International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2023.9.8.5

Volume 9, Issue 8
August - 2023

# Subject Review: Detecting Cyber Security Attacks

**Haitham Salman Chyad[1], and Raniah Ali Mustafa[2]**

[1,2]Computer Science Department

College of Education

Mustansiriyah University,

Baghdad, Iraq

## ABSTRACT

*Attacks against cyber security are increasing in frequency and complexity over the years. Due to the complexity and level of sophistication that are increasing, defensive strategies need to be developed further and continuously innovated. Traditional strategies to intrusion detection and deep packet inspection continue to be utilized and suggested, but they are adequate for addressing the requirements of changing security threats. As processing power increases and the cost of doing so drops, machine learning is seen as a complementary method or additional defense against malware, botnets, and other attacks. Deep learning algorithms in particular have piqued the interest of academics recently because of their unparalleled excellent performance in many areas that depend on prediction. This study paper presented promising applications of machine learning and deep learning, a branch of artificial intelligence built on many layers of artificial neural networks, in Various kinds of security-related assignments. We describe the distinguished features of sample machine learning & deep learning architectures used in cybersecurity attacks decisively previously and comparably assessing state-of-the-art solutions from the literature. We outline necessary resources, such as a general framework for detection cyber security attacks and appropriate datasets, and we highlight the newest trends in machine learning and deep learning.*

**Keywords**: Cyber-Attacks, Deep Learning (DL), Internet of Things (Iot), Malware, Machine Learning (ML).

## 1. INTRODUCTION

The fast advancement and expansion of IT technology has made cyber-attacks a significant threat to network telecommunications. Using malware designed to breach network security, the bulk of cyberattacks are conducted via circumventing network protection [1]. Malware attacks frequently cause a secure network to become vulnerable by adding a destructive external component; as a result, the network's protected perimeter region is where the attack originated. Worms, viruses, trojan horses, and additional malware attack tools are only a few examples [2]. It's essential to stay in mind that a security breach in this case could result in data being altered or disrupted, sensitive data being sent via phishing, or even an attack that overwhelms network resources with an unusually high volume of traffic preventing access to network services (also often referred to a denial of service, or DoS) attack. However, malware attacks share the common trait that the prospective attack originates from as an unrelated source; in theory, it can be said to be an external attack. Consequently, an exterior defense system made up of firewalls, antivirus software, with intrusion detection tools is an effective method for network security to stop such a dangerous exterior component from violating security laws [3].

A cyber-threat is any attempt or presence that aims at stealing information, break integrity rules, or harm a computer system or network. Cyber threats comprise things like phishing, malware, attacks on Internet of Things (IoT) devices, denial-of-service attacks, spam, intrusions into networks or mobile devices, financial fraud, as well as ransom ware [4].

Unwanted or unsolicited email is referred to as spam email. The majority of spam emails spread advertisements or fake content. It uses up time, memory, and network bandwidth on the machine and on the network. Malware is another form of online threat. Malicious software, also referred to as malware, is software that is installed on a computer with the intention of preventing it from functioning effectively and damaging the electronic data on it. Trojan horses, worms, ransomware, adware, spyware, additional adware are important kinds of malware. Malicious attacks through computer networks with devices are a further threat to cyberspace. Those intrusions are utilized to determine then examine a computer system's or network's vulnerabilities.

To avoid these intrusions, a device referred to as an IDS (intrusion detection system) is utilized. Infiltration can be classified as hybrid, anomaly-depend, or signature/misuse-depend.

Machine learning, also referred to as ML, is a highly efficient and critical method for fending off cyber-attacks and getting around the limitations of conventional security solutions. Machine learning algorithms have drawbacks and restrictions despite all its attractiveness. Artificial intelligence (AI) includes a subclass called machine learning [5]. The fascinating feature of machine learning schemes is that they may produce outcomes automatically through learning from expertise without additionally requiring for particular programming.

Utilizing machine learning has many benefits, which are why its applications are expanding in almost every area of life, such as medical research, education, intrusion detection, spam detection, with malware detection [6]. The majority of popular machine learning approaches have been utilized to categorize and recognize various cyber threats. Some examples of frequently used machine learning algorithms include decision trees, random forests, naive bayes, support vector machine algorithms, K-nearest neighbors, deep belief networks, artificial neural networks, in addition K-means [7,8].

