder-Based DDoS Detection Model

Decoder LSTM: The generated output sequence from the second layer LSTM in the Encoder LSTM is fed in as the input to the first layer of the Decoder LSTM. This is a fixed-size reduced representation of the input data in the latent space. This decoder model reconstructs the reduced representation by minimizing reconstruction error which is used to specify a threshold that is utilized in identifying anomalies. The decoder's input is the encoder's output hence the design of the decoder layer is such that it is configured to unfold the encoding. Because of this required configuration, the decoder layers are stacked in the reverse order of the encoder. The first decoder layer is the same as the second encoder layer. The final output $(\hat{x}_1, \hat{x}_2, \hat{x}_3, \ldots, \hat{x}_n)$ from the decoder is the reconstruction of the input to model.

DDoS Detection: To detect any anomaly such as DDoS, the model specifies a threshold to determine the extent of deviation from normal network traffic. The dataset is partitioned into training and test datasets with no anomalies present in the training dataset. This is to provide reconstruction error only on the basis of normal data points. The training dataset is passed to the model during the model training and after training, all distinct reconstruction errors are computed and the distribution of the reconstruction error values is

observed from where a suitable threshold for DDoS or anomaly detection is selected. The trained model is subsequently tested on the test data including both positively and negatively labeled responses. For every data point in the test dataset, a value for reconstruction error is calculated. Data points are classified as an abnormal if the corresponding reconstruction error surpasses the threshold or normal if the reconstruction error is within range of the threshold.

VI. Conclusion and Future Research Directions

The escalating sophistication and frequency of DDoS attacks in IoMT environments necessitate innovative, adaptive, and resource-efficient detection mechanisms. Our deep learning-based framework, augmented with optimization strategies, demonstrates promising potential to enhance the security posture of IoMT systems. Continued research and development in this domain are imperative to realize secure, reliable, and resilient healthcare IoT ecosystems capable of withstanding evolving cyber threats. Whereas the proposed framework marks a novel contribution to the existing approaches to improve DDoS detection and mitigation mechanisms, there are still more to do in other to continue improving in this area. Future research should focus on integrating edge computing to enable the deployment of lightweight solution on IoMT devices to address the real-time and decentralization requirement of modern DDoS attacks detection. It will also be of great benefit if substantial effort is directed towards developing adaptive-enable models to continuously learn to adapt to evolving attack patterns with little retraining. Considering privacy of health data is a priority, hence future works should also be focused on research in privacy-preserving schemes (such as federated learning and other privacy-preserving methods) to ensure compliance to healthcare privacy regulations (e.g. HIPAA) concerning sharing and analysis of data.

VII. Acknowledgment

This review paper originated from the Research Methodology course during my PhD in Cybersecurity. We are deeply grateful to Professor Opeyemi Osanaiye of Nile University of Nigeria, Abuja for hatching the idea which resulted in the formulation of this review paper. His insightful guidance and constructive feedback cannot be ignored. On behalf of my co-authors, I also value the discussions and encouragement offered by my colleagues and peers which contributed immensely to the success of this work. Lastly, we would like to thank the editors and reviewers for their time and thoughtful evaluation.

References

[1] S. F. Ahmed, S. Sharmin, S. Kuldeep, S. A. Lameesa, A. Alam, S. B. Liu, and A. H. Gandomi, "Transformative impacts of the internet of medical things on modern healthcare," *Results Eng.*, vol. 25, p. 103787, Mar. 2025, doi: 10.1016/j.rineng.2024.103787.

[2] S. Chaudhary and P. K. Mishra, "DDoS attacks in Industrial IoT: A survey," Comput. Netw., vol. 236, p. 110015, 2023, doi: 10.1016/j.comnet.2023.110015.

[3] L. Bing et al., "Ultra reliability and massive connectivity provision in integrated internet of military things (IoMT) based on tactical datalink," Def. Technol., vol. 33, pp. 386–398, 2024, doi: 10.1016/j.dt.2023.02.023.

[4] P. G. Shambharkar and N. Sharma, "Deep learning-empowered intrusion detection framework for the Internet of Medical Things environment," Knowl. Inf. Syst., vol. 66, no. 10, pp. 6001–6050, 2024, doi: 10.1007/s10115-024-02132-z.

