Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(REVIEW ARTICLE)

Check for updates

Assessment of existing cyber-attack detection models for web-based systems

Odiaga Gloria Awuor *

Jaramogi Oginga Odinga, University of Science and Technology, Kenya.

Global Journal of Engineering and Technology Advances, 2023, 15(01), 070–089

Publication history: Received on 06March 2023; revised on 19 April 2023; accepted on 21 April 2023

Article DOI: https://doi.org/10.30574/gjeta.2023.15.1.0075

Abstract

In the current technological environment, different entities engage in intricate cyber security approaches in order to counter damages and disruptions in web-based systems. The design of the security protocols relies on the guarantee that attacks are prevented in the web-based systems. Prevention and detection using techniques such as access control tools, encryption and firewalls present limitations in the full protection of web-based systems. Furthermore, despite the sophistication of current systems, there are still shortfalls in high false positive and false negative threat detection rates, which is attributed to poor adaptation by systems and networks to the changing threats and behavior of cyber-criminals. In this perspective, this survey paper discusses the existing cyber-attack detection models, and recommends the cyber-attack detection models and techniques that are appropriate for web-based systems. It is evident that deep learning techniques offer better performance and robustness compared to traditional machine learning techniques and other non-artificial intelligence-based techniques. Deep learning techniques learn and extract features automatically without human intervention and can also handle big and multidimensional data more conventionally than the other techniques.

Keywords: Cyber-Attack; Web-Based Systems; Detection Models; Machine Learning; Deep Learning

1. Introduction

Cyber-attacks are delineated as forms of maneuvers which groups or individuals offensively employ, targeting computer systems, infrastructure, networks or personal devices for malicious outcomes [1], [2], [3]. Characteristically, cyber-attacks are anonymous and target susceptible networks and systems to either alter, steal or destroy their targets [4], [5], [6]. There are different contexts regarding cyber-attacks, which are also referred to as cyber terrorism, cyber warfare and cyber campaigns. Cyber-attacks may differ from simple installation of software on a system or a network to destroying the network in its entirety [7].

Information security and cyber-attacks have been the primary focus of researchers, with the main aim being the allocation of resources to detect and prevent attacks on networks and systems [8], [9]. Many organizations have become vulnerable as a result of easily available and accessible nature of the Internet and are as a result, a high potential attraction for cyber-security threats [10]. Therefore, it has become pertinent that information and transactions be safeguarded and secured through various techniques such as firewalls, authentication, encryption, CADSs (Cyber Attack Detection Systems) and other software and hardware solutions.

The contributions of this paper are as follows:

- Presentation of the common forms of cyber-attacks on web-based systems
- Discussion of the existing cyber-security solutions as Artificial Intelligence (AI) based and non- AI based techniques

*Corresponding author: Odiaga Gloria Awuor

Copyright © 2023 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

- Identification of the research gaps and intervention areas as refers to techniques employed in detection of cyber-attacks in web-based systems

The rest of the paper is organized as follows: Section 2 looks at the common forms of attacks on web-based systems. Section 3 discusses the existing cyber-security solutions which are characterized as either Artificial Intelligence (AI) based or Non-AI based techniques. Section 4 presents the identified research gaps. Section 5 provides the conclusion and direction for further research.

1.1. Common Forms of Cyber Attacks in Web-Based Systems

In the execution of a cyber-attack, various repeated stages are involved. Therefore, basically the various forms of attacks and the stages through which the attack is executed need to be understood if protection from intended attacks is to be successful [11], [12], [13], [14]. Broadly, there are two categories of attacks, untargeted and targeted. In a targeted attack, attackers are concerned with specific organizations, with the aim of causing more damage compared to an untargeted attack. Examples of targeted attacks include botnets and phishing. Alternately, untargeted attacks involve attackers targeting a wide array of users and devices, taking advantage of the internet's openness. In this case, examples of such attacks also include scanning, ransomware and phishing [15], [16], [17], [18], [19], [20], [21]. There are various forms of cyber-attacks such as are described:

1.2. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

DoS attacks are primarily aimed at overrunning resources of systems and networks such that requests of service are not answered [22]-[25]. Host machines are affected by software controlled by cyber-criminals in the instance of a DDoS attack. Resources are thus rendered unavailable to users as the host service which is linked to the internet is disturbed [26]. Specifically, DoS and DDoS attacks include botnets, ping of death, smurf attacks, Transmission Control Protocol Finish (TCP FIN) flood attacks and teardrop attacks [27], [28]. Prevention of DoS attacks is quite difficult due to the challenge of differentiating between valid ad invalid threats from the requests in the system's or network's traffic [29]. This is because the same protocol and port is used in making the requests. Protection of the system from DoS attacks needs the network to have DDoS, IDS protection. Bandwidth surplus is also instrumental for organizations, as it protects the organization against DDoS attacks that are executed on the low scale [30].

1.3. Man-in- the-middle (MitM) Attacks

MitM attacks occur when third parties disturb communications between servers and clients [31], [32], [33]. Information is gained by the attacker impersonating both the server and client, hence the threat is that the attacker is able to capture, receive and sent information that is intended for another person on the network [34], [35]. In this attack, real time operations of information exchange, transactional operations and communication are interfered with [36]. Different types of attacks in this case are spoofing of IP and hijacking of sessions on the network [37], [38], [39]. Systems to detect intrusions may be implemented to prevent this level of attack as they give alerts when intrusions are executed. Additionally, VPNs are also instrumental in preventing such attacks as they help in creating more layers of security when confidential layers of the company's network are accessed, especially when done through wireless connections [40], [41], [42].

1.4. Drive by Download

This is a common form of cyber-attack which is used in spreading malware to gain access to the system. The system gets infected just by users visiting specific websites [43], [44], [45]. Attackers are known to use valid websites and injecting malware into them which may include links, iFrames, JavaScript codes, cross site scripts and redirects [46]. Malicious code is injected into the browser when users visit infected pages, which then scans the system for vulnerabilities [47], [48]. This form of attack is prevented by regular scanning of the system, removing unwanted plug-ins and software, using web filters and firewalls. System access can also be separated with different accounts, with one account being for regular users and the other account restricted by administrator privileges [49].

1.5. Password Attacks

Passwords are the common approach of user authentication in prevention of attacks. However, passwords can be decrypted or obtained by attackers simply by accessing databases and network sniffing [50], [51]. Cracking software, sniffers are different approaches implemented by attackers [52]. Prevention can however be achieved by making regular password changes and adding complexity to the password patterns [53]. Brute force is also a method that attackers implement in obtaining passwords. This involves the attackers trying out different passwords in the hope that they will succeed to gain entry to the system or network [54], [55].

1.6. Structured Query Language (SQL) Injection

SQL attack is a method where the attacker uses malicious cod to gain access to information by backend database manipulation [56]. Information attackers target may be details of the targeted organization, details of the company's customers or users of the company's systems and networks which results to illegitimate viewership of sensitive information, deletion or modification [57], [58], [59]. SQL injections can be prevented by implementing input validation which would flag unlawful input. However, this approach is considered unsuitable as input mapping is infeasible. Due to this challenge, firewalls are adopted to remove SQL injections [60]. IP reputation, recognition of signatures can also be used in identifying and blocking SQL injections, their advantage being that they do not have a high outcome of false positives [61].

1.7. Cross Site Scripting (XSS)

A popular injection attack is XSS which injects malicious code into valid sites or in web applications [62], [63], [64]. This form of attack occurs when attackers insert JavaScript or code into the databases of websites, which makes users to download them. Upon the victim executing the script, their cookies are accessed by the attacker [65], [66]. Forms of XSS attacks are persistent, reflected and Document Object Model (DOM) based. The persistent form of the attack, the code arises from the database of infected websites, in the reflected form of the attack, the code arises with the request executed by the user and in the DOM based form the threat is primarily on the user's end rather than on the server's end. XSS attacks are preventable by validation and encoding techniques [67].

1.8. Eavesdropping

This form of attack is also identified by other delineations such as snooping or sniffing [68]. Attackers primarily hack data on digital devices using insecure networks to receive and send data. It is characterized by the fact that it doesn't show abnormalities in transmission operations hence detection is quite difficult [69]. Attackers using this method aim to access private and sensitive information such as credit card numbers and passwords passed across networks. Sniffers could be introduced to carry out this attack and seize transmitted data [70], [71]. Eavesdropping is broadly categorized into two; active and passive eavesdropping. In the passive method, the attacker listens to network transmissions to gain access to data, while in the active method, the attacker poses as a unit in the network that wouldn't be flagged by users [72]. Prevention of this attack is achieved through anti-virus programs, implementing firewalls, using VPNs, encryption and not transmitting private data on public networks [73].