It's possible to categorize deep learning as a subset of machine learning. The growth and development of this discipline depend heavily on algorithm research. Machine learning emphasizes generalization and empirical data, but deep learning uses artificial neural networks designed to mimic the cognitive procedures of individuals [9] Up until recently, the complexity of neural networks was constrained by the computing power available Businesses can better deploy their resources because it cuts down on the time spent on repetitive tasks. In summary, deep learning can improve cybersecurity by making it simpler, more preventative, less expensive, and more efficient [10]. This, however, will only be feasible if the machine learning data supports a precise representation of the environment. According to the saying, "if you put garbage in, you'll get garbage out [11].

Cybersecurity operations are breached by sophisticated attackers [12]. Figure 1 lists the most typical cyberattacks. Also applications deep learning(DL) in cyber security are illustrated in the figure 2 [13,14].

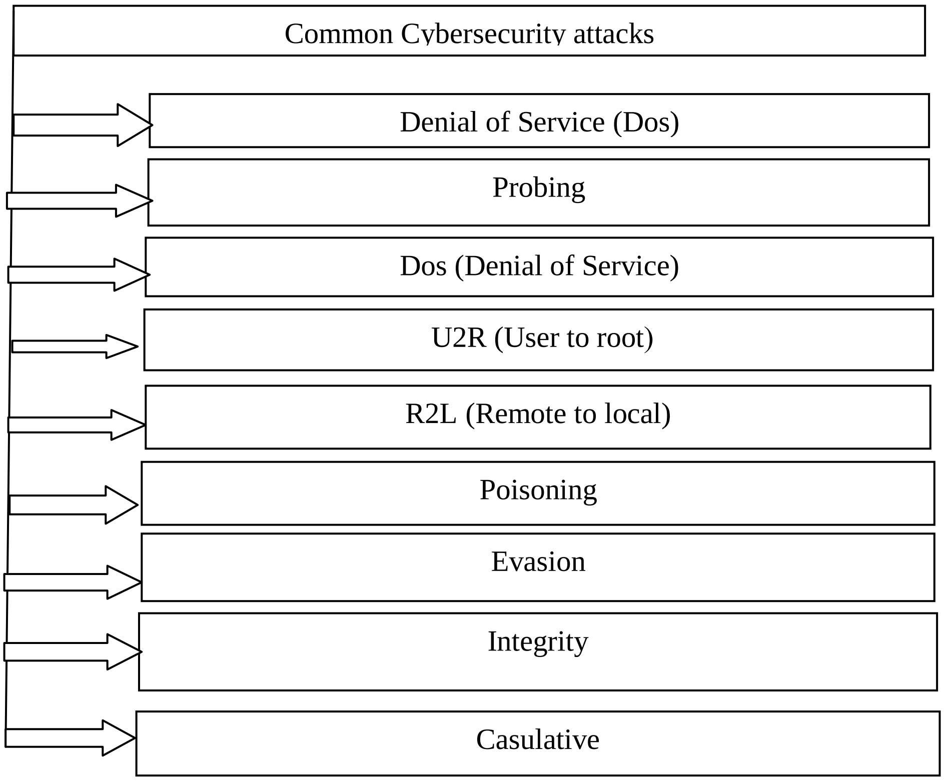

**Figure1.1: Typical Cyber attacks**

DOI: 10.31695/IJASRE.2023.9.8.5

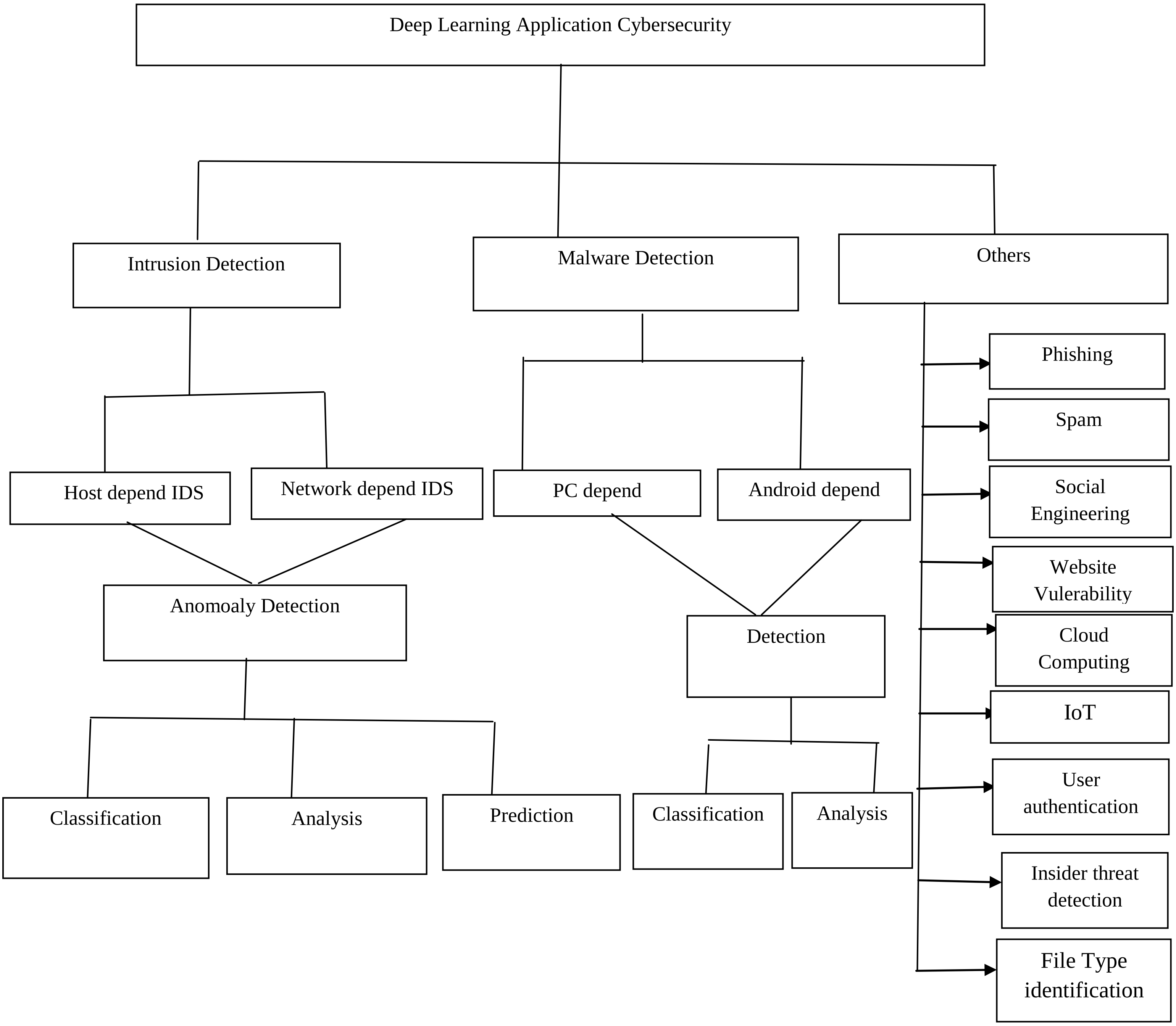

**Figure2.2: Deep learning (DL)'s primary applications in cyber security**

In the present paper, we aim to fill the present study gaps in the field of IoT security through investigating and analyzing both Deep learning is also referred as (DL) together with machine learning is also known as (ML) methods used for the detection of cyber security attacks in the networks and also internet of things devices through creating and handling research challenges, and through attempting to circumvent drawbacks in the current research [12].

## 2.LITERATURE SURVEY

### 2.1 Literature Survey for Machine Learning

The model you suggested can help to improve a system's overall security by identifying and with protection from malicious attacks in real time [15]. Massive amounts of data may be evaluated using machine learning algorithms., utilizing sophisticated algorithms, discover anomalies and patterns, and take suitable countermeasures to avoid a security attack. As a result, there are fewer false positives and higher detection ratios., providing a stronger defense against cyberattacks as a result. Furthermore, the concept may be utilized to develop novel enterprises along with organization security structures. These structures can contain,

