A Survey on Deep Learning Models for Cyber Threat Detection Systems

Tolulope Olufemi and Wilson Sakpere

March 8, 2023

A SURVEY ON DEEP LEARNING MODELS FOR CYBER THREAT DETECTION SYSTEMS

ABSTRACT

New organizational innovations and ideal model implementations are making present interruption detection and protection approaches outdated. These improvements will require new methodologies. Future technology will create huge volumes of data at lightning-fast speeds. Network safety frameworks will need to adapt to meet the expanding number of new needs. Conventional Internet-based techniques of managing data and information are being phased out in favor of electronic device applications. As a result, the information and data at issue are exposed to attacks meant to steal or destroy them. Each attack might bring down the entire system. This paper presents a deep-learning-based cyber-attack detection method for wireless sensor networks (WSN). This approach considers WSN node operations and MQTT data transport capabilities. This solution uses a deep learning model overview rather than a regular machine learning model, which improves detection accuracy. Deep learning models that use network stream data may identify network digital risks, which are cyberthreats.

1. Introduction

It is becoming more common to save things like books, movies, pictures, and even medical information online. This move to digital data is being driven by laptops, tablets, smartphones, and wearables, all of which are becoming increasingly integrated into our everyday lives. As a result of our growing popularity as a target, fraudsters have discovered that we make an easy target. Digital forensics is a part of the investigating process for cybercrime. Cyberattacks that are based on botnets are the most dangerous ones online (Ometov et al. 2021).

It might be challenging to digitally investigate attacks that are carried out utilizing botnets. The development of more sophisticated attacks that make use of botnets is now facilitated more easily by hackers. In order to mount an effective defense against attacks of this sort, improvements in digital forensics are necessary. In order to increase the speed and accuracy with which botnet assaults may be detected, the application of machine learning is essential. In the field of network forensics, there are a variety of approaches that may be taken, each of which makes use of machine learning algorithms (Koroniotis, Moustafa, and Sitnikova 2019). Data from the Internet of Things (IoT) and other complicated settings have shown that machine learning is a promising approach for mining vast datasets and addressing a range of challenges. This is shown by the fact that the technology has been proven to be effective. The employment of machine learning algorithms allows for the detection and avoidance of attacks carried out by botnets, which are both observable and avoidable. An examination into the several varieties of botnet attacks and the digital forensic investigation strategies that may be implemented to thwart botnet assaults has been made accessible, and its findings have been analyzed. Standardization is required in the field of botnet detection forensics before evidence can be presented in court. This is necessary in order for evidence to be presented. You may be able to retrieve data from a suspect's device by conducting an investigation utilizing digital forensics, even if the data was deleted, moved, or encrypted without the knowledge of the suspect (Iqbal and Abed Alharbi 2020). There is no possibility for the government to conduct a comprehensive investigation of cybercrime with the resources and staff that are now available to them. Regrettably, the approaches and procedures that are now used for digital investigations call for a large degree of human input. As a result, the process moves at a pace that is insufficient to keep up with the rate at which digital crimes are perpetrated. Machine learning (ML) and deep learning (DL) are the subfields of computer science that serve as the scientific bases upon which artificial intelligence (AI) is constructed (AI). With the current state of technology, it is possible to duplicate human-like behavior by the use of certain programming. Automated learning systems and other types of machine intelligence may be of considerable assistance to digital investigators throughout many phases of the digital investigation process. This can result in significant gains for the digital investigators involved (Sarker 2021).

This study intends to uncover research gaps, foster innovation, and bring attention to key problems. Its major focus is on research on cyberthreat detection systems that are based on deep learning, and its primary objective is to draw attention to crucial concerns.

2. Related Works

Rughani's (2017) study purportedly offered an AI-based digital forensics system. Most framework functions are driven by trained intelligence and need little human input. Here's a strategy to improve digital forensics based on this findings. The architecture outlined in this research has the potential to be very effective if taught correctly and with enough rigor. This technology might save human resources while investigating digital crimes. Using this methodology, more cases may be processed more precisely and quickly, leading to a greater cybercrime conviction rate.

Deep learning and botnet forensics were presented for application in IoT contexts, along with an assessment of their difficulties and potential solutions (Koroniotis, Moustafa, and Sitnikova 2019). There's a new taxonomy of network forensic solutions for traditional and IoT networks. Here are solutions. Deep learning in network forensics is also studied, as well as the Internet of Things and future research potential in this domain. The merits and downsides of Network Forensic techniques that may be used to battle Botnets in non-IoT and IoT contexts are presented. Honeypots, packet flow analysis, attack identification, and network information presentation. Intrusion detection systems are important for network forensics. Due to cloud computing, regional jurisdiction issues, limited evidence storage, and interoperability must be addressed to maintain evidence integrity. We addressed future directions for this sector's research. This study analyzed honeypots and network traffic, processed high-speed and heterogeneous IoT data, and determined that any solutions provided are forensically sound and acceptable in court.

This research assessed cyberthreats (Jang-Jaccard and Nepal 2014). Because more individuals have internet access, cyberattacks have skyrocketed, often with disastrous and life-threatening results. Malware is the most popular cybercrime weapon because it exploits flaws or uses new technology to its advantage. In cybersecurity, establishing novel, effective anti-malware tactics is a priority. First, they describe the most common hardware, software, and network vulnerabilities. After then, a study of the most cutting-edge mitigation techniques and why they work or fail follows. Then they discuss new attack patterns in social media, cloud computing, smartphones, and critical infrastructure. In conclusion, future study ideas were discussed.

Network security and forensics evidence collecting was suggested (Rughani 2017). Any internet-connected item is susceptible in today's society. Unauthorized network access attempts must be identified for network security and forensics (servers, end-hosts, and so on). In this circumstance, they focus on finding network traffic patterns linked to suspicious behavior. A solution must initially discover aberrant patterns before identifying as many sorts of attacks and malicious behavior as feasible. Our evidence-gathering strategy includes previously established patterns, which boosts detection confidence and reduces false positives. They prove our technique's usefulness by using a dataset with malware and normal traffic. Time-tested traffic was gathered.