[5] S. K. Sarangi et al., "Malicious detection and trust calculation using residual recurrent neural network..." Eng. Appl. Artif. Intell., vol. 161, p. 112130, 2025, doi: 10.1016/j.engappai.2024.112130.

[6] M. Tayebi and S. El Kafhali, "Performance analysis of recurrent neural networks for intrusion detection systems in Industrial-Internet of Things," Franklin Open, vol. 12, p. 100310, 2025, doi: 10.1016/j.fraope.2024.100310.

[7] M. S. Alshehri et al., "A self-attention-based deep convolutional neural networks for IIoT networks intrusion detection," IEEE Access, vol. 12, pp. 45762–45772, 2024, doi: 10.1109/ACCESS.2024.3382435.

[8] A. Jokić et al. "A convolutional neural network-enhanced attack detection framework with explainable artificial intelligence..." Eng. Appl. Artif. Intell., vol. 158, p. 111358, 2025, doi: 10.1016/j.engappai.2024.111358.

[9] Vinayak and T. Jarin, "A hybrid model for detecting intrusions using stacked autoencoders and extreme gradient boosting," Comput. Secur., vol. 150, p. 104212, 2025, doi: 10.1016/j.cose.2024.104212.

[10] J. Yang et al., "Llm-ae-mp: Web attack detection using a large language model with autoencoder and multilayer perceptron," Expert Syst. Appl., vol. 274, p. 126982, 2025, doi: 10.1016/j.eswa.2024.126982.

[11] S. Han et al., "Adapting Convolutional Autoencoder for DDoS Attack Detection via Joint Reconstruction Learning and Refined Anomaly Scoring," Comput. Mater. Contin., vol. 82, no. 1, 2025, doi: 10.32604/cmc.2025.067211.

[12] S. Ameur et al., "Spatial-temporal generative network based on deep long short-term memory autoencoder..." Eng. Appl. Artif. Intell., vol. 161, p. 112289, 2025, doi: 10.1016/j.engappai.2025.112289.

[13] J. Gao et al., "Particle Swarm Optimization with Problem-Aware Hyperparameter Design for Feature Selection in High Dimensions," Inf. Sci., vol. 692, p. 122638, 2025, doi: 10.1016/j.ins.2024.122638.

[14] M. Ibrahim and A. Al-Wadi, "Enhancing IoMT network security using ensemble learning-based intrusion detection systems," J. Eng. Res., 2024, doi: 10.1016/j.jer.2024.01.018.

[15] S. T. Anuva, "LIDIT: Low-Latency Intrusion Detection in IoMT Devices using TinyML," Doctoral dissertation, 2025, doi: 10.13140/RG.2.2.14562.13761.

[16] X. Chen et al., "Real-time DDoS defense in 5G-enabled IoT: A multidomain collaboration perspective," IEEE Internet Things J., vol. 10, no. 5, pp. 4490–4505, 2022, doi: 10.1109/JIOT.2022.3219920.

[17] B. Bhasker et al., "Optimizing energy task offloading technique using IoMT cloud in healthcare applications," J. Cloud Comput., vol. 14, no. 1, p. 9, 2025, doi: 10.1186/s13677-024-00582-w.

[18] Z. Liu et al., "Jaqen: A High-Performance, Switch-Native approach for detecting and mitigating volumetric DDoS attacks..." Proc. 30th USENIX Secur. Symp., 2021, doi: 10.5555/3488932.3489199.

[19] M. Kumar et al., "Hybrid deep learning-based cyberthreat detection and IoMT data authentication model in smart healthcare," Future Gener. Comput. Syst., vol. 166, p. 107711, 2025, doi: 10.1016/j.future.2024.107711.

[20] M. A. Haque et al., "Device access control and key exchange (DACK) protocol for Internet of Things," Int. J. Cloud Appl. Comput., vol. 12, no. 1, pp. 1–14, 2022, doi: 10.4018/IJCAC.297098.

[21] E. Elbasi, "B-DCT based Watermarking Algorithm for Patient Data Protection in IoMT," 2020 International Conference on Information Security and Cryptology (ISCTURKEY), Ankara, Turkey, 2020, pp. 1-4, doi: 10.1109/ISCTURKEY51113.2020.9307963.

