A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model

Sangeetha Prabhu[1] & Nethravathi P. S.[2]

[1]Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India.

ORCID: 0000-0002-8026-1133; E-mail: sangeethaprabhu96@gmail.com

[2] Professor, College of Computer and Information Sciences, Srinivas University, Mangalore, India.

ORCID: 0000-0001-5447-8673; Email: nethrakumar590@gmail.com

Subject Area: Computer Science.
Type of the Paper: Review based Research Analysis.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.6349848
Google Scholar Citation: IJAEML

How to Cite this Paper:

Prabhu, Sangeetha, & Nethravathi, P. S., (2022). A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *6*(1), 149-159. DOI: https://doi.org/10.5281/zenodo.6349848

International Journal of Applied Engineering and Management Letters (IJAEML)
A Refereed International Journal of Srinivas University, India.

Crossref DOI : https://doi.org/10.47992/IJAEML.2581.7000.0126

Received on: 24/02/2022
Published on: 14/03/2022

A Review on Conceptual Model of Cyber Attack Detection and Mitigation Using Deep Ensemble Model

Sangeetha Prabhu[1] & Nethravathi P. S.[2]

[1]Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India.

ORCID: 0000-0002-8026-1133; E-mail: sangeethaprabhu96@gmail.com

[2] Professor, College of Computer and Information Sciences, Srinivas University, Mangalore, India.

ORCID: 0000-0001-5447-8673; Email: nethrakumar590@gmail.com

ABSTRACT

Purpose: *When communication networks and the internet of things are integrated into business control systems, they become more vulnerable to cyber-attacks, which can have disastrous consequences. An Intrusion Detection System is critical for identifying and blocking attacks in IoT networks. As a result, utilizing a unique Classification and Encryption approach, this article offered a novel architecture for attack node mitigation.*

Design/Methodology/Approach: *This study reviews the current status of various cyber-attack detection models and their mitigation techniques. The proposed model works so that the system is first trained on the dataset, including the DDoS attack and ransomware components. The model examines if it contains malware from DDoS or Ransomware. When tested, we use trained information or a data set to provide the results on attack existence and what sort of attack we offer the extracted characteristics of the input. When the model identifies the attacker node, it is removed via the BAIT technique from the network.*

Findings/Result: *Recognizing the importance of information security is critical to combating cybercrime and encouraging cyber security. There are numerous tactics, strategies, and equipment currently in use to detect intrusion in a computer network, and continuing research is being conducted to improve their ability to detect intrusion. The basic version of a cyber-assault detection and mitigation system using the BRELU-RESNET method was evaluated in this study.*

Originality/Value: *This review-based research article examines the present state of cyber-attack detection and mitigation, as well as the research gaps and research goals.*

Paper Type: *Review-based research analysis*

Keywords: Cyber-attack detection, BAIT approaches, Cryptosystem, Feature extraction, Deep Ensemble Model, Cyber-attack mitigation

1. INTRODUCTION :

The virtual revolution of big-scale production environments promotes the usage of massive statistics analytics in solving plant outages, equipment breakdowns, fault prediction, and ensuring cybersecurity through the extension of computer networks and interconnectivity of computer systems in cyber-physical structures [1] [2]. The topic of cyber-defense has aroused academics' interest in recent years, particularly as cyber-physical networks have evolved into extremely dangerous cyber-assaults that might endanger any section of the unexploited cyber surface [3]. This highlights the need of implementing area green identification algorithms and robust solution mechanisms that protect both the cyber and physical parts of the infrastructure - a necessary precondition for improving operational technologies [3] [4]. Many contributions have been made throughout this field of operational technologies by the process automation and control group in particular.

CPS (Cyber-Physical Systems) is a term used to describe the mixture of computational, communication, and physical components [5] [6]. Cyber-Physical Systems CPS is a modeling tool that can be used to simulate a wide range of applications, including sophisticated critical infrastructures. Indeed, the widespread integration of Cyber-Physical Systems in vital infrastructures has increased their significance in sustaining economic growth, and their stability and durability have

become essential in all facets of modern life [7] [8]. Security incidents and component faults are two of the biggest abnormalities that can disrupt CPS's daily function. Since CPS are so essential to contemporary society's day-to-day activities, they've become a tempting choice for cybercriminals. Because of their extensive use, their attack surface has grown significantly [9]. Various components of the CPS, like every other physical control device, will malfunction at the same time. Both faults and attacks can cause the machine to behave abnormally, but the consequences can be somewhat different. CPS operators may select the appropriate rehabilitation actions that mitigate the detrimental consequences of irregular behavior as they can differentiate [10]. Defining the criteria that could lead to such distinction is a difficult challenge that necessitates a thorough examination of individual components in a CPS structure before arriving at a holistic solution [11] [12].

