OPEN ACCESS

ISSN: 2996-4954

Pradeep Rao V, et al. (2023) 152-160
J Contemp Edu Theo Artific Intel: 2023(5):100110
DOI: 10.71010/2996-4954/JCETAI-e110

Research Article

Journal of Contemporary Education Theory & Artificial Intelligence

A Survey on Cyberattack Mitigation Techniques: DDoS, Spoofing, and Ransomware Detection Using ML/DL

Pradeep Rao Vennamaneni[1*], Venkata Phaneendra Reddi[2], Sri Prudhvi Adusumilli[3], Khaja Moiezuddin Mohammed[4], Rashmika Jalagam[5], Sridevi Allu[6]

[1]JPMC - Senior Software Engineer, praovennamaneni@gmail.com
[2]Atlantic Health systems - Oracle Integrations Developer, v3nkata@gmail.com
[3]Charter Communications, Sr Software Developer, prudhvi2379@gmail.com
[4]Iqvia - Sr Data Engineer, moiezmohammed81@gmail.com
[5]Matilda Cloud - Cloud Engineer/Python Developer, rashmikaj@gmail.com
[6]American Airlines, AI/ML Engineer, srideviallu14@gmail.com

[*]**Corresponding author:** Pradeep Rao Vennamaneni

Citation: Pradeep Rao V, Venkata Phaneendra Reddi, Sri Prudhvi A, Khaja Moiezuddin M, Rashmika J, et al. (2023) A Survey on Cyberattack Mitigation Techniques: DDoS, Spoofing, and Ransomware Detection Using ML/DL. J Contemp Edu Theo Artific Intel: ICETAI-110. DOI: 10.71010/2996-4954/jcetai-e110.

Received Date: 12 November, 2023; **Accepted Date:** 18 November, 2023; **Published Date:** 25 November, 2023

Abstract

In the modern world, cyberattacks are emerging as a significant threat to information systems. Still, they target information networks, information devices, and information applications to steal, modify, or destroy sensitive information. These traditional methods of mitigation namely signature-based as well as rule-based detection are applicable in detecting and removing the known types of attacks, but not the zero-day attacks, polymorphic malware and wide traffic. The constantly evolving threats, including Distributed Denial of Service (DDoS), spoofing and ransomware, reiterate the need to have more adaptable defences. To overcome these impediments, cybersecurity systems are adopting machine learning (ML) and deep learning (DL). ML methods are more effective at identifying anomalies and preventing intrusion, but DL models can learn features automatically and classify complex threats effectively. Such intelligent methods are typically applied in anomaly detection and malware detection, phishing prevention, and monitoring network intrusions. The solutions provided through data-driven intelligence make use of both ML and DL to provide adaptive, scalable, and proactive mitigation against cyberattacks, which is a great improvement to the mitigation of cyber threats as compared with traditional defences because of the ever-evolving and dynamic nature of the cyber threat environment.

Keywords: *Cyberattack Mitigation, Distributed Denial of Service (DDoS), Spoofing, Ransomware, Machine Learning (ML), Deep Learning (DL).*

I. Introduction

Cybersecurity can be described as the safety of information systems, networks, and data against theft, compromise, or disruption. It contains the techniques and technologies used to defend online resources against unethical practices. The current data-driven and interconnected world has made cybersecurity a crucial necessity, where failure to adopt IT systems to store and transmit sensitive information cannot be afforded by any industry [1]. The problem of cyberattacks has already become international, and there are fears that a mass breach of the system would not only endanger individual companies but also compromise the overall stability of the global economy [2]. Addressing this challenge requires multidimensional and multi-layered interventions across several domains.

Data privacy and security are ever-present threats in today's society due to the prevalence of big data, social media, online shopping, information kept or handled online, and automated procedures carried out by means of information technology [3]. The frequency and severity of cyberattacks, as well as the tools and strategies used to perpetrate them, are on the rise. One of the most prevalent and destructive types of cybercrime is the distributed denial-of-service (DDoS) attack. Attackers cause a "denial of service," or DoS, when they flood servers with malicious data. Distributed denial of service attacks occur when a large number of compromised systems or computers attempt to overwhelm a single application [4]. Distributed denial of service (DDoS) attacks are changing, becoming more complex and more common as new, potentially disruptive technologies appear on the Internet.

Cybercrime tracing and identifying the offender becomes much more challenging when spoofing is involved [5]. Internet Protocol spoofing is a typical tactic employed by malevolent DDoS attackers. When using IP for communication, the header field includes both the source and destination IP addresses, as determined by the network socket's general operations [6] [7]. Similarly, ransomware has emerged as a critical cyber threat, with Ransomware-as-a-Service (RaaS) proliferating through underground marketplaces on the dark web [8]. Attackers use social engineering and vulnerability exploitation to deliver ransomware, which encrypts files and demands payment for their release [9]. Ransomware directly presents the victims with ransom demands unlike general malware which tends to do so in the background [10].

Firewalls, intrusion detection systems based on signatures, and rule-based systems are often inadequate in the face of such new threat developments [11]. Cybersecurity is increasingly incorporating AI systems, particularly ML and DL, to address these deficiencies. ML can be applied to improve cyberattack detection using signature-based analysis, as well as anomaly-based analysis. DL methods are more accurate and have faster processing capabilities due to their high pattern recognition and self-learning capabilities [12]. Since traditional methods are also limited and the use of DL in other areas has proven to be successful, the implementation of a cybersecurity solution is rather promising.