[22] A. K. Srivastava et al., "A Paradigm Shift from Human-Centred to Life-Centred Design," Proc. 15th EAD, 2023, doi: 10.5117/9789048557344/EAD.2023.012.

[23] B. Bhushan et al., "Towards a secure and sustainable internet of medical things (IoMT)..." Sustainability, vol. 15, no. 7, p. 6177, 2023, doi: 10.3390/su15076177.

[24] K. Zwingina et al., "Impact of DDoS attacks on critical national information infrastructure..." Int. J. Conflict Secur. Manag., vol. 1, no. 5, 2024, doi: 10.59573/ijcsm.2024.1.5.8.

[25] S. Traer and P. Bednar, "Motives behind ddos attacks," Digital Transformation and Human Behavior, 2020, doi: 10.1007/978-3-030-47539-0_9.

[26] S. A. Alavi et al., "Beyond botnets: Autonomous Firmware Zombie Attack in industrial control systems," Int. J. Crit. Infrastruct. Prot., vol. 48, p. 100729, 2025, doi: 10.1016/j.ijcip.2024.100729.

[27] W. Havenga et al., "Autonomous Threat Detection and Response for Self-Protected Networks," Proc. 2022 ICTAS, 2022, doi: 10.1109/ICTAS53252.2022.9744643.

[28] A. A. J. Al-Abadi et al., "Robust and Reliable Security Approach for IoMT..." Int. J. Recent Innov. Trends Comput. Commun., vol. 11, pp. 239–247, 2023, doi: 10.17762/ijritcc.v11i5s.6622.

[29] D. M. A. A. Afraji et al., "Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments," Cyber Secur. Appl., p. 100085, 2025, doi: 10.1016/j.csa.2024.100085.

[30] M. Ouhssini et al., "Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments..." Egypt. Informatics J., vol. 27, p. 100517, 2024, doi: 10.1016/j.eij.2024.100517.

[31] M. Anagnostopoulos et al., "Large-scale empirical evaluation of DNS and SSDP amplification attacks," J. Inf. Secur. Appl., vol. 66, p. 103168, 2022, doi: 10.1016/j.jisa.2022.103168.

[32] K. B. Adedeji et al., "DDoS attack and detection methods in internet-enabled networks..." J. Sens. Actuator Netw., vol. 12, no. 4, p. 51, 2023, doi: 10.3390/jsan12040051.

[33] A. Reed et al., "SA-IDS: A single attribute intrusion detection system for Slow DoS attacks in IoT networks," Internet Things, p. 101512, 2025, doi: 10.1016/j.iot.2024.101512.

[34] D. M. Sharif and H. Beitollahi, "Detection of application-layer DDoS attacks using machine learning and genetic algorithms," Comput. Secur., vol. 135, p. 103511, 2023, doi: 10.1016/j.cose.2023.103511.

[35] B. B. Gupta and A. Tewari, A Beginner's Guide to Internet of Things Security. CRC Press, 2020, doi: 10.1201/9781003046042.

[36] M. Abbasi et al., "Deep learning for network traffic monitoring and analysis (NTMA): A survey," Comput. Commun., vol. 170, pp. 19–41, 2021, doi: 10.1016/j.comcom.2021.01.021.

[37] M. Baskar et al., "Low-rate DDoS mitigation using real-time multi threshold traffic monitoring system," J. Ambient Intell. Humaniz. Comput., 2021, doi: 10.1007/s12652-021-03014-w.

[38] A. El-Sayed et al., "Deception and cloud integration: A multi-layered approach for DDoS detection..." Comput. Electr. Eng., vol. 126, p. 110543, 2025, doi: 10.1016/j.compeleceng.2024.110543.

[39] M. Li et al., "Real-time monitoring model of DDoS attacks using distance thresholds in Edge cooperation networks," J. Inf. Secur. Appl., vol. 89, p. 103972, 2025, doi: 10.1016/j.jisa.2025.103972.

[40] S. R. Sindiramutty et al., "Generative AI in Network Security and Intrusion Detection," IGI Global, 2025, doi: 10.4018/979-8-3693-5599-2.ch004.