A survey on IoT assaults in key infrastructures was conducted (Divakaran et al. 2017). As IoT becomes more intertwined into our lives, cyberattack access points increase. IoT makes Critical Infrastructure (CI) hardware and applications more vulnerable to cyberattacks. Specialists must gain a foothold in the cyber-attack battle zone to protect these systems. These professionals can learn more about the assaults by categorizing the multiple attacks on their systems. This article discusses IoT Critical Infrastructure wireless applications and security. It analyzes threat categorization methods. This can help future researchers choose acceptable classification techniques. Correctly classifying assaults speeds up detection, identification, and recovery. As a result, it's crucial to have a complete view of each system's threat landscape.

Cyberattacks, cybersecurity trends, and developments were analyzed (Staddon, Loscri, and Mitton 2021). Cybersecurity requires current IT facts. Researchers from throughout the world have invented several cyber-defense measures. Various techniques are in development. Cyber security improvements will be studied along with the obstacles, shortcomings, and benefits of the unique approaches in this study. All recent descendant assaults are detailed. Early cyber-security techniques, traditional security frameworks, and their histories are explored. Other topics include contemporary cyber security technical developments and industrial challenges. The IT and cyber security researchers' extensive review should be helpful.

Examining Security Logs to Detect Data Losses (Villa et al. 2021). The researchers detected 20 types of attacks in public datasets and 30 data leakage detection methods. The researchers also identified the 20 most utilized public threat databases. According to the chosen publications, scholars interested in this field of study might take many various approaches. This article examines studies on using security logs to detect abnormalities and data breaches. We derived five strong hypotheses after reviewing 33 studies. Quantity and quality of data used in training and model construction are important since they affect training outcomes. According to our research, it must have precise labels, be updated, have true traffic statistics, and not be anonymised. The PREDICT dataset accounts for all 20 stated features. PREDICT doesn't guard against all assaults, though. The importance of assessments and validations before creating data sets cannot be overstated.

Better network intrusion detection was recommended (Kotecha et al. 2021). A smart network intrusion detection system must have a high detection rate and low false alarm rate to detect irregularities. Models based on older datasets lacked the generalizability to be used to contemporary attacks since they didn't capture the attack schema for current attacks. This analysis uses the UNSW-NB15 Dataset, one of the most complete depictions of recent attacks, to build several models. Our dialogue should end with the model that provides the best outcomes according to a range of assessment measures. Along with modeling, the dataset's features are thoroughly examined. This study uses correlation, variance, and other aspects to create a comprehensive view. Also mentioned are future network intrusion detection technologies, modeling, and dataset creation.

Using particle deep, a deep learning-based network forensic architecture for IoT networks was created (Li and Liu 2021). Internet of Things (IoT) technologies allow household gadgets to be automated and offered real-time services. This wasn't possible before. Despite their lightweight design and low power consumption, their vulnerabilities provide cyber risks that affect their network system. Identifying threat sources and obfuscating and encrypting network traffic complicates safeguarding IoT networks. The Particle Deep Framework (PDF) study shows how to monitor attack activity in IoT networks using digital investigative phases. This was PDF research. The proposed framework uses a Particle Swarm Optimization (PSO) method to dynamically update deep learning parameters and a Deep Neural Network (DNN) based on the PSO algorithm to discover and track anomalies in smart home IoT networks.

Bot-IoT and UNSW NB15 datasets are used to compare the recommended PDF with other deep learning algorithms. The recommended architecture helps discovering and tracing cyberattack occurrences easier, according to testing.

Using supervised machine learning, IoT forensic investigators may do emergent configuration analysis (ECO) (Kebande et al. 2020). Machine learning is a promising technology for mining large datasets and addressing problems, as shown by IoT and other complicated data. In this article, we study whether live digital forensics may be done using classic machine learning methods such as K-Nearest Neighbor, Support Vector Machines, Naive Bayes, and Random Forest. Due to these problems, live forensic analysis in an IoT environment requires an on-the-fly, context-dependent technique. Context-aware systems can do this. We leverage NIST SP 800-86 and supervised machine learning in our conceptual framework. This unique method to Internet of Things forensics has the potential to alter the business, but it must be verified on a wide range of datasets from several applications. Various evaluation factors must be considered. A researcher may want to talk to numerous stakeholders to build assessment scenarios. After our framework's prototypes are produced, these assessment scenarios will use them. This may limit machine learning methodologies, situations, or settings.

Machine learning approaches are recommended for botnet investigation (Koroniotis, Moustafa, and Sitnikova 2020). Digital forensics is used to investigate computer crimes. Botnets make cyberattacks among the most dangerous online. Digitally examining botnet attacks is difficult. Hackers can now create more complex botnet attacks. This type of attack requires improved digital forensics. Machine learning improves botnet attack detection speed and accuracy. Network forensics uses machine learning. Machine learning can detect and prevent botnet attacks. This study discusses botnet attacks and digital forensics. Standardization in botnet detection forensics is needed for court evidence. The study also examines network forensics. Botnet forensics have made little progress. The use of machine learning algorithms to detect Botnets has generated much interest, but the evidence must be presented in court using a defined framework for forensic Botnet detection investigation.

Machine learning improves automated digital forensics (Manzoor 2021). 2021 Manzoor Books, films, pictures, and medical records are increasingly stored digitally. Computers, tablets, smartphones, and wearables are driving this digital data transition and quickly becoming part of our daily lives. Our expansion has made us a target for cybercriminals. Digital inquiry can recover deleted, missing, or hidden files on a suspect's computer. With current government resources and manpower, cybercrime can't be thoroughly investigated. Unfortunately, the methods and processes currently used for digital investigations require a lot of human participation, which slows down the process. Machine learning (ML) is AI's guiding principle (AI). Programming can mimic human behavior in current technology. Digital investigators may benefit from using machine learning and automation throughout the investigation process. This chapter presents machine learning-based digital forensics research.

"How to Effectively Collect and Process Network Data for Intrusion Detection" addressed a research gap in identifying and investigating valuable NetFlow schema features that enable efficient machine learning-based network intrusion detection in the real world. [Cite] (Komisarek et al. 2021). Five flow-based network intrusion detection datasets were used to create a comprehensive and informative flow-based feature collection. The authors' experience installing this type of system reveals that tagged end-user data is essential to apply machine-learning-based intrusion detection in the real world. Both goals require this. This project aims to find the least data needed to train machine learning algorithms for intrusion detection. If given the correct inputs, the final model may work with only ten attributes and minimal data.