1.9. Phishing

This kind of attack involves attackers fraudulently sending emails whose origins seem to be from valid sources [74]. The aim of this attack is to gain credential and personal data [75], [76].Phishing is a social engineering attack as the emails contain hyperlinks embedded which release malware into the network of system, or sometimes leads users to websites that release malware into the network [77] , [78]. Common forms of phishing attacks are pharming, whaling and spear phishing [79]. Prevention of these attacks requires users to analyze emails received and implementing sandboxing in cases where they come across suspected links and emails [80].Table 1 below provides a summary of the common attacks in web-based systems.

Table 1 Summary of common attacks in web-based systems

Author (s)	Identified attack (s)
[20] - [24]	Denial of Service (DoS) and Distributed Denial of Service (DDoS)
[25] - [30]	Man in the Middle (MitM)
[31] - [34]	Drive by Download
[35] - [38]	Password attacks
[39] - [42]	SQL Injection
[5], [43] - [44]	Cross Site Scripting (XSS)
[45] – [49]	Eavesdropping
[2], [6], [50] – [52]	Phishing

2. Cyber-Attack Detection Techniques

Cyber-attack detection techniques can be broadly categorized into two: AI based and non-AI based techniques.

2.1. Common Non- Artificial Intelligence Based Techniques

According to [81], with various cyber-attack detection systems in existence, security engineers and managers have to pinpoint packets of attack in the network mostly through detecting signatures, for instance a CADS identifies packets that have been attacked by recognizing identifiable signatures and fingerprints as they cross the gateway threshold of the network.

Recent surveys in [82], [83], [84], [85] have concluded that cyber-attacks have been increasing annually and that despite the implementation of security guidelines and strategies such as firewalls and their capacity to practically protect against threats, they are still imperfect and also vulnerable [86]. Similarly, the surveys in [87], [88] have also established that on a monthly basis, several attempts are made by assailants for purposes of gaining entry and access to systems. Therefore such, cyber-attack detection mechanisms need to be given more emphasis across the variety of systems and networks [89]. According to [90], the commercial and political environment is currently rife with engagement in cyber-warfare, purposely aimed at damaging, disrupting or censoring content and information in networks. The design of strategies and protocols [91] in networks calls for high levels of reliability to protect from intrusion by attackers who would take control or throw the network into disarray [92], [93]. A network intrusion has two main outcomes, passive attacks or active attacks. Passive attacks in this case include non-participation and eavesdropping, whereas active attacks include forging, jamming, corruption and message dropping, which are the major concerns for cyber security engineers [94].

The detection of network intrusion is a procedure whereby events in a network or system are monitored dynamically, analyzed for any incidents and signs and thereafter unauthorized access is interdicted [95], [96]. In this procedure, information is automatically collected from myriad network and system sources and analyzed for possibilities of security concerns. For web-based systems, security and protection against attacks is a primary question, the reason being that, there is a significant growth in networks and the wide array of applications by both groups and individuals, in systems that are either for commercial or individual use [97]. In large networks, cyber-attacks pose heavy losses. Solutions such as firewalls, data encryption and authentication are insufficient to counter threats due to the ever-changing threats. For instance, whereas firewalls control network access, they fall short in providing signals in the event of an attack [98]. Therefore, it is pertinent that systems such as IDS (Intrusion Detection System) be adopted [99]. An IDS detects network infectiousness and policy violations. Threats are identified and abnormalities in the network are flagged, such as DoS (Denial of Service) attacks. It also locates, decides and controls unauthorized behavior in the network [100], [101], [102]. However, IDSs also have to deal with various challenges for instance uneven distribution of data, high volumes in traffic, decision difficulties between boundaries of abnormal and normal behavior and a necessity for adaptability to a dynamic environment [103], [104]. Overall, the main challenge is efficacy in capturing and classifying different behaviors in a network or a system.

Threat classification strategies are categorized into two; anomaly and misuse detection. In misuse detection, the techniques applied examine activities in the system and in the network, checking for misuse instances using matching signatures, hence they are effective techniques for detecting attacks which are known already [105], [106]. However, the shortcoming is that with the reliance on “known” attacks, new attacks are missed, leading to false negatives [107]. The IDS may generate alerts but the system may be rendered unstable due to the resources [108] and time needed to react to every single alert. Empirical evidence suggests that overcoming this problem needs IDS to delay procedures of elimination and only act on elimination when enough correlated information has been collected to support the decision, rather than making the decision upon detecting an initial symptom [109]. The researchers in [90] add that in the ever-changing scope of cyber security, it is challenging to justify or quantify the elucidations why the impact of cyber security is outsized. Allowing threats to take control anyhow, anytime and anywhere regardless of the context is by far unacceptable and would undoubtedly lead to irredeemable harm. This follows the consideration that consumers use the internet and information about companies in a way that cyber security finds it had to contain and shield. Cyber security is necessary not only for companies, political and social establishments, but also for families so long as their operations are carried out within the global network [110].

Currently, the technological infrastructure with high networks and systems, is collecting significant data amounts and analytics which are instrumental for critical cyber security systems [111]. Majority of threat detection systems focus on surface attacks, such as firewalls, whose protection is medial and doesn’t account for lateral threats that infiltrate networks, remaining unseen [112], [113].The studies in [114], [115], [116] have established that only about 20% of

threats are medial. Upon detection of an intrusive activity, the Intrusion Detection System (IDS) reports the intrusion to a SIEM (Security Information and Event Management) system where determination of valid threats is carried out amidst every other alarm, false or not [117. However, with much time spent in threat determination, there is a window for more damage to be perpetrated on the system or network because whereas IDSs are instrumental in network monitoring, the significance of their implementation relies on what is done with the information they generate, which means that they do not necessarily resolve security issues hence cannot add security layers unless appropriate policies to stop the identified threats are administered [118].

The necessity of a more reliable cyber security system than IDSs is cemented by the fact that encrypted packets [119] are unseen by IDSs, hence these violations will not be registered earlier on in the process of intrusion, only to be realized when they have penetrated the network much deeply [120]. Subsequently, attackers mainly use them as the pathway to enter systems and networks [121]. Essentially, in such cases, the systems and networks are vulnerable until the issue is resolved. Coupled with the fact that data security relies heavily on encryption, this is a cause of concern for cyber security. The researchers in [122] posit that another issue is the prevalent false positive alerts associated with IDSs instead of actual alerts. It has been suggested that the problem of false positives can be solved by tuning the IDS to reduce the frequency of false positives, which would reduce the percentage of real threats slipping through the system or the network.

2.2. Artificial Intelligence Based Techniques

Recently, artificial intelligence (AI) techniques have significantly influenced the development and application of cyber security in different systems and networks. There are various AI techniques but the most prevalent use of AI in cyber-security is from the machine learning (ML) perspective. Considering that it is difficult to control exactly where, when and how cyber-attacks may occur, and there is not guarantee for total prevention, early detection seems to be the best approach to counter risks whose damage may be irreparable. An ideal outcome would be for organizations to either utilize solutions already existing or develop their own solutions for cyber-attack detection where the need for human intervention is minimized. The authors in [123] posit that in the last decade, various ML (Machine Learning) techniques [124] have been implemented to detect system and network intrusion to improve detection rates and to keep their knowledge base comprehensive and up to date. Nevertheless, various techniques have been adopted in issues of threat detection, and with improvements in cyber systems, adaptability is the key characteristic of cyber systems [125]. Literature surmises that with ML, it is possible that the scope of cyber security can be advanced [126].

2.2.1. Traditional Machine Learning Techniques

ML techniques are being applied to improve cyber security and early detection of several automated and new attacks and in phishing detection [127]. In detection of cyber-attacks, ML is a predominant approach that utilizes AI, has an auto-learning capacity and is precise in its learning outcomes. ML algorithms use existing techniques of classification and computations with improvement projects and datasets to provide responses to issues and enhance proficiency [128], [129]. Well-known methods of learning begin with data insights, recognizing data models and progressively making decisions, and utilizing recent models to come up with future implementation. The aim of auto-learning is to give computers the capacity of adjusting without relying on help or affiliation from humans. In ML algorithms, large data proportions are inspected rapidly, giving precise results. The survey in [130] found that most of the proposed methods are realized through transformation of the basic AI methods. In their survey, 24% of the cyber-attack detection methods discussed, used Convolutional Neural Network (CNN), 15% of the methods used Support Vector Machine (SVM), and 12% of the methods used Artificial neural networks (ANN). These models can achieve high accuracy but, with unknown events, the model accuracy may require substantiation which may also point to skeptical decision-making process.ML models also have a high demand for data, without which they may not make timely conclusions in case of an attack [130].

