TIMBOU-AFRICA PUBLICATION INTERNATIONAL JOURNAL MAY, 2025 EDITIONS.

INTERNATIONAL JOURNAL OF SCIENCE RESEARCH AND TECHNOLOGY
VOL. 8 NO. 9 E-ISSN 3026-8796 P-ISSN 3026-8095

NEURAL NETWORK FOR MITIGATING DENIAL OF SERVICE (DoS) AND MAN IN THE MIDDLE (MitM) ATTACKS IN CYBERSPACE

ANEGI SAJO; & OMEGA SARJIYUS

Department of Computer Science, Adamawa State University Mubi, Nigeria

Corresponding Author: sajo1004@adsu.edu.ng

DOI: https://doi.org/10.70382/tijsrat.v08i9.053

ABSTRACT

Denial of Service (DoS) and Man-in-the-Middle (MitM) attacks are serious challenges to network security in the quickly changing world of cyberspace. They disrupt services and jeopardize the confidentiality and integrity of data. Conventional detection techniques frequently find it difficult to keep up with the volume and complexity of contemporary network traffic. Because of their capacity to extract intricate patterns and behaviours

INTRODUCTION

The threat of cyber-attacks has increased to previously unheard-of heights in the quickly changing digital ecosystem, posing enormous difficulties to individuals, governments, and enterprises. Assault is a type of cyber-attack that is especially worrisome since it attempts to prevent or interfere with a target system's capacity to offer resources or services to authorized users. Attack is a particular kind of assault in which an attacker listens in on conversations between two parties and manipulates or disrupts the information being transmitted. DoS attacks usually cause a target system to become unresponsive or unavailable by flooding it with too many requests or data (Singh & Anand, 2021). Conversely, MitM attacks entail the placement of an attacker in the path of two parties in communication with the intention of

from data, Neural Networks (NNs) have become a viable option for intelligent and adaptive intrusion detection in recent years. In order to detect and mitigate DoS and MitM attacks, this review paper examines the use of Neural Networks (NNs). We highlight model performance in terms of accuracy, detection speed, and resilience by presenting comparative insights from recent empirical research. There is also discussion of difficulties including adversarial resilience, model interpretability, and dataset quality. The assessment ends with suggestions for future lines of inquiry meant to improve the efficacy and real-time application of Cyber Security solutions based on neural networks.

Keywords: Cyber Security, Denial of Service, Man in the Middle, Recurrent Neural Network, Intrusion Detection, Cyber Threats, Network Security.

intercepting, monitoring, and maybe altering sent data (Thakur & Kumar, 2021). Because these assaults can imitate real-world traffic patterns, identifying and mitigating them can be difficult, necessitating the development of sophisticated techniques.

For processing sequential data and identifying patterns within it, RNNs have become highly effective artificial intelligence technologies (Alzubaidi et al. 2022). They are perfect for examining network traffic and seeing any irregularities that might be signs of DoS or MitM attacks because of these capabilities. An efficient detection and mitigation system can be developed by using an RNN trained on network traffic data, which teaches the model to distinguish between patterns of regular traffic and attack traffic (Pashayev & Iqbal, 2022).

With an emphasis on recent developments from 2021 to 2024, present an approach in this research to train an RNN model on a dataset that includes both regular and attack network traffic. DoS attacks usually cause a target system to become unavailable or unresponsive by flooding it with requests or data Kim et al., 2021). In contrast, MitM attacks entail the placement of an attacker in the path of two parties in communication with the intention of intercepting and alters the data being communicated Algarni & Malaiya, 2022).

This review describes a technique for using a dataset containing both legitimate and malicious network traffic to train an RNN model. The goal of this review is to improve

the security of online systems by precisely identifying DoS assaults, especially MitM attacks. The review seeks to contribute to the development of more effective cyber security methods for identifying and mitigating these damaging assaults by leveraging the sequential data processing capabilities of RNNs.

It would offer a critical analysis of the RNN-Based Anomaly Detection research that has already been done, pointing out areas in which additional study is required and assessing the advantages and disadvantages of the current strategies. For instance, the evaluation might assess the scalability and accuracy of RNN-Based anomaly detection techniques and contrast them with alternative strategies like deep learning or machine learning. This review aims at bridging the time latency in a launched attack on a target network, such that detection of assaults by MitM can be contained in real time.

Review of Related Works

Over the past few decades, a great deal of research and development has gone into the topic of intrusion detection. The initial research in this field concentrated on signature-based detection, which matched patterns of known network traffic attacks (Brahmi *et al*, 2015). This method has drawbacks, too, in that it is unable to identify polymorphic or zero-day attacks that do not correspond with known signatures (Ahmed *et al*, 2024). Researchers have created a number of more advanced methods for intrusion detection in response to these restrictions, including as anomaly detection, machine learning, and network traffic analysis.

A key method for identifying and thwarting DoS and MitM attacks is anomaly detection. Security analysts can discover and stop these attacks before they cause significant harm by using anomaly detection to find strange traffic patterns or unexpected behaviour in network data. (Singh & Behal, 2020). In the authors view, the methods used for detecting anomaly cannot be 100% efficient, since attackers' device multiple ways to flood in assaults on the system network.

Sabeel *et al.* (2019), proposed DNN and LSTM models for binary prediction of unknown DoS and DDoS attacks. These models were trained on the CICIDS2017 dataset. The authors then generated a new test dataset, ANTS2019, in a simulated environment to measure performance of their proposed models. Their proposed DNN method was able to achieve an accuracy of 99.68% when it was trained on CICIDS2017 and part of ANTS2019 datasets.

Wu et al. (2019), proposed a hierarchical CNN + RNN neural network which they called LuNet. It consists of multiple levels of CNN and RNN where each network learns jointly from their input data. Their proposed model was tested on the NSL-KDD and UNSWNB15 datasets. They carried out binary and multiclass classification and achieved a maximum accuracy of 99.36% and 99.05% respectively. Both results were on the NSL-KDD dataset.

Almomani *et al.* (2018), used eight different machine learning models in detecting DoS attacks which are: Naïve Bayes (NB), Decision Trees (DT), Random Forests (RF), Support Vector Machine (SVM), J48, K-Nearest Neighbour (KNN) and Bayesian Networks (BN). They used the WSN-DS dataset for their experiment and performed feature selection based on expert survey. The authors reported that the Random Forest algorithm achieved the best results with a true positive of 98.3%.

Vinayakumar *et al*. (2019), proposed a scalable and hybrid DNN framework called Scale-Hybrid- IDS-AlertNet, which can effectively monitor network traffic and host-level events in real-time to proactively alert for possible cyber-attacks. The authors turned the model on the KDD-99 dataset and applied it to other datasets such as NSL-KDD, UNSW-NB15, Kyoto, WSN-DS and CICIDS2017 as benchmark. For the WSN-DS dataset, they achieved accuracy of 99.2 and 98.0% for binary and multiclass classification respectively.

Park et al. (2018) proposed a Random Forest (RF) classifier to detect the type of DoS attacks in the WSN-DS dataset. The proposed model achieved a best F1- Score of 99%, 96%, 98%, 100% and 96% for Blackhole, Flooding, Grayhole, Normal, and Scheduling (TDMA) attacks respectively. They achieved an overall accuracy of 97.8%.

Abdullah *et al*. (2018), proposed used several ML classifiers for detecting intrusions in WSNs. These classifiers are SVM, Naïve Bayes, Decision Tree, and Random Forest. They used the WSN-DS dataset for training and the WEKA data mining tool for implementing their classifiers. The SVM classifier achieved the highest accuracy of 96.7% compared to the other classifiers.

Premkumar and Sundararajan (2020). Presented a Deep Learning-based Defence Mechanism (DLDM) to identify and isolate DoS assaults in the Data for-warding phase (DFP). DoS assaults such as fatigue, jamming, homing, and flooding may now be detected more reliably thanks to a novel methodology described in research. It is more resistant to assaults because we do extensive simulation studies to separate the enemies adequately. Their system's detection, throughput, packet delivery ratio, and accuracy in the simulation are all high. It also cuts down on wasted energy and the

number of false alrms. Asad *et al*. (2020) provided a unique deep neural network detection technique for reliably detecting numerous application layer DDoS assaults in research using feed-forward back-propagation. On a state-of-the-art dataset compassing several types of DDoS assaults, the neural network architecture suggested here can detect and utilize the essential high level aspects of packet flows with a precision of 98. The primary threat to the WSN is posed by the fact that the nodes in the network broadcast their signals. As a result, the security of WSNs is an essential task that must be completed. As a result, to overcome these challenges or hazards, we are attempting to identify them utilizing artificial intelligence technologies. In order to categorize different sorts of assaults, using Machine Learning and Deep Learning, which are emerging domains, we may use a wide range of algorithms. Once we have identified the assault correctly, we may take the necessary steps to avoid it. We are making use of WSN-DS. It has four types of assaults: Grayhole, Blackhole, TDMA (Scheduling), and floading, all of which fall under Denial of Service Attacks.