DOI: 10.31695/IJASRE.2023.9.8.5

among other things, network security, data protection, device security, and identities administration. This study proposes a cyber-security-depend approach that assists in ensuring that each vital asset is safeguarded from cyber-attacks and critical data isn’t disclosed or stolen. Cybersecurity systems that incorporate machine learning (ML) together with artificial intelligence (AI) have the potential to significantly enhance an organization's general security posture and assistance it defends against the rising threat of cyberattacks. [16] Its study looks at how cyber training may be employed for both offensive & defense, including details on online threats as well as machine learning techniques. Algorithms based on machine learning are utilized to evaluate the more prevalent kinds of cyber security concerns, should indicate how machine learning is utilized for computer defense including recognizing and preventing threats, identification of vulnerabilities and scanning, and general internet risk estimate. [17] This article suggests utilizing artificial intelligence (AI) to determine application layer attacks. The graph-depend approach to dividing and dynamic programming are utilized to generate instances for the model (in the form of PCRE identical articulations). The normal articulations are utilized as a guide to demonstrate the actually conduct of the applications and to determine digital attacks. Furthermore, we showed results demonstrating how the proposed algorithm may be utilized to effectively locate application layer attacks. [18] in this paper, the use of novel innovations provides incalculable advantages for individuals, Governments as well as institutions; nonetheless, others are hostile toward them. For instance, information assurance is crucial, data stage security, accessibility of data, etc. Dependent on these difficulties, sophisticated anxiety-depend on abuse may be one of the most pressing challenges today. Computerized fear, which has caused numerous troubles for both individuals as well as organizations, has reached a level that might undermine open and national security through various social events, for example, criminal association, able humans and experienced activists. Thus, Intrusion Detection Systems (IDS) were generated to preserve a critical distinction from sophisticated attacks. At this time, reinforcement learning support vector machine (SVM) projections were employed to recognize efforts at port compasses based on precision rates that were cultivated individually. [19] in this article, the use of new innovations provides incalculable benefits to individuals, organizations, and governments; nonetheless, others are opposed to them. For instance, essential information assurance, data stage security, data accessibility, etc. Dependent on these concerns, advanced anxiety-based on abuse may be one of the most serious problems today. Computerized fear, which has resulted in several troubles for both individuals as well as institutions, has reached a level that might undermine open and national security through various social events, for instance, criminal association, persons with expertise, and modern activists. Thus, Intrusion Detection Systems (IDS) were designed to sustain a critical distinction from sophisticated attacks. Learning the reinforce support vector machine (SVM) assumptions were employed at this time to perceive port compass efforts based on The version of CICIDS2017 dataset was developed separately and has rates of precision of 97.80% & 69.79%. Probably in additional to SVM, we might offer some more calculations, like CNN, ANN, and Random Forest, with correctnesses of 93.29 for SVM, 63.52 for CNN, 99.93 for Random Forest, & 99.11 for ANN. [20] in this research article, we will look at how to combat implementation layer cyber-attacks, that are regarded as the much significant threats and the most critical test for network and cyber security. The majority of this essay is devoted to machine learning as a technique for dealing with model normal utilize and detecting cyber threats. For obtaining samples utilizing Perl Compatible Regular Expressions (PCRE) recurring expressions, the chart-depend on division technique with dynamic programming were employed. The model collects information by HTTP requests sent through the client to an online provider. We were able to demonstrate the success of our strategy utilizing the CSIC 2010 HTTP Dataset. [21] the goal of this article was to determine IoT network assaults utilizing machine learning algorithms. Due to its frequent revisions, diverse attack strategies, and numerous network protocols, the Bot IoT was applied as a dataset in this context. CICFlowMeter was utilized to derive flow-depend characteristics from raw traffic traces. CICFlowMeter generates the dataset's 84 network traffic features, which define the network flow. The Random Forest Regressor method was utilized during implementation to identify which characteristics would be used in the machine learning algorithms through calculating the significance of weights. When performing these calculations, two methodologies were used. The significance weights for this group were determined in the second technique after the significance weights for each attack type had been calculated independently in the first approach. In other words, the common characteristics that made each attack type significant were identified. Lastly, the data was subjected to the application of seven popular machine learning algorithms, differing in quality. The following are these algorithms and the obtained F-measure achievement percentages: F-measure had a value among zero and one, while the values for Naive Bayes, QDA, Random Forest, ID3, AdaBoost, MLP, and K Nearest Neighbors were each among 0.77 & 0.97. F-measure also had a value among zero with one.

## 2.1 LITERATURE SURVEY FOR DEEP LEARNING

[22] we suggest a deep learning method for building innovative balanced representations of imbalanced data sets. A deep learning attack identification model made especially for an ICS system is loaded with the unique representations. To determine cyber-attacks from the novel representations, the suggested attack detection model employs decision tree (DT) in addition to deep neural network (DNN) classification. The suggested model's achievement is estimated utilizing 10-fold cross-validation on two real ICS datasets. The findings demonstration that the suggested techniques surpasses standard classifiers comprise Random Forest (RF), DNN, and AdaBoost, as well as recently published models. The suggested technique is a generalizing strategy that may be easily deployed in current ICS infrastructures. The suggested model's performance is validated utilizing two independent ICS datasets