The internet of things (iot) is a network of common items equipped with a modest amount of computer power to establish a network forensic mechanism for botnet activities using machine learning techniques. "Iot" stands for internet of things (Koroniotis et al. 2018). This year, botnets affected the

Internet of Things in several cases (IoT). Due to botnets' history of harm and security difficulties, there are no network forensic tools that can identify and monitor today's sophisticated botnet activity. Signature-based commercial solutions can't detect new botnets. Hence. Training and testing an attack definition model with ML is possible. Due to the complexity of investigating botnet trails, these models have a high false alert rate. This study addresses the role of machine learning in building network forensic systems that can monitor suspected botnet activity using network flow IDs. The UNSW-NB15 dataset was used to evaluate machine learning techniques using flow IDs. The systems were able to identify botnet attacks and their traces.

Machine Learning-Based Digital Forensics was investigated (Oladipo et al. 2020). Digital forensics examines video surveillance footage and forensic images, thus object recognition is crucial. In recent years, object class recognition using computational approaches has attracted much attention. This is a popular issue in recent years. The most prominent technique and approach for object identification and recognition is machine learning, which is becoming more popular and provides outstanding system performance. This paper examines the foundations and applications of machine learning in object detection and classification, focusing on digital forensics. Kitchenham's exclusion criteria were used to select the study's candidate papers, which were published between 2007 and 2019. Digital forensic studies were divided into six areas to improve future study, and a convolutional neural network was selected as the most effective machine learning approach for digital forensics.

Pattern-evidence disciplines are subjective, a research on machine learning in forensics found (Carriquiry et al. 2019). Ten years ago, machine learning techniques were created to overcome this problem. CSAFE researchers are paving the path for forensic learning. These researchers are at the forefront of using machine learning to transform how forensic experts assess evidence. No algorithm can examine and understand evidence like a person. Using the right databases and putting them through rigorous testing can help eliminate some of the subjectivity that underlies most forensic disciplines and estimate forensic judgment uncertainty.

Communications Security Establishment and Canadian Institute of Cybersecurity worked together to develop machine learning algorithms for network intrusion detection for current internet traffic using the CSE-CIC-IDS2018 dataset. These algorithms are used to monitor for malicious activity on computer networks (Ilyas and Alharbi 2022). (Ilyas and Alharbi 2022). Only lately did a sizable network traffic trace collection become available, and it comprises many different kinds of assaults. First network intrusion detection systems were developed using KDD Cup'99 data. This was before to the widespread usage of mobile computing, Web 2.0/3.0, as well as social networking, streaming video, and SSL. In light of recent Internet developments, intrusion detection systems must be rethought and redesigned. CSE-CIC-IDS2018 was used to build machine learning classifiers. One of these attributes isn't dataset-invariant. Few researchers have examined whether all available characteristics can be used in datasets with fewer than a few hundred examples of each attack class. This study evaluates the stability and generalization of the classifiers by presenting the average performance during 10-fold cross-validation and the degree of change from one-fold to a further cross-validation step.

Nigeria recently presented a machine learning system for mobile forensics to tackle cybercrime (Goni and Mohammad 2020). Due to Big Data, IoT, and the rise in mobile devices, traditional data mining approaches are no longer viable (the so-called Internet of Things). We designed a machine learning-based mobile forensics system to better identify illicit behavior. Intelligent media towers and satellites were utilized to categorize calls as threats and relay notifications to the Nigerian Communication Commission's forensic lab.

3. Materials and Methods

This study aims to design an appropriate data strategy for detecting network intrusions to analyze cyberthreat detection qualities. This will help the study's principal goal. Along with machine learning algorithms.

3.1 Datasets

Machine learning models are created by collecting data. If the algorithm's training data are high-quality, it can learn to its full potential and be used to its full extent. Malware is linked to many internet crimes. These include spreading worms and viruses, denial-of-service attacks, and hosting hazardous or illegal websites. Kaggle and Mendeley are two important open data sources, say industry experts. UNSW-NB15 1, 2, 3, and 4 are the most common CSV files. This article covers the ISCX Intrusion Detection Evaluation DataSet (UNB ISCX, 2016), the NSL-KDD dataset for identifying user-to-root and remote-to-local attacks, the KDD Cup99 dataset, BoT-IoT, ToN-IoT, CSE-CIC-IDS2018, and UQ-NIDS, and additional intrusion detection datasets. (Sarhan et al. 2021; Komisarek et al. 2021; Sarhan, Layeghy & Portmann 2021; Moustafa and Slay 2015; Koroniotis et al. 2019; Alsaedi et al. 2020; Sarhan, Layeghy et al. 2021; Portmann et al. 2021; Almulla, Iraqi, and Jones 2014).

3.2 Forensics

Forensics is a term that relates to the utilization of scientific methods or processes, and it is defined as "the application of scientific techniques or processes to the process of criminal investigation" by the Oxford Dictionary. "Digital Forensics," or "digital forensics" for short, is a phrase that refers to both the procedures and the technology that are applied in the investigation and prosecution of cybercrime. The word "digital forensics" was first coined in the year 2000. Acquisition, analysis, and presentation are the three procedures that make up forensics, regardless of whether it is digital or conventional. The term "digital forensics," or "digital forensics" for short, is a term that refers to both the methods and technology that are utilized in the investigation and prosecution. When these scientific procedures or tests are utilized in the investigation of digital crimes, the practice is referred to as "Digital Forensics." Both of these classifications are applicable to forensics in some capacity. As a response by law enforcement to the shift of criminal conduct into cyberspace, a new field of study known as "digital forensics" came into being as a term and as an academic discipline. Because cybercriminals exploit technology for their own benefit, law enforcement authorities needed a new strategy to investigate the crimes that are committed online by cybercriminals. The year 1984 marked the beginning of the process by which law enforcement agencies situated all throughout the country, including the FBI laboratory, began creating programs to investigate crimes connected to computers. Specifically, the FBI laboratory was one of the agencies that began this process. In recent years, a large number of inquiry models have surfaced as a direct response to the proliferation of definitions and standards that have been developed over the course of time by a wide range of organizations. These definitions and standards are dispersed throughout a number of different resources that are available to the public. These models are comparable in that they all incorporate the same fundamental procedures, but they were designed to be used in a broad variety of contexts, therefore their applicability varies considerably (Koroniotis, Moustafa, and Sitnikova 2019).