A. Structure of the Paper

The paper is organized as follows: Section II outlines the cyberattack landscape, focusing on DDoS, spoofing, and ransomware. Section III examines the conventional mitigation methods and their drawbacks. Section IV examines ML and DL approaches for cyberattack mitigation. Section V presents a literature review of key studies, challenges, and future directions. Implications and future study directions are presented in Section VI.

II. Cyberattack Landscape

A cyberattack can take many forms, but the overarching goal is the same: to steal, alter, or destroy material that is crucial to the target. Anyone or anything that gains access or uses it without authorization is deemed an attacker. Anyone or any organization can initiate a cyberattack. Getting into a target's or management's computer system is the ultimate goal of a cyberattack [13]. Computer data, code, or logic can be altered by malicious code, which is used in cyberattacks. This causes problems and puts data at risk, which in turn leads to cybercrimes including identity and information theft.

A. Characteristics of Cyber Attacks

A cyberattack is an intentional effort to gain unauthorized access to computer systems, networks, and software by using known vulnerabilities. The objectives of these attacks may include compromising services, stealing sensitive data, or gaining unauthorized access for financial gain, strategic advantage, or malicious purposes.

1) Distributed Denial of Service (DDoS) Attacks

The goal of a DoS attack is to block access to network resources for users who are not malicious. A DDoS attack occurs when different compromised devices in different places are used to conduct such attacks. A classic DOS attack involves an attacker secretly injecting malicious code into networked systems by taking advantage of security holes [14]. The attacker then issues commands through masters or command-and-control (C2) servers, which coordinate the actions of slave devices (bots). These bots simultaneously flood the targeted victim with massive volumes of traffic, overwhelming its resources and disrupting services while concealing the true origin of the attack. Figure 1. A hierarchical DDoS network. An attacker issues commands to one or more masters (C2/handlers), which control multiple compromised slaves (bots). The bots then flood the victim with coordinated traffic, overwhelming services and obscuring the true source of the attack.

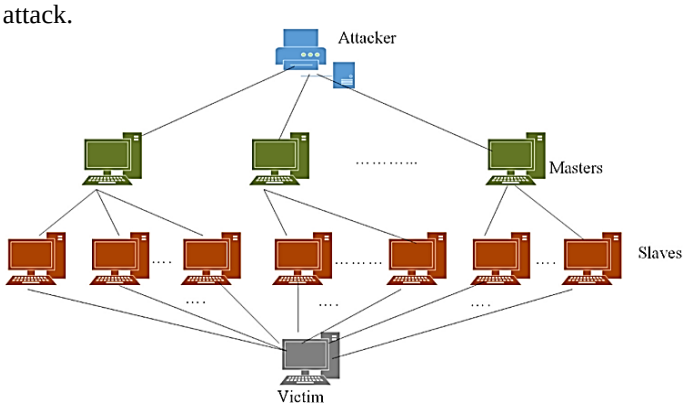


Fig 1: Structure of the DDoS Attack

2) Spoofing Attacks

Spoofing refers to a cyberattack technique in which an attacker falsifies information to deceive systems or users. It can take multiple forms, all involving some type of false representation or impersonation [15]. Various methods exist, and this paper introduces and explains the following major types of spoofing attacks.

a) IP and DNS Spoofing

Attacks based on IP and DNS spoofing are types of network-centric vulnerability attacks aimed at allowing the attacker to impersonate a trusted system and manipulate and/or redirect network traffic using their trust relationship with the system. The goal of IP spoofing is to obtain unauthorized access by changing the source address of data packets to bypass security restrictions. In DNS spoofing, the attacker modifies the name-resolution process to redirect users from a trusted domain to a malicious one. When either technique is successful, the attack has the potential to turn into an even more potent attack, like a man-in-the-middle, where passwords and other sensitive user information, including financial details, could be compromised.

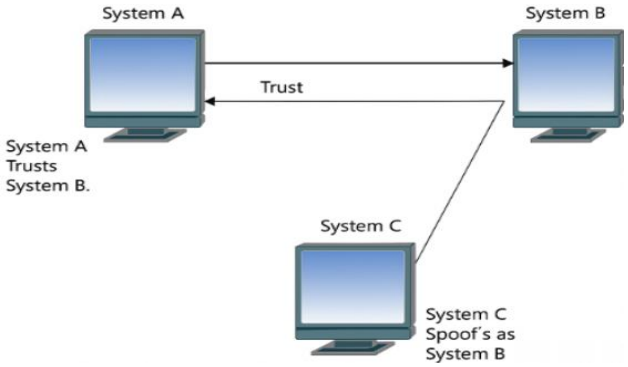


Fig 2: IP Spoofing.

For example, as shown in Figure 2, the attacker (System C) has spoofed or impersonated a trusted system (System B) to act as a trusted intermediary to fool System A. With this trust, the attacker can issue requests with false values to execute unauthorized actions against the system or its resources or obtain sensitive information.

b) Email and ARP Spoofing

Email and ARP spoofing target users and local networks by misrepresenting source information to take advantage of packaging inherent trust [16]. Email spoofing presents malicious emails as being from a legitimate source, which could be used for either phishing or malware delivery. ARP spoofing presents false IP-to-MAC address mappings in an attempt to capture, alter, or reroute traffic on a local network. Both methods leverage deception: users trust the sender's email address; network devices trust the IP-ARP mappings, allowing attackers access or control over communications.