acquired from real essential infrastructure sites. In both datasets assessed, our suggested technique outperformed traditional classifiers with a better f1-score and provided higher precision, with%95.86 for the Gas Pipeline dataset as well as %99.67 for the Secure Water Treatment dataset. The results were analysed and compared with those of conventional classification, like RF, DNN, and ADA, as well as several peer-suggested techniques in the current literature. In each four evaluation metrics, the suggested approach outperformed competing techniques. [23] in this paper, we suggested an IoT/Fog network attack detection solution depend on distributed deep learning. The experiment demonstrated the effective use of artificial intelligence to cybersecurity, and the scheme for attack identification in distributed structure of IoT applications like smart cities was built and deployed. The examination procedure used precision, detection ratio, false alarm ratio, and other achievement measures to demonstrate the superiority of deep models over shallow models. The experiment proved that distributed attack detection could detect cyber-attacks better than centralized algorithms due to parameter sharing, that could avoid local minimums in training. When tested on previously unseen test data, our deep model outperformed existing machine learning methods such as softmax for network data classification into normal/attack. [24] in this research tackles this issue through presenting a deep learning-depend attack detection model for energy systems which could be trained utilizing data and logs collected through phasor measurement units (PMUs). To build characteristics, property or specification creating is utilized, and data is transmitted to different machine learning algorithms, of which random forest has been specified as the basic classifier of AdaBoost. The model, which includes 37 energy scheme event case studies, is tested utilizing open-source simulated energy scheme data. Finally, the proposed model was comparison to different layouts using different evaluation measures. According to the simulation results, this model obtains a detection ratio of 93.6% with a precision ratio of 93.91%, which is higher than the existence techniques. [25] this study proposes a distributed framework depend on deep learning (DL) to avoid multiple sources of susceptibility at the similar period, each within the same security system. Feed forward neural network and long short-term memory are two various DL models that are analyzed. The models are assessed in terms of performance and identifying various types of attacks utilizing two various datasets (NSL-KDD and BoT-IoT). The results show which the suggested distributed framework is efficient in detecting different types of cyber-attacks, with a precision of up to 99.95% across various setups. [26] Depend on the VGG16 classifier deep learning model, this study presents an intrusion detection model for IVNs to learn attack behavior features and identify threats. The Hacking and Countermeasure Research Lab (HCRL) provided the experimental dataset to test classification achievement for denial of service (DoS), fuzzy assaults, spoofing gear, and RPM in vehicle communications. To identify threats from in-vehicle networks, the suggested classifier's achievement was comparison to that of the XBoost ensemble learning method. To assure determine accuracy and identify false alarm risks, the test cases could detect anomalies in terms of accuracy, precision, recall, and F1-score. The experimenting results reveal that the classification accuracy of the dataset for HCRL Car-Hacking through the VGG16 and XBoost classifiers (n = 50) on the testing data attained 97.8241% with 99.9995%, for the 5-subcategory classification results. [27] in this study, we present a novel deep learning network model depend on the association and integration of various deep learning models to improve the procedure of determine cyber-attacks. We integrate two deep learning models, Convolutional Neural Network (CNN) and Long Short Term Memory (LSTM), into a combination deep learning network for identifying cyber-attacks depend on network traffic. The experimental results in Section IV.D show that our concept for identifying cyber-attacks depend on network traffic utilizing the CNN-LSTM deep learning model is completely, as the results of this model outperform some individual deep learning models on each measures. [28] in this paper describes a high- achievement system that employs an artificial intelligence technique to safeguard the vehicle network against cyber threats. Utilizing deep learning algorithms, the technology protects the autonomous vehicle against intrusions. The suggested security solution was validated utilizing a genuine automatic vehicle network dataset, which included spoofing, flood, replaying, and benign packets. Pre-processing was utilized to transform categorical data to numerical data. To identify attack messages, this dataset was processed utilizing the convolution neural network (CNN) with a hybrid network combining CNN and long short-term memory (CNN-LSTM) models. The findings demonstrated that the model performed well in terms of precision, recall, F1 score, and accuracy. The suggested system was highly accurate (97.30%). In addition to the empirical demonstration, the suggested system improved detection with classification precision when comparison to existence systems and was shown to have higher achievement for real-time CAN bus security.

## 3.COMPARATIVE ANALYSIS FOR DETECTING CYBER SECURITY ATTACKS

### 3.1COMPARATIVE ANALYSIS FOR DETECTING CYBER SECURITY ATTACKS USING MACHINE LEARNING

In the table 1 will illustrate the comparison between the previous systems for detecting cyber security attacks utilizing Machine Learning (ML).