A malfunction that influences any of CPS's components will cause it to behave abnormally (nodes). Fault detection in CPS has proven to be a difficult challenge due to the system's complexity and large size, as well as the fact that flawed activity is a complex and diverse problem [13]. Traditional CPS fault detection methods focus on the operator's knowledge, while more recent approaches, which characterize the modern IoT age, rely on sensor and alarm data. Machine learning methods and human expertise are combined in certain IoT solutions for fault diagnosis [14] [15]. Synthetic neural networks, for example, are used in defect detection in power and smart grid systems because they are adaptable systems inspired by organic systems. Radial Basis Function and Support Vector Machines are two popular methods in artificial neural networks. Other methods [16] make use of logic to avoid latent faults that can occur when a stable environment is caused by a control system for a failure condition. Existing CPS security procedures are usually classified according to the security triad of secrecy, transparency, and availability [17] [18]. A security reason is frequently linked to the right mitigation measures that are looking for an adversary to safeguard a cps machine defined by a certain device version.

The proposed model works so that the system is first trained on the dataset, including the DDoS attack and ransomware components. The model examines if it contains malware from DDoS or Ransomware. When tested, we use trained information or a data set to provide the results on attack existence and what sort of attack we offer the extracted characteristics of the input. When the model identifies the attacker node, it is removed via the BAIT technique from the network.

2. OBJECTIVES OF THE PROPOSED WORK :

From cyber-attacks, cyber defense ensures the secrecy of computer-linked structures, software, hardware, and data. Without a security policy in place, an attacker can easily gain access to your device and misuse your personal information, client information, business intelligence, and much more. This analysis is being completed with the goal of better understanding the definitions of cybercrime and cyber security, as well as proposing effective and appropriate therapies to address these issues in today's internet world. Similarly, the purpose of the examination is to give a framework for brand spanking new analysis possibilities. The following items are essential for achieving the desired result:

(1) To review the recent cyber-attack system, and also to define the clear problem statement on the same aspect.
(2) To introduce a new cyber-attack detection, particularly focusing on anomaly behavior from attacks like DDoS and ransomware attacks.
(3) To introduce the deep ensemble technique for detecting the presence of attack in the network and also to mitigate it using the BAIT approach.
(4) To process the BAIT model for mitigating the attacker from the network.
(5) To assess the feasibility of the proposed system concerning certain performance metrics against other state-of-the-art frameworks.

3. OVERVIEW OF SYSTEMATIC LITERATURE REVIEW METHODOLOGY :

The review of literature is an important procedure that offers a strong foundation for the growth of knowledge. It makes it easier to look at areas where more research is needed [5]. The goal of this project is to undertake a comprehensive review of the literature to provide current research solutions for the development of a cyber-assault detection and mitigation device. To create a literature review framework, we used Kitchenham's [4] systematic literature review tips. The process for conducting a literature review to address the study's objectives is discussed in the subsections that follow. In the following subsections, the literature assessment framework outlines the questions for studies to

consider, the technique for discovering relevant studies, the selection of studies to include in the literature overview, the evaluation of reviewed articles, and the synthesis of study findings.

3.1 Research Queries for Study:

The following research questions were derived from the goals of the literature review and were concerned in responding to the following research problems:
Q1: What are the various tactics for detecting and mitigating cyber-attacks?
Q2: What are the most up-to-date ways for imposing a model for detecting and mitigating cyber-attacks?
Q3: What are the research gaps in cyber-attack detection and mitigation strategies?

3.2 Search strategy:

This section covers the method for generating search keywords, the search approach, the scanned databases, and seeking literature.

3.2.1 Look for keywords and approach:

The keywords we chose for our search were identified from previous experience in the field of study. The key database seeks string is "cyber-attack detection and mitigation" to raise awareness of the many processes that go into place to detect cyber-attacks.