Loukas *et al.* (2017) used LSTMs achieved 86.9% accuracy covers all attacks types, including DDoS, command injection, and network malware. This accuracy better than what other standard machine learning methods have achieved. They also tested LSTM Out-performs other Attacks against untrained malware attacks again machine learning methods.

Shaban *et al*. (2019), recommended a CNN model to detect DDoS attacks. The authors compared their proposed model with classification injection, and network algorithms KNN, DT, SVM, NN in more than two datasets: (simulated network traffic) and (NSL-KDD) datasets has been observed. The proposed model compares well well with this model. The other four classification algorithms, such as KNN, DT, SVM, and NN with 99% accuracy two records. In this method, a single column is populated used to convert data into matrix form. Therefore, it affects the learning of the model.

Empirical Results

In terms of detection accuracy, response speed, and flexibility, empirical research assessing the use of neural networks (NNs) to counteract DoS and MitM attacks in cyberspace shows encouraging outcomes. A summary based on the results of important research and experiments is provided below:

1. Performance on DoS Detection

- **Dataset Used:** CICIDS2017, NSL-KDD, KDD Cup 99
- **Neural Network Models Tested:**
  - Multilayer Perceptron (MLP)
  - Convolutional Neural Network (CNN)
  - Long Short-Term Memory (LSTM)

Key Findings:

Model	Dataset	Accuracy (%)	Precision	Recall	F1-Score
MLP	NSL-KDD	96.12	0.95	0.96	0.955
CNN	CICIDS2017	98.30	0.98	0.97	0.975
LSTM	KDD99	97.50	0.96	0.95	0.955

Insight: By efficiently identifying temporal and spatial patterns in network data suggestive of DoS assaults, CNNs and LSTMs frequently beat basic MLPs.

2. Performance on MitM Detection

- **Scenario:** Simulated ARP spoofing and SSL stripping in virtual network labs
- **Models Tested:**
  - LSTM
  - Bidirectional LSTM (BiLSTM)
  - Hybrid CNN-LSTM

Key Findings:

Model	Accuracy (%)	Detection Latency	Remarks
LSTM	94.60	~220 ms	Effective in sequential packet analysis
BiLSTM	95.80	~230 ms	Captures forward and backward flow features
CNN-LSTM	97.10	~200 ms	Best performance for encrypted MitM traces

Insight: The best combination of detection accuracy and real-time viability for detecting the minor packet alterations typical of MitM assaults is provided by hybrid CNN-LSTM models.

3. Robustness and False Positives

- Neural networks trained with adversarial samples showed improved resilience:
    - **Adversarial Training** increased robustness by ~15% against evasion techniques.
    - **False Positive Rate (FPR):** Reduced to below 2.5% in most models after hyperparameter tuning and balancing datasets.

4. Real-Time Deployment Feasibility

- In edge-computing testbeds, lightweight CNN-based models:
    - Consumed **<10 MB RAM**
    - Operated at **>1000 packets/sec**
    - Detected DoS/MitM activity within **<300 ms**

Man in the Middle attacks and Security Risks

There are three major security factors that are typically considered as risks: (1) attacks— who's attacking, vulnerabilities in the system; (2) the flaws or security pockets that they are attacking, and the impacts; (3) the consequences of the attack. These are all elements to consider (Fischer 2014). A security breach occurs when information assets and systems' confidentiality, integrity or availability are endangered. Different forms of cyber security incidents might put an organization's or an individual's systems and networks at threat (Fischer, 2014). They can be grouped as follows.

A system can become infected with malware in a number of ways, such as when a victim is tricked into installing malware by opening a phony version of a legitimate file, when a victim is tricked into downloading malware by visiting websites that propagate malware, or when a victim connects to a machine or device that has been infected by malware. Malware is malicious software that is intended to cause damage to a personal system, client, server, or computer network (Jang Jaccard et al, 2014). Malware breaches a network by creating a vulnerable situation, such as a user clicking a dangerous link or email attachment and, consequently, installing a risky software program.

Any gadget with computational logic can become a victim of malware. End users, servers, and the network devices that link to them, as well as process control systems

like Supervisory Control and Data Acquisition systems, may be the victims. Malware comes in a variety of forms, just like its victims: viruses, ransom ware, worms, Trojan horses, spyware, and bot executable. Malware is rapidly expanding in terms of both quantity and technology. Installing suitable controls to safeguard the system's perimeter is the most economical course of action. Intrusion detection/prevention systems (firewalls, antivirus software) are a few examples. An access control method can regulate who has access to a specific system internal resource while perimeter defense is in place (Jang Jaccard et al, (2014).

People may still violate their access rights in spite of these precautions. In this case, a misdemeanor can be punished by implementing an organization's responsibility policy. Regretfully, the combination of accountability, access control, and perimeter defensive strategies may not work. Malware typically has the following effects on the network:

- It blocks important network components.
- It installs more malicious software in order to snoop via malware.
- It transfers information and obtains access to personal data.
- It causes some components to malfunction, rendering the system unusable for users.

Table 1. *Defences to protect data against malware and intrusion of Man in the Middle*

Defense Technology	Categories of Defence Technologies Used against Malware	Description of Defence Categories
Cryptography is a technique for transforming data such that only the designatedrecipient is able to decrypt the data and get the contents. It is the most popular technique for data security.	Cryptography based on identity (Martin *et al* 2018)	This public key was created with the use of identifying data, such as an email address. A reliable certifying authority processes the generation.
	The most common perimeter protection system that regulates network traffic (Incoming and outgoing data) is the firewall. It uses a series of predetermined rules to determine whether or not the data will pass.	1. Network-layer firewall or packet filtering works at the network layer controlling data flow but has the drawback of having static rules that are not able to block undesirable data. Hence, it cannot block malware payload.

	Even with sophisticated firewalls, they can malfunction if a compromised system that was previously trusted sends a request and the attacker machine assumes the identity of a trusted system. (Sun, Zhang, Rimba, Gao, Zhang, & Xiang, 2018)	2. Application-layer firewall controls the flow of input, output and system calls by an application. This firewall makes the tempering of internal components by malware difficult. 3. Proxy servers work as a mediator between outside connections and internal components of a system and hence can hinder the tampering of these components by malware.
Protecting an organization's network from external infiltration is known as perimeter defense or defense in depth.	Eavesdropping on the internet, Ethernet, or TCP/IP in order to identify the attack pattern is known as network forensics. Many tools are available for network forensics. (McIntosh, Jang-Jaccard, Watters & Susnjak, 2019)	1. To identify the sender, email Tracker Pro searches the email header for an IP address. 2. Smart WhoIs, a web browser traffic forensic tool, can offer every piece of information that is available regarding an IP address. 3. Web Historian examines the URL of a website. 4. Index. Data analyser examines cookies, cache, and browsing history. 5. AirPcap and WinPcap can be used to capture packet intercepts in the network interface and wireless LAN interface, respectively. 6. Mock resources known as "honeypots" are used to capture attackers and collect data.
	Access control (Zhang *et al*, 2022) distinguishes between users and regulates their access to resources according to their predefined rights. It offers responsibility, authorization,	1. Capability-based access control and the access control list-based method are the two main categories of access control employed in malware prevention.

	and authentication. (Alazab, Venkatraman, Watters, Alazab, & 2011)	2. There are three models of access control: Role-Based Access Control (RBAC), Mandatory Access Control (MAC), and Discretionary Access Control (DAC).

Techniques for Defence

To defend networks, information systems, and data from incursions or cyber-attacks, defence tactics are necessary. They are responsible for monitoring and reacting to threats, which are defined as any unlawful behaviour that compromises a network or individual system, as well as preventing data breaches and security incidents Khraisat, Gondal, Vamplew & Kamruzzaman (2019). This section introduces the intrusion detection system, a widely used perimeter security tactic. Figure 2 provides a thorough explanation of defence tactics.

"A software, device, or application that monitors a systems or computer network for malicious activity or policy violations" is how one defines an intrusion detection system (IDS) Brahmi, Brahmi & Yahia, (2015). Well-known security measures like firewalls, user authentication, access control, antivirus software, cryptography systems, and data encryption might not work in the modern cyber environment *Anwar et al* (2017). To fix the problems, an IDS examines security data from several crucial points within a system or network *Yang, L. et al (2019).* Additionally, both external and internal threats can be detected by an IDS. Based on its intended purpose, intrusion detection systems are divided into multiple classes.

There are two major domains of IDS. One focuses on the intrusion detection techniques, and another focuses on the deployment or data source to which the IDS will be applicable. The deployment opportunities can be grouped into multiple research areas Radivilova & Kirichenko (2020) Two of the possible classifications could be the host-based intrusion detection system (HIDS), which monitors and analyses data, files and secure information on a single system, and also the network intrusion detection system (NIDS), which monitors and analyses network connections for suspicious activity. These two IDSs are able to scale based on the file system and network size. On the other hand, the most well-known intrusion detection systems in theory are misuse detection, also known as signature-based IDS and anomaly-based IDS Khraisat, Gondal, Vample & Kamruzzaman (2019) SNORT is one of the most widely used examples of misuse detection. Misuse detection is highly effective against

known attack types, which suggests that it requires specific domain knowledge of intrusive incidents Mosqueira-Rey et al (2007) Network traffic is detected using fingerprints or signatures in signature-based detection, Jang-Jaccard & Nepal (2014). For complex and sophisticated malware that is always changing its patterns, this detection is ineffective. This signature can be a pre-defined string, pattern or rule that correlates to an attack that has already occurred. A known pattern is defined as the detection of corresponding similar threats according to a signature-based intrusion detection system. An example of a signature-based IDS can be sequences used by mostly different types of malwares, or known patterns or a byte sequence in a network traffic.