DOI: 10.31695/IJASRE.2023.9.8.5

**Table1.1 Comparative Analysis for Some detecting cyber security attacks utilizing Machine Learning (ML)**

| Ref. | Year | Dataset | Methods/ Technique | Detecting cyber security attacks | Accuracy |
|---|---|---|---|---|---|
| Muneer et al. | 2023 | | machine learning (ML) in cyber security incident detection | Combining artificial intelligence and machine learning (ML) approach into cybersecurity systems has the probable to greatly enhance an organization's current state of security and provide protection against the growing threat of cyberattacks. | utilize of real-time data analyses and machine learning algorithms allows the model to constantly adapting and improvement its precision, making it a highly efficient resolution for cyber incident detection |
| Vadivelan et al. | 2022 | A diverse experiment was conducted in cybersecurity databases to test the feasibility of the DT design | machine learning (ML) in cyber security, recurrent neural networks (RNNs) | Deep belief networks as well as feature selection techniques for intrusion detection Artificial neural networks and CNNs are utilized to identify malware. portable/a droid Malware detection utilizing static characteristics and superficial machine learning algorithms Fraud and spam detection utilizing Naive Bayes, Ml, and DL models | LR = 0.85<br>RF= 0.94<br>ANN= 0.96<br>DT= 0 .98 |
| G UTHEJ et al. | 2022 | | Machine Learning (ML) technologies could be utilized to train and detect cyber-attacks (utilized Support Vector Machine (SVM)) | DoS/DDoS attack or not | The results demonstrate how the proposed algorithm may be utilized to effectively locate application layer attacks. |
| Akhtar et al. | 2023 | CICIDS2017 dataset | reinforce support vector machine (SVM), ANN, RF, CNN | Intrusion Detection Systems (IDS) | This study assists in determining the best forecasting algorithms, assisting in predicting the best results to ascertain whether or not digital assaults occurred. |
| Diwakar Reddy M et al. | 2021 | CICIDS2017 dataset | 1. Every data set should be normalized.<br>2. Create training as well as testing datasets utilizing that dataset.<br>3. Create IDS models with assistance of RF, ANN, CNN, as well as SVM techniques.<br>4. Calculate the performances of every model. | Intrusion Detection Systems (IDS) | 97.80% and 69.79% precision rates |
| Mounika and Reddemma | 2022 | CSIC 2010 HTTP dataset | This article suggests utilizing artificial intelligence (AI) to detect implementation layer attack. | For the development of typical HTTP requests given through clients to the web application, a graph-based solution is suggested. | the results demonstrating how the proposed algorithm may be utilized to effectively locate implementation layer attacks |

DOI: 10.31695/IJASRE.2023.9.8.5

| | | | | | |
|---|---|---|---|---|---|
| Alsamiri and Alsubhi | 2019 | Bot-IoT dataset | utilizing machine learning (ML) techniques to solve recognizing attacks issues (we utilized K-nearest neighbors (KNN), ID3 (Iterative Di chotomiser 3), Quadratic discriminant analyses (QDA), Random Forest, AdaBoost, Multilayer perceptron (MLP), as well as Naive Bayes (NB) as machine learning algorithms). | An enhancement in IoT network attack prediction | F-measure had a value among zero and one, Naive Bayes, QDA, Random Forest, ID3, AdaBoost, MLP, as well as K Nearest Neighbors each had values among 0.77 and 0.97. |

## 3.2COMPARATIVE ANALYSIS FOR DETECTING CYBER SECURITY ATTACKS USING DEEP LEARNING

In the table 2 will illustrate the comparison between the previous systems for detecting cyber security attacks utilizing deep learning (DL)