3) Ransomware Attacks

Ransomware is malicious software that extorts money from unsuspecting users. "Ransomware" comes from the practice of encrypting files or devices and then requesting payment from the victim to either decrypt them or stop the attacker from releasing sensitive information. The most typical ways it spreads are through malicious attachments in emails, broken software, infected external drives, and compromised websites. While most software tries to stay hidden, ransomware reveals itself halfway through its execution to demand payment from the victim.

a) Attack Vectors for Distributing Ransomware.

Cybercriminals use numerous methods to deceive prospective victims into executing ransomware, elevate privileges, and ultimately extort payment. Typical vectors for infection encompass social engineering, botnets, downloader trojans, drive-by downloads, exploit kits, and harmful attachments in phishing emails. Phishing remains the most common method employed, often used in conjunction with privilege escalation, data exfiltration, or lateral movement to increase its impact [17]. Effective defences rely on user awareness, timely patching, endpoint protection, traffic segmentation, and reliable offline backup retention times to limit damage and reduce the time to recovery. Attackers often encrypt mission-critical data and/or exfiltrate sensitive information to increase their leverage and extort a victim.

b) Situational Awareness Model for Ransomware Mitigation.

The situational awareness (SA) paradigm enables informed decision-making by providing a precise understanding of the status of devices and networks [18]. It encompasses identifying and monitoring elements, as well as aggregating, correlating, analyzing, and forecasting data. The process involves three stages: Perception, which gathers and organizes raw data; Comprehension, which correlates and filters information for analysis; and Projection, which forecasts system behavior, evaluates past countermeasures, and enables proactive and reactive responses.

By integrating the SA model with the ransomware life cycle, organizations can detect early signs of infection, anticipate attacker actions, and implement timely countermeasures. Figure 3 illustrates a situation awareness model, where Perception gathers data from sources such as files, databases, and network devices. These stages guide Decision-making, followed by Action, which in turn alters the environment and generates new data, creating a continuous cycle.

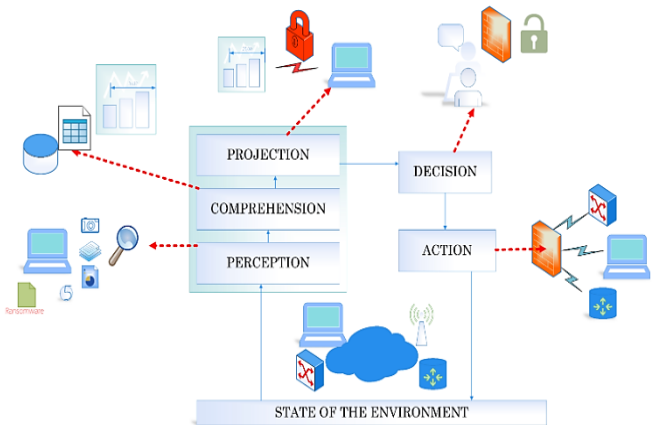


Fig 3: Situational Awareness Model and Ransomware Protection & Mitigation.

B. Challenges of Cyber Attack Prevention.

Preventing cyberattacks is a significant challenge due to the rapidly evolving threat landscape. More commonly than ever, criminals are leveraging technology to advance the speed of crimes involving fraud, identity theft, and data breaches, are given below:

1) Ransomware Evolution

The data on a victim's device is encrypted by ransomware, a type of malware that necessitates payment before the data is released. Data professionals, cybersecurity professionals, executives, and information technology professionals are all plagued by ransomware. The frequency of ransomware attacks in cybercrime regions is increasing daily [19]. A robust response strategy against Ransomware attacks is essential for corporate proprietors and IT practitioners. Data and service retrieval from businesses and customers, together with reporting of Notifiable Data Breaches violations, requires careful planning.

2) Blockchain Revolution

The most significant technological advancement to date is blockchain technology. For the first time in human history, an ideal native digital medium for peer-to-peer value exchange is available. The blockchain system generates Bitcoin, a cryptocurrency. The blockchain is a vast, global network that enables two or more parties to engage in business or conduct transactions without the use of a trusted third party.

3) IoT Threats

The term "Internet of Things" (IoT) refers to a system of physical objects that can communicate with one another and the wider web [20]. Connected hardware devices have a unique identifier (UID) and can send data over a network without an intermediary, be it a person or a computer. Internet of Things (IoT) devices are vulnerable to hacking because of the software and firmware that runs on them. In the planning of IoT projects, the use of cybersecurity for commercial purposes is not considered.

4) AI Expansion

The primary advantage of AI in information defence approach is its ability to secure and defend an infrastructure before the occurrence of a malware attack, thereby reducing its impact. If

a business is affected by a hazard, AI promptly responds to the malicious attacks. AI is perceived by IT business leaders and information security management teams as a future protective control that enables organisations to remain at the forefront of cybersecurity development.

III. Traditional Mitigation Techniques

Mitigation measures protect end users by identifying and mitigating malicious attacks. To further combat the assault, high-priority switches have new flow rules that work in tandem with the rule for suspect packets [21]. The precision of the mitigation protocols is contingent upon the extent of the attack's information that can be harvested. The traditional mitigation strategies for cyber-attack detection are discussed below:

A. Signature-Based Detection

Pattern matching techniques, sometimes called Knowledge-based Detection or Misuse Detection, are used to identify known attacks [22]. A signature-based matching method can detect a past incursion. What this means is that the signature database will trigger an alarm signal if the signature of an intrusion matches that of an earlier incursion [23]. A conventional cybersecurity approach, signature-based detection compares files, programs, or network traffic to a database of recognized malicious patterns, or signatures, to identify potential threats. It is efficient in identifying malware and previously identified attacks, and it provides rapid scanning with minimal false positives. But its primary limitation is its inability to identify new or zero-day threats until their signatures are generated and incorporated into the database. This makes it reliable for known attacks but less effective against evolving or polymorphic malware, requiring constant updates to maintain effectiveness.