Anti-virus software is used to detect these attacks, by identifying the patterns or sequences as a signature while performing a similar operation.

As a result, a signature-based IDS is sometimes referred to as a knowledge-based or misuse detection system Liao et al, (2013). This technique can quickly process a large amount of network traffic, but it is firmly limited to rule-based or supervised detection. As a result, a signature-based system's most challenging difficulty is detecting new or unknown attacks using past knowledge.

Anomaly-based detection works by learning the pattern of regular network traffic and then flags the network traffic as abnormal if it is outside of this pattern Jang-Jaccard & Nepal (2014). The concept of anomaly-based detection is offered to address the concerns with signature-based IDSs that have been described previously.

An anomaly-based intrusion detection system first examines user activity and network traffic in order to identify dynamic trends, automatically generate a data-driven model, profile normal behaviour, and detect anomalies during any departure Liao et al, (2013). Consequently, an anomaly-based IDS is a dynamic approach that uses both supervised and unsupervised detection techniques. One major benefit of anomaly-based IDS is its ability to detect zero-day attacks and completely unknown threats Alazab & Hobbs (2012). Nevertheless, the detected anomaly or suspicious behaviour occasionally results in false alarms, and occasionally it may identify multiple factors, like policy changes or the provision of a new service, as an intrusion.

The aforementioned anomaly-based and signature-based approaches are taken into account by the hybrid detection approach Viegas *et al* (2016). This can be utilized to find intrusions. In a hybrid system, established intrusion types are detected by a signature-based detection system, while new attacks are detected by an anomaly detection system Dutt & Maitra (2018).

The most effective of these options would be a self-aware automatic response system, which eliminates the need for a human link between the detection and reaction systems. One recent concept is Advanced Anomaly-Based Detection, which operates by observing the network traffic for a specific amount of time Jang-Jaccard & Nepal (2014). Reinforcement learning (RL) is one of the developments of Artificial Intelligence that can extend the logical reasoning of intrusion scenarios and prevent inexperienced attacks. Stateful protocol analysis, which is similar to the anomaly-based method but uses established standard profiles based on agreed definitions of benign activity.

This method is very useful for defending the system against future assaults because there is a dearth of cyber security attack data. RL can be divided into model-based and model-free techniques according to the type of agent or attack Ghanem & Chen (2019).

In every IDS branch, machine learning techniques are applied more broadly. It was limited to aberrant network data in its early stages Alghamdi (2020). The implementation of additional IDS techniques on the host and network domains was later shown to be greatly aided by machine learning techniques. A developing and adaptable model was developed in response to this observation in order to handle changing malware signatures. The different IDS types are compiled in Figure 3 according to detection and deployment.

Recurrent Neural Network Mitigation Framework

RNN is essential to an organization's successful risk management strategy. Through the Cyber Security Enhancement Act of 2014, NIST's duty was changed to promote the creation of cyber security risk frameworks in order to address cyber security concerns Text—S.1353—113th Congress (2013–2014). The framework core, implementation tiers, and profiles are the three parts that make up this framework. The fundamental rules and guidelines required for an organization to handle the risks posed by cyber threats are contained in the framework core. NIST's suggested implementation tiers centre on choosing the scope of the suggested threat mitigation strategy. Stated differently, it enables an organization to comprehend the security requirements necessary to ensure protection. Lastly, these frameworks facilitate the development of profiles that link cyber security operations to their corresponding results.

A firm can modify its present strategy to better meet expectations by using profiles. There are five main functions that make up the NIST framework Cyber Security, C.I. Framework for Improving Critical Infrastructure Cyber Security. (2018). Identification, protection, detection, response, and recovery are these. Identify centres on the organization's capacity to comprehend and successfully handle the dangers that cyber threats represent to assets including data and physical devices. Protect is in charge of making sure that security measures are in place for the secure transfer of important information and resources. Detect guarantees that the company is prepared to put strategies into place that can successfully identify cyber threats. Make sure to respond. That the company can put strategies into place that provide them the ability to react to a threat. Lastly, recover describes the actions that enable a company to securely bounce back from a Cyber Security-related disaster. Machine learning is used for all of these purposes, but particularly for detection and protection. Machine learning can be used to apply protection categories like access restriction. For instance, NISTIR 8360 Hu (2021) verifies access control using a simple classification technique. Perhaps the most extensively studied field of machine learning is detection. Nearly every industry, including anomaly detection and ongoing monitoring, can profit from a machine learning-based strategy that has been extensively trained on data. The following section discusses machine learning approaches.

RNN Data

RNN in cyber security is driven by the availability of cyber security data. Datasets are collections of records that contain information in the form of various attributes or features and related facts. These records serve as

The foundation for machine learning approaches in cyber security. Understanding the nature of cyber security data, which includes a variety of cyber events and crucial elements, is therefore essential. The idea is that different patterns of security occurrences can be examined using raw security data obtained from comparable cyber sources or analysis of spam.

Table 2 lists a variety of dataset types, along with their various features and incidents that are available online. We highlight their use in a range of machine learning-based cyber applications that efficiently analyse and handle these networks.

Table 2. *Cyber Security databases*

Datasets	Description
ADFA IDS	This incursion dataset, which is provided by the Australian Defense Academy (ADFA), comes in two versions: ADFA-LD and ADFA-WD. The purpose of this dataset is to assess host-based IDS.
UNSW-NB15	Its 49 distinct properties, which were collected from the University of New South Wales (UNSW) Cyber Security lab in 2015, are distributed among nine distinct threat types, including DoS. ML-based anomaly detection systems in cyber applications can be evaluated using UNSW-NB15.
DARPA	Attack scenario information from the Authenticated Intrusion Detection System (IDS) for LLDOS1.0 and LLDOS2.0.2. The DARPA dataset is used by MIT Lincoln Laboratory to gather data traffic and threats for network intrusion detection system (NIDS) evaluation.
NSL-KDD	The KDD'99 Cup dataset's updated variant. Duplicate records have been eliminated. It also discusses problems related to class disparity.
KDD99 Cup	Includes forty-one features that can be used to assess machine learning models. Threats are divided into four main target labels, including user-to-remote (U2R), denial of service (DoS), remote-to-local (R2L), and probing.
KYOTO	Traffic information from the honeypots at Kyoto University.
SNAP	There are a number of pertinent graph datasets that are not specifically related to security.
IMPACT	PREDICT, or the Protected Repository for the Defense of Infrastructures Against Cyber Threats, is a group that generates research and data related to network operations that are security-relevant. The repository offers often updated information on network operations related to the advancement of cyber protection technologies.

MAWI	Cyber Security dataset that is frequently used to identify and evaluate DDoS attacks using machine learning techniques and is governed by Japanese academic and network research institutions.
CERT	In order to validate insider-threat detection methods in this dataset, user activity logs were created. It may be used to monitor and assess user behavior because it is based on machine learning.
Bot-IoT	This is a dataset that includes authentic and simulated Internet of Things (IoT) network traffic, as well as various assaults for network forensic analytics in the IoT space. Bot-IoT is primarily used in forensics to assess reliability using multiple statistics and machine learning techniques
DGA	The Alexa Top Sites dataset reliably hosts domain names that are benign. Malicious domain names are collected from OSINT and DGArchive. These datasets find perfect application in DGAbotnet detection or domain classification using automated ML models.
CTU-13	This is a labeled malware dataset including background traffic, botnet and normal user activities, which was captured at CTU University, Czech Republic. CTU-13 is used for data-driven malware analysis using machine learning techniques and to evaluate the standard malware detection system
CAIDA	DDoS attack traffic as well as typical traffic history are included in the CAIDA'07 and CAIDA'08 datasets. They are mostly employed to identify online DOS activity and evaluate machine learning-based DDoS assault detection techniques.
CDX 2009 Network USMA	The correlation between IP addresses linked to PCAP files and hosts on the internal USMA network is highlighted in this dataset. This dataset does not include all network alterations.
DREBIN	These publicly accessible datasets were produced by researchers as part of the Drebin project to support and advance studies on Android malware. This collection contains 5560 programs that cover 179 distinct malware categories. The MobileSandbox project made the samples, which were gathered between August 2010 and October 2012, publicly accessible to cybersecurity professionals.
EnronSpam	Email-based datasets are difficult to collect because of privacy concerns. This dataset is a collection of emails with spam and ham classification

MALWARE	This group of harmful files comes from a number of malware-based datasets, including Microsoft, DREBIN, Comodo, Contagio, VirusTotal, Virus Share, and the Genome Project. These datasets are frequently used for machine learning-based data-driven malware analysis and assessment of current malware detection systems.
ISCX'12	There are 19 features in this dataset, and DDoS attacks account for 19.11% of network traffic. The Canadian Institute for Cyber Security documented ISCX'12, which is widely recognized for its application in assessing the efficacy of machine learning-based network intrusion detection modeling.
CIS-DDoS2019	A database of past DDoS attacks has been developed by the Canadian Institute for Cyber Security. Using machine learning techniques, CIC-DDoS is a great network traffic behavioral analytics tool for identifying DDoS attacks.