3.2.2 Database searches:

We developed a list of probable databases for laptop technological know-how study using the Google search engine. The following indexed databases were searched:

- Research Gate
- IEEE Xplore
- Science Direct
- Google Scholar

Non-refereed papers were excluded because the database search option allows for a more advanced search, and we may also want to limit papers by the problem to laptop science. Between January 2001 and December 2021, the search was carried out.

3.3 Three selections of observers:

This phase indexes the technique and specific documentation used to select studies for a systematic literature evaluation for enforcing a model of attack detection and mitigation.

3.3.1. Method of deciding what to look at:

Three steps of selection are used to select papers for inclusion in the systematic literature review. (1) Preliminary research selection based on name; (2) research selection technique mostly based on evaluating the abstract concept; and (3) Research selection procedure primarily based on reviewing the abstract concept. (4) Fourth method of selection is based on the general content of the article. The range of articles being reviewed at each stage of the choice procedure is shown in table 2.

Table 2: shows the number of papers reviewed at each stage of the selection process.

Stages	Selection Process	Total Papers
Phase 1	Based on the title	632
Phase 2	By reviewing the abstract concept	153
Phase 3	By reading the full article	75
Phase 4	Studies selected	28

Except for convention proceedings, we started with 632 papers from the database search in section 1 and selected 153 papers for the next section of paper screening. In section 3, 75 papers had relevant ideas that necessitated a thorough reading of the articles, and 28 papers were chosen as the very last to be reviewed.

3.3.2. Documentation of the studies chosen:

Before the selection of papers for review, redundant papers were identified using advanced database keyword searches. Studies research assessed at each aspect of the screening system were documented

in distinct spreadsheets in the excel spreadsheet utility for each segment of the decision technique. Non-refereed publications were eliminated because the database search option allows for a more advanced search, and we may also want to limit papers by the problem to laptop science. Between January 2003 and December 2021, the search was carried out.

3.4 Three options for observation:

This phase indexes the method and documentation used to select research for a comprehensive literature evaluation for imposing a model of attack detection and mitigation.

3.4.1. Choosing a look is done in a certain way:

Three steps of selection are used to select papers for inclusion in the systematic literature review. (1) Preliminary research selection based on name; (2) research selection technique mostly based on evaluating the abstract concept; and (3) research selection procedure primarily based on reviewing the abstract concept.

4. OVERVIEW OF RELATED WORK :

This section gives an extensive review of the cyber-attack detection and mitigation system:

Zhe et al. [19] proposed an RNN-based kingdom reconstruction approach for state estimation of nonlinear strategies after the discovery of cyber-assaults on sensor data in 2020. The suggested approach was adopted to detect cyber-attacks in closed-loop operations using machine-learning-based detection systems, and an RNN model was created to recreate process states using fraudulent state measures to quantify control behavior. The RNN-based configuration re-constructor was used in real-time inside LMPC and LEMPC to give correct balance analysis and ensure closed-loop consistency of the nonlinear techniques upon cyber-assault detection. Using a chemical procedure context and min-max, surge, and geometric cyber-attacks, the country's re-efficacy constructors in reassembling system states for both LMPC and LEMPC were demonstrated.

Georgios et al. [20] investigated an Energy-Aware Smart Home system's internal connectivity climate in 2020. In EASH, the issue of distinguishing between equipment failure and network attacks was described in terms of their impact on communication. The relationship between these abnormality sources was shown, and a machine learning-based architecture for the differentiation issue was developed. The suggested method was calibrated in both a simulation and a real-time testbed setting, and it demonstrated a positive classification performance of over 85%. Obtained from experimental findings, a quantitative description of the considered classes was given, as well as functionality used in the suggested method to increase classification accuracy.

In 2018, Wang et al. [21] proposed a two-stage sparse cyber-assault model for smart grids with complete and partial network data that was situation-based. The presented cyber-attacks were successfully detected, and a unique security technique based on interval nation estimation was implemented. To maximize the function variable's variance cycles, the top and decreasing limits of each country variable were represented as a twin optimization issue using this strategy. Furthermore, the stacked auto-encoder, a well-known deep learning set of rules, was used to collect nonlinear and non-stationary data in electric-powered load outcomes. Such features were then used to increase predictive performance for electric loads, resulting in state variables with a narrow width. A parametric Gaussian distribution was used to represent the variance of forecasting errors. Comprehensive studies on numerous IEEE benchmarks have been used to show the validity of the current cyber-attack models and security mechanisms.