B. Rule-Based Detection Heuristic Approach

Rule-based techniques rely on pre-set rules to identify unusual behaviours or traffic patterns. Heuristic methods, by contrast, try to detect anomalies by reviewing behaviours that deviate from typical behaviours in the system or network [24]. Heuristic techniques can detect unknown attacks, including variations of known threats, by logical inference or behavioural patterns. Heuristic detection techniques have advanced beyond basic signatures, assessing the behaviour and characteristics of hypothetical threats. These threats can be assessed collaboratively (or in a federated environment) across organizations in the same business sector (financial, healthcare, etc.) [25]. Use these flags to classify attacks based on severity, type, geographic range, user action required, and system availability. This also allows adaptive and contextual responses to threats, as each organization can have its own flag parameters according to its local security policy. Collaborative heuristic methods enhance overall threat detection, thereby improving responses to both known and unknown cyberattacks.

C. Limitations of the Conventional Techniques

Conventional cybersecurity defence mechanisms, including firewalls, IDS, and signature-based antivirus software, have been extensively employed to identify and mitigate cyberattacks. Although these methods are effective against recognized threats, they encounter substantial obstacles as the cyber landscape continues to evolve [26]. Inadequate for detecting novel, sophisticated, or polymorphic attacks, they frequently depend on predefined rules and signatures. Notable examples include:

- **Signature Dependency:** Traditional IDS and antivirus tools rely on predefined signatures or rules.
- **Inability to Handle Evolving Threats:** Conventional systems are not adaptive; attackers can easily bypass them by slightly modifying attack vectors (e.g., encrypted traffic or obfuscation).
- **Scalability Issues:** Rule-based firewalls and signature-based IDS struggle with large-scale, high-speed network traffic (e.g., DDoS).
- **Limited Context Awareness:** Traditional methods typically inspect packets or files in isolation without analyzing behavioral patterns or contextual correlations.

IV. ML-DL-Based Approaches for Cyberattack Mitigation

Traditional machine learning methods are still the gold standard for cyber-attack detection since they are less resource-intensive, easier to understand, and more interpretable than deep learning methods. Nevertheless, deep learning is rapidly evolving and provides the foundation of an increasing variety of mitigating approaches. Since they are more efficient and effective, ML and DL techniques are widely used in technical and scientific writings.

A. Machine Learning Approaches

ML is becoming more popular and widely used. Their capacity to comprehend and resolve actual problems is greatly valued, and current approaches are being enhanced accordingly. Machine learning has been widely used in various sectors due to these advancements; such examples include computer vision, medical analysis, gaming, and social media marketing [27]. When compared to more conventional rule-based algorithms or even human operators, machine learning methods can sometimes outperform the competition [28]. Even in cybersecurity, this trend is having an impact, as ML components are being used to update detection systems.

1) Decision Tree (DT)

One method of machine learning is the decision tree, which displays all possible decision outcomes in a top-down tree format. A decision node, a branch, and a leaf node are the three parts that make up the tree. The leaf node represents an item's class or label, a possible attribute value by a branch, and the if-then condition by the decision node.

2) Naïve Bayes (NB)

A statistical classifier, Naïve Bayes is founded on the Bayes' theorem. This probabilistic machine learning method outperforms competing classifiers when working with limited datasets and categorical values. Multinomial Naïve Bayes, Gaussian Naïve Bayes, and Bernoulli Naïve Bayes are the three Neural Network algorithms. Some of the approaches employed are: Naïve Bayes with a Gaussian distribution for continuous data, a Bernoulli distribution for binary values, and a multinomial distribution for discrete values.

3) Logistic Regression (LR)

LR is a commonly used classification method for categorical target variables, specifically if the outcome is binary. Unlike fitting a straight regression line, logistic regression fits an "S"-shaped sigmoid function that predicts class membership probabilities. Instead of finding a value between -∞ and +∞ and mapping it to a prior class, the sigmoid function provides a value between 0 and 1 that predicts a given instance's likelihood for a class. Logistic regression is frequently used in cybersecurity and intrusion detection systems to help distinguish between malicious and normal actions.

4) XGBoost (XGB)

XGBoost, or Extreme Gradient Boosting, is a type of advanced gradient boosted machine learning based on decision trees that enables the building of prediction models with a high degree of accuracy [29]. Sequentially building weak learners enables the algorithm to correct mistakes made by earlier trees and prevent overfitting through regularisation. Anomaly detection related to harmful behaviours, such as intrusion detection, phishing, or a DDoS assault, is a common use case for XGBoost in breach mitigation. This subset of machine learning algorithms can differentiate between benign and harmful actions because it can process massive, multi-dimensional datasets and learn intricate data correlations. As such, it highlights the capabilities of automated systems that detect cyber threats.

B. Deep Learning Approaches

DL process-defined representation learning, which relies on a multi-layered representation of the input data, makes automated feature selection possible [30]. DL algorithms rely on DNNs as their foundation. See below for an example of a DNN in action; these massive, multi-layered neural networks are capable of autonomous representation learning:

1) Multilayer Perceptron (MLP)

Data categorization and classification are just two of the many tasks that artificial neural networks can accomplish after being trained to mimic any function. This specific kind of ANN allows for the non-looping transfer of various system data from one node to another. MLPs learn to differentiate between safe and harmful actions based on structured data and find intrusions, anomalies, and infections.