Summary of Cyber Security Databases in Table 2 Above

Information about security threats, vulnerabilities, attacks, and tools is gathered, stored, arranged, and shared using cyber security databases. They assist with a variety of cyber security tasks, such as research, incident response, vulnerability management, and threat detection. Below is a summary of their functions:

Susceptibility Recognition and Handling: Keep track of and rank software and system security vulnerabilities. Assist enterprises with risk mitigation and patching. E.g., vulnerabilities, NVD, and CVE.

Intelligence and Detection of Threats: Exchange details regarding malicious IPs, malware hashes, malicious domains, etc. Make proactive defenses and early warning systems available. Examples include AbuseIPDB, MISP, and AlienVault OTX.

Analysis of Malware: Keep known malware samples safe and permit analysis. Assist analysts and researchers in comprehending malware signatures and behavior. MalwareBazaar and VirusTotal are two examples.

Attack Patterns and Adversary Strategies: Create a map of the tactics, methods, and procedures used by attackers. Boost security measures and model actual threats. SIEM systems, CAPEC detection, and MITRE ATT&CK are a few examples.

Verification of Exploits and Penetration Testing: Give real-world exploits and proof-of-concept code. Utilized for vulnerability validation and red teaming. Examples are Packet Storm and Exploit DB.

Exposure Mapping on the Internet: Find devices with internet access that are unprotected or improperly configured. Assist with risk assessments and asset finding. Censys and Shodan are two examples.

Academic Use and Security Research: Provide organized datasets so that new models, algorithms, or tools for cyber security can be developed and tested. Use: In SIEM systems, anomaly detection, and machine learning.

Integration and Automation: These databases are integrated with numerous security platforms (firewalls, SIEM, and EDR) to provide automated responses and real-time threat feeds.

Recurrent Neural Network in Cyber Security

In tasks involving sequential data, such network traffic analysis, intrusion detection, and threat intelligence extraction, recurrent neural networks (RNNs), in particular Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU), have become essential to cyber security. An outline of RNN-based learning strategies in cyber security, backed by current academic studies Yin, Zhu, Fei, & He, (2017). Therefore, there are several benefits to using recurrent neural networks, especially LSTMs and GRUs, in cyber security applications that use sequential data. They are appropriate for applications like anomaly detection, intrusion detection, and information extraction because of their capacity to model temporal dependencies Wang, et al. (2017). To guarantee the dependability and security of RNN-based models in practical applications, however, issues like susceptibility to hostile attacks call for the creation of strong defence mechanisms.

Examples of some RNN learning techniques in Cyber Security include:

a. Supervised Learning

Use cases for supervised learning include phishing detection and malware classification.

Method: RNNs are trained on labelled data (malicious vs. benign) to identify trends. The models that were employed were GRUs (Gated Recurrent Units), LSTMs (Long Short-Term Memory), and vanilla RNNs.

b. Learning without Supervision

Use case: Finding anomalies in network traffic or logs.

Method: RNNs are trained to forecast a sequence's subsequent event. When the forecast errors are high, anomalies are reported.

Methods: Sequence modelling and auto encoders

c. Learning that is semi-supervised

Use case: Threat identification using a little amount of tagged data.

Method: To boost performance, mix huge unlabelled datasets with modest amounts of labelled data.

d. Less frequently used Reinforcement Learning

Use case: Dynamic firewalls and other adaptive defence systems.

Method: To learn the best defensive tactics over time, RNNs are employed in an RL framework.

Analysis of the Existing System

- A lot of existing systems today use *Static* rules such that they detect assaults by using signatures, which are easily circumvented by attackers using novel or unidentified attack techniques.
- They use limited adaptability over time, which become less effective because of their inability to adjust to shifting network conditions or new attack types.
- They also use high false positive rates which might cause legitimate users' traffic to be stopped and cause disruptions.
- It's possible that the system won't be able to recognize brand-new, undiscovered threats.
- These systems might not function as well in the face of low-latency attacks or heavy traffic volumes.

- The system might not be able to recognize abnormalities in real time if the training set of data that was used to create the model is not representative of real-world data.

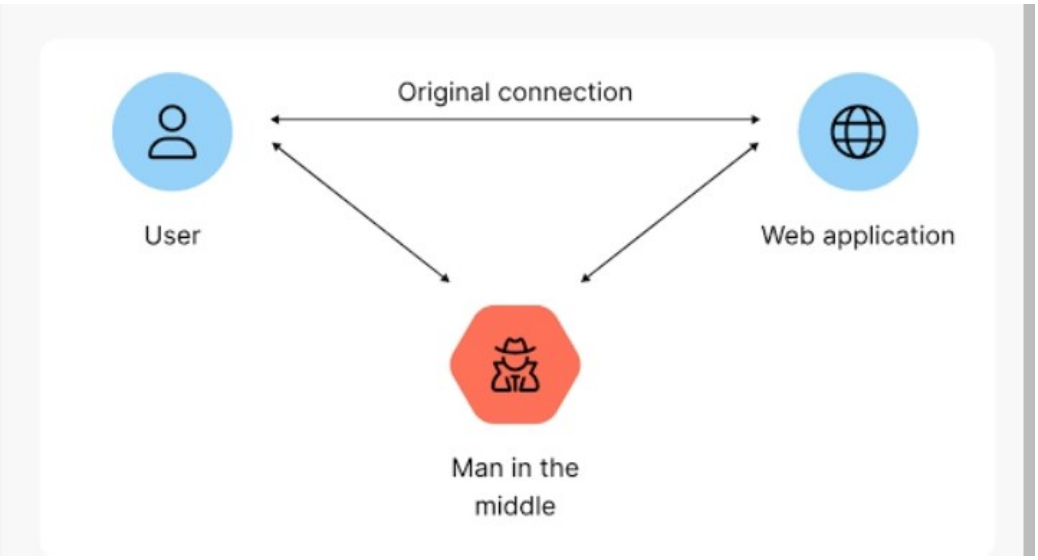

Figure 1: Existing model of Man in the Middle attack

Proposed System

Since detection latency exists in the existing system where time lag is ten (10) minutes between the launch of an attack, and the system's inability to detect it, this proposed system seeks to bridge the detection latency between the launch of an attack and the ability of the system to detect it in real-time.

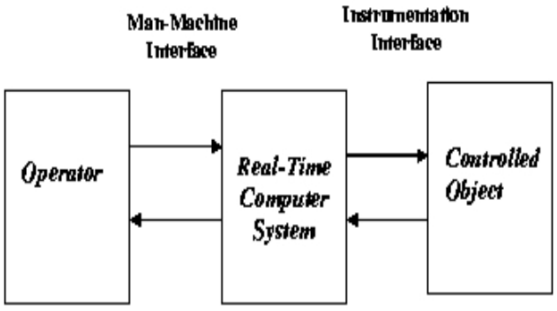

Figure 2: Structure of the proposed model

Stages of Cyber-Attacks

Businesses are able to recognize specific security risks and evaluate their own Cyber Security risk. After that, they can put security measures or controls in place to counter these dangers. They can employ the National Institute of Standards and Technology (NIST) Special Publications, however they may not be a US federal agency or affiliated contractor Force, J.T. (2020). For government information systems, NIST Special Publications offer detailed instructions on how to implement a risk management framework. This advice identifies a number of security concerns and provides a list of common controls or procedures to counter them. Machine learning methods were proposed as effective controls or measures in a recent study Breier, J. (2012). Such methods can be applied to all five phases of a cyber-attack.

A cyber attack can be divided into five stages. They are reconnaissance, scanning, attack (including denial-of-service attacks, network, operating system, and application attacks), sustain access (via the use of Trojan horses, backdoors, rootkits, etc.), cover tracks, and hiding. Any disruption at any stage has the potential to disrupt or stop the attack process altogether. Throughout each of these stages, machine learning algorithms can be employed to disrupt the attacker's workflow and aid in the defence against cyber attacks. In the reconnaissance or preparation stage of the attack, an adversary employs tactics like social engineering attacks (phishing, malicious calls, etc.). Machine learning algorithms can search for email signatures, identify malicious or phishing email signatures, and block them. In certain situations, an attacker calls the target organization and poses as a third party in order to obtain important information (voice phishing or "vising"); call source analysis using machine learning algorithms can flag and block such calls. Another example of how machine learning is used is scanning any external devices connected to the organization's property, such as a USB device, which stops malicious software from spreading through such devices.