In 2019, Defu et al. [22] proposed a device learning-based completely attack detection version for energy structures that was taught using data and logs obtained via phasor size units. The findings demonstrate that the data processing method could increase the model's precision, and the AWV model could efficiently identify 37 different types of power grid behaviors. The feature development engineering was completed, and the data was then sent to various machine learning models, with the random forest being selected as AdaBoost's simple classifier. Finally, various comparison criteria were used to equate the proposed model to other ones. The experimental findings show that this model can reach a 93.91 percent accuracy rate and a 93.6 percent identification rate, which is better than eight recently established techniques.

In the year 2020, Perez et al. [23] suggested a flexible modular architecture for detecting and mitigating LR-DDOS threats in SDN environments. The intrusion detection system was trained in the structure using six system mastering (ml) models, and their overall performance was assessed using the dos dataset from the Canadian Institute of Cybersecurity. Despite the challenges of detecting LR-

DoS attacks, the results of the analysis show that this approach accomplished a detection rate of 95%. The eminent virtual gadget's OS controller is utilized to keep our simulated environment as close to genuine production networks as possible. All attacks experienced by the intrusion prevention detection device inside the testing topology are mitigated by the intrusion prevention detection device. This demonstrates how effective our system is at recognizing and stopping LR-DDOS attacks.

The unattended detection of anomalies based on the statistical correlation between measurements was proposed by Karimipour et al. [24] in 2019. The objective of the adopted model was to develop a configurable anomaly detection engine for high-scale intelligent networks that distinguished between an actual failure and a disorder and an intelligent cyber-attack. To reduce computation complexity while finding causal relationships across subsystems, the strategy presented utilizes symbolic dynamic filtering. The simulation results of IEEE 39, 118, and 2848 bus structures confirm the approach's performance under a variety of operating situations. The findings demonstrate that 99% of the positive and false-positive rates are genuinely positive and less than 2%.

In 2020 Wei et al. [25] established a recovery strategy for the optimal re-closure of the trickled transmission lines. In specific, a framework for deep strengthening learning (RL) has been created to enable the strategy to adapt the unpredictable cyber-attack scenarios and to take decision-making capabilities in real-time. In this context, an environment has been created for simulating energy device dynamics and generating training data during the assault-recovery process. The profound RL strategy to determine the optimal lock-up time was trained with this information. Numerical outcomes demonstrate that the approach utilized would minimize cyber-attack effects in different circumstances.

Ismail et al. [26] investigated energy theft inside the dg domain in the year 2020. In this attack, malevolent clients hack the smart meter to monitor their renewable dg devices and exploit their records so that it declares more power to the grid. Deep system learning has been investigated as a means of detecting such harmful behavior. This research found that combining dg smart meters, weather reviews, and SCADA metering parameters in a deep co-evolutionary-neural network yields the greatest detection rate (99%) and the lowest false alarm rate (≈ 0%).

5. IDEA BEHIND IMPLEMENTATION OF A CYBER ATTACK DETECTION AND MITIGATION MODEL :

It's becoming more difficult to prioritize and respond to threats as there are more digital operations and a more complex threat landscape. The consequences of an event are extended to third parties and the cloud through digital transformation. As a result, with threat identification and remedy integrations, it is critical to include integrated hazard control as part of the mitigation strategy. Before displaying unusual actions that could suggest a compromise, Ml algorithms learn about their environment and organize baseline norms. However, if the cy is continually reinventing itself to meet business agility needs and the dynamic environment lacks a consistent baseline, the set of rules will be unable to establish what is normal and will raise red flags for seemingly innocuous behaviors. The most common critique of ml-detection software is the "impossible" number of signs it generates thousands of alarms each day, thereby handing out a denial-of-service attack to analysts. While a real alert will make its way to a security analyst's queue, this effective correlation will take the arrival of a black box and leave nothing more than a ticket that says "alert." From there, an analyst will have to sift through logs and activities to figure out what caused the movement.