"Cloud forensics" is a subset of digital forensics that focuses specifically on investigating and analyzing incidents that occur inside cloud-based security systems. This subset of digital forensics is often referred to as "cloud-based forensics." Because of the provider's location in Europe, it may be difficult to ascertain which jurisdiction governs the situation at hand because the services are being offered for sale in the United States. This is due to the fact that the provider is based in Europe. When an investigative machine offers its services to several clients, including potential criminals, there is a greater risk that privacy rules may be broken than when the computer works just for one consumer. When conducting an investigation, using an e-discovery tool might lead to an increase in the overall quantity of data that is created throughout the course of the investigation. This could be a result of the increased efficiency with which the tool processes the data. As time goes on, the discipline of forensics that is related to the Internet of Things continues to make consistent strides forward. Conventional methods of digital forensics are challenging to utilize when conducting investigations into incidents that include the Internet of Things (IoT) due to the various nature of the systems and data that are involved in these investigations. This is because of the tremendous quantity of data that is produced in addition to the lightning-fast rate at which it is generated (Stoyanova et al. 2020).

The inspection of the source code of malicious software and the software's reverse engineering are the two key focuses of the area of computer forensics known as malware analysis. Malware analysis is one of the many subfields that fall under the larger umbrella of computer forensics. Malware can be analyzed in a static, dynamic, or coding fashion, depending on the method that is used to examine it. Static analysis is the most common. This distinction is determined based on the kind of analysis that was carried out. In addition to the more conventional approaches, the behavior of malware can also be analyzed with the help of virtual machines, which provide a higher level of protection than the other methods. In recent years, it has become increasingly common for attackers to attempt to evade capture by using logic that is resistant to forensic investigation. This is done in an effort to keep their actions hidden from the investigators who are looking into the matter. Anti-forensics and other measures, which enable malware to alter its behavior in response to the detection of a virtual environment, have led to the rising resistance of infections. This resistance has contributed to the increasing number of successful attacks. Because of this increased resistance, there has been a rise in the number of defenses that are effective against infestations.

3.3 Cyberthreat Detection System

Distributed network intrusion detection and prevention systems, often known as distributed NIDS, are devices that monitor network traffic in a way that is not invasive while it passes through the devices on which they are installed. In order to connect their cyberthreat detection systems to different network media such as Ethernet, FDDI, and others, the various manufacturers of cyberthreat detection systems make use of a wide variety of hardware and software. Two network ports are often included in the design of cyberthreat detection systems as this is the standard. The primary responsibility of the first is close-quarters listening, while the primary roles of the second are command and control as well as information gathering (Kilincer, Ertam, and Sengur 2021).

Because switching isolates unicast conversations to the ingress and egress switch ports, vendors of network infrastructure have developed solutions for port mirroring in order to repeat all network traffic to cyberthreat detection systems. These solutions have been developed since switching was first introduced. The reiteration of all network traffic is accomplished with the help of these technologies. Taps on the network can also be used to deliver traffic to the intrusion detection system if it is configured to do so. In order to do this, Cisco outfits its network devices with Switched Port Analyzer (SPAN) features, whereas other manufacturers of network equipment integrate cyberthreat detection system components directly into the switch. Cisco is the only company that does this. Protection Against Attempts Made to Penetrate a Network Network Intrusion Prevention Systems (NIPS) are proactive protection systems, as opposed to cyberthreat detection systems (CTDS), which are designed to monitor traffic in a passive manner and sound alarms when they identify activity that appears to be suspicious. NIPS are designed to protect against attempts made to penetrate a network. It is standard procedure to immediately insert the NIPS device into the flow of traffic that is being monitored. [Citation needed] The network will only let packets to proceed that either do not match a signature or exceed an abnormality threshold. Both of these conditions must be met for a packet to be considered abnormal. In the case that suspicious packets are discovered, an alarm will be triggered, and the packets will be prohibited from further use (Conrad, Misenar, and Feldman 2017).

NIPS, in contrast to passive monitoring systems for the identification of cyberthreats, is equipped with the ability to actively intervene and put a stop to threats that have already been identified. As a direct result of this, the National Intrusion Prevention System (NIPS) is subject to the identical limitations and downsides as a cyberthreat detection system. A large dependence on static signatures, an inability to evaluate communication that has been encrypted, and issues with extremely fast network speeds are some of these challenges. In the event that a false alarm is triggered, the NIPS has the ability to eliminate communication that is not hostile. This would make false alarms even more detrimental to the system. It is probable that this will have a major impact on the performance of vital systems that are either mission-critical or used in crucial commercial operations. A training phase is required to be completed by the NIPS before it can be given permission to begin blocking any potentially malicious traffic. During this phase, the NIPS is painstakingly calibrated, and during this time, it must not throw away any packets (Pandya 2013).

Traditional security solutions such as anti-virus software and firewalls are unable to provide adequate protection against the increasingly sophisticated harmful attacks that are being conducted against networks and wireless devices. Intrusion detection systems, often known as IDSs, are responsible for monitoring both incoming and outgoing network traffic. The major goal of these systems is to identify illegal network use and misuse. Detection systems for cyberthreats are an inherent need for computer networks that have both high-speed connection and enormous traffic volumes. The current generation of cyberthreat detection technologies is not yet capable of identifying all newly developing dangers in high-speed situations. This is as a result of the fact that the major purpose of flood assaults (UDP, TCP, ICMP, and HTTP) is simply to deliver more data at high rates to systems in an effort to halt or slow down the operation of the system. When dealing with situations that are always changing, this presents a big obstacle. We have constructed a real network that is suited for the purpose in order to demonstrate the limitations of cyberthreat detection systems, such as their propensity to drop packets without first inspecting them and their inability to analyze a large number of packets at a high rate of speed. In order to do this, we have built a network that is suitable for the purpose and has been designed accordingly.

3.4 Machine Learning Models for Cyberthreat Detection Systems

It is vital to explore artificial intelligence (AI), machine learning (ML), and deep learning (DL) in order to identify how they could help to the solution of problems with DF and how they differ from one another. Image recognition, natural language processing, and other activities of a similar nature are some examples of the kinds of labor that have traditionally been carried out by humans. The goal of artificial intelligence is to give machines the ability to perform labor that has traditionally been carried out by humans (AI). It is important to distinguish artificial intelligence from machine learning and intelligent machines. Remember to take note of this distinction. The phrase "artificial intelligence" (AI) refers to anything that can execute human jobs and make such tasks simpler to accomplish for a human operator. Specifically, AI refers to anything that can execute human tasks. As a direct and immediate consequence of the proliferation of artificial intelligence (AI) technology, there has been an increase in the number of criminal acts that have been taking place (Chen 2019).