During the scan phase, sometimes referred to as "Weaponization," the cyber-attacker or adversary exploits the vulnerabilities of the target system using automated tools like Metasploit, Autopilot and Sakthivel *et al.* (2020).. An ethical hacker can use machine learning algorithms to automatically scan and find the vulnerabilities before the reconnaissance step is completed. Another example is when the adversary wants to guess the access password to obtain unauthorized access (violating confidentiality).

The implementation of a machine learning-based penetration test, for instance, can be accomplished by incorporating the algorithms into penetration testing tools, such as Metasploit. When a pen tester uses these algorithms, they can identify new vulnerabilities.

An effective defence against attacks (phase 3 of a Cyber Attack) is machine learning algorithms. Linear regression, logistic regression, polynomial regression, naïve Bayes classifier, support vector machine, decision tree, nearest neighbour, clustering, dimensionality reduction, linear discriminant analysis, and boosting are machine learning algorithms that can be utilized to provide Cyber Security Alazab *et al* (2021). These algorithms are used to detect spam (including phishing), malware, denial-of-service attacks (including DDoS), and network anomalies as a defence against Cyber Security issues. Social media analytics, identity theft detection, biometric recognition, and authentication are linked to further types of attacks. Other contemporary threats that require attention include software vulnerability identification, hidden channel detection, advanced persistent threat detection, or APT.

Malware, such as Trojan horses, backdoors, or rootkits, is employed by the attacker to sustain access during phase four of a Cyber Attack. When the malware contacts the attacker and vice versa, machine learning algorithms are able to identify such malware communication packets. Support vector machines (SVM), for instance, are a useful choice for malware detection Thomas *et al*. (2020). Static features analysis was used to develop SVM utilizing Wekatodetect Android OS malware (260 samples). Instead of running the malware, the black box approach in this case was examining its behaviour. The initial phase was extracting the functionality of Android application packages (APKs), one package at a time, using Python code. APKs that were both benign (59 samples) and malicious (201 samples) were chosen.

In order to detect malware from these APKs, an SVM classifier (Weka and LibSVM classifier) was trained using these attributes in the second stage. The employed APKs were obtained from the following repositories throughout the testing phase: Android, Malware Dataset, Kaggle, Drebin, Android Malshare, and APKPure. The result was displayed using the receiver operating characteristic, or ROC curve. This application was improved by utilizing the dynamic qualities of malware, which is always evolving.

A collection of network packet features can be used to train an SVM model to perform binary classification. By distinguishing between typical and anomalous network data,

the trained classifier can identify DDoS attacks, particularly for Internet of Things devices.

The destination IP address, sequence number, minimum, maximum, and average packets for each destination IP address, received signal strength indication, network allocation vector, value injection rate, inter-arrival time between consecutive frames, etc. are a few examples of features that are used to train machine learning algorithms. For a traffic session lasting 15 to 20 minutes, sensors were positioned at key network nodes, such as the gateway level, to gather traffic data. This classifier can be added to IDS as an additional security layer.

The use of several clustering approaches, such as K-means, DB SCAN, and Hierarchical, is another example Thomas *et al* (2020). Spam filtering, virus detection, phishing attack detection, and side channel attack detection—a broader family of software defects—all benefit from clustering.

Malware and good ware Android APKs were both installed on an Android emulator in Thomas *et al* (2020). They then recorded their CPU and RAM consumption statistics for each of the three clustering methods. A total of 217 data instances—145 for training and 72 for testing—were employed for all three clustering techniques. CPU-RAM consumption data were found to be an ineffective tool for grouping malware and good ware together.

In access control, the nearest neighbourhood (NN) search is employed. For instance, by classifying biometrics (like fingerprints) according to their patterns, a NN can distinguish between real and fake biometrics Thomas et al (2020). Ten individuals, totalling one hundred fingers, had their fingerprints scanned using the CSD200 model. These pictures were transformed into an array or matrix using MATLAB.

Such a machine learning algorithm is capable of automatically determining if a biometric is authentic or fake. Decision trees, such as Iterative Dichotomizes 3 (ID 3) and its successor, C4.5, were employed in Thomas *et al* (2020). To effectively identify malware. The Cardiff University Research Portal provided the dataset. Sakthivel *et al* (2020). In a different study unusual services that are present in computer systems both online and offline,

Verified by the use of principle component analysis (PCA), neural network-based models (NARX-RNN), AI-based multi-perspective SVM, and hierarchical process tree-based reinforcement learning approaches.

The attacker wants to make sure that their identity is not being followed during phase five, often known as the concealing tracks phase. To misidentify their data, they use a

variety of strategies, such as tampering with the training data of machine learning systems. Although the training data for machine learning algorithms may not be reliable, the methods themselves may be. Inaccurate training data renders the algorithm ineffective. Adversarial machine learning (AML) is the term for this technique of creating fake training data. For Cyber Security applications, the severity is severe.

Game theory (non-cooperative game/Nash equilibrium, zero-sum versus non-zero sum game, simultaneous move versus sequential game, or Bayesian game) is one of the defences against such contaminated data Dasgupta *et al* (2019).

Classification of network traffic is an illustration of AML. When the communication payload is encrypted, deep packet inspection becomes challenging De Lucia *et al*. (2019). An opponent may trick a machine learning classifier (such as a network scanning detector) into classifying such traffic as benign NMap network scanning traffic, malware, or botnet communications. The attacker may be able to derive the classification output by imitating the characteristics of benign traffic. What occurs if the traffic coming from the adversary is deemed malicious? Although the enemy does not receive any feedback, their traffic is most likely going to be stopped. The adversary will be prompted to alter the traffic signature as a result of receiving notification that their traffic has been deemed hostile.

There are established machine learning strategies that can be used as a defence against hostile attacks Xi (2020). An activation clustering technique, for instance, was developed to locate the deep neural network's hidden layer, which contains an adversarial trigger. When poisoning assaults occur against an SVM, poisoned data points can be recognized using empirical learning algorithms.

Supervised Learning

The foundation of supervised learning is the valuable knowledge found in previous labelled data. When goals are predetermined to be achieved from a specific set of inputs, supervised learning is carried out (task-driven approach). The most often used supervised learning strategies are regression and classification Sarker (2019). These techniques are often used to categorize or forecast the target variable for a specific security risk. In Cyber Security, for instance, classification techniques can be used to distinguish between different types of network threats, like scanning and spoofing, or to signal whether a denial-of-service (DoS) assault is occurring. Among the most

popular classification methods in shallow models are Naive Bayes, logistic regression Le Cessie et al (1992).

Naive Bayes finds a good amount of usage in cyber security. For training and testing, the authors in Panda M. (2007), used KDD'99 data using the naive Bayes classifier from the Weka package.

The four attack types—probe and scan, DoS, U2R, and R2L—were represented in the data, and the classifier's testing accuracy was 96%, 99%, 90%, and 90%, respectively. Three percent was the cumulative false positive rate. Using the KDD'99 data, the authors in (Amor 2004) created a framework utilizing a basic Bayesian network and employed categories to represent various attack scenarios. The stated results for solving an anomaly detection problem were 97%, 96%, 9%, 12%, and 88% accuracy for normal, DoS, R2L, U2R, and probeorscan categories, respectively. The false positive rate was not stated but can be assumed to be less than 3%.

In order to tackle a DoS problem, Naive Bayes was also employed as one of the techniques in (Carl 2006). This method sought to identify the existence and origin of the botnet by resolving the botnet traffic in filtered Internet Relay Chat (IRC). TCP-level data from 18 distinct sites on the Dartmouth University campus' wireless network was used in the study. Over the course of four months, this data was collected. IRC data was extracted from the network traffic using a filter layer. The study used simulated data for the tests because labelling was difficult. The Bayesian network demonstrated a 93% precision rate and a 1.39% false positive rate. For comparison, C4.5 decision trees were also employed and attained 97% precision, but the false positive rates were greater, at 1.47% and 8.05%, respectively.

To identify DDoS attacks in a software-defined network, the authors in (Kokila R. et al. 2014) employed an SVM classifier. The DARPA dataset was used for experiments that compared the SVM classifier to other widely used classification methods. The classifier was more accurate, but the SVM took longer, which is a clear drawback. In (Amiri F. 2014) the authors employed a least-squares SVM to minimize the training time on huge datasets. Using three distinct feature extraction algorithms, they reduced the number of features from 41 to 19.

Each of the five classes in the KDD'99 dataset had about 7000 occurrences after the data were resampled. The overall categorization was reported to be 93% for U2R and 99% for DoS, probe or scan, R2L, and normal classes.

A robust SVM, a variant of SVM in which the regularization value is automatically selected and the discriminating hyper plane is averaged to be smoother, was used in

the research in (Hu *et al* 2014) The Basic Security Module from the DARPA 1998 dataset was used for pre-processing, training, and testing. 100% accuracy with 3% erroneous positives and 75% accuracy with no false positives were demonstrated.