6. CURRENT APPROACHES FOR IMPLEMENTING CYBER ATTACK AND DETECTION MODEL :

Table 1 shows the reviews on cyber-attacks-based machine learning techniques. Initially, the RNN model was deployed in [19], which presents small deviation, reliable correction, and maximum destabilizing effects; however, the starting state reconstruction was not limited. ANN classifier [20] was used to increase the classification performance, low energy failure, and less packet drop failure, but the proposed study stated that the outcomes of the classification should be changed to include/remove attributes from descriptive datasets. Moreover, a stacked auto-encoder (SAE) model was deployed in [21] that offers high detection accuracy, MAPE, and robustness. However, an algorithm for the solution of the L0-norm minimization problem must be created. Likewise, the AWV model was exploited in [22], which offers a better classification effect, high accuracy, improved precision, maximum recall, and higher F1 score. However, the related data must be increased and a deep learning model combined with big data analytics must be created. The SDN model has been used

in [23] with maximum accuracy, false alarm rate, high precision, improved retrieval, and maximum F1; but the proposed model does not include newer Machine Learning or deep learning techniques. In addition, the DBN model was introduced in [24], which offers better accuracy, true positive rate, and less FPR. However, the proposed scheme's success rate does not depend on the attack scenarios. Deep reinforcement learning (RL) framework was suggested in [25] that offers to minimize cyber-attack impacts, low MSE, and improve the system stability. However, the training data did not include the data produced in Scenario 1 and Scenario 2. Finally, in [8], the hybrid C-RNN detector model offered the lowest detection rate and false alert but the solidity of the adopted detector against new cyber-attacks was seen not in the training period of the detector. For cyber-assaults-based entire system mastering tactics in the gift to work effectively, such constraints must be taken into mind.

Table 1: summary of current approaches being used in cyber-attacks detection and mitigation

Author	Adopted methods	Features	Challenges
Zhe *et al.[* 2020][19]	RNN model	• Small deviation • Reliable correction • Maximum destabilizing effects	• The starting state reconstruction was not limited.
Georgios *et al.[2020]* [20]	ANN classifier	• Improved classification accuracy • Low Energy Failure • Less Packet Drooped failure	• The classification findings will benefit from the addition/removal of features from the illustrative datasets.
Wang *et al.[2018]* [21]	SAE model	• High detection accuracy • MAPE • Robustness	• The development of an algorithm to solve the L0-norm minimization problem must be prioritized.
Defu *et al.* [2019][22]	AWV model	• Better classification effect • High accuracy • Improved precision • Maximum recall • Higher F1 score	• The amount of relevant data must be increased, and progress on a deep learning platform that is integrated with Big Data analytics must be undertaken.
Pérez *et al. [2020]* [23]	SDN model	• Maximum accuracy • False alarm rate • High precision • Better recall • Maximum F1-measure.	• The proposed model did not incorporate the more recent ML and deep learning strategies.
Karimipour *et al. [2019]* [24]	DBN model	• Better accuracy • True positive rate • Less FPR	• The proposed scheme success rate does not depend on the attack scenarios.
Wei *et al.[2020]* [25]	Deep RL framework	• Minimize cyber-attack impacts • Low MSE • Improve the system stability	• The training facts no longer included the statistics created in scenario 1 and state of affairs 2.
Ismail *et al.* [2020] [26]	Hybrid C-RNN detector model	• Highest detection rate • Lowest false alarm	• The resilience of the following detector was put to the test in opposition to fresh cyber-attacks that were not existent at the time of the detector's training.

7. RESEARCH GAP :

The internet has evolved into a key infrastructure for both businesses and individual users, and its security has become a major concern. Protection is also a significant component in inspiring the purchaser confidence required to achieve commercial success for the new technologies that are emerging in today's connected world. Regression may be used to solve fraud detection in cybersecurity. It determines fraudulent transactions once a model is discovered from the historical transaction database, mostly based on observable attributes of recent transactions. System analysis methodologies are commonly used to solve a variety of cybersecurity issues. Advances in the realm of device understanding and deep mastery have the potential to provide viable answers to cybersecurity challenges. However, understand which set of rules is appropriate for particular usefulness. To keep the solution resistant to malware attacks and achieve high detection rates, multi-layered processes are required. When it comes to resolving cybersecurity difficulties, the choice of a selected version is crucial.