Intelligent agents are computer programs that are able to learn new things on their own and come to their own conclusions. These agents may also teach other programs new things. The process of intelligent beings connecting with the environment that surrounds them uses intelligent agents as intermediaries. This strategy will be utilized by the agent in order to ascertain the surrounding environment, and after that objective has been reached, the agent will proceed to take action in order to influence the current state of affairs. The gathering of information from various sensors and the subsequent mapping of that information to various actuators are two of the most essential facets of the technology behind artificial intelligence. This is due to the fact that the functions included inside the agents are able to carry out the consequences that were stated previously since these processes are how they are carried out. The goal of research and development in the area of artificial intelligence (AI) is to one day build a computer that is capable of thinking and behaving in the same way that humans do. The only way to effectively accomplish this project, which has the main objective of constructing a model of how the learning process happens in the human brain, is to use learning algorithms. This is the only approach that has been proven to be successful. Technologies that are based on artificial intelligence (AI) have a bright future ahead of them and provide consumers a broad variety of advantages. When these devices are used, it nearly usually leads to the conduct of major felonies like kidnapping and murder (Xu et al. 2021).

Machine Learning is one of the approaches that is applied in Artificial Intelligence (AI), which involves a system that is capable of learning on its own (ML). In addition to reducing the need for manual work and saving time, this technology also has a wide range of applications in the field of artificial intelligence, including the simulation of many aspects of human behavior. As an alternative to programming, which is the method that is most commonly used today, machine learning (ML) might be thought of as a system that learns from prior experiences and examples. To put it another way, the term "machine learning" refers to the capability of a computer system to continually learn and develop judgments not based on the code it executes but rather on the data it consumes. Both Artificial Intelligence (AI) and machine learning (ML) are relatively new technologies that are helping to advance the capabilities of computers and are finding applications in a variety of fields, including industry and research. The acronyms for artificial intelligence and machine learning are "AI" and "ML" correspondingly. The use of autonomous solutions that are founded on machine learning has the potential to be advantageous to a wide range of industries, including engineering, robotics, medical research, and others. Deep learning, for example, is used in the process of image identification in order to discover patterns within pictures by applying machine learning algorithms. This is accomplished through the utilization of deep learning.

3.4.1 Dimensionality Reduction

"Dimension reduction" refers to the act of reducing the number of dimensions that a set of data possesses. Dimensional reduction is required for all parts of statistical analysis, including regression, classification, feature analysis, and visualization. Recently, within the realm of adequate dimension reduction, it has emerged as a topic that is both extensive and topical in scope. This is because of recent developments in the field. In spite of the fact that dimension reduction strategies have been used to address a wide range of data problems, very little attention has been paid to them in the context of survey data analysis. The dimensional reduction model is made up of two parts: the process of selecting features to include and the process of extracting features from the data. Methods for reducing the number of dimensions that range from the most elementary, such as principal component analysis (PCA), to the most sophisticated, such as nonlinear PCA (Davenport et al. 2020).

It is conceivable to think of a dataset as having more than one dimension; when this occurs, the data is referred to as high-dimensional data. For instance, it is usually discovered that vast amounts of components are either the same as one another or are connected to one another. The elimination of incompatibilities such as these is the primary objective of dimension reduction. When referring to a technique that takes use of pre-existing feature parameters in order to lower the overall size of the feature space, the phrase "feature dimensionality reduction" is the appropriate word to use. This method also gets rid of data that is unnecessary or irrelevant, which enables the useful information contained in the initial features to be mapped onto a smaller number of features in a more accurate manner. Another benefit of this method is that it reduces the amount of features that need to be mapped.

We are able to cut down on the total number of characteristics by selecting those features that aren't absolutely necessary to the resolution of the problem at hand. This allows us to pick fewer features overall. Extraction is considered a preprocessing operation when viewed in the context of the feature space. The selection of features is dependent on a wide range of parameters, such as the capability of a feature to increase performance or the capability of another feature to effectively categorize data. On the basis of this premise, it is feasible to remove features from datasets that do not contribute value to the data without having a detrimental influence on the quality of the data as a whole by deleting features from datasets that do not add value to the data. According to the findings of a number of studies, proper feature selection has the potential to improve the efficacy of learning methods by lowering the likelihood of overfitting and simplifying the model that is generated. This can be accomplished by reducing the amount of data that is used to train the model. This has the potential to result in an increase in the effectiveness of the learning process as a whole. As a direct result of this, the elements comprising the input space ought to be simplified until they are reduced to their most elemental forms. This technique of filtering provides feature space projections that reflect subsets of features that are capable of displaying the data in a more realistic manner. In order to accomplish this, a score is allotted to every feature in order to evaluate its potential for discrimination in the learning job.

Embedding methods are those that select features with the assistance of learning predictors, whereas filter methods are those that select features without using a learning predictor. Wrapper methods are those that use learning algorithms as "black boxes" to score a subset of features based on classification effectiveness. These three categories can be used to classify the various feature selection methods.

It is standard procedure for intrusion detection systems to use ANOVA in conjunction with various other statistical methods such as t-tests and genetic algorithms in order to choose the features that will prove to be most helpful for subsequent analysis.

When it comes to the extraction of features, you have the option of using either linear or nonlinear strategies. In order to reduce the dimensionality of high-dimensional data sets, IDS makes use of a number of different methods, such as principal component analysis (PCA), factor analysis, independent component analysis, linear discriminant analysis, and others. Techniques that reduce the dimensionality of the data have taken on a greater level of significance in recent years as a result of the increased volume of data that needs to be analyzed. It is essential to select features using a variety of approaches, and it is also essential to extract features using a variety of approaches.