In (Vuong et al 2015), the authors used decision trees to create detection rules against command injection and denial-of-service attacks on robotic vehicles. The results indicated that different attacks had different effects on robotic behaviour. In (Moon *et al*, 2017) the authors implemented a decision tree-based intrusion detection system that may change after intrusion by analysing the behaviour data through a decision tree. The model was used to prevent advanced persistent threat (APT) attacks, which use social engineering to launch various forms of intrusion attacks; the detection accuracy in their experiments was 84.7%, which is very high for this experiment. In (Kruegel *et al*, 2003) the authors substituted decision trees for the misuse detection engine of SNORT, a well-known tool that employs a signature-based methodology.

The authors used a variant of the ID3 technique to create a decision tree after employing clustering of rules. The decision tree found the most discriminating aspects of the data, enabling simultaneous feature evaluation, and rule clustering decreased the number of comparisons needed to identify which rules were triggered by the input data. The 1999 DARPA intrusion detection dataset showed better performance from this approach than from SNORT. Depending on the type of traffic, the outcomes differed significantly. The quickest were up 105%, with an average of 40.4% and at least 5% faster than SNORT's typical detection performance. Additionally, the number of rules was raised from 150 to 1581, leading to a noticeable speedup in comparison to SNORT.

Research on Cyber Security has also looked into ensemble learning strategies like random forest (RF). Random forest can be more accurate than a single decision tree because it employs several decision trees to reach its conclusions. To detect misuse, anomalies, and hybrid-network-based intrusions, the authors of (Zhang *et al*, 2008) used a random forest technique on the KDD dataset. The random forest generated patterns, which were then compared with the network to identify instances of misuse. The random forest used outliers to find new invasions in order to identify anomalies. New outliers were also found using the patterns the model had constructed. A complete system solution, including anomaly detection, was put into practice for the study.

Majority assaults and minority attacks were used to categorize the data. The hybrid system demonstrated exceptional performance in detecting misuse, with an error rate of 1.92% on the original dataset and 0.05% on the balanced dataset.

The main difference between classification and regression is that in classification, the projected output is categorical or discrete, whereas in regression, the output variable is numerical or continuous. Ensemble learning is an extension of supervised learning that combines various shallow models, such as XGBoost and random forest learning (Breiman *et al*, 2021), to accomplish a specific security task. Regression algorithms are useful for forecasting a continuous target variable or numeric values, such as total phishing attacks over a period of time or network packet properties (Watters *et al*, 2012).

Future Improvements and Challenges for RNN-Based Cyber Security

Due to their capacity to model sequential and time-dependent data, recurrent neural networks (RNNs) have demonstrated promise in a number of cyber security applications, including intrusion detection, malware classification, and anomaly detection. Nevertheless, there are both encouraging prospects for future advancements and significant obstacles in the use of RNNs for cyber security.

Future improvements

a. Integration with Transformer Models:

More potent sequential models such as Transformers may replace or supplement RNNs; hybrid models may use RNNs for temporal context and Transformers for attention-based filtering.

b. Explainable AI (XAI):

Enhancing the interpretability of RNN decisions is crucial; new techniques to visualize hidden states and attention mechanisms can make these models more transparent and reliable in security contexts.

c. Online and Continuous Learning:

Improving RNNs' ability to learn from data in real time without forgetting historical information (overcoming catastrophic forgetting) is essential for adapting to changing threats.

Multimodal Threat Detection:
Future systems may integrate RNNs with other AI components to analyse logs, network traffic, user behaviour, and sensor data concurrently.

Edge Computing Optimization:
Lightweight RNN variants can be deployed on edge devices for local.

Challenges:
a. Limited Learning of Long-Term Dependencies
Typical While LSTMs and GRUs help to some degree, RNNs have trouble learning long-range dependencies. When modelling intricate assault sequences, this still acts as a bottleneck.

b. Labelling and Data Quality
In Cyber Security, high-quality labelled data is hard to come by. Training supervised RNNs is hampered by adversarial, noisy, or unbalanced datasets.

c. Attacks by Adversaries
Adversarial inputs intended to trick the model can affect RNNs. One of the main concerns is making sure it is resistant against such manipulations.

d. Idea Drift
Cyber threats are constantly changing. Without frequent retraining, which requires a lot of resources, RNNs trained on outdated data may become outdated.

e. Costs of Computation
Deep RNNs can be computationally costly to train and implement, particularly in large-scale settings or high-frequency data streams.

Table 3: Summary of Related Literatures

S/No	Author's Name	Title of Journal	Publication Year	Strength	Limitation
1	**Li *et al***	IoT a survey	2015	Predicted incident of cyber security as a driven data	No detection of launched attack was fully detected
2	**Alazab *et al***	Zero day Malware detection	2011	They supervised learning algorithms of API call signature.	There was no adequacy of entropy- based in their work for maximum protection.
3	**Craigen & Diakun**	Technology innovation management review	2014	They worked on different types of adopted Cyber Security Technologies with their attributes managing attacks.	The result obtained in that research is 78% achieved.
4	**Shaw A.**	Data breach	2009	Notification to prevention of attacks using PCT DSS	The limitation of this method is that no prompt alertness of attack notification on the system.
5	**Fischer E.A**	Creating a National framework for Cyber Security	2014	Analysis of issues and options in detecting cyber attacks	Consistency in detecting attack is not given much priority due to options given at random
6	**Gubta *et al***	Fighting against phishing attacks.	2017	State of the art and future challenges.	The weakness from this work can be seen because of the recommendation they gave in the research instead of giving a proper solution to the mitigation of the attacks
7	**Tapiador *et al***	A key anomaly detection and response system.	2013	Key recovery attacks on kids.	The work didn't specify the children based of their categories and age limit exposed to such attacks
8	**Anwar *et al***	Intrusion detection system.		Intrusion detection is applauded in their research work.	No definite type of intrusion on discussion.
9	**Joye *et al***	Identity based Cryptography	2009	Cryptography in securing a system is indeed one of the best ways to secure data on a network.	The detailed cryptography type was was not vividly specified.

10	**Gisin *et al***	Quantum cryptography	2002	The technology of securing data is one of the best as far as the cyber security is concern.	The was no parameter of how data can be secured in the research work.
11	**Zou *et al***	A firewall Network system	2004	Worm defense in Enterprise Networks	The defensive mechanism was not captured, since there are different types of software versions and models in the market today.
12	**Rizk *et al***	Data Science	2020	They Developed theoretical contributions in information system via text analytics.	The weakness of the research conducted by the authors is that signature authentication ws not included in the text analytics which makes it very easy to attack such a system.
13	**Khraisat *et al***	Survey of intrusion detection system	2019	Techniques, datasets and challenges was involved in the work carried out.	The study didn't reveal a defined survey to tackle intrusion detection.
14	**Hu**	Machine learning for access control policy verification.	2021	He gave a technical report on the control policy of verification.	It did not give a reliable and vivid source of the policy verification.
15	**Brahmi *et al***	A multi agent's intrusion detection system.	2015	Ontology and clustering techniques	The multi agent detection has poor intrusion time detection.
16	**Alghamdi**	Survey on application of Deep Learning	2020	He explored Machine Learning techniques for Cyber Security	The research work didn't explain the type of deep learning techniques to deploy.
17	**Ghanem *et al***	Reinforcement learning for efficient network testing	2020	The protocol exhibited by the reinforcement of testing the network is partially addressed	No adopted single network testing module was presented to tackle the efficiency of the reinforcement.
18	**Dutt *et al***	Real time hybrid intrusion detection system	2018	They used machine learning to detect intrusion on a network	The research gave false negative return result as image in order to gain access.
19	**Radivilova *et al***	The complex method of intrusion detection	2020	The research was carried out based on anomaly detection and misuse detection.	The complexity method explained in this work couldn't solve two third of the expected result.

20	**Liao *et al***	A comprehensive review of intrusion detection system.	2013	The strength of their work was mainly on review.	No standard of deployment of review was vividly explained in the entire work.
21	**Alazab *et al***	Feature selection for intrusion detection system.	2012	The research work was a presentation at an international symposium on how to detect intrusion on a network.	Time laxity became the major reason for inability to detect intrusion.
22	**Viegas *et al***	Towards an energy efficient anomaly intrusion.	2016	Their research aimed at engine embodiment detection.	Other sources were not explored to curtail the intrusion on the network.
23	**Force**	Risk management framework for information systems and organizations.	2018	The formation of risk management gave much strength to securing the network as shown in this work.	The framework was belated and not deeply explored by the authors in order to achieve the desired goal.
24	**Breier *et al***	Risk management framework for Machine Learning security.	2020	Risk management in this work gave more strength to the in	The weakness of the research work shows no other method used to manage risks. This cannot give perfect result.
25	**Buchaman *et al***	Automating Cyber Attacks	2020	The work was seen as breakthrough to Cyber Attacks in the contemporary world.	The weakness of the research is that there was no regular update as to unforeseen coming attacks
26	**Thomas *et al***	Machine Learning approaches in Cyber Security analysis.	2020	Machine learning is a core mitigating approach to solving cyber security as explained by the authors in this research work.	The weakness of this work is that machine learning is not the only method o
27	**Sakthiyel *et al***	Core-level Cybersecurity assurance.	2020	The research was a cloud based adaptive Machine Learning techniques for manufacturing industries.	The weakness of the research work is that modern industries evolved with more security demand than ever which cannot be handled by this method explained.
28	**Dasgupta *et al***	A survey of game theoretic approaches for adversarial machine learning in	2019	The task explained in the research could be addressed in a better technical method like this. It is commendable	The survey carried out was partially done since some valid part of the expected result were not seen in the entire work.