ML algorithms depending on the methodology applied can be classified as supervised, unsupervised, reinforcement and semi-supervised techniques. Supervised ML algorithms characterize labeled data by using classification tasks. The targeted labels or classes are already known for the data, and those labels and classes are used to learn for the computations, e.g. classification and regression [127]. The algorithms contain predicted dependent data from predefined non-dependent data set. This form of ML is primarily used for classification and regression tasks [131]-[136]. In the unsupervised algorithm, any outcome/target or dependent factors are not adopted in the ML prediction. Unlabeled data is used to train computers. Further, it is used to cluster data and group them differently. The primary application of unsupervised algorithms is pattern detection and descriptive modeling [137], [138], [139], [140]. In unsupervised ML, the targeted value is not already known and the focus is on establishing the relationships by finding patterns among data for instance, clustering. In semi-supervised ML, part of the data is labeled or may require human expertise during data acquisition [127]. In reinforcement learning there is input to the algorithms, against any incorrect

predictions, however, the algorithm is not instructed on how to correct it but figures out by trying out several possibilities until it learns the correct response hence more of a reward and penalty technique [127]. Semi-supervised algorithm uses the benefits of both unsupervised and supervised algorithms, involving non-named and marked data respective to circumstances and issues [141], [142], [143], [144], [145]. This algorithm exploits the probability that despite the non-named characteristic of data, the data still has critical information

ML algorithms are implemented in training and detecting the occurrence of cyber-attacks [146], [147]. Upon detection of an attack, notifications can be relayed to users or engineers, upon which algorithms can classify whether the threat is a DDoS/DoS threat or not [148]. An example of such an algorithm is the SVM (Support Vector Machine), a supervised learning approach with which data is analyzed and patterns are recognized [149]. SVM is the most used ML technique for cyber security [127]. SVM needs training at different time intervals for better results to learn the dynamic user's behavior and the kernel function and parameters can also affect its performance. Decision Tree (DT) is a supervised ML technique that is based on recursive tree-structure and comprises of a root or intermediate node, path and leaf node. Classification and Regression Tree (CART), C4.5, and Iterative Dichotomiser 3 (ID3) are considered as essential DT algorithms [127]. ID3 works based on a greedy approach but, cannot handle numeric attributes. C4.5 is an improvement of ID3 that overcomes the limitations of ID3 by taking care of over-fitting using tree pruning where branches in a DT that do not significantly contribute to the overall decision-making procedure are removed.

DT, K-nearest neighbors (KNN), Multi-Layer Perceptron (MLP), and SVM were applied to detect intrusion on mobile devices with DT outperforming with an accuracy of 97.04%[127]. According to [105], the most commonly used ML techniques are Random Forest (RF), DT, and KNN. They reviewed learning techniques using different types of cyber-attacks, such as DoS, distributed denial-of-service (DDoS), probing, user-to-root (U2R), remote to-local (R2L), botnet attack, spoofing, and MitM attacks. In KNN an unknown class is able to identify its neighboring classes and ultimately it can also estimate its own class. Random forest (RF) is an ensemble learning technique with multiple decision trees operating together, with different samples of the dataset. Each tree individually provides a class, and the class with most votes becomes the final class prediction [105]. Researchers in [140] proposed a network threat situation assessment (NTSA) model through unsupervised models, that use unlabeled data in the detection of threats in IoT systems. The model performed better than the traditional supervised based model that use labeled data to detect cyber threats.

The researchers in [134] proposed a supervised ML technique by using RF classifier for a uniform detection system. They achieved a 99.9 % accuracy in intrusion detection with reduced amount of time and energy in learning and prediction capability. Researchers in [135] developed a multi-layer security monitoring system called IoTArgos to address the security challenges of IoT systems in smart homes by extracting data communication features and developing a supervised learning method for classifying intrusion activities. For potential zero-day or unknown attacks, it integrates unsupervised learning algorithms to discover unusual or behaviors in smart home IoT systems. It had a precision of 0.9876 and a recall of 0.9763. Authors in [136] performed various supervised feature selection methods and employed three classifiers Support Vector Classifier (SVC), Random Forest, and eXtreme Gradient Boosting (XGBoost) on IoT network data which predicted malicious network traffic with high accuracy. They also compared feature selection methods to arrive at the best that can be used for network intrusion prediction. They also noted that performance of supervised learning depends on the quality of data used for training and the features that are selected. Feature selection measures must therefore, be chosen cautiously as they significantly determine attack predictions. In their study, XGBoost gave the highest accuracy of above 99% regardless of the feature selection method that was applied.

The researchers in [129] evaluated the performance of various supervised ML algorithms in detecting SYN-DoS attacks, on IoT systems using the Apache Spark Machine Learning Library (MLlib) andgenerated99% accuracy with RF. They also achieved short training and application times with the Apache Spark. They proposed a hybrid approach for the detection of SYN-DoS attacks specifically with RF model implemented on IoT devices directly, and second level analysis or training done in a cloud setup. The researchers in [150] also tested four algorithms of Apache Spark MLlib, namely, SVM, Naïve Bayes, Decision Tree and Random Forest, on UNSW-NB15 dataset. Random Forest had the best performance with an accuracy of 97.5%. A very similar result for RF was archived in [151]. They evaluated the performance of four classification algorithms SVM, Naïve Bayes, Decision Tree and Random Forest using Apache Spark on the UNSW-NB15 dataset for network intrusion detection.

ML models can detect up to 98% of attacks [152]. For instance, most ML based [153] phishing detection approaches extract features from the URL, search engine, third-party, web traffic, DNS (domain name system), etc. [154]. According to [155], ML techniques differ in terms of, the type and number of features extracted; algorithms used to identify best feature sets and assign weights; type and number of ML or classification algorithms applied to these features; use of optimization algorithms, and use of logic from other anti-phishing techniques. These features play an important role in

designing a system which can recognize a phishing website such as the hypertext mark-up language (HTML) based, JavaScript based, address bar based, domain-based features among others. Table 2 presents some of the conventional machine learning techniques for attack detection.

Table 2 Traditional ML techniques for cyber-attack detection

Algorithm/Technique	Accuracy/Performance/Significance	Challenge	Author
24% of the methods used CNN, 15% used SVM, and 12% used ANN	High accuracy	The model accuracy may require substantiation with unknown events which may also point to skeptical decision-making process	Zhang et al. [130]
SVM, DT, KNN, MLP	SVM commonly used algorithm in the survey DT outperformed other three with 97.04% accuracy	SVM needs training at different time intervals for better results to learn the dynamic user's behavior Kernel function and parameters can also affect SVM performance	Shaukat, et al. [127]
DT Algorithms; CART, C4.5, and ID3	High accuracy	Over-fitting data but can be sorted through pruning as in C4.5	Shaukat, et al. [127]
RF, DT and KNN	Commonly used algorithm is RF	Semi-supervised and reinforcement learning methods have not been well explored for malicious attack detection in IoT systems	Inayat et al. [105]
Network threat situation assessment (NTSA) model through unsupervised models	Model performed better than traditional supervised models	-	Yang et al. [140]
RF classifier for a uniform detection system	99.9 % accuracy in intrusion detection with reduced time and energy in learning and prediction capability	RF has higher computational costs	Rani et al. [134]
Multi-layer security monitoring system called IoTArgos with supervised learning method for classifying intrusion activities	Precision of 0.9876 and a recall of 0.9763 Integrates unsupervised learning algorithms for potential unknown attacks	-	Wan et al. [135]
Supervised feature selection methods and three classifiers SVC, RF, and XGBooston IoT network data	XGBoost gave the highest accuracy of above 99% regardless of the feature selection method applied.	-	Krishnan et al. [136]
Evaluation of performance of various supervised ML algorithms in detecting SYN-DoS attacks using Apache Spark MLlib	99% accuracy with RF Proposed hybrid approach of RF and training in a cloud environment	-	Morfino et al. [129]
Tested four algorithms of Apache Spark MLlib, namely, SVM, Naïve Bayes, DT and RF	RF had the best accuracy of 97.5%.	-	Othman et al. [150]

Evaluated performance of four classification algorithms; SVM, Naïve Bayes, DT and RF using Apache Spark for network intrusion detection	RF had highest accuracy	-	Belouch et al. [151]

2.2.2. Deep Learning (DL) techniques

DL is a branch of ML that is a potential and efficient solution for cyber-attack detection. According to [156], an efficient DL model can give a better performance than the other detection methods. DL provides new techniques for cyber security and has shown significant improvements over traditional ML techniques [157], [158], [l59]. Popular approaches in the scope of DL are boost algorithms [160] and deep belief network (DBN). DBN is a commonly used algorithm consisting of an input layer (visible) and multiple latent components (hidden). Therefore, the algorithm is layered and works as such. The first visible layer sends data to the first hidden layer, processing it. Since there are multiple hidden layers, each subsequent layer treats the previous hidden layer as an input layer and the process is repeated until the output is shown at the last layer [161],[162],[163], [164].They are a class of Deep Neural Networks (DNNs) composed of multiple layers of hidden units with connections between layers but not between units in each layer [165], [166], [167], [168]. DBNs are trained in an unsupervised manner by adjusting weights in each hidden layer individually to reconstruct the input. DBN simulates the human brain to process complex data and recognize complex patterns and can be referred to as a stack of Restricted Boltzmann Machine (RBM) with an essential generative nature. However, unlike RBM, in DBN, there is no node to node communication within the same layer of the network. Each node of the DBN is connected with all the previous and next layer nodes DBN takes input in the form of probabilities and each layer needs to learn complete input to generate output. Each layer keeps generating optimal choices at each step and this is repeated until the training stage is completed to a desired level [127].