**Table2.2 Comparative Analysis for Some detecting cyber security attacks utilizing deep learning (DL)**

| Ref. | Year | Dataset | Methods/ Technique | Detecting cyber security attacks | Accuracy |
|---|---|---|---|---|---|
| Al-Abassi et al. | 2020 | two real ICS datasets. | Cyberattack detection utilizing Deep Neural Network (DNN) as well as Decision Tree (DT) classifiers | Intrusion Detection Systems (IDSs) | The results of the experiment demonstrate that the suggested strategy outperforms common classifiers like Random Forest (RF), Deep Neural Network (DNN), as well as AdaBoost. (In both datasets assessed, our suggested technique outperformed traditional classifiers with a better f1-score as well as better precision, with%99.67 for the Secure Water Treatment dataset and%95.86 for the Gas Pipeline dataset.) |
| Diro and Chilamkurti | 2017 | KDDCUP99, ISCX & NSL-KDD | Utilizing a distributed attack detection technique, deep learning (DL) | (normal, DoS, Probe, R2L.U2R) | For a classification that is binary, the deep model has a recall of 99.27% compared to the traditional model's 97.50%. In a similar manner DM's average memory is 96.5%, while SM's average recall in the multiple classification test was 93.66%. |
| Almalaq et al. | 2022 | ICS cyber-attack data set | Support vector machine (SVM), k-nearest neighbor (KNN), extreme gradient boosting (XGBoost), | To detect errors and cyberattacks in the electrical system, a strategy is suggested. | 93.6% & an precision rate of 93.91% |

DOI: 10.31695/IJASRE.2023.9.8.5

| | | | | | |
|---|---|---|---|---|---|
| | | | gradient boosting decision tree (GBDT), and convolution neural network (CNN) | | |
| Jullian et al. | 2023 | NSL-KDD & BoT-IoT dataset | a new distributed deep learning (DL)-depend on attack detection structure in IoT networks | FFNN with LSTM models are compared to find the better model for various cyberattacks. | A precision achieved up to 99.95% |
| Lin et al. | 2022 | HCRL Car-Hacking dataset | utilizing the VGG16 model to verify achievement | replies to the VGG16 classifier deep learning model (DL) with a suggestion for an intrusion detection model for IVNs. | 97.8241% & 99.9995% |
| Duong | 2021 | UNSW - NB15 dataset | suggest employing the CNN-LSTM deep learning model to analyze network traffic to identify cyberattacks. | CNN-LSTM deep learning (DL) model | Precision of 98.1%, Precision of 94.5%, & Recall of 90.2 %. |
| Aldhyani and Alkahtani | 2022 | CAV dataset | For long-term knowledge reliance, LSTM is given as a temporal recurrent neural network (RNN). | For recognizing attack messages, convolution neural networks (CNN) with a hybrid network (CNN-LSTM) model which utilizes CNN and long short-term memory (models) were utilized. | high precision (97.30%) |

## 4. CONCLUSION

Deep learning (DL) together with machine learning (ML) are becoming more and more significant in the field of cybersecurity. We have conducted a comprehensive review of recent work on both machine learning combined with deep learning for cyber security attack detection in this article. We compiled key ideas from numerous machine learning (ML) together with deep learning (DL) models as well as their more complex principles. We also provided the required tools, such as datasets and a general framework. We examined the state-of-the-art machine learning (ML) along with deep learning (DL)-based on cybersecurity solutions in a variety of application scenarios.

## REFERENCES

[1] JANG-JACCARD, J. & NEPAL, S., "A survey of emerging threats in cybersecurity", Journal of computer and system sciences, 2014, 80, 973-993.

[2] NAWAY, A. & LI, Y., "A review on the use of deep learning in android malware detection", arXiv preprint arXiv:1812.10360 , 2018.

[3] ALSHEHRI, A., KHAN, N., ALOWAYR, A. & ALGHAMDI, M. Y., "Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics", Computer Systems Science & Engineering, 44, 2023.

[4] EL-REWINI, Z., SADATSHARAN, K., SELVARAJ, D. F., PLATHOTTAM, S. J. & RANGANATHAN, P., "Cybersecurity challenges in vehicular communications", Vehicular Communications, 23, 100214, 2020.

[5] GHAZAL, S. F. & MJLAE, S. A., "Cybersecurity in Deep Learning Techniques: Detecting Network Attacks", International Journal of Advanced Computer Science and Applications, 13, 2022.

[6] SHAUKAT, K., LUO, S., CHEN, S. & LIU, D., "Cyber threat detection using machine learning techniques: A performance evaluation perspective", 2020 international conference on cyber warfare and security (ICCWS), 2020. IEEE, 1-6.

[7] "What is Cyber-Security?" https://www.kaspersky.com.au/resource-center/definitions/what-is-cyber-security (accessed January 11, 2020).

[8] BERMAN, D. S., BUCZAK, A. L., CHAVIS, J. S. & CORBETT, C. L, "A survey of deep learning methods for cyber security". Information, 10, 122, 2019.

[9] BARIK, K., MISRA, S., KONAR, K., FERNANDEZ-SANZ, L. & KOYUNCU, M., “Cybersecurity deep: approaches, attacks dataset, and comparative study”, Applied Artificial Intelligence, 36, 2055399, 2022.