[41] K. Shaukat et al., "A review of time-series anomaly detection techniques," Proc. FICC, 2021, doi: 10.1007/978-3-030-73103-8_59.

[42] I. Bozcan and E. Kayacan, "Context-dependent anomaly detection for low altitude traffic surveillance," Proc. 2021 ICRA, 2021, doi: 10.1109/ICRA48506.2021.9560877.

[43] W. Shi, D. Karastoyanova, Y. Ma, Y. Huang, and G. Zhang, "Clustering-based granular representation of time series with application to collective anomaly detection," IEEE Trans. Instrum. Meas., vol. 72, pp. 1–12, 2023, doi: 10.1109/TIM.2023.3325521.

[44] A. Toshniwal et al., "Overview of anomaly detection techniques in machine learning," Proc. 2020 I-SMAC, 2020, doi: 10.1109/I-SMAC49090.2020.9243329.

[45] R. Swami et al., "IQR-based approach for DDoS detection and mitigation in SDN," Def. Technol., vol. 25, pp. 76–87, 2023, doi: 10.1016/j.dt.2023.03.018.

[46] A. B. Nassif et al., "Machine learning for anomaly detection: A systematic review," IEEE Access, vol. 9, pp. 78658–78700, 2021, doi: 10.1109/ACCESS.2021.3083060.

[47] A. A. Alsadhan et al., "Kernel-Based Machine Learning Intrusion Detection Systems for ICMPv6 DDoS Detection," Results Eng., p. 106940, 2025, doi: 10.1016/j.rineng.2025.106940.

[48] A. Srivastava and D. Sinha, "FP-growth-based signature extraction and unknown variants of DoS/DDoS attack detection," J. Inf. Secur. Appl., vol. 89, p. 103996, 2025, doi: 10.1016/j.jisa.2025.103996.

[49] E. Iqbal et al., "Multi-scale feature reconstruction network for industrial anomaly detection," Knowl.-Based Syst., vol. 305, p. 112650, 2024, doi: 10.1016/j.knosys.2024.112650.

[50] J. V. Iyer, "Intrusion detection system using signature-based detection and data mining technique," World of Business with Data and Analytics, 2022, doi: 10.1007/978-981-16-7132-6_11.

[51] M. Thankappan et al., "A signature-based wireless intrusion detection system framework..." IEEE Access, vol. 12, pp. 23096–23121, 2024, doi: 10.1109/ACCESS.2024.3364467.

[52] G. R. Enjam, "AI-Powered API Gateways for Adaptive Rate Limiting and Threat Detection," IJAIDML, vol. 5, no. 4, 2024, doi: 10.5121/ijaidml.2024.5408.

[53] M. Bartkov and D. Borovikov, "Selection of A Suitable Algorithm for the Implementation of Rate-Limiter Based on Bucket4j," iJOE, vol. 16, no. 4, 2022, doi: 10.3991/ijoe.v18i04.28859.

[54] S. Zhu et al., "On Rate-Limiting in Mobile Data Networks," IEEE Trans. Mob. Comput., vol. 23, no. 12, 2024, doi: 10.1109/TMC.2024.3398125.

[55] X. Tao et al., "User behavior threat detection based on adaptive sliding window gan," IEEE Trans. Netw. Serv. Manag., vol. 21, no. 2, 2024, doi: 10.1109/TNSM.2023.3323497.

[56] T. Xu et al., "Mitigating the table-overflow attack in software-defined networking," IEEE Trans. Netw. Serv. Manag., vol. 14, no. 4, 2017, doi: 10.1109/TNSM.2017.2721151.

[57] Y. Li et al., "Trident: Defensing synergetic denial-of-service attacks in underwater named data networking," IEEE Internet Things J., vol. 10, no. 23, 2023, doi: 10.1109/JIOT.2023.3297334.

[58] J. K. Madhloom et al., "An information security engineering framework for modeling packet filtering firewall..." Computers, vol. 12, no. 10, p. 202, 2023, doi: 10.3390/computers12100202.

[59] M. Umizaki et al., "Understanding the Characteristics of Public Blocklist Providers," 2022 IEEE Symposium on Computers and Communications (ISCC), Rhodes, Greece, 2022, pp. 01-07, doi: 10.1109/ISCC55528.2022.9913009.