Researchers in [169] proposed an intrusion detection approach based on improved DBN and achieved 96.17% and 86.49% classification accuracy and False Positive Rate (FPR), respectively, a significant improvement compared with other IDS approaches. However, this was not implemented in a real and complex network setup. According to the survey in [165], performance of DL techniques; Convolutional Neural Network (CNNs), Recurrent Neural Networks (RNNs), and Generative Adversarial Networks (GANs) varied greatly across different security domains. DL techniques appeared to have the most consistent performance for identifying malicious domain names generated by Domain Generation Algorithms (DGAs), where True Positive Rate (TPR) varied between 96.01% and 99.86%, FPR ranged between 1%and 1.95%, while accuracy ranged between 0.9959 and 0.9969 [165]. In contrast, performance of DL techniques for detection of network intrusion had a broader performance range with TPR between 92.33% and 100%,FPR between 1.58% and 2.3%, and accuracy between 44% and 99%.

RNNs handle variable lengths of inputs and processes the inputs one element at a time, using output of the hidden units as additional input for the next element. Therefore, RNNs can address speech and language problems as well as time series problems [165]. CNN is a neural network meant to process input stored in arrays such as an image, which is ideally a two-dimensional (2D) array of pixels. CNNs are typically used with spatial or temporal ordering and consists of three layers: convolution layers, pooling layers, and classification layer [165], [170], [171], [172]. The authors in [173] proposed a framework for DL techniques in cyber-security, and analyzed CNN, RNN, and DNN. The results showed that the CNN model provided the highest accuracy at 98.64% with a precision of 98% with a binary class, followed by RNN model that offered an accuracy of 97.75%. Also, the CNN model provided the highest accuracy of 98.42% with a multiclass class.

On the other, the researchers in [174] developed an ensemble of deep RNN for detecting IoT cyber-attacks [175] using network traffic. They integrated a set of Long-Short-Term-Memory (LSTM) modules into an ensemble of detectors and the modules were merged using a DT to achieve a final aggregated output. An accuracy rate of over 99% in detection of cyber-attacks for IoT devices was obtained. Table 3 gives a summary of the deep learning techniques for attacks detection.

It is evident that the CNN gives the highest accuracy in DL while in traditional ML techniques, RF which is an ensemble of DTs yields the highest accuracy. Common issues for most DL algorithms are manual parameter tuning, longer training time, and detection accuracy issues [176]. ML provides high accuracy and low FPR but DL models, unlike ML models, can learn and extract features automatically without human intervention. This, therefore, eliminates the need for manual feature extraction and selection and third-party services dependency. In the current big data era, manual feature engineering in ML models may fail to deal with multi-dimensional and larger datasets. DL techniques, however, can handle big data and are potentially powerful in the cyber-attack detection sphere that evidently requires more attention

in the cyber-security domain especially in web-based systems. Table 4 presents a comparison of the conventional and deep learning attack detection techniques.

Table 3 DL techniques for cyber-attack detection

Algorithm/Technique	Accuracy/Performance/Significance	Challenge	Author
DBN for intrusion detection system (IDS)	96.17% and 86.49% classification accuracy and False Positive Rate (FPR) respectively	Not implemented in a real and complex network setup Higher hardware resource and time consumption due to additional layers	Tian et al. [169]
CNNs, RNNs, and GANs in identifying malicious domain names generated by DGAs	Accuracy range of 99.59%to 99.69% TPR varied between 96.01% and 99.86% FPR ranged between 1%and 1.95%	Performance of DL techniques varied greatly across different security domains	Berman et al. [165]
CNNs, RNNs, and GANs for detection of network intrusion	TPR between 92.33% and 100% FPR between 1.58% and 2.3% Accuracy between 44% and 99%.	Broader performance range	Berman et al. [165]
CNN, RNN and DNN	CNN highest accuracy at 98.64%	CNN requires more convolutional layers and larger datasets for proper functioning. RNN may face short term memory issues and is difficult in training and vanishing and exploding gradient problems	Barik et al. [173]
Ensemble of deep RNN for detecting IoT cyber-attacks using network traffic	Long-Short-Term-Memory (LSTM) modules with accuracy of over 99% achieved	-	Saharkhizan et al. [174]

Table 4 Comparison of traditional ML and DL cyber-attack detection techniques

Cyber-attack detection	General Strengths	General Weaknesses
Traditional ML techniques	high accuracy low false positive rates	need for manual feature extraction and selection, and third-party services dependency
DL techniques	learn and extract features automatically without human intervention can handle big and multidimensional data	manual parameter tuning, longer training time, detection accuracy issues

3. Research Gaps

Majority of cyber-attack detection and prevention methods implemented in current systems are inadequate in dealing with the dynamism and complexity of cyber-attacks [177]-[184]. Therefore, it is necessary for the adaptive AI based techniques provided by ML and DL to be implemented with a high capacity for positive outcomes, with regard to increased rates of detection, low rates of false alarms and reasonable costs of communication and computation. The

features of ML and DL make them capable for designing detection systems that would achieve these thresholds by adapting to the changing techniques employed by cyber-criminals. Existing detection approaches still struggle with accuracy of performance issues and in some cases, an inability to detect unknown attacks, even with constant developments and improvements over the years [185]-[188]. Web based systems are globally available and accessible from anywhere and anytime. It is therefore imperative to develop cyber-attack detection systems for protection of sensitive and personal data as well as online transactions and data exchanges. These detection techniques can therefore be revised and improvised for better performance. With reference to performance metrics, accuracy alone is not a good measure of the performance of a model or system, for instance when the data has imbalanced classes. More information and metrics are necessary to understand how a model truly performs. It is important to note that, there are limited studies on the application of DL techniques in specific cyber-attack detection domains, for instance, for phishing attacks [156], [176], [189]-[195].

4. Conclusion

Reliance on the internet and the technological environment has ultimately made it pertinent for professionals to be on alert to the rising cyber-attack instances. Professionals have to be proactive so as to be able to prevent and detect any form of threat from having a negative impact on the system or the network. Introduction of measures that would successfully mitigate regular attacks is a key component of cyber security as attackers are constantly devising new ways of infiltrating systems and networks and being knowledgeable of the threats is a crucial starting point of maintaining cyber security. Whereas intrusion detection systems can be developed to protect networks and devices, they are also capable of tracking the source of threats to the network. Subsequently, security frameworks need to be developed and adhered to, to protect systems and networks from illegal access and destabilization.

Various methods and techniques are available for cyber-attack detection. However, in the context of this paper, stable mechanisms and robustness in implemented security frameworks is critical in detection and prediction of attacks in organizational systems and networks. The dynamism of networks and systems lead to variations in the modes of attacks that they are vulnerable to. In this perspective, it is notable that detection and prevention systems need multiple layers for interpretation of the variations and dynamism in the network environment, which would be more effective compared to dependence on stored patterns and signatures of recognized attacks, which offer partial network security and has a high occurrence of false positives. Research shows evidence that ML leads to more accurate results and the occurrence of false positives is lower while simultaneously learning and understanding novel threats. Compared to ML, DL is evidenced to be powerful, especially when used with DBN whose multiple nodes allow for more calculations to be performed, leading to more accurate outcomes. Future research should focus on performance metrics used in different detection models and model reliability when detecting cyber-attacks.

Compliance with ethical standards

Acknowledgments

My appreciation goes to everyone who assisted some assistance during the course of development of this research work.

References

[1] Zhang F, Kodituwakku HA, Hines JW, Coble J. Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. IEEE Transactions on Industrial Informatics. 2019 Jan 6;15(7):4362-9.

[2] Zhao N, Zhao X, Xu N, Zhang L. Resilient event-triggered control of connected automated vehicles under cyber attacks. IEEE/CAA Journal of AutomaticaSinica. 2023 Mar 28.

[3] Ghiasi M, Niknam T, Wang Z, Mehrandezh M, Dehghani M, Ghadimi N. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electric Power Systems Research. 2023 Feb 1;215:108975.