		Cyber Security tasks.			
29	**De Lucia *et al***	Adversarial machine learning for cyber security	2019	Machine learning for cyber security in the context of this research work was addressed to some extend	Only 68% was achieved in the course of this research work.
30	**Xi B.**	Adversarial machine learning for cyber security and computer vision	2020	The research work mainly discussed on the framework of mitigating cyber attacks using machine learning.	The achieved goal of this research using adversarial machine learning was not clearly defined.
31	**Sarker *et al***	Effectiveness analysis of machine learning.	2019	The work was carried out based on classification of models for predicting personalized context on smartphone usage.	The weakness of this research shows that many manufactured smartphones today comes with built-in AI features, thereby making this research obsolete.
32	**Panda *et al***	Network intrusion detection using naïve bayes	2007	The naïve bayes intrusion detection method was premium to stand the test of time on a network system.	No standard intrusion detection method was effective
33	**Amor et *al***	Naïve bayes vs decision trees in intrusion detection systems	2004	Naïve bayes has tremendously helped in achieving this research goal to some extent.	The research work didn't solve the intrusion detection because of porous security breach detected at the backend.
34	**Kokila *et al***	DDoS detection and analysis in SDN-based environment.	2014	The authors used support vector machine classifier to detect and analyse the SDN environment.	The entire work just achieved 76% of the total expected result due to variation of datasets run by the team of researchers.
35	**Amiri *et al***	Mutual information based feature selection for intrusion detection systems.	2011	On the research carried out shows the basic selection method to curtail intrusion on a network.	Lengthy time line in the execution of the detection was observed in research work.
36	**Hu *et al***	Vector machines for anomaly	2003	Similarity to machine learning techniques was applied in the research in	Only 74% of result was achieved in the entire work, which is the major setback.

		detection in Computer Security		order to detect anomaly detection in computer security.	
37	**Vuong *et al***	Decision tree based detection of denial of service.	2015	They used command injection attacks on robotic vehicles detect movement using decision tree.	the weakness of this research is that manual testing was not carried out to ascertain the standard of denial of service.
38	**Moon *et al***	An intrusion detection system based on decision tree.	2017	This research work clearly shows the behaviour analysis for preventing APT attacks.	The research work achieved just 89% of the expected result.
39	**Kruegel *et al***	Using decision trees to improve signature-based detection	2003	The tree decision method to improve signature in validation of an intruder is worked	Somme decisions in the research work was not harmonised.
40	**Waters *et al***	Characterising and predicting cyber-attacks.	2012	The work was featured on cyber-attacks profile model for the prediction.	The prediction didn't have an accuracy of the expected result needed.

The summary of the related works above shows the contribution made by different authors and publishers on Cyber Security related subjects. It categorically narrated the authors' name, title of journal, year of publication, strength and limitation of their research.

Conclusion

The review and survey carried out in this research suggested an RNN-based system, capable of mitigating DoS and MitM attacks in network traffic data. By leveraging sequential data-processing capabilities, the review can achieve high accuracy and reliability in identifying various attack types. The experimental results to be obtained in the further research work can underscore the effectiveness of RNNs in learning complex patterns within network traffic, validating the model's practical application in cyber security.

Despite the scope of this review, the system can demonstrate excellent generalization and robustness; which can enhance online system security, reduce the impact of cyber-attacks, and contribute to advancing intelligent threat detection systems.

Recommendations to Researchers:

1. Create Diverse and More Realistic Datasets: Existing datasets are frequently out-of-date or lack real-world diversity. The creation or enhancement of datasets that represent contemporary network topologies and threat vectors, such as encrypted traffic and zero-day assaults, should be the main goal of researchers.
2. Examine Ensemble and Hybrid Models: To improve detection accuracy and lower false positives, look into combining neural networks with conventional machine learning techniques or rule-based systems.
3. Give Model Explainability and Trust Top Priority: Integrate Explainable AI (XAI) frameworks to give security analysts insight into neural network decision-making, which is essential for them to trust and respond to alerts.
4. Increase the Model's Resistance to Adversarial Attacks: Adversarial examples can affect neural networks. To strengthen models, adversarial training and defensive distillation should be used in future research.
5. Adjust for Environments with Limited Resources: Create neural architectures that are lightweight and appropriate for use in IoT systems, mobile networks, and edge devices with constrained processing power.
6. Model Attack Situations in Real Time: To assess model performance under real-world network loads and attack scenarios, run experiments in simulated or real-time environments.
7. Encourage Open Research and Reproducibility: To promote reprehensibility and cooperative advancements among researchers, make sure that experimental configurations, code, and datasets are publicly accessible.

References

Ahmad, F., Adnane, A., Franqueira, V. N., Kurugollu, F., & Liu, L. (2018). Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies. *Sensors*, *18*(11), 4040.

Ahmed, F., Sumra, I. A., & Jamil, U. (2024). A Comprehensive Review on DDoS Attack in Software-Defined Network (SDN): Problems and Possible Solutions. *Journal of Computing & Biomedical Informatics*, *7*(01).

Aizuddin, A. A., Atan, M., Norulazmi, M., Noor, M. M., Akimi, S., & Abidin, Z. (2017, January). DNS amplification attack detection and mitigation via sFlow with security-centric SDN. In *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication* (pp. 1-7).

Alashhab, A. A., Zahid, M. S. M., Azim, M. A., Daha, M. Y., Isyaku, B., & Ali, S. (2022). A survey of low rate ddos detection techniques based on machine learning in software-defined networks. *Symmetry*, *14*(8), 1563.

Alghazzawi, D., Bamasag, O., Ullah, H., & Asghar, M. Z. (2021). Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. *Applied Sciences*, *11*(24), 11634.

Ali, M., Benamrane, F., Luong, D. K., Hu, Y. F., Li, J. P., & Abdo, K. (2019, September). An AI based approach to secure SDN enabled future avionics communications network against DDoS attacks. In *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)* (pp. 1-7). IEEE.

Ali, S., & Li, Y. (2019). Learning multilevel auto-encoders for DDoS attack detection in smart grid network. *IEEE Access*, *7*, 108647-108659.

Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., & Kim, K. I. (2022). Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection. Electronics 2022, 11, 3934.

Ali, T. E., Chong, Y. W., & Manickam, S. (2023). Machine learning techniques to detect a DDoS attack in SDN: A systematic review. *Applied Sciences*, *13*(5), 3183.

Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. *IEEE Access*, *9*, 42236-42264.

Almomani, I. M., & Alenezi, M. (2018). Efficient Denial of Service Attacks Detection in Wireless Sensor Networks. *J. Inf. Sci. Eng.*, *34*(4), 977-1000.

Alzubaidi, M., Hasan, K. N., & Meegahapola, L. (2022, November). Identification of the Impact of Wind Speed and Load Uncertainties on Short-term Voltage Stability. In *2022 IEEE PES 14th Asia-Pacific Power and Energy Engineering Conference (APPEEC)* (pp. 1-7). IEEE.

Asad, M., Asim, M., Javed, T., Beg, M. O., Mujtaba, H., & Abbas, S. (2020). Deepdetect: detection of distributed denial of service attacks using deep learning. *The Computer Journal*, *63*(7), 983-994.

Assis, M. V., Carvalho, L. F., Lloret, J., & Proença Jr, M. L. (2021). A GRU deep learning system against attacks in software defined networks. *Journal of Network and Computer Applications*, *177*, 102942.

Aupetit, M., Zhauniarovich, Y., Vasiliadis, G., Dacier, M., & Boshmaf, Y. (2016, October). Visualization of actionable knowledge to mitigate DRDoS attacks. In *2016 IEEE symposium on visualization for cyber security (VizSec)* (pp. 1-8). IEEE.

Azzedin, F. (2023). Mitigating Denial of Service Attacks in RPL-Based IoT Environments: Trust-Based Approach. *IEEE Access*, *11*, 129077–129089. https://doi.org/10.1109/access.2023.3331030

Bhardwaj, A., Mangat, V., & Vig, R. (2020). Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud. *IEEE Access*, *8*, 181916-181929.

Bhayo, J., Hameed, S., & Shah, S. A. (2020). An efficient counter-based DDoS attack detection framework leveraging software defined IoT (SD-IoT). *IEEE Access*, *8*, 221612-221631.

Li, S.; Da Xu, L.; Zhao, S. The internet of things: A survey. Inf. Syst. Front. 2015, 17, 243–259. [CrossRef] 2. 3. 4. 5. 6. 7. 8. 9.

Sun, N.; Zhang, J.; Rimba, P.; Gao, S.; Zhang, L.Y.; Xiang, Y. Data-driven cybersecurity incident prediction: A survey. IEEE Commun. Surv. Tutor. 2018, 21, 1744–1772. [CrossRef]

McIntosh, T.; Jang-Jaccard, J.; Watters, P.; Susnjak, T. The inadequacy of entropy-based ransomware detection. In Proceed ings of the International Conference on Neural Information Processing, Sydney, Australia, 12–15 December 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 181–189.