[10] CHYAD, H. S., MUSTAFA, R. A. & GEORGE, D. N., “Cloud resources modelling using smart cloud management”, Bulletin of Electrical Engineering and Informatics, 11, 1134-1142, 2022.

[11] CHYAD, H. S., MUSTAFA, R. A. & SALEH, K. T., “Study and implementation of resource allocation algorithms in cloud computing”, International Journal of Engineering & Technology, 7, 591-594, 2018.

[12] MUSTAFA, R. A., CHYAD, H. S. & MUTAR, J. R., “Enhancement in privacy preservation in cloud computing using apriori algorithm”, Indonesian Journal of Electrical Engineering and Computer Science, 26, 1747-1757, 2022.

[13] HUSSEIN, S. A., “A New wireless sensor networks Routing Algorithm Based on SPIN Protocols and Circumference Technique”, 2020.

[14] KAREEM, E. I. A. & HUSSEIN, S. A., “Optimal CPU Jobs Scheduling Method Based on Simulated Annealing Algorithm”, Iraqi Journal of Science, 3640-3651, 2022.

[15] MUNEER, S. M., ALVI, M. B. & FARRAKH, A., "Cyber Security Event Detection Using Machine Learning Technique, International Journal of Computational and Innovative Sciences, 2, 42-46, 2023.

[16] VADIVELAN, N., BHARGAVI, K., KODATI, S. & NALINI, M., "Detection of cyber attacks using machine learning", AIP Conference Proceedings, 2022. AIP Publishing.

[17] G UTHEJ, K MOHAMMED HUZAIFA, BALA SURESH BABU, A SAI KUMAR, Dr. C.GULZAR., "DETECTION OF CYBER ATTACK IN NETWORK BY USING MACHINE LEARNING", Journal of Engineering Science. ISSN NO:0377-9254, Vol 13, Issue 06, June,2022.

[18] AKHTAR, C. G., HARIKA, N. S., PALLAVI, K., AKHILA, P. & SRINAINA, T., "CYBER ATTACK DETECTION USING MACHINE LEARNING", Turkish Journal of Computer and Mathematics Education (TURCOMAT), 14, 344-348, 2023.

[19] Diwakar Reddy M, Bhoomika T Sajjan, Anusha M, Syed Jafar Sadiq B M , Shambulingappa H S., "Detection of Cyber Attack in Network using Machine Learning Techniques", International Journal of Advanced Scientific Inovation. ISSN: 2582-8436. Volume 01 Issue 02, May 2021.

[20] MOUNIKA, V. & REDDEMMA, B., "Detecting Cyber Attacks by Applying Machine Learning Techniques", ISSN: 0974-5823, ol. 7 No. 1 January 2022.

[21] ALSAMIRI, J. & ALSUBHI, K., "Internet of things cyber attacks detection using machine learning", International Journal of Advanced Computer Science and Applications, 10, 2019.

[22] AL-ABASSI, A., KARIMIPOUR, H., DEHGHANTANHA, A. & PARIZI, R. M., "An ensemble deep learning-based cyber-attack detection in industrial control system", IEEE Access, 8, 83965-83973, 2020.

[23] DIRO, A. A. & CHILAMKURTI, N., "Distributed attack detection scheme using deep learning approach for Internet of Things", Future Generation Computer Systems, 82, 761-768, 23 August 2017.

[24] ALMALAQ, A., ALBADRAN, S. & MOHAMED, M. A., "Deep machine learning model-based cyber-attacks detection in smart power systems", Mathematics, 10, 2574, 2022.

[25] JULLIAN, O., OTERO, B., RODRIGUEZ, E., GUTIERREZ, N., ANTONA, H. & CANAL, R., "Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework", Journal of Network and Systems Management, 31, 33, 2023.

[26] LIN, H.-C., WANG, P., CHAO, K.-M., LIN, W.-H. & CHEN, J.-H., "Using deep learning networks to identify cyber attacks on intrusion detection for in-vehicle networks", Electronics, 11, 2180, 2022.

[27] DUONG, L. V., "Optimization of cyber-attack detection using the deep learning network. International Journal of Computer Science & Network Security", 21, 159-168, 2021.

[28] ALDHYANI, T. H. & ALKAHTANI, H., "Attacks to automatous vehicles: A deep learning algorithm for cybersecurity", Sensors, 22, 360, 2022.