[4] Qiu H, Dong T, Zhang T, Lu J, Memmi G, Qiu M. Adversarial attacks against network intrusion detection in IoT systems. IEEE Internet of Things Journal. 2020 Dec 30;8(13):10327-35.

[5] Bitirgen K, Filik ÜB. A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid. International Journal of Critical Infrastructure Protection. 2023 Mar 1;40:100582.

[6] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[7] Kumar R, Goyal R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review. 2019 Aug 1; 33:1-48.

[8] Stabili D, Romagnoli R, Marchetti M, Sinopoli B, Colajanni M. A multidisciplinary detection system for cyber attacks on Powertrain Cyber Physical Systems. Future Generation Computer Systems. 2023 Jul 1;144:151-64.

[9] De Arroyabe IF, Arranz CF, Arroyabe MF, de Arroyabe JC. Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Computers & Security. 2023 Jan 1;124:102954.

[10] Bhamare D, Zolanvari M, Erbad A, Jain R, Khan K, Meskin N. Cybersecurity for industrial control systems: A survey. computers & security. 2020 Feb 1;89:101677.

[11] Vander–Pallen MA, Addai P, Isteefanos S, Mohd TK. Survey on Types of Cyber Attacks on Operating System Vulnerabilities since 2018 onwards. In2022 IEEE World AI IoT Congress (AIIoT) 2022 Jun 6 (pp. 01-07). IEEE.

[12] Wan Y, Dragičević T. Data-driven cyber-attack detection of intelligent attacks in islanded dc microgrids. IEEE Transactions on Industrial Electronics. 2022 May 25;70(4):4293-9.

[13] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[14] Guembe B, Azeta A, Misra S, Osamor VC, Fernandez-Sanz L, Pospelova V. The emerging threat of ai-driven cyber-attacks: A Review. Applied Artificial Intelligence. 2022 Dec 31;36(1):2037254.

[15] Sadiku MN, Ajayi-Majebi AJ, Adebo PO. Cyber manufacturing. InEmerging Technologies in Manufacturing 2023 Mar 16 (pp. 247-257). Cham: Springer International Publishing.

[16] Zhou S, Liu C, Ye D, Zhu T, Zhou W, Yu PS. Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity. ACM Computing Surveys. 2022 Dec 23;55(8):1-39.

[17] Khan Z, Chowdhury M, Khan SM. A Hybrid Defense Method against Adversarial Attacks on Traffic Sign Classifiers in Autonomous Vehicles. arXiv preprint arXiv:2205.01225. 2022 Apr 25.

[18] Mbow M, Sakurai K, Koide H. Advances in Adversarial Attacks and Defenses in Intrusion Detection System: A Survey. InScience of Cyber Security-SciSec 2022 Workshops: AI-CryptoSec, TA-BC-NFT, and MathSci-Qsafe 2022, Matsue, Japan, August 10–12, 2022, Revised Selected Papers 2023 Jan 1 (pp. 196-212). Singapore: Springer Nature Singapore.

[19] Jiang X, Ge Z. Attacks on data-driven process monitoring systems: Subspace Transfer Networks. IEEE Transactions on Artificial Intelligence. 2022 Jan 25;3(3):470-84.

[20] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[21] Sakthivelu U, Vinoth Kumar CN. An Approach on Cyber Threat Intelligence Using Recurrent Neural Network. InICT Infrastructure and Computing: Proceedings of ICT4SD 2022 2022 Nov 8 (pp. 429-439). Singapore: Springer Nature Singapore.

[22] Tahirou A, Konate K. A Survey of the Security and DDoS Attacks in the Software Defined Network. InInnovations in Smart Cities Applications Volume 6: The Proceedings of the 7th International Conference on Smart City Applications 2023 Mar 2 (pp. 426-441). Cham: Springer International Publishing.

[23] Zhao N, Zhao X, Chen M, Zong G, Zhang H. Resilient Distributed Event-Triggered Platooning Control of Connected Vehicles Under Denial-of-Service Attacks. IEEE Transactions on Intelligent Transportation Systems. 2023 Mar 6.

[24] Wen G, Wang P, Lv Y, Chen G, Zhou J. Secure consensus of multi-agent systems under denial-of-service attacks. Asian Journal of Control. 2023 Mar;25(2):695-709.

[25] Guo S, Xu Y, Ma Y, Fu L. Observer-based event-triggered non-PDC control for networked TS fuzzy systems under actuator failures and aperiodic DoS attacks. Information Sciences. 2023 Jun 1;629:276-98.

[26] Devi RS, Bharathi R, Kumar PK. Investigation on Efficient Machine Learning Algorithm for DDoS Attack Detection. In2023 International Conference on Computer, Electrical & Communication Engineering (ICCECE) 2023 Jan 20 (pp. 1-5). IEEE.

[27] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[28] Alexandre RC, Martins LE, Gorschek T. Cybersecurity Risk Assessment for Medium-Risk Drones: A Systematic Literature Review. IEEE Aerospace and Electronic Systems Magazine. 2023 Mar 3.

[29] Alazab A, Khraisat A, Singh S, Bevinakoppa S, Mahdi OA. Routing Attacks Detection in 6LoWPAN-Based Internet of Things. Electronics. 2023 Mar 10;12(6):1320.

[30] Kaur J, Agrawal A, Khan RA. P2ADF: a privacy-preserving attack detection framework in fog-IoT environment. International Journal of Information Security. 2023 Jan 18:1-4.

[31] Kaushik K, Singh V, Manikandan VP. A Novel Approach for an Automated Advanced MITM Attack on IoT Networks. InAdvancements in Interdisciplinary Research: First International Conference, AIR 2022, Prayagraj, India, May 6–7, 2022, Revised Selected Papers 2023 Jan 21 (pp. 60-71). Cham: Springer Nature Switzerland.

[32] Liu F, Sarkar S, Wang G, Meier W, Isobe T. Algebraic meet-in-the-middle attack on LowMC. InAdvances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part I 2023 Jan 25 (pp. 225-255). Cham: Springer Nature Switzerland.

[33] Tsompanoglou P, Iliadis A, Kantelis K, Petridou S, Nicopolitidis P. Countermeasuring MITM Attacks in Solar-Powered PON-Based FiWi Access Networks. Electronics. 2023 Feb 20;12(4):1052.

[34] Padmavathi G. Hybrid Detection and Mitigation of DNS Protocol MITM attack based on Firefly algorithm with Elliptical Curve Cryptography. EAI Endorsed Transactions on Pervasive Health and Technology. 2023 Jan 19;9(1).

[35] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432).

[36] Khan AA, Beg OA. Cyber Vulnerabilities of Modern Power Systems. InPower Systems Cybersecurity: Methods, Concepts, and Best Practices 2023 Feb 9 (pp. 47-66). Cham: Springer International Publishing.

[37] Alomar MA. An IOT based smart grid system for advanced cooperative transmission and communication. Physical Communication. 2023 Apr 3:102069.

[38] Toro-Alvarez MM. Hacking. InHandbook on Crime and Technology 2023 Mar 28 (pp. 334-357). Edward Elgar Publishing.

[39] Mangalampalli S, Karri GR. Cloud Environment Limitations and Challenges. Big Data, Cloud Computing and IoT: Tools and Applications. 2023 Apr 19.

[40] Steyn C, Blaauw DN. Towards a Critical Review of Cybersecurity Risks in Anti-Poaching Systems. InInternational Conference on Cyber Warfare and Security 2023 Feb 28 (Vol. 18, No. 1, pp. 560-568).

[41] Dayaratne TT, Jaigirdar FT, Dasgupta R, Sakzad A, Rudolph C. Improving Cybersecurity Situational Awareness in Smart Grid Environments. InPower Systems Cybersecurity: Methods, Concepts, and Best Practices 2023 Feb 9 (pp. 115-134). Cham: Springer International Publishing.

[42] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[43] Tatara BA, Abdurachman B, Mustofa DL, Yacobus D. The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation. NUANSA: JurnalPenelitianIlmuSosialdanKeagamaan Islam. 2023 Feb 24;20(1):19-37.

[44] Ghafir I, Prenosil V. Malicious file hash detection and drive-by download attacks. InProceedings of the Second International Conference on Computer and Communication Technologies: IC3T 2015, Volume 1 2016 (pp. 661-669). Springer India.

[45] Joshi G, Padmavathy R, Pinapati A, Kumar MB. BrowserGuard2: A Solution for Drive-by-Download Attacks. InProceeding of the Second International Conference on Microelectronics, Computing & Communication Systems (MCCS 2017) 2019 (pp. 739-750). Springer Singapore.

[46] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics. 2023 Mar 11;12(6):1333.

[47] Lee K, Lee J, Yim K. Classification and Analysis of Malicious Code Detection Techniques Based on the APT Attack. Applied Sciences. 2023 Feb 23;13(5):2894..