Alazab, M.; Venkatraman, S.; Watters, P.; Alazab, M. Zero-day malware detection based on supervised learning algorithms of API call signatures. In Proceedings of the Ninth Australasian Data Mining Conference (AusDM'11), Ballarat, Australia, 1–2 December 2011.

Anwar, S.; Mohamad Zain, J.; Zolkipli, M.F.; Inayat, Z.; Khan, S.; Anthony, B.; Chang, V. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms 2017, 10, 39. [CrossRef]

Mohammadi,S.; Mirvaziri, H.; Ghazizadeh-Ahsaee, M.; Karimipour, H. Cyber intrusion detection by combined feature selection algorithm. J. Inf. Secur. Appl. 2019, 44, 80–88.

Tapiador, J.E.; Orfila, A.; Ribagorda, A.; Ramos, B. Key-recovery attacks on KIDS, a keyed anomaly detection system. IEEE Trans. Dependable Secur. Comput. 2013, 12, 312–325.

Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. J. Comput. Syst. Sci. 2014, 80, 973–993.

Joye, M.; Neven, G. Identity-Based Cryptography; IOS Press: Amsterdam, The Netherlands, 2009; Volume 2,

Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity 2019, 2, 1–22. [CrossRef]

Brahmi, I.; Brahmi, H.; Yahia, S.B. A multi-agents intrusion detection system using ontology and clustering techniques. In Proceedings of the IFIP International Conference on Computer Science and Its Applications, Saida, Algeria, 20–21 May 2015; Springer: Berlin/Heidelberg, Germany, 2015, pp. 381–393.

Qu,X.; Yang, L.; Guo, K.; Ma, L.; Sun, M.; Ke, M.; Li, M. A survey on the development of self-organizing maps for unsupervised intrusion detection. Mob. Netw. Appl. 2019, 26, 808–829.

Radivilova, T.; Kirichenko, L.; Alghawli, A.S.; Ilkov, A.; Tawalbeh, M.; Zinchenko, P. The complex method of intrusion detection based on anomaly detection and misuse detection. In Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 14–18 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 133–137.

Liao, H.J.; Lin, C.H.R.; Lin, Y.C.; Tung, K.Y. Intrusion detection system: A comprehensive review. J. Netw. Comput. Appl. 2013, 36, 16–24. [CrossRef]

Alazab, A.; Hobbs, M.; Abawajy, J.; Alazab, M. Using feature selection for intrusion detection system. In Proceedings of the 2012 International Symposium on Communications and Information Technologies (ISCIT), Sydney, Australia, 9–12 September 2012; IEEE: Piscataway, NJ, USA, 2012, pp. 296–301.

Viegas, E.; Santin, A.O.; Franca, A.; Jasinski, R.; Pedroni, V.A.; Oliveira, L.S. Towards an energy-efficient anomaly-based intrusion detection engine for embedded systems. IEEE Trans. Comput. 2016, 66, 163–177. [CrossRef]

Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine learning and deep learning methods for cybersecurity. IEEE Access 2018, 6, 35365–35381. [CrossRef]

Dutt,I.; Borah, S.; Maitra, I.K.; Bhowmik, K.; Maity, A.; Das, S. Real-time hybrid intrusion detection system using machine learning techniques. In Advances in Communication, Devices and Networking; Springer: Berlin/Heidelberg, Germany, 2018; pp. 885–894.

Ghanem,M.C.; Chen, T.M. Reinforcement learning for efficient network penetration testing. Information 2019, 11, 6. [CrossRef]

Alghamdi, M.I. Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security. Int. J. Interact. Mob. Technol. 2020, 14, 210–224. [CrossRef]

Text—S.1353—113th Congress (2013–2014): Cybersecurity Enhancement Act of 2014|Congress.gov|Library of Congress. Avail able online: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text (accessed on 10 May 2022).

Cybersecurity, C.I. Framework for Improving Critical Infrastructure Cybersecurity. 2018. p. 4162018. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP (accessed on 10 May 2022).

Hu,V. Machine Learning for Access Control Policy Verification; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021.

Rizk, A.; Elragal, A. Data science: Developing theoretical contributions in information systems via text analytics. J. Big Data 2020, 7, 1–26. [CrossRef]

Force, J.T. Risk management framework for information systems and organizations. NIST Spec. Publ. 2018, 800, 37.

Breier, J.; Baldwin, A.; Balinsky, H.; Liu, Y. Risk Management Framework for Machine Learning Security. arXiv 2020, arXiv:2012.04884.

Buchanan, B.; Bansemer, J.; Cary, D.; Lucas, J.; Musser, M. Automating Cyber Attacks: Hype and Reality; Center for Security and Emerging Technology: Washington, DC, USA, 2020. [CrossRef]

Thomas, T.; Vijayaraghavan, A.P.; Emmanuel, S. Machine Learning Approaches in Cyber Security Analytics; Springer: Berlin/Heidelberg, Germany, 2020.

Sakthivel, R.K.; Nagasubramanian, G.; Al-Turjman, F.; Sankayya, M. Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry. Trans. Emerg. Telecommun. Technol. 2020, 33, e3947. [CrossRef]

Dasgupta, P.; Collins, J. A survey of game theoretic approaches for adversarial machine learning in cybersecurity tasks. AI Mag. 2019, 40, 31–43. [CrossRef]

DeLucia, M.J.; Cotton, C. Adversarial machine learning for cyber security. J. Inf. Syst. Appl. Res. 2019, 12, 26.

Xi, B. Adversarial machine learning for cybersecurity and computer vision: Current developments and challenges. Wiley Interdiscip. Rev. Comput. Stat. 2020, 12, e1511. [CrossRef]

Sarker, I.H.; Kayes, A.; Watters, P. Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage. J. Big Data 2019, 6, 1–28. [CrossRef]

Breiman, L. Random forests. Mach. Learn. 2001, 45, 5–32. [CrossRef]

LeCessie, S.; Van Houwelingen, J.C. Ridge estimators in logistic regression. J. R. Stat. Soc. Ser. Appl. Stat. 1992, 41, 191–201. [CrossRef]

Panda, M.; Patra, M.R. Network intrusion detection using naive bayes. Int. J. Comput. Sci. Netw. Secur. 2007, 7, 258–263.

Amor,N.B.; Benferhat, S.; Elouedi, Z. Naive bayes vs decision trees in intrusion detection systems. In Proceedings of the 2004 ACMSymposiumonAppliedComputing, Nicosia, Cyprus, 14–17 March 2004; pp. 420–424.

Carl, L. Using machine learning technliques to identify botnet traffic. In Proceedings of the 2006 31st IEEE Conference on Local Computer Networks, Tampa, FL, USA, 14–16 November 2006; IEEE: Piscataway, NJ, USA, 2006.

Kokila, R.; Selvi, S.T.; Govindarajan, K. DDoS detection and analysis in SDN-based environment using support vector machine classifier. In Proceedings of the 2014 Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, 17–19 December 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 205–210.

Amiri, F.; Yousefi, M.R.; Lucas, C.; Shakery, A.; Yazdani, N. Mutual information-based feature selection for intrusion detection systems. J. Netw. Comput. Appl. 2011, 34, 1184–1199. [CrossRef]

Hu,W.;Liao, Y.; Vemuri, V.R. Robust Support Vector Machines for Anomaly Detection in Computer Security. In Proceedings of the ICMLA, Los Angeles, CA, USA, 23–24 June 2003; pp. 168–174.

Vuong, T.P.; Loukas, G.; Gan, D.; Bezemskij, A. Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. In Proceedings of the 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 16–19 November 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–6.

Moon,D.; Im, H.; Kim, I.; Park, J.H. DTB-IDS: An intrusion detection system based on decision tree using behavior analysis for preventing APT attacks. J. Super Computer. 2017, 73, 2881–2895.

Kruegel, C.; Toth, T. Using decision trees to improve signature-based intrusion detection. In Proceedings of the International Workshop on Recent Advances in Intrusion Detection, Pittsburgh, PA, USA, 8–10 September 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 173–191.

Zhang, J.; Zulkernine, M.; Haque, A. Random-forests-based network intrusion detection systems. IEEE Trans. Syst. Man Cybern. Part Appl. Rev. 2008, 38, 649–659. [CrossRef]

Watters, P.A.; McCombie, S.; Layton, R.; Pieprzyk, J. Characterising and predicting cyber-attacks using the Cyber Attacker Model Profile (CAMP). J. Money Laund. Control 2012, 15, 430–441.

Hu, V.C.; Ferraiolo, D.; Kuhn, D.R. Assessment of Access Control Systems; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2006.

Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cyber security. J. Computer. Syst. Sci. 2014, 80, 973–993.

Wang, W., Sheng, Y., Wang, J., et al. HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection, 2017.

Yin, C., Zhu, Y., Fei, J., & He, X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks, 2017.