2) Convolutional Neural Network (CNN)

CNNs are designed to handle data structures resembling grids, like images or sequences, by using linear filters to discern spatial and/or temporal relationships. CNNs are applied in the field of cyberattack attenuation, where network traffic is analyzed, features are extracted based on system logs, and malware patterns are identified that lead to the detection of threats in large data volumes.

3) Long-Short Term Memory (LSTM) and Gate Recurrent Unit (GRU)

LSTM and GRU are a specialized form of recurrent neural networks (RNN) that are capable of time-dependent sequential dependencies. They are commonly highly effective models for time series-based cyberattack detection issues like DDoS detection, ransomware spreading detection, and abnormal user behaviour detection [31]. LSTMs and GRUs do so by preserving some pertinent data of the past execution of the network and learning the time series of network traffic.

C. Applications of ML-DL in Cybersecurity Technologies

Deep learning has become a game changer in network cybersecurity, offering a more sophisticated way to detect and prevent threats. Deep Learning applications and techniques of DL that are seen in other technology sectors:

- **Anomaly Detection:** CNNs and RNNs are likely to be highly effective in identifying abnormal traffic sequences within the network that needs to be a cyber threat. Such types of DL models can compute volumes of data that are huge in real-time, early detection of potential attacks.
- **Malware Detection:** The behaviour and properties of malware can be learned using deep learning techniques to determine and categorize various types of malicious software. This helps identify new and emerging threats that would otherwise be missed by conventional signature methods.
- **Phishing Detection:** The deep learning classifiers and architectures that will be trained based on analyzing email content and structure will be able to remember phishing attacks with a high level of precision. It helps to prevent social engineering attacks that can be directed at individual persons and organizations.
- **Network Intrusion Detection:** The deep learning pattern and models can monitor network traffic and detect intrusions and attacks of unauthorized access. These models can be used to expand upon past data and establish patterns with respect to cyberattacks, enabling a timely response to eradicate threats.

V. Literature Review

This literature summary explores various cyberattack mitigation techniques, focusing on methodologies, key findings, challenges, and future directions in DDoS, spoofing, and ransomware detection, with an emphasis on ML and DL approaches.

Fernando, Komninos and Chen (2020) examine well-known academic papers that all demonstrate the use of DL or ML techniques for ransomware detection. As the IoT becomes more pervasive in both commercial and residential settings, they set out to test how the studies above fare as malware evolves. The purpose of this survey is to examine the literature on the topic of ransomware detection techniques that use ML and DL. The devastating effects of ransomware, the difficulty of recovering from an infection, and the critical importance of detection before infection are the primary reasons for this study [32].

P R and Paul (2020) The automated detection of such attacks has been greatly enhanced with the advent of intelligent systems, including techniques based on machine learning and deep learning. It is also possible to effectively classify data by utilizing machine learning based algorithms like SVMs or DT, or NB. Additionally, it is possible to design deep neural networks that can help recognise threats with the assistance of CNN or other algorithms. Detection techniques of the distributed denial of service attacks are well addressed in this

paper. An EDOS attack is used to take down a website or services by overwhelming the network with traffic [33].

El Houda, Hafid and Khoukhi (2019) The proposal of Co-IoT, which is a decentralized model of collaborative DDoS mitigation based on blockchain technology. It uses smart contracts to facilitate collaboration between SDN-based domains and decentralises information sharing of attack information. The Co-IoT implementation is currently operational in Ripstein, which is the official Ethereum test network. According to the experiment's results, Co-IoT is a practical way to minimise the effects of distributed denial of service (DDoS) attacks due to its versatility, effectiveness, security, and affordability. Nevertheless, Distributed Denial-of-Service (DDoS) attacks grow in popularity as the rate of unprotected devices on the Internet of Things (IoT) grows exponentially [34].

Steinberger et al. (2018) explored the applicability of current moving-target defence strategies to the context of giant cyberattacks on Internet Service Providers. Moreover, they also take the opportunity to utilize Software Defined Networks in a group to deploy shifting target defence methods. Their primary goal is to concentrate on ISPs collaborating with trusted partners. In their study, they found that Software Defined Networking and the moving-target defence can significantly limit the effects of a massive cyberattack. Furthermore, they prove that SDN is an appropriate approach to reduce the effects of massive cyberattacks by requiring the implementation of the moving target defence [35].

Bhunia and Gurusamy (2017) propose a secure IoT system based on SDN called SoftThings to detect malicious activity early and limit potential threats. Machine Learning provides the SDN controller with the ability to monitor and comprehend the patterns of the actions of the devices in the IoT as time goes by. The use of IoT is gaining momentum due to the spread of intelligent devices and the reduction in the cost of sensing units. There is a higher risk of assaults or compromises using these IoT devices, which could result in DoS and DDoS attacks. The large number of heterogeneous Internet of Things devices amplifies security risks. There is currently no standard in place to ensure the safety of IoT devices [36].

Al-Mohannadi et al. (2016) aim to identify the network's susceptibility and the adversary's actions and objectives by analysing several kinds of current attack modelling methodologies. Cyberattacks are sensitive topics in the field of Internet security. Companies and governments throughout the world are putting a lot of resources into data security. Competitors are attempting to penetrate security and inject harmful software like botnets, viruses, trojans, etc., in an effort to access critical data, while they are employing a variety of tools and strategies to keep the company functioning. The network and its precious data are at grave danger when dealing with a continuous attack, thus immediate action is required [37]. Table II provides a summary of key studies on cyberattack mitigation techniques, highlighting their focus areas, methodologies, major findings, challenges, and future directions, with applications spanning DDoS, spoofing, and ransomware.