[48] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[49] Rains T, CISSP TY. Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization. Packt Publishing Ltd; 2023 Jan 25.

[50] Le Thanh Thai B, Tanaka H. A Novel Metric for Password Security Risk Against Dictionary Attacks. InInformation Security Applications: 23rd International Conference, WISA 2022, Jeju Island, South Korea, August 24–26, 2022, Revised Selected Papers 2023 Feb 4 (pp. 291-302). Cham: Springer Nature Switzerland.

[51] Alotaibi N, Williamson J, Khamis M. ThermoSecure: Investigating the effectiveness of AI-driven thermal attacks on commonly used computer keyboards. ACM Transactions on Privacy and Security. 2023 Mar 13; 26(2):1-24.

[52] Hall RC, Hoppa MA, Hu YH. An Empirical Study of Password Policy Compliance. InJournal of the Colloquium for Information Systems Security Education 2023 Mar 8 (Vol. 10, No. 1, pp. 8-8).

[53] Georgiadou A, Michalitsi-Psarrou A, Askounis D. A Security Awareness and Competency Evaluation in the Energy Sector. Computers & Security. 2023 Mar 22:103199.

[54] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[55] Patil S, Vanmali A, Bansode R. Cyber Security Concerns for IoB. Internet of Behaviors (IoB). 2023 Jun 6:141-55.

[56] Crespo-Martínez IS, Campazas-Vega A, Guerrero-Higueras ÁM, Riego-DelCastillo V, Álvarez-Aparicio C, Fernández-Llamas C. SQL injection attack detection in network flow data. Computers & Security. 2023 Apr 1;127:103093.

[57] Abdullayev V, Chauhan AS. SQL Injection Attack: Quick View. Mesopotamian Journal of CyberSecurity. 2023 Feb 14;2023:30-4.

[58] Alarfaj FK, Khan NA. Enhancing the Performance of SQL Injection Attack Detection through Probabilistic Neural Networks. Applied Sciences. 2023 Mar 29;13(7):4365.

[59] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1;23(4):145-62.

[60] Lodha S, Gundawar A. SQL Injection and Its Detection Using Machine Learning Algorithms and BERT. InCognitive Computing and Cyber Physical Systems: Third EAI International Conference, IC4S 2022, Virtual Event, November 26-27, 2022, Proceedings 2023 Mar 25 (pp. 3-16). Cham: Springer Nature Switzerland.

[61] Srivastava V, Majumdar A. Prevention of SQL Injection Attacks in Web Applications. Journal of Survey in Fisheries Sciences. 2023 Mar 13;10(2S):1113-9.

[62] Kaur J, Garg U, Bathla G. Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review. Artificial Intelligence Review. 2023 Mar 23:1-45.

[63] Thajeel IK, Samsudin K, Hashim SJ, Hashim F. Dynamic feature selection model for adaptive cross site scripting attack detection using developed multi-agent deep Q learning model. Journal of King Saud University-Computer and Information Sciences. 2023 Jan 23.

[64] Hu T, Xu C, Zhang S, Tao S, Li L. Cross-site scripting detection with two-channel feature fusion embedded in self-attention mechanism. Computers & Security. 2023 Jan 1;124:102990.

[65] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[66] Alaoui RL. Cross Site Scripting Attack Detection Approach Based on LSTM Encoder-Decoder and Word Embeddings. International Journal of Intelligent Systems and Applications in Engineering. 2023 Feb 22;11(2):277-82.

[67] Yadav MK, Khan M. Introduction to Web Terminology and Web Application Attacks. Journal of Web Development and Web Designing. 2023 Jan 19;8(1):1-2.

[68] Farraj A. Coordinated Security Measures for Industrial IoT Against Eavesdropping. In2023 IEEE Texas Power and Energy Conference (TPEC) 2023 Feb 13 (pp. 1-5). IEEE.

[69] Wang Z, Li Y, Wu S, Zhou Y, Yang L, Xu Y, Zhang T, Pan Q. A survey on cybersecurity attacks and defenses for unmanned aerial systems. Journal of Systems Architecture. 2023 Apr 3:102870.

[70] Haifa Ali SA, Vakula Rani J. Attack Detection in IoT Using Machine Learning—A Survey. InIntelligent Cyber Physical Systems and Internet of Things: ICoICI 2022 2023 Feb 4 (pp. 211-228). Cham: Springer International Publishing.

[71] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[72] Yao Y, Zhao J, Li Z, Cheng X, Wu L. Jamming and Eavesdropping Defense Scheme based on Deep Reinforcement Learning in Autonomous Vehicle Networks. IEEE Transactions on Information Forensics and Security. 2023 Jan 13.

[73] Liu L, Zhou Y, Xi Z, Wu J, Xu J. Defense Against Underwater Spy-robots: A Distributed Anti-Theft Topology Control Mechanism for Insecure UASN. Computers & Security. 2023 Mar 30:103214.

[74] Alghenaim MF, Bakar NA, Abdul Rahim F, Vanduhe VZ, Alkawsi G. Phishing Attack Types and Mitigation: A Survey. InData Science and Emerging Technologies: Proceedings of DaSET 2022 2023 Apr 1 (pp. 131-153). Singapore: Springer Nature Singapore.

[75] Dhanavanthini P, Chakkravarthy SS. Phish-armour: phishing detection using deep recurrent neural networks. Soft Computing. 2023 Mar 27:1-3.

[76] Xu T, Singh K, Rajivan P. Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. Applied Ergonomics. 2023 Apr 1;108:103908.

[77] Werner MJ, Njenga K. Phishing Attack Victims and the Effect on Work Engagement. InDigital-for-Development: Enabling Transformation, Inclusion and Sustainability Through ICTs: 12th International Development Informatics Association Conference, IDIA 2022, Mbombela, South Africa, November 22–25, 2022, Revised Selected Papers 2023 Mar 18 (pp. 203-217). Cham: Springer Nature Switzerland.

[78] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[79] Tufan A, Tuna G. Benefits of Information Security Awareness Training Against Phishing Attacks: A Field Study. InHandbook of Research on Cybersecurity Risk in Contemporary Business Systems 2023 (pp. 49-78). IGI Global.

[80] Jha AK, Muthalagu R, Pawar PM. Intelligent phishing website detection using machine learning. Multimedia Tools and Applications. 2023 Feb 24:1-26.

[81] Tabrizchi H, Kuchaki Rafsanjani M. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing. 2020 Dec;76(12):9493-532.

[82] Farivar F, Haghighi MS, Jolfaei A, Alazab M. Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. IEEE transactions on industrial informatics. 2019 Nov 28;16(4):2716-25.

[83] Gunduz MZ, Das R. Cyber-security on smart grid: Threats and potential solutions. Computer networks. 2020 Mar 14;169:107094.

[84] Tian Z, Luo C, Qiu J, Du X, Guizani M. A distributed deep learning system for web attack detection on edge devices. IEEE Transactions on Industrial Informatics. 2019 Aug 30;16(3):1963-71.

[85] Parra GD, Rad P, Choo KK, Beebe N. Detecting Internet of Things attacks using distributed deep learning. Journal of Network and Computer Applications. 2020 Aug 1;163:102662.

[86] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[87] Kaloudi N, Li J. The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR). 2020 Feb 5;53(1):1-34.

[88] Humayun M, Niazi M, Jhanjhi NZ, Alshayeb M, Mahmood S. Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering. 2020 Apr;45:3171-89.

[89] Dey AK, Gupta GP, Sahu SP. Hybrid Meta-Heuristic based Feature Selection Mechanism for Cyber-Attack Detection in IoT-enabled Networks. Procedia Computer Science. 2023 Jan 1;218:318-27.

[90] Arpitha B, Sharan R, Brunda BM, Indrakumar DM, Ramesh BE. Cyber Attack Detection and notifying system using ML Techniques. International Journal of Engineering Science and Computing (IJESC). 2021.

[91] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[92] Tekerek A. A novel architecture for web-based attack detection using convolutional neural network. Computers & Security. 2021 Jan 1;100:102096.

[93] Zhou X, Liang W, Li W, Yan K, Shimizu S, Kevin I, Wang K. Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system. IEEE Internet of Things Journal. 2021 Nov 24;9(12):9310-9.

[94] Salau AO, Marriwala N, Athaee M. Data security in wireless sensor networks: Attacks and countermeasures. InMobile Radio Communications and 5G Networks: Proceedings of MRCN 2020 2021 (pp. 173-186). Springer Singapore.

[95] Bin Sulaiman R, Rahi MA. A Framework to Mitigate Attacks in Web Applications. IUP Journal of Computer Sciences. 2021 Jan 1;15(1).

[96] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec;11(4):66.

[97] Anthi E, Williams L, Rhode M, Burnap P, Wedgbury A. Adversarial attacks on machine learning cybersecuritydefences in industrial control systems. Journal of Information Security and Applications. 2021 May 1;58:102717.