Research gap 1: ANN classifier method entails evaluating online data sets to solve the problem of malicious attack detection. This is accomplished by utilizing an iteratively naïve Bayesian classifier. Active learning, on the other hand, allows the problem to be solved using a limited set of specified data points, which are also very expensive to obtain.

Research gap 2:: Any statistically-based fully discriminating technique must effectively describe the baseline network conduct, which is extremely difficult to do given the dynamic nature of today's networks. Person conduct modeling tactics are a problem in almost all of the jobs. Data mining of internet server logs to simulate the baseline surfing behavior of genuine users is a time-consuming and error-prone task.

Research gap 3: The public of the available replies is mere of educational relevance because they are aware of detecting DDOS attacks with a high detection rate or a low false alarm rate. Only a few of these have been put into practice in real-time.

Research gap 4: Some academics have attempted to employ simulation and emulation-based research to synthesize datasets using a set of benchmark DDOS attack gear, however, those datasets are missing important site visitor elements. In an ideal world, the collected community hint would contain a balanced mix of practical heritage traffic and assault site visitors, with no preference for one type of traffic over the other. However, because there is no established formula for effectively modeling net visitors, it is difficult to ensure a proper mix of regular and assaultive visitors in a real-world dataset.

8. METHODOLOGY :

The Cyber-Physical System (CPS) connects the physical and electronic worlds and is typically used for industrial manufacturing control systems (ICS) to allow people to understand all types of necessary information in real-time. The use of CPS in places like power generation grids and waste-water treatment plants has a lot of promise. However, CPS security concerns are distinct from conventional cybersecurity concerns in that they concern confidentiality, integrity, and availability. This proposal intends to introduce a novel DDoS and ransomware attack detection as well as a mitigation model. The input data is first subjected to the identification process, which distinguishes the types of attacks as well as detects their presence. The detection phase will include feature extraction and attack detection. Flow-based features like flow rate, flow byte, total forward packet, and total backward packet are extracted from the raw data collected. Moreover, the sequential frequent pattern features are extracted using the Apriori framework. To make the detection more precise, an ensemble classifier will be constructed by enclosing the Support Vector Machine 1 (SVM 1), SVM 2, and Neural Network (NN) and optimized Deep Convolutional Neural Network (DCNN). The ensemble classifier's SVM 1, SVM 2, and NN will be trained with the extracted features. Then, the outcome from SVM 1, SVM 2, and NN will be fed as input to optimized CNN, whose weights will be fine-tuned via a new hybrid optimization model such as SeaLion Optimization (S) algorithm and Whale Optimization Algorithm (WOA). EHO [27] is a modern swarm-based meta-heuristic search approach that is motivated by elephant communities led by a female matriarch. WOA [28] is a modern optimization strategy for solving optimization problems that use three operators to mimic humpback whale foraging activity such as searching for food, encircling prey, and using bubble nets. The suggested work's design is shown in Figure 1.