Table I. Summary of A Study on Cyberattack Mitigation Techniques

Author	Approches	Datasets / Tools	Objectives	Key Findings	Limitations
Fernando, Komninos & Chen (2020)	Detecting malware with ML and DL	Various ransomware malware datasets (not specified)	To review ML/DL approaches for ransomware detection and analyze impact of malware evolution, especially with IoT growth	ML/DL methods are promising for ransomware detection; early detection is critical due to destructive nature	Lack of standardized datasets; ransomware evolution reduces detection accuracy over time
P R & Paul (2020)	ML (SVM, Decision Trees, NB) & DL (CNN)	DDoS traffic datasets (not specified)	To review and discuss ML (SVM, DT, NB) and DL (CNN, DNN) methods for detecting DDoS	ML/DL methods improve automatic detection of DDoS with higher efficiency	Scalability issues; real-world deployment challenges; lack of universal benchmark dataset
El Houda, Hafid & Khoukhi (2019)	Blockchain-based Co-IoT with SDN	Ethereum (Ropsten testnet), SDN domains	To propose Co-IoT, an architecture for pooled DDoS defence that utilises blockchain and SDN,	As a result of Co-IoT, large-scale DDoS mitigation became more cost-effective, secure, and flexible.	Dependent on blockchain scalability; high IoT device growth increases vulnerability
Steinberger et al. (2018)	Using SDN for Moving Target Defence (MTD)	ISP network simulations	To evaluate MTD strategies against large-scale cyber-attacks in ISP environments	MTD with SDN reduces impact of cyber-attacks; ISP collaboration improves resilience	Implementation complexity; performance trade-offs in large-scale networks
Bhunia & Gurusamy (2017)	SDN-based IoT security (SoftThings) + ML	IoT device behavioural data	Presently, SoftThings proposes an SDN-based architecture for IoT anomaly detection.	ML at SDN controller detects abnormal IoT behaviours early; mitigates DoS/DDoS	No protocol ensures IoT security universally; heterogeneous devices increase risk
Al-Mohannadi et al. (2016)	Methods for creating attack models	Survey of attack modelling techniques	To analyze attack modelling approaches and understand adversary goals	Highlights strengths/weaknesses of existing attack models; stresses need for proactive defence	Lack of unified modelling standard; limited real-world applicability

VI. Conclusion and Future Work

Cyberattack mitigation involves the deployment of strategies, techniques, and mechanisms designed to prevent, detect, and reduce the impact of malicious activities aimed at compromising computer systems, networks, and data. The objective of mitigation is not only to block or neutralize ongoing threats but also to ensure the continuity of business operations, minimize downtime, and safeguard sensitive information from theft or misuse. Cyberattacks like DDoS attacks, spoofing, and ransomware are growing in frequency and complexity as digital technology continues to expand at a rapid pace, putting organizations in a continuously changing danger scenario. Conventional mitigation solutions, including signature-based and rule-based detection systems, remain effective in identifying known threats based on predefined patterns and traffic characteristics. ML and DL solutions have proven to be extremely promising in enhancing cyber defence through automated anomaly detection, malware classification, phishing prevention, and network intrusion monitoring. These models are effective alternatives to traditional defences, as they are highly responsive and offer a high degree of flexibility and detection, resulting in a high level of accuracy.

Future research should focus on developing hybrid ML-DL models that are efficient and interpretable, thereby enhancing the trust and transparency of cybersecurity systems. The exploration of lightweight architectures on real-time detection on resource-constrained IoT devices is a response to the advent of smart environments that is needed. Adversarial robustness should also be given attention, as attackers are increasingly taking advantage of ML/DL vulnerabilities. Blockchain can be used to further advance cyber defences, which securely share data, utilise hierarchical learning to train privacy-aware models, and employ explainable AI, thereby enabling a deeper understanding of the decisions.