3.4.2 Classification

After running the typical feature selection or feature extraction models, creating a model, and generating some output in the form of a probability or a class, it is required to evaluate the performance of the model utilizing test datasets. This may be done by running the model on the datasets. Neural networks and support vector machines are two examples of tools that may be utilized to categorize a substantial amount of data points. When it comes to classification, there are many different metrics that can be utilized to compare and contrast the various Machine Learning Algorithms that are available. It is possible to use Log-Loss, accuracy, AUC (Area under the Curve), and other other classification performance indicators. It is also feasible to use measures such as accuracy and recall in conjunction with other metrics when doing an analysis of machine learning algorithms in order to categorize methods that are predominantly utilized by search engines. It is absolutely essential to select the appropriate measures before analyzing the success of your machine learning model. The performance of different machine learning algorithms may be assessed and compared on the basis of the metrics that are used (Tan et al. 2010).

3.4.3 Deep Learning

When it comes to processing data for use in the detection of objects, recognition of voice, translation of languages, and making judgments, deep learning is a function of artificial intelligence that mimics the workings of the human brain. Deep learning can also be used to translate languages. It is conceivable for an artificial intelligence that uses deep learning to learn without the supervision of a person by drawing on material that is both unstructured and unlabeled. Applications of deep learning may be found in a wide variety of fields, ranging from medical technology to autonomous vehicles. Deep learning is being used by researchers in the field of automated driving to recognize things like stop signs and traffic lights. Deep learning also allows for the detection of pedestrians, which helps cut down on the amount of accidents that occur. There is a wide variety of approaches to deep learning. The DL method is considered to be one of the more complex approaches to machine learning. By evaluating a significant quantity of data, it is possible to anticipate and head off problems with cyber security. Artificial Neural Network, Convolutional Neural Networks (CNNs), Long Short-Term Memory Networks (LSTMs), Recurrent Neural Networks (RNNs), Generative Adversarial Networks (GANs), Radial Basis Function Networks (RBFNs), Multilayer Perceptrons (MLPs), Self-Organizing Maps (SOMs), and Deep Belief Networks are all types of neural networks that are created by artificial intelligence (DBNs).

An artificial neural network may be defined as any structure made up of neurons that are linked to one another and exchange information with one another (ANN). For instance, single hidden-layer neural networks are distinguished from deep-learning networks (also known as deep neural networks or DNNs) by their depth. This refers to the high number of node layers through which input is processed in a multistep pattern recognition process.

Techniques for machine learning that are based on deep convolutional neural networks One disadvantage of DNN is that the layers are fully interconnected (i.e., all neurons in adjacent layers are coupled), which might lead to problems in situations when the input space has a large dimensionality. Even with a straightforward design consisting of only one layer, this neuron would be quite challenging to instruct. Overfitting is a possibility because of the significant number of factors at play and the ineffective utilization of full connectivity. On the other hand, CNNs were developed specifically to analyze data that is presented in the form of multiple arrays; as a result, they are able to scale quite effectively when applied to full pictures. Convolutional filters are utilized in order to modify either the input data or the feature maps of the layer that came before it in order to produce output feature maps. An activation function, such as ReLU, is applied to the model's output in order to incorporate nonlinearities into the structure of the model. The max pooling technique, which takes the maximum value of each subregion in the feature map and discards the remainder of the values, is one of the most popular and extensively used algorithms for pooling data.

A recurrent neural network, often known as an RNN, is a sort of neural network. The RNN model architecture boosts the model's dependability by retaining data from earlier inputs. This is accomplished by the use of a feedback loop between the layers. The "depth" of an RNN is solely constrained by the amount of time it takes for new data to arrive. RNNs are incredibly helpful tools for performing analysis on information sequences. One of the most significant drawbacks of RNNs is that their gradients tend to fade and grow with time. Memory blocks are a tool that may be utilized to solve this issue since the LSTM design features connections that occur repeatedly. Memory cells inside each memory block are responsible for storing the temporal states of the network. In addition to that, it possesses gated units, which are used to restrict the flow of data. Utilizing RNN and its variants' effectiveness in managing sequential data enables the construction of cyber-defense systems that may be used to Internet of Things situations (e.g., time series data).

The abbreviation for "Deep Belief Networks." A DBN is a component of a deep-generational model that consists of a visible layer as well as numerous hidden layers of latent variables. Although the units inside each layer are not linked to one another, the layers themselves are interrelated. As a method for the extraction of features, DBNs may be utilized to help reduce the dimensionality of a dataset. On the other hand, a DBN is utilized for classification purposes if class labels are linked to feature vectors. As a consequence of this, DBNs are able to learn high-dimensional representations in addition to being able to do classification tasks. Using an unsupervised greedy learning technique, a DBN may be pre-trained and fine-tuned to learn a similarity representation over a nonlinear, high-dimensional space. This can be accomplished by learning a similarity representation.

Data-driven classification (DDC) is when a DBM is trained with a significant quantity of unlabeled data and then fine-tuned with labeled data. This allows the DBM to function effectively as a classifier. Its construction is built on random decisions, and the generic Boltzmann machine (BM) serves as its inspiration. These decisions determine the on and off states of the many units that make up a network of units. In spite of how easy it is to train the BM algorithm, utilizing it takes a significant amount of time. When a DBM is reduced to having only one hidden layer, this gives rise to the concept of a Restricted Boltzmann Machine (RBM). According to Salakhutdinov, there are a great many benefits that come along with using Deep Boltzmann machines. DBMs, just like DBNs, have the capacity to develop more complex internal representations for the data they process. A further advantage of utilizing large volumes of unlabeled sensory data to develop high-level representations is that only a small quantity of labeled data has to be used to fine-tune the model for a particular activity. This opens up the possibility of more efficient use of the data. As a consequence of this, deep Boltzmann machines are better equipped to handle ambiguous inputs as a result of the incorporation of top-down feedback into the approximation inference process. This is in addition to the first bottom-up pass.

Neural networks are networks that have been trained to replicate their input by employing an intermediary representation that is referred to as an Auto-Encoder (AE) (code). Both RBMs and Auto-Encoders share a similar design, which consists of three layers: an input layer representing the data, a hidden layer representing the code to be learned, and a network of weighted connections connecting the two layers. The input layer represents the data; the hidden layer represents the code to be learned; and the network connects the two layers. In order to reduce the amount of error introduced by the reconstruction process, an additional layer is built on top of the auto-encoder to provide a representation of the original data. This indicates that the weights used in each set are the same. It is also possible to produce useful representations from unlabeled data, which may then be utilized in the construction of deeper networks. When the representation size, also known as the hidden layer, is larger than the input layer, the Auto-Encoder model faces the danger of learning an identity transformation that is both unnecessary and redundant (the so-called over-complete case). It has been demonstrated that the basic model version known as Denoising Auto-Encoders (DAE) is capable of effectively overcoming this potential disadvantage. The fundamental concept is to trick the encoder/decoder system into recreating the clean input by providing it with a tainted version of the original data that it is supposed to process. Because of this very little enhancement, the DAE can now learn effective representations even when presented with an over-complete dataset. AE architectures are able to acquire significant higher-level representations (features) for intrusion detection from the raw traffic data that they receive.