[98] Sarker IH, Khan AI, Abushark YB, Alsolami F. Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications. 2022 Mar 14:1-7.

[99] Ullah I, Mahmoud QH. Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access. 2021 Jul 1;9:103906-26.

[100] Bedi P, Gupta N, Jindal V. I-SiamIDS: an improved Siam-IDS for handling class imbalance in network-based intrusion detection systems. Applied Intelligence. 2021 Feb;51:1133-51.

[101] Gupta N, Jindal V, Bedi P. LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system. Computer Networks. 2021 Jun 19;192:108076.

[102] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[103] Abdullahi M, Baashar Y, Alhussian H, Alwadain A, Aziz N, Capretz LF, Abdulkadir SJ. Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics. 2022 Jan 10;11(2):198.

[104] Apruzzese G, Andreolini M, Ferretti L, Marchetti M, Colajanni M. Modeling realistic adversarial attacks against network intrusion detection systems. Digital Threats: Research and Practice (DTRAP). 2022 Sep 12;3(3):1-9.

[105] Inayat U, Zia MF, Mahmood S, Khalid HM, Benbouzid M. Learning-based methods for cyber attacks detection in IoT systems: a survey on methods, analysis, and future prospects. Electronics. 2022 May 7;11(9):1502.

[106] Wang X, Ding D, Ge X, Han QL. Neural-network-based control for discrete-time nonlinear systems with denial-of-service attack: the adaptive event-triggered case. International Journal of Robust and Nonlinear Control. 2022 Mar 25;32(5):2760-79.

[107] Ghelani D, Hua TK, Koduru SK. Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. Authorea Preprints. 2022 Sep 22.

[108] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17.

[109] Achar S. Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. International Journal of Computer and Systems Engineering. 2022 Sep 13;16(9):379-84.

[110] Dash B, Ansari MF. An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. Int. Res. J. Eng. Technol.(IRJET). 2022;9.

[111] Carneiro J, Oliveira N, Sousa N, Maia E, Praça I. Machine learning for network-based intrusion detection systems: an analysis of the CIDDS-001 dataset. InDistributed Computing and Artificial Intelligence, Volume 1: 18th International Conference 18 2022 (pp. 148-158). Springer International Publishing.

[112] Ahsan M, Nygard KE, Gomes R, Chowdhury MM, Rifat N, Connolly JF. Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy. 2022 Jul 10;2(3):527-55.

[113] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[114] Tran MQ, Elsisi M, Liu MK, Vu VQ, Mahmoud K, Darwish MM, Abdelaziz AY, Lehtonen M. Reliable deep learning and IoT-based monitoring system for secure computer numerical control machines against cyber-attacks with experimental verification. IEEE Access. 2022 Feb 22;10:23186-97.

[115] Horchulhack P, Viegas EK, Santin AO. Toward feasible machine learning model updates in network-based intrusion detection. Computer Networks. 2022 Jan 15;202:108618.

[116] Alani MM, Tawfik H. PhishNot: A Cloud-Based Machine-Learning Approach to Phishing URL Detection. Computer Networks. 2022 Dec 9;218:109407.

[117] Muhammad MU, Saleem AM. Intelligent Intrusion Detection System for Apache Web Server Empowered with Machine Learning Approaches. International Journal of Computational and Innovative Sciences. 2022;1(1):1-8.

[118] Suresh P, Logeswaran K, Keerthika P, Devi RM, Sentamilselvan K, Kamalam GK, Muthukrishnan H. Contemporary survey on effectiveness of machine and deep learning techniques for cyber security. InMachine Learning for Biometrics 2022 Jan 1 (pp. 177-200). Academic Press.

[119] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[120] Liu Z, Xu B, Cheng B, Hu X, Darbandi M. Intrusion detection systems in the cloud computing: A comprehensive and deep literature review. Concurrency and Computation: Practice and Experience. 2022 Feb 15;34(4):e6646.

[121] Onyema EM, Dalal S, Romero CA, Seth B, Young P, Wajid MA. Design of intrusion detection system based on cyborg intelligence for security.

[122] Le KH, Nguyen MH, Tran TD, Tran ND. IMIDS: An intelligent intrusion detection system against cyber threats in IoT. Electronics. 2022 Feb 10;11(4):524.

[123] Dixit P, Silakari S. Deep learning algorithms for cybersecurity applications: A technological and status review. Computer Science Review. 2021 Feb 1;39:100317.

[124] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[125] Oliveira N, Praça I, Maia E, Sousa O. Intelligent cyber attack detection and classification for network-based intrusion detection systems. Applied Sciences. 2021 Feb 13;11(4):1674.

[126] Saheed YK, Abiodun AI, Misra S, Holone MK, Colomo-Palacios R. A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal. 2022 Dec 1;61(12):9395-409.

[127] Shaukat K, Luo S, Varadharajan V, Hameed IA, Xu M. A survey on machine learning techniques for cyber security in the last decade. IEEE Access. 2020 Dec 2;8:222310-54.

[128] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[129] Morfino V, Rampone S. Towards near-real-time intrusion detection for IoT devices using supervised learning and apache spark. Electronics. 2020 Mar 6;9(3):444.

[130] Zhang Z, Ning H, Shi F, Farha F, Xu Y, Xu J, Zhang F, Choo KK. Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review. 2022 Feb 1:1-25.

[131] Ioannou C, Vassiliou V. Experimentation with local intrusion detection in IoT networks using supervised learning. In2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS) 2020 May 25 (pp. 423-428). IEEE.

[132] Ioannou C, Vassiliou V. Classifying security attacks in IoT networks using supervised learning. In2019 15th International conference on distributed computing in sensor systems (DCOSS) 2019 May 29 (pp. 652-658). IEEE.

[133] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25;4(1):10-9.

[134] Rani D, Kaushal NC. Supervised machine learning based network intrusion detection system for Internet of Things. In2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2020 Jul 1 (pp. 1-7). IEEE.

[135] Wan Y, Xu K, Xue G, Wang F. Iotargos: A multi-layer security monitoring system for internet-of-things in smart homes. InIEEE INFOCOM 2020-IEEE Conference on Computer Communications 2020 Jul 6 (pp. 874-883). IEEE.

[136] Krishnan S, Neyaz A, Liu Q. IoT network attack detection using supervised machine learning. Int. J. Artif. Intell. Expert Syst. 2020 Feb 10: 18–32.

[137] Al Shorman A, Faris H, Aljarah I. Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection. Journal of Ambient Intelligence and Humanized Computing. 2020 Jul;11:2809-25.

[138] Janjua ZH, Vecchio M, Antonini M, Antonelli F. IRESE: An intelligent rare-event detection system using unsupervised learning on the IoT edge. Engineering Applications of Artificial Intelligence. 2019 Sep 1;84:41-50.

[139] Ghrabat MJ, Hussien ZA, Khalefa MS, Abduljabba ZA, Nyangaresi VO, Al Sibahee MA, Abood EW. Fully automated model on breast cancer classification using deep learning classifiers. Indonesian Journal of Electrical Engineering and Computer Science. 2022 Oct;28(1):183-91.

[140] Yang H, Zeng R, Wang F, Xu G, Zhang J. An unsupervised learning-based network threat situation assessment model for internet of things. Security and Communication Networks. 2020 Nov 28;2020:1-1.

[141] Khonde SR, Ulagamuthalvi V. Ensemble-based semi-supervised learning approach for a distributed intrusion detection system. Journal of Cyber Security Technology. 2019 Jul 3;3(3):163-88.

[142] Cheng Y, Xu Y, Zhong H, Liu Y. HS-TCN: A semi-supervised hierarchical stacking temporal convolutional network for anomaly detection in IoT. In2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC) 2019 Oct 29 (pp. 1-7). IEEE.

[143] Li W, Meng W, Au MH. Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments. Journal of Network and Computer Applications. 2020 Jul 1;161:102631.

[144] Liu S, Hao X, Chen X. A semi-supervised dynamic ensemble algorithm for IoT anomaly detection. In2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics) 2020 Nov 2 (pp. 264-269). IEEE.

[145] Ravi N, Shalinie SM. Semisupervised-learning-based security to detect and mitigate intrusions in IoT network. IEEE Internet of Things Journal. 2020 May 8;7(11):11041-52.

[146] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[147] Abu Al-Haija Q, Krichen M, Abu Elhaija W. Machine-learning-based darknet traffic detection system for IoT applications. Electronics. 2022 Feb 12;11(4):556.

[148] Halbouni A, Gunawan TS, Habaebi MH, Halbouni M, Kartiwi M, Ahmad R. Machine learning and deep learning approaches for cybersecuriy: A review. IEEE Access. 2022 Feb 11.