References

1. M. S. Hoque, M. A. Mukit, and M. A. N. Bikas, "An Implementation of Intrusion Detection System Using Genetic Algorithm," *Int. J. Netw. Secur. Its Appl.*, vol. 4, no. 2, pp. 109–120, Mar. 2012, doi: 10.5121/ijnsa.2012.4208.\
2. S. Prabhu and S. Bhat, "Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic – A Review of Literature," *Int. J. Case Stud. Business, IT, Educ.*, 2020, doi: 10.47992/ijcsbe.2581.6942.0078.
3. A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," *Procedia Econ. Financ.*, vol. 28, no. April, pp. 24–31, 2015, doi: 10.1016/s2212-5671(15)01077-1.
4. D. Baldev Singh, D. S.N. Panda, and D. Gurpinder Singh Samra, "Slow flooding attack detection in cloud using change point detection approach," *Int. J. Eng. Technol.*, vol. 7, no. 2.30, p. 33, May 2018, doi: 10.14419/ijet.v7i2.30.13459.
5. A. Vaidya, S. Jaiswal, and M. Motghare, "A review paper on spoofing detection methods in wireless LAN," in *Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016*, 2016. doi: 10.1109/ISCO.2016.7727054.\
6. J.-W. Seo and S. Lee, "A study on the detection of DDoS attack using the IP Spoofing," *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 25, pp. 147–153, 2015, doi: 10.13089/JKIISC.2015.25.1.147.
7. R. Singh, K. Thakur, G. Singh, and S. Gupta, "Prevention of IP spoofing attack in cyber using artificial bee colony and artificial neural network," in *ACM International Conference Proceeding Series*, 2019. doi: 10.1145/3339311.3339327.
8. X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention," *Inf. Syst. Secur.*, 2007, doi: 10.1080/10658980701576412.
9. S. Poudyal and D. Dasgupta, "AI-Powered Ransomware Detection Framework," in *2020 IEEE Symposium Series on Computational Intelligence, SSCI 2020*, 2020. doi: 10.1109/SSCI47803.2020.9308387.\
10. B. M. Khammas, "Ransomware Detection using Random Forest Technique," *ICT Express*, vol. 6, no. 4, pp. 325–331, Dec. 2020, doi: 10.1016/j.icte.2020.11.001.
11. J. Alsamiri and A. Khalid, "Internet of things cyber attacks detection using machine learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, p. 627, 2019, doi: 10.14569/ijacsa.2019.0101280.
12. Y. N. Imamverdiyev and F. J. Abdullayeva, "Deep learning in cybersecurity: Challenges and approaches," *Int. J. Cyber Warf. Terror.*, vol. 10, no. 2, pp. 82–105, 2020, doi: 10.4018/IJCWT.2020040105.
13. J. M. Biju, N. Gopal, and A. J. Prakash, "Cyber Attacks And Its Different Types Related Papers Cyber Attacks And Its Different Types," *Int. Res. J. Eng. Technol.*, vol. 6, no. 3, 2019.
14. J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Comput. Sci. Rev.*, vol. 37, p. 100279, Aug. 2020, doi: 10.1016/j.cosrev.2020.100279.
15. R. Babu, L. Bhaskari, and CH.Satyanarayana, "A Comprehensive Analysis of Spoofing," *Int. J. Adv. Comput. Sci. Appl.*, vol. 1, no. 6, 2010, doi: 10.14569/IJACSA.2010.010623.
16. P. Pathak, A. Shrivastava, and S. Gupta, "A Survey on Various Security Issues in Delay Tolerant Networks," *J. Adv. Shell Program.*, vol. 2, no. 2, pp. 12–18, 2015.
17. D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection," 2016.
18. J. A. Herrera Silva, L. I. Barona López, Á. L. Valdivieso Caraguay, and M. Hernández-Álvarez, "A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters," *Remote Sens.*, vol. 11, no. 10, p. 1168, May 2019, doi: 10.3390/rs11101168.
19. S. Prabhu and S. Bhat, "Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic – A Review of Literature," *Int. J. Case Stud. Business, IT, Educ.*, vol. 4, no. 2, pp. 40–64, Dec. 2020, doi: 10.47992/IJCSBE.2581.6942.0078.
20. D. D. Rao, "Multimedia Based Intelligent Content Networking for Future Internet," in *2009 Third UKSim European Symposium on Computer Modeling and Simulation*, 2009, pp. 55–59. doi: 10.1109/EMS.2009.108.
21. J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, "Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach," *Sensors*, vol. 20, no. 3, p. 816, Feb. 2020, doi: 10.3390/s20030816.