Networks of Generative Adversarial Nodes: GANs are comprised of two primary components: the generating networks and the discriminator networks (i.e., the generator and the discriminator). A new set of data is produced by the generator once it has first learned the distribution from an existing set of data. The discriminator is responsible for determining whether the data that were created by the generators were legitimate or fraudulent. The production of pictures, the alteration of images, the synthesis of images, and the enhancement of their resolution are some of the most typical applications of GAN. It is possible to generate new things with the help of GANs by utilizing the data that is currently available. This design makes it possible to develop adversarial assaults and malware samples, both of which may be used to mislead cyber-defense systems.

Conclusion

This report provides up-to-date information about deep learning-based cyber threat detection systems. This will help new researchers. A rigorous method was used to choose important AI-based cyberthreat detection system articles. AI-based cyberthreat detection performed this selection. The research articles studied in preparation for this analysis deconstructed cyberthreat detection system categorization methodologies. This study found that deep learning-based algorithms can improve cyberthreat detection accuracy and reduce false positives. [Cyberthreat detection] The research contains freely accessible statistics that track evolving trends. Improving model efficacy requires simulating low-frequency assaults in a realistic situation and inventing techniques to reduce model complexity. Future study may focus on developing a simpler deep learning technique and a more effective NIDS detection mechanism. With machine learning-based cyberthreat detection, a novel, lightweight, and efficient approach will be created to recognize network intruders. This approach identifies cybercriminals.

References

Almulla, Sameera, Youssef Iraqi, and Andrew Jones. 2014. “A State-Of-The-Art Review of Cloud Forensics.” *Journal of Digital Forensics, Security* *and Law*. https://doi.org/10.15394/jdfsl.2014.1190.

Alsaedi, Abdullah, Nour Moustafa, Zahir Tari, Abdun Mahmood, and Adna N Anwar. 2020. "TON-IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems." *IEEE Access* 8: 165130–50. https://doi.org/10.1109/ACCESS.2020.3022862.

Ávila, Ricardo, Raphaël Khoury, Richard Khoury, and Fábio Petrillo. 2021. "Use of Security Logs for Data Leak Detection: A Systematic Literature Review." Edited by Flavio Lombardi. *Security and Communication Networks* 2021, no. March: 1–29. https://doi.org/10.1155/2021/6615899.

Carriquiry, Alicia, Heike Hofmann, Xiao Hui Tai, and Susan VanderPlas. 2019. "Machine Learning in Forensic Applications." *Significance* 16, no. 2: 29–35. https://doi.org/10.1111/j.1740-9713.2019.01252.x.

Chen, Qian. 2019. "Toward Realizing Self-Protecting Healthcare Information Systems: Design and Security Challenges." In , 113–49. https://doi.org/10.1016/bs.adcom.2019.02.003.

Conrad, Eric, Seth Misenar, and Joshua Feldman. 2017. "Domain 7." In *Eleventh Hour CISSP®*, 145–83. Elsevier. https://doi.org/10.1016/B978-0-12-811248-9.00007-3.

Davenport, Thomas, Abhijit Guha, Dhruv Grewal, and Timna Bressgott. 2020. "How Artificial Intelligence Will Change the Future of Marketing." *Journal of the Academy of Marketing Science* 48, no. 1: 24–42. https://doi.org/10.1007/s11747-019-00696-0.

Divakaran, Dinil Mon, Kar Wai Fok, Ido Nevat, and Vrizlynn L.L. Thing. 2017. "Evidence Gathering for Network Security and Forensics." *Digital Investigation* 20, no. March: S56–65. https://doi.org/10.1016/j.diin.2017.02.001.

Engel, Daniel, Lars Hüttenberger, and Bernd Hamann. 2012. "A Survey of Dimension Reduction Methods for High-Dimensional Data Analysis and Visualization." *OpenAccess Series in Informatics* 27: 135–49. https://doi.org/10.4230/OASIcs.VLUDS.2011.135.

Goni, Ibrahim, and Murtala Mohammad. 2020. "Machine Learning Approach to Mobile Forensics Framework for Cyber Crime Detection in

Nigeria." *Journal of Computer Science Research* 2, no. 4. https://doi.org/10.30564/jcsr.v2i4.2147.

Hira, Zena M., and Duncan F. Gillies. 2015. "A Review of Feature Selection and Feature Extraction Methods Applied on Microarray Data." *Advances in Bioinformatics* 2015, no. June: 1–13. https://doi.org/10.1155/2015/198363.

Ilyas, Muhammad U., and Soltan Abed Alharbi. 2022. "Machine Learning Approaches to Network Intrusion Detection for Contemporary Internet Traffic." *Computing*, January. https://doi.org/10.1007/s00607-021-01050-5.

Iqbal, Salman, and Soltan Abed Alharbi. 2020. "Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics." In *Digital Forensic Science*. IntechOpen. https://doi.org/10.5772/intechopen.90233.

Janarthanan, T., M. Bagheri, and S. Zargari. 2021. "IoT Forensics: An Overview of the Current Issues and Challenges." In , 223–54. https://doi.org/10.1007/978-3-030-60425-7_10.

Jang-Jaccard, Julian, and Surya Nepal. 2014. "A Survey of Emerging Threats in Cybersecurity." *Journal of Computer and System Sciences* 80, no. 5: 973–93. https://doi.org/10.1016/j.jcss.2014.02.005.

Jia, Weikuan, Meili Sun, Jian Lian, and Sujuan Hou. 2022. "Feature Dimensionality Reduction: A Review." *Complex & Intelligent Systems*, January. https://doi.org/10.1007/s40747-021-00637-x.