[149] Veena K, Meena K, Teekaraman Y, Kuppusamy R, Radhakrishnan A. C SVM classification and KNN techniques for cyber crime detection. Wireless Communications and Mobile Computing. 2022 Jan 17;2022:1-9.

[150] Othman SM, Ba-Alwi FM, Alsohybe NT, Al-Hashida AY. Intrusion detection model using machine learning algorithm on Big Data environment. Journal of big data. 2018 Dec;5(1):1-2.

[151] Belouch M, El Hadaj S, Idhammad M. Performance evaluation of intrusion detection based on machine learning using Apache Spark. Procedia Computer Science. 2018 Jan 1;127:1-6.

[152] Yungaicela-Naula NM, Vargas-Rosales C, Perez-Diaz JA. SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning. IEEE Access. 2021 Jul 30;9:108495-512.

[153] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[154] Tupsamudre H, Singh AK, Lodha S. Everything is in the name–a url based approach for phishing detection. InCyber Security Cryptography and Machine Learning: Third International Symposium, CSCML 2019, Beer-Sheva, Israel, June 27–28, 2019, Proceedings 3 2019 (pp. 231-248). Springer International Publishing.

[155] Cohen A, Nissim N, Rokach L, Elovici Y. SFEM: Structural feature extraction methodology for the detection of malicious office documents using machine learning methods. Expert Systems with Applications. 2016 Nov 30;63:324-43.

[156] Patil S, Dhage S. A methodical overview on phishing detection along with an organized way to construct an anti-phishing framework. In2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS) 2019 Mar 15 (pp. 588-593). IEEE.

[157] Farhin F, Sultana I, Islam N, Kaiser MS, Rahman MS, Mahmud M. Attack detection in internet of things using software defined network and fuzzy neural network. In2020 Joint 9th International Conference on Informatics, Electronics & Vision (ICIEV) and 2020 4th International Conference on Imaging, Vision & Pattern Recognition (icIVPR) 2020 Aug 26 (pp. 1-6). IEEE.

[158] Ge M, Syed NF, Fu X, Baig Z, Robles-Kelly A. Towards a deep learning-driven intrusion detection approach for Internet of Things. Computer Networks. 2021 Feb 26;186:107784.

[159] Al-Hawawreh M, Sitnikova E, Den Hartog F. An efficient intrusion detection model for edge system in brownfield industrial internet of things. InProceedings of the 3rd International Conference on Big Data and Internet of Things 2019 Aug 22 (pp. 83-87).

[160] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[161] Yang A, Zhuansun Y, Liu C, Li J, Zhang C. Design of intrusion detection system for internet of things based on improved BP neural network. Ieee Access. 2019 Jul 19;7:106043-52.

[162] Telikani A, Gandomi AH. Cost-sensitive stacked auto-encoders for intrusion detection in the Internet of Things. Internet of Things. 2021 Jun 1;14:100122.

[163] Li F, Shi Y, Shinde A, Ye J, Song W. Enhanced cyber-physical security in internet of things through energy auditing. IEEE Internet of Things Journal. 2019 Feb 14;6(3):5224-31.

[164] Thamilarasu G, Chawla S. Towards deep-learning-driven intrusion detection for the internet of things. Sensors. 2019 Apr 27;19(9):1977.

[165] Berman DS, Buczak AL, Chavis JS, Corbett CL. A survey of deep learning methods for cyber security. Information. 2019 Apr 2;10(4):122.

[166] Smys S, Basar A, Wang H. Hybrid intrusion detection system for internet of things (IoT). Journal of ISMAC. 2020 Sep 30;2(04):190-9.

[167] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[168] Li J, Sun B. A network attack detection method using SDA and deep neural network based on internet of things. International Journal of Wireless Information Networks. 2020 Jun;27:209-14.

[169] Tian Q, Han D, Li KC, Liu X, Duan L, Castiglione A. An intrusion detection approach based on improved deep belief network. Applied Intelligence. 2020 Oct;50:3162-78.

[170] NG BA, Selvakumar S. Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment. Future Generation Computer Systems. 2020 Dec 1;113:255-65.

[171] Uchiyama T, Sogi N, Niinuma K, Fukui K. Visually explaining 3D-CNN predictions for video classification with an adaptive occlusion sensitivity analysis. InProceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision 2023 (pp. 1513-1522).

[172] Xie P, Cui Z, Du Y, Zhao M, Cui J, Wang B, Hu X. Multi-scale local-temporal similarity fusion for continuous sign language recognition. Pattern Recognition. 2023 Apr 1;136:109233.

[173] Barik K, Misra S, Konar K, Fernandez-Sanz L, Koyuncu M. Cybersecurity deep: approaches, attacks dataset, and comparative study. Applied Artificial Intelligence. 2022 Dec 31;36(1):2055399.

[174] Saharkhizan M, Azmoodeh A, Dehghantanha A, Choo KK, Parizi RM. An ensemble of deep recurrent neural networks for detecting IoTcyber attacks using network traffic. IEEE Internet of Things Journal. 2020 May 21;7(9):8852-9.

[175] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[176] Do NQ, Selamat A, Krejcar O, Herrera-Viedma E, Fujita H. Deep learning for phishing detection: Taxonomy, current challenges and future directions. IEEE Access. 2022 Feb 17.

[177] Genge B, Kiss I, Haller P. A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection. 2015 Sep 1;10:3-17.

[178] Krundyshev V, Kalinin M. Hybrid neural network framework for detection of cyber attacks at smart infrastructures. InProceedings of the 12th International Conference on Security of Information and Networks 2019 Sep 12 (pp. 1-7).

[179] Zha L, Liao R, Liu J, Xie X, Tian E, Cao J. Dynamic event-triggered output feedback control for networked systems subject to multiple cyber attacks. IEEE Transactions on Cybernetics. 2021 Nov 19;52(12):13800-8.

[180] Roumani MA, Fung CC, Choejey P. Assessing economic impact due to cyber attacks with System Dynamics approach. In2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) 2015 Jun 24 (pp. 1-6). IEEE.

[181] Tan Y, Xiong M, Zhang B, Fei S. Adaptive event-triggered nonfragile state estimation for fractional-order complex networked systems with cyber attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2021 Jan 20;52(4):2121-33.

[182] Pan R, Tan Y, Du D, Fei S. Adaptive event-triggered synchronization control for complex networks with quantization and cyber-attacks. Neurocomputing. 2020 Mar 21;382:249-58.

[183] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[184] Zhang Q, Yan H, Zhang H, Chen S, Wang M. H∞ control of singular system based on stochastic cyber-attacks and dynamic event-triggered mechanism. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2020 Feb 21;51(12):7510-6.

[185] Ujjan RM, Pervez Z, Dahal K, Bashir AK, Mumtaz R, González J. Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Generation Computer Systems. 2020 Oct 1;111:763-79.

[186] Pecori R, Tayebi A, Vannucci A, Veltri L. IoT Attack detection with deep learning analysis. In2020 International Joint Conference on Neural Networks (IJCNN) 2020 Jul 19 (pp. 1-8). IEEE.

[187] Seibold C, Samek W, Hilsmann A, Eisert P. Detection of face morphing attacks by deep learning. InDigital Forensics and Watermarking: 16th International Workshop, IWDW 2017, Magdeburg, Germany, August 23-25, 2017, Proceedings 16 2017 (pp. 107-120). Springer International Publishing.

[188] Aldhyani TH, Alkahtani H. Artificial Intelligence Algorithm-Based Economic Denial of Sustainability Attack Detection Systems: Cloud Computing Environments. Sensors. 2022 Jun 21;22(13):4685.

[189] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[190] Catal C, Giray G, Tekinerdogan B, Kumar S, Shukla S. Applications of deep learning for phishing detection: a systematic literature review. Knowledge and Information Systems. 2022 Jun;64(6):1457-500.

[191] Benavides E, Fuertes W, Sanchez S, Sanchez M. Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review. Developments and Advances in Defense and Security: Proceedings of MICRADS 2019. 2020:51-64.

[192] Asiri S, Xiao Y, Alzahrani S, Li S, Li T. A Survey of Intelligent Detection Designs of HTML URL Phishing Attacks. IEEE Access. 2023 Jan 18.

[193] Yoro RE, Aghware FO, Akazue MI, Ibor AE, Ojugo AA. Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. International Journal of Electrical and Computer Engineering. 2023 Apr 1;13(2):1943.

[194] Ayaburi EW, Andoh-Baidoo FK. How do technology use patterns influence phishing susceptibility? A two-wave study of the role of reformulated locus of control. European Journal of Information Systems. 2023 Mar 6:1-21.

[195] Karim A, Shahroz M, Mustofa K, Belhaouari SB, Joga SR. Phishing Detection System through Hybrid Machine Learning Based on URL. IEEE Access. 2023 Mar 3.