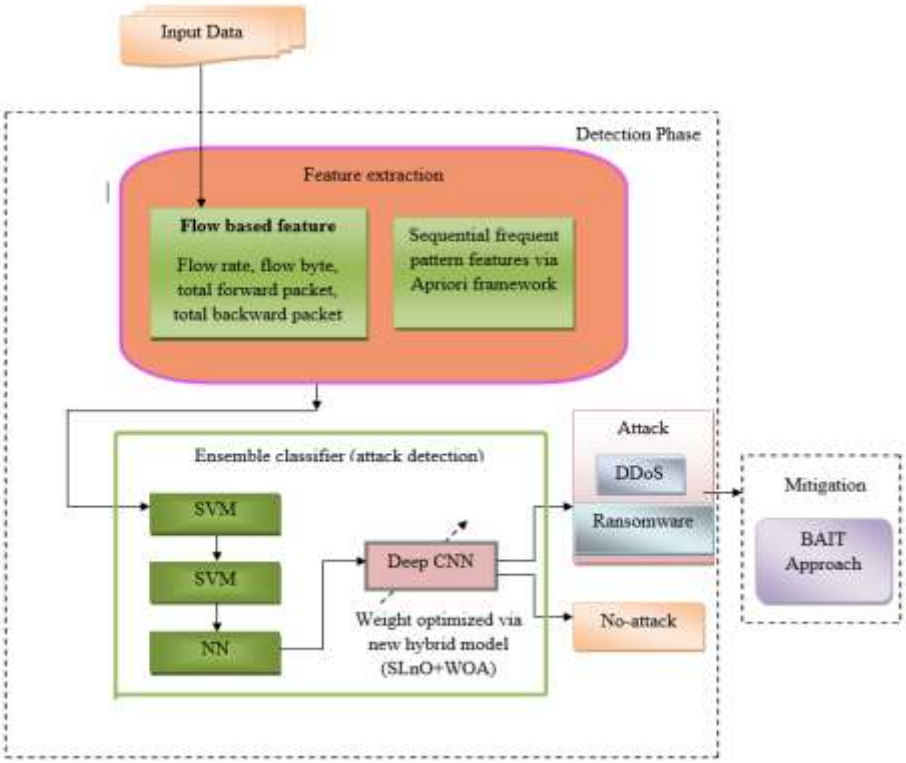

Fig. 1: Architecture of proposed work [29]

9. EXPECTED OUTCOME OF THE PROPOSED STUDY :

The suggested model, which is based on cyber-attacks and uses machine learning methods, will be simulated in MATLAB, and an experiment will be conducted. The proposed model would be compared to other state-of-the-art models in terms of accuracy, recall, precision, false alarm rate, and F1measure, among other metrics.

10. CONCLUSION :

The majority of current intrusion detection algorithms are unable of dealing with the dynamic and complicated nature of cyber-attacks on laptop networks. As a result, green adaptive strategies such as various gadget researching techniques can result in decreased false alarm rates, greater detection costs, and reasonable calculation and verbal exchange fees. The work has proposed a novel approach of BRELU-ResNet based Cyber-Attack Detection System with a BAIT-based approach for mitigation. This approach involved several operations for the efficient detection of cyber-attacks. Overall, the proposed cyber-assault detection methodology outperforms current state-of-the-art methodologies and is more reliable and robust. The study may be expanded in the future with a few more advanced neural networks, as well as a focus on specific sorts of rational attacks.

REFERENCES :

[1] Samy, A., Yu, H., & Zhang, H. (2020). Fog-based attack detection framework for the internet of things using deep learning. *IEEE Access*, *8*(1), 74571-74585.
Google scholar↗

[2] Subroto, A., & Apriyana, A. (2019). Cyber risk prediction through social media big data analytics and statistical machine learning. *Journal of Big Data*, *6*(1), 1-19.
Google scholar↗

[3] Ramotsoela, D. T., Hancke, G. P., & Abu-Mahfouz, A. M. (2019). Attack detection in water distribution systems using machine learning. *Human-centric Computing and Information Sciences*, *9*(1), 1-22.
Google scholar↗

[4] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H. & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, 6(1), 35365-35381.
Google scholar↗

[5] Kanimozhi, V., & Jacob, T. P. (2021). Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *ICT Express*, *7*(3), 366-370.
Google scholar↗

[6] Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*, *96*(1), 227-242.
Google scholar↗

[7] Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, M. (2020). Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for the internet of things in a smart city. *Future Generation Computer Systems*, *107*, 433-442.
Google scholar↗

[8] Gopalakrishnan, T., Ruby, D., Al-Turjman, F., Gupta, D., Pustokhina, I. V., Pustokhin, D. A., & Shankar, K. (2020). Deep learning enabled data offloading with a cyber-attack detection model in mobile edge computing systems. *IEEE Access*, *8*(1), 185938-185949.
Google scholar↗

[9] Hussain, B., Du, Q., Sun, B., & Han, Z. (2020). Deep learning-based DDoS-attack detection for the cyber-physical system over 5G network. *IEEE Transactions on Industrial Informatics*, *17*(2), 860-870.
Google scholar↗

[10] Aamir, M., & Zaidi, S. M. A. (2021). Clustering-based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University-Computer and Information Sciences*, *33*(4), 436-446.
Google scholar↗

[11] Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in the industrial control system. *IEEE Access*, *8*(1), 83965-83973.
Google scholar↗