22. A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "Hybrid Intrusion Detection System Based on the Stacking Ensemble of C5 Decision Tree Classifier and One Class Support Vector Machine," *Electronics*, vol. 9, no. 1, p. 173, Jan. 2020, doi: 10.3390/electronics9010173.
23. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, 2019, doi: 10.1186/s42400-019-0038-7.
24. S. Gupta and A. Mathur, "Enhanced Flooding Scheme for AODV Routing Protocol in Mobile Ad Hoc Networks," in *2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies*, IEEE, Jan. 2014, pp. 316–321. doi: 10.1109/ICESC.2014.60.
25. R. Basnet, A. H. Sung, and Q. Liu, "Rule-Based Phishing Attack Detection," 2012.
26. A. S. Choudhary, P. P. Choudhary, and S. Salve, "A Study on Various Cyber Attacks and A Proposed Intelligent System for Monitoring Such Attacks," in *Proceedings of the 3rd International Conference on Inventive Computation Technologies, ICICT 2018*, 2018. doi: 10.1109/ICICT43934.2018.9034445.
27. M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science (80-.).*, vol. 349, no. 6245, pp. 255–260, 2015, doi: 10.1126/science.aaa8415.
28. A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.
29. T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016, pp. 785–794. doi: 10.1145/2939672.2939785.
30. G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the Effectiveness of Machine and Deep Learning for Cyber Security," *Int. Conf. Cyber Conflic*, vol. 28, no. 4, pp. 2861–2879, 2018, doi: 10.1007/s11831-020-09478-2.
31. Bandaru, S. R., Shyam, D., Manoharan, P., Syed, M. H., Ragireddy, U. K., & Addepalli, P. V. (2022). A Review of Frameworks, and Impact on the Software Development Life Cycle with Artificial Intelligence in Software Engineering. *American International Journal of Computer Science and Technology*, *4*(1), 44-53.
32. Manoharan, P., Syed, M. H., Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., & Shyam, D. (2022). Understanding the Use of Agile Development Practices Alongside Quantum Computing in Modern Engineering Projects. *International Journal of Emerging Research in Engineering and Technology*, *3*(1), 136-143
33. Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., Shyam, D., Manoharan, P., & Syed, M. H. (2022). Intelligent Predictive System of Cloud Resource Utilization Forecasting with Advanced Deep Learning. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 143-151.
34. Syed, M. H., Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., Shyam, D., & Manoharan, P. (2022). A Survey of Statistical Process Control and Its Applications in Manufacturing Quality Assurance. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(1), 127-135.
35. Addepalli, P. V., Bandaru, S. R., Shyam, D., Manoharan, P., Syed, M. H., & Ragireddy, U. K. (2022). Survey on Blockchain Integration with Sap S/4hana for Transparent and Secure Supply Chains. *International Journal of AI, BigData, Computational and Management Studies*, *3*(1), 161-170.
36. Mylavarapu, K. B., Pilli, J., Jannu, P. K., Mohammad, J. A., & Panchali, S. H. (2022). Comparative Performance of Machine Learning Techniques for Sentiment and Insight Analysis in Amazon Product Reviews. *American International Journal of Computer Science and Technology*, *4*(1), 54-64.
37. Mohammad, J. A., Panchali, S. H., Mylavarapu, K. B., Pilli, J., & Jannu, P. K. (2022). An Ensemble Machine Learning Approach for Reliable Fake News Detection on Social Media Platforms. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 152-161.
38. Pilli, J., Jannu, P. K., Mohammad, J. A., Panchali, S. H., & Mylavarapu, K. B. (2022). Review of Supply Chain–Integrated CRM Systems for Business Agility. *International Journal of Emerging Research in Engineering and Technology*, *3*(1), 155-163.
39. Panchali, S. H., Mylavarapu, K. B., Pilli, J., Jannu, P. K., & Mohammad, J. A. (2022). Predictive Maintenance in Smart Manufacturing: A Review of Machine Learning and Digital Twin Approaches. *International Journal of AI, BigData, Computational and Management Studies*, *3*(1), 150-160.
40. Jannu, P. K., Mohammad, J. A., Panchali, S. H., Mylavarapu, K. B., & Pilli, J. (2022). Heat Dissipation Strategies for High-Performance Computing: A Review of Air and Liquid Cooling Efficiency. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(1), 145-153.
41. Taluri, R. (2022). Cloud Data Engineering Strategies for Large-Scale Financial Data Integration and Intelligent Corporate Performance Reporting. International Journal of Emerging Research in Engineering and Technology, 3(4), 176-188. https://doi.org/10.63282/3050-922X.IJERET-V3I4P119
42. Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., Dasari, A., Chilakapati, V. K., & Keshireddy, S. R. (2022). Machine Learning-Driven Threat Analysis for Enhancing Security in Data Center Networking. *American International Journal of Computer Science and Technology*, *4*(1), 65-76.
43. Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., Dasari, A., & Chilakapati, V. K. (2022). Towards Secure and Reliable IoT: A Review on Anomaly Detection and Predictive Analytics in Sensor Networks. *International Journal of AI, BigData, Computational and Management Studies*, *3*(1), 140-149.

44. Pathani, A. K., Dasari, A., Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., & Kavuluri, H. V. R. (2022). Effective Monitoring of Sensor-Actuator Integration Methods for Real-Time Controlling in Smart Device Networks. *International Journal of Emerging Research in Engineering and Technology*, *3*(1), 144-154.
45. Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., & Dasari, A. (2022). Review on Network Virtualization and SDN in Industrial IoT (IIoT). *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 162-172.
46. Dasari, S., Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., & Pathani, A. K. (2022). Networking Paradigms for Large-Scale IoT Deployments: A Survey on Reliability, Latency, and Scalability. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(1), 136-144.
47. Taluri, R. (2021). Cloud-Native Architectures for Enterprise Financial Data Management, Analytics, and Regulatory Reporting Compliance. International Journal of Emerging Trends in Computer Science and Information Technology, 2(2), 101-111. https://doi.org/10.63282/3050-9246.IJETCSIT-V2I2P112
48. K. Cho *et al.*, "Learning Phrase Representations using RNN Encoder–Decoder for Statistical Machine Translation," in *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2014, pp. 1724–1734. doi: 10.3115/v1/D14-1179.
49. D. W. Fernando, N. Komninos, and T. Chen, "A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques," *IoT*, vol. 1, no. 2, pp. 551–604, Dec. 2020, doi: 10.3390/iot1020030.
50. V. P R and G. Paul, "A Survey on DDoS Attack Detection Methods Employing Intelligent Techniques," *Int. J. Comput. Trends Technol.*, vol. 68, no. 11, pp. 83–85, Nov. 2020, doi: 10.14445/22312803/IJCTT-V68I11P113.
51. Z. A. El Houda, A. Hafid, and L. Khoukhi, "Co-IoT: A Collaborative DDoS Mitigation Scheme in IoT Environment Based on Blockchain Using SDN," in *2019 IEEE Global Communications Conference (GLOBECOM)*, IEEE, Dec. 2019, pp. 1–6. doi: 10.1109/GLOBECOM38437.2019.9013542.
52. J. Steinberger *et al.*, "DDoS defense using MTD and SDN," in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, IEEE, Apr. 2018, pp. 1–9. doi: 10.1109/NOMS.2018.8406221.
53. S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in IoT using SDN," in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, IEEE, Nov. 2017, pp. 1–6. doi: 10.1109/ATNAC.2017.8215418.
54. H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, "Cyber-Attack Modeling Analysis Techniques: An Overview," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, IEEE, Aug. 2016, pp. 69–76. doi: 10.1109/W-FiCloud.2016.29.

Copyright: © 2023 *Pradeep Rao V. This Open Access Article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.*