Kebande, Victor R., Richard A. Ikuesan, Nickson M. Karie, Sadi Alawadi, Kim-Kwang Raymond Choo, and Arafat Al-Dhaqm. 2020. "Quantifying the Need for Supervised Machine Learning in Conducting Live Forensic Analysis of Emergent Configurations (ECO) in IoT Environments." *Forensic Science International: Reports* 2, no. December: 100122. https://doi.org/10.1016/j.fsir.2020.100122.

Kilincer, Ilhan Firat, Fatih Ertam, and Abdulkadir Sengur. 2021. "Machine Learning Methods for Cyber Security Intrusion Detection: Datasets and Comparative Study." *Computer Networks* 188, no. April: 107840. https://doi.org/10.1016/j.comnet.2021.107840.

Komisarek, Mikołaj, Marek Pawlicki, Rafał Kozik, Witold Hołubowicz, and

Michał Choraś. 2021. “How to Effectively Collect and Process Network Data for Intrusion Detection?” *Entropy* 23, no. 11: 1532. https://doi.org/10.3390/e23111532.

Koroniotis, Nickolaos, Nour Moustafa, and Elena Sitnikova. 2019. “Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions.” *IEEE Access* 7: 61764–85. https://doi.org/10.1109/ACCESS.2019.2916717.

———. 2020. “A New Network Forensic Framework Based on Deep Learning for Internet of Things Networks: A Particle Deep Framework.” *Future Generation Computer Systems* 110, no. September: 91–106. https://doi.org/10.1016/j.future.2020.03.042.

Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Jill Slay. 2018. “Towards Developing Network Forensic Mechanism for Botnet Activities in the IoT Based on Machine Learning Techniques.” *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST* 235: 30–44. https://doi.org/10.1007/978-3-319-90775-8_3.

Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Benjamin Turnbull. 2019. “Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset.” *Future Generation Computer Systems* 100: 779–96. https://doi.org/10.1016/j.future.2019.05.041.

Kotecha, Ketan, Raghav Verma, Prahalad V. Rao, Priyanshu Prasad, Vipul Kumar Mishra, Tapas Badal, Divyansh Jain, Deepak Garg, and Shakti Sharma. 2021. “Enhanced Network Intrusion Detection System.” *Sensors* 21, no. 23: 7835. https://doi.org/10.3390/s21237835.

Li, Yuchong, and Qinghui Liu. 2021. “A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments.” *Energy Reports* 7, no. November: 8176–86. https://doi.org/10.1016/j.egyr.2021.08.126.

Manzoor, Nosheen. 2021. “Role of Machine Learning Techniques in Digital Forensic Investigation Of,” no. February. https://doi.org/10.34218/IJM.12.2.2021.057.

Mauro, M. Di, G. Galatro, G. Fortino, and A. Liotta. 2021. “Supervised

Feature Selection Techniques in Network Intrusion Detection: A Critical Review.” *Engineering Applications of Artificial Intelligence* 101, no. May: 104216. https://doi.org/10.1016/j.engappai.2021.104216.

Moustafa, Nour, and Jill Slay. 2015. “UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set).” *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*. https://doi.org/10.1109/MilCIS.2015.7348942.

Oladipo, Francisca, Emeka Ogbuju, Femi S Alayesanmi, and Abraham E. Musa. 2020. “The State of the Art in Machine Learning-Based Digital Forensics.” *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3668687.

Ometov, Aleksandr, Viktoriia Shubina, Lucie Klus, Justyna Skibińska, Salwa Saafi, Pavel Pascacio, Laura Flueratoru, et al. 2021. “A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges.” *Computer Networks* 193, no. July: 108074. https://doi.org/10.1016/j.comnet.2021.108074.

Pandya, Pramod. 2013. “Local Area Network Security.” In *Computer and Information Security Handbook*, e1–20. Elsevier. https://doi.org/10.1016/B978-0-12-803843-7.00016-8.

Rocha, Jorge, Inês Boavida-Portugal, and Eduardo Gomes. 2017. “Introductory Chapter: Multi-Agent Systems.” In *Multi-Agent Systems*. InTech. https://doi.org/10.5772/intechopen.70241.

Rughani, Parag H. 2017. “ARTIFICIAL INTELLIGENCE BASED DIGITAL FORENSICS FRAMEWORK.” *International Journal of Advanced Research in Computer Science* 8, no. 8: 10–14. https://doi.org/10.26483/ijarcs.v8i8.4571.

Sarhan, Mohanad, Siamak Layeghy, Nour Moustafa, and Marius Portmann. 2021. “NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems.” *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST* 371 LNICST: 117–35. https://doi.org/10.1007/978-3-030-72802-1_9.

Sarhan, Mohanad, Siamak Layeghy, and Marius Portmann. 2021. “Towards a Standard Feature Set for Network Intrusion Detection System Datasets." *Mobile Networks and Applications*. https://doi.org/10.1007/s11036-021-01843-0.

Sarker, Iqbal H. 2021. "Machine Learning: Algorithms, Real-World Applications and Research Directions." *SN Computer Science* 2, no. 3: 160. https://doi.org/10.1007/s42979-021-00592-x.

Staddon, Edward, Valeria Loscri, and Nathalie Mitton. 2021. "Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey." *Applied Sciences* 11, no. 16: 7228. https://doi.org/10.3390/app11167228.

Stoyanova, Maria, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis. 2020. "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues." *IEEE Communications Surveys and Tutorials* 22, no. 2: 1191–1221. https://doi.org/10.1109/COMST.2019.2962586.

Tan, Zhiyuan, Aruna Jamdagni, Xiangjian He, and Priyadarsi Nanda. 2010. "Network Intrusion Detection Based on LDA for Payload Feature Selection." In *2010 IEEE Globecom Workshops*, 1545–49. IEEE. https://doi.org/10.1109/GLOCOMW.2010.5700198.

Thampi, Sabu M., Gregorio Martinez Perez, Ryan Ko, and Danda B. Rawat, eds. 2020. *Security in Computing and Communications*. Vol. 1208. Communications in Computer and Information Science. Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-4825-3.

Xu, Yongjun, Xin Liu, Xin Cao, Changping Huang, Enke Liu, Sen Qian, Xingchen Liu, et al. 2021. "Artificial Intelligence: A Powerful Paradigm for Scientific Research." *The Innovation* 2, no. 4: 100179. https://doi.org/10.1016/j.xinn.2021.100179.