[12] Saharkhizan, M., Azmoodeh, A., Dehghantanha, A., Choo, K. K. R., & Parizi, R. M. (2020). An ensemble of deep recurrent neural networks for detecting IoT cyberattacks using network traffic. *IEEE Internet of Things Journal*, *7*(9), 8852-8859.
Google scholar↗

[13] Pan, Y., Sun, F., Teng, Z., White, J., Schmidt, D. C., Staples, J., & Krause, L. (2019). Detecting web attacks with end-to-end deep learning. *Journal of Internet Services and Applications*, *10*(1), 1-22.
Google scholar↗

[14] Ibor, A. E., Oladeji, F. A., Okunoye, O. B., & Ekabua, O. O. (2020). The conceptualization of Cyberattack prediction with deep learning. *Cybersecurity*, *3*(1), 1-14.
Google scholar↗

[15] Fang, X., Xu, M., Xu, S., & Zhao, P. (2019). A deep learning framework for predicting cyberattacks rates. *EURASIP Journal on Information security*, *2019*(1), 1-11.
Google scholar↗

[16] Beno, M. M., I. R, V., S. M, S., & Rajakumar, B. R. (2014). Threshold prediction for segmenting tumors from brain MRI scans. *International Journal of Imaging Systems and Technology*, *24*(2), 129-137.
Google scholar↗

[17] Wang, H., Ruan, J., Ma, Z., Zhou, B., Fu, X., & Cao, G. (2019). Deep learning aided interval state prediction for improving cyber security in the energy internet. *Energy*, *174*, 1292-1304.
Google scholar↗

[18] Karie, N. M., Kebande, V. R., & Venter, H. S. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. *Forensic Science International: Synergy*, *1*(1), 61-67.
Google scholar↗

[19] Wu, Z., Chen, S., Rincon, D., & Christofides, P. D. (2020). Post-cyber-attack state reconstruction for nonlinear processes using machine learning. *Chemical Engineering Research and Design*, *159*(1), 248-261.
Google scholar↗

[20] Tertytchny, G., Nicolaou, N., & Michael, M. K. (2020). Classifying network abnormalities into faults and attacks in IoT-based cyber-physical systems using machine learning. *Microprocessors and Microsystems*, *77*(1), 103121.
Google scholar↗

[21] Wang, H., Ruan, J., Wang, G., Zhou, B., Liu, Y., Fu, X., & Peng, J. (2018). Deep learning-based interval state estimation of AC smart grids against sparse cyber-attacks. *IEEE Transactions on Industrial Informatics*, *14*(11), 4766-4778.
Google scholar↗

[22] Wang, D., Wang, X., Zhang, Y., & Jin, L. (2019). Detection of power grid disturbances and cyber-attacks based on machine learning. *Journal of information security and applications*, *46*(1), 42-52.
Google scholar↗

[23] Perez-Diaz, J. A., Valdovinos, I. A., Choo, K. K. R., & Zhu, D. (2020). Flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, *8*(2), 155859-155872.
Google scholar↗

[24] Karimipour, H., Dehghantanha, A., Parizi, R. M., Choo, K. K. R., & Leung, H. (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access*, *7*(1), 80778-80788.
Google scholar↗

[25] Wei, F., Wen, Z., & He, H. (2019). Cyber-attack recovery strategy for smart grid based on deep reinforcement learning. *IEEE Transactions on Smart Grid*, *11*(3), 2476-2486.
Google scholar↗

[26] Ismail, M., Shaaban, M. F., Naidu, M., & Serpedin, E. (2020). Deep learning detection of electricity theft cyber-attacks in renewable distributed generation. *IEEE Transactions on Smart Grid*, *11*(4), 3428-3437.
Google scholar↗

[27] Behal, S., Kumar, K., & Sachdeva, M. (2017). Characterizing DDoS attacks and flash events: Review, research gaps, and future directions. *Computer Science Review*, *25*(1), 101-114.
Google scholar↗

[28] Singh, R., Kumar, H., Singla, R. K., & Ketti, R. R. (2017). Internet attacks and intrusion detection system: A review of the literature. *Online Information Review*, *41*(2), 171-184.
Google scholar↗

[29] Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network intrusion detection combined hybrid sampling with the deep hierarchical network. *IEEE Access*, *8*(1), 32464-32476.
Google Scholar↗

****