[60] U. Kumarasinghe et al., "Blocklist-Forecast: Proactive Domain Blocklisting by Identifying Malicious Hosting Infrastructure," Proc. 27th RAID, 2024, doi: 10.1145/3678890.3678925.

[61] N. Jayakrishna and N. Prasanth, "Detection of DDOS attacks in Vehicular Ad Hoc Networks..." Results Eng., p. 107022, 2025, doi: 10.1016/j.rineng.2025.107022.

[62] A. V. Kachavimath and D. G. Narayan, "A Hybrid Deep Learning Model with Consensus-Based Feature Selection for DDoS Attacks Detection in SDN," Procedia Comput. Sci., vol. 252, 2025, doi: 10.1016/j.procs.2025.02.068.

[63] M. Chaira et al., "Enhancing DDoS Attacks Mitigation Using Machine Learning and Blockchain-Based Mobile Edge Computing in IoT," Computation, vol. 13, no. 7, 2025, doi: 10.3390/computation13070158.

[64] P. Kaliyaperumal et al., "Enhancing cybersecurity in Agriculture 4.0: A high-performance hybrid deep learning-based framework..." Comput. Electr. Eng., vol. 126, p. 110431, 2025, doi: 10.1016/j.compeleceng.2024.110431.

[65] R. Aboalela et al., "Harnessing feature pruning with optimal deep learning-based distributed denial of service..." Alexandria Eng. J., vol. 120, 2025, doi: 10.1016/j.aej.2024.12.034.

[66] P. Chaudhary et al., "Dynamic multiphase DDoS attack identification and mitigation framework to secure SDN-based fog-empowered consumer IoT Networks," Comput. Electr. Eng., vol. 123, 2025, doi: 10.1016/j.compeleceng.2024.110226.

[67] G. Sripriyanka and A. Mahendran, "Securing IoMT: A hybrid model for DDoS attack detection and COVID-19 classification," IEEE Access, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3354034.

[68] G. Zachos et al., "Implementing Anomaly-Based Intrusion Detection for Resource-Constrained Devices in IoMT Networks," Sensors, vol. 25, no. 4, 2025, doi: 10.3390/s25041216.

[69] A. Khan et al., "Deep Learning-Driven Anomaly Detection for IoMT-Based Smart Healthcare Systems," Comput. Model. Eng. Sci., vol. 141, no. 3, 2024, doi: 10.32604/cmes.2024.054380.

[70] T. Liu et al., "High-Ratio Lossy Compression: Exploring the Autoencoder to Compress Scientific Data," IEEE Trans. Big Data, 2021, doi: 10.1109/TBDATA.2021.3066151.

[71] R. Senaratne, "Anomaly Detection using LSTM Autoencoder," Medium; Heartbeat, 2022. (N/A - Blog post)

[72] T. Finke et al., "Autoencoders for unsupervised anomaly detection in high energy physics," J. High Energy Phys., vol. 2021, no. 6, 2021, doi: 10.1007/jhep06(2021)161.

[73] N. Tavakoli et al., "An autoencoder-based deep learning approach for clustering time series data," SN Appl. Sci., vol. 2, no. 5, 2020, doi: 10.1007/s42452-020-2584-8.

[74] S.-M. Kim and Y. S. Kim, "Enhancing Sound-Based Anomaly Detection Using Deep Denoising Autoencoder," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3414435.

[75] F. A. Zaini et al., "A review on the applications of PSO-based algorithm in demand side management," IEEE Access, vol. 11, 2023, doi: 10.1109/ACCESS.2023.3278261.

[76] F. Pourpanah et al., "A review of artificial fish swarm algorithms: Recent advances and applications," Artif. Intell. Rev., vol. 56, no. 3, 2023, doi: 10.1007/s10462-022-10214-4.

[77] S. Yadav et al., "Information theoretic-PSO-based feature selection: an application in biomedical entity extraction," Knowl. Inf. Syst., vol. 60, no. 3, 2019, doi: 10.1007/s10115-018-1270-2.

[78] S. Maurya, "Particle Swarm Optimization (PSO)," Medium; Grid Solutions, 2022.