Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions

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: Research Article.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.6350841
Google Scholar Citation: IJAEML

How to Cite this Paper:

Sangeetha Prabhu, & Nethravathi, P. S., (2022). Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions. *International Journal of Applied Engineering and Management Letters (IJAEML), 6*(1), 176-183. DOI: https://doi.org/10.5281/zenodo.6350841

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.2581.7000.0128

Received on: 20/02/2022
Published on: 15/03/2022

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

Novel SHP-ECC Mechanism Architecture for Attack Node Mitigation and to Predict Future Community Intrusions

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: *Because of the apparent rapid advancement in the field of information and communication technology and its constant connection to the internet, customer and organizational data have become vulnerable to cyber-attacks, necessitating the explanation of solutions to ensure the security and protection of information throughout the industry. Today, it is critical for governments and major corporations to implement cybersecurity systems to ensure the confidentiality and security of data in the face of cyber-attacks. As community-based fully systems have become more important in today's society, they've become targets for malicious actions, prompting both industry and the research community to place a greater emphasis on resolving community intrusion detection difficulties. In network intrusion detection challenges, gadget examining algorithms have proven to be a valuable tool.*

Design/Methodology/Approach: *This research provided a fully unique architecture for attack node mitigation as a result of the use of a novel type and encryption mechanism. First, the UNSW-NB15 dataset is received and separated into training and testing data. Within the Training section, information is first and foremost pre-processed, and capabilities are extracted. The relevant features are then chosen using the Taxicab Woodpecker Mating algorithm (TWMA). The BRELU-ResNet classifier is then used to classify the attacked and non-attacked data. The typical statistics are encrypted using the ESHP-ECC method, which is then saved in the security log report. Following that, the shortest distance will be calculated using Euclidean distance. Finally, the information is decrypted utilizing a set of ideas known as DSHP-ECC. If the entry appears in the log record while testing, it is marked as attacked statistics and will not be communicated. The method of detecting cyber-assaults will continue if it is not detected.*

Findings/Result: *The analysis is based on the UNSW-NB 15 dataset, which shows that the proposed approach achieves an excessive security level of 93.75 percent.*

Originality/Value: *This experimental-based research article examines the malicious activities in the cyberspace and mitigated by using a SHP-ECC mechanism.*

Paper Type: *Research Article*

Keywords: Cyber-attack detection, Attack node mitigation, BAIT approaches, Feature extraction, Future Community Intrusions, SHP-ECC Mechanism.

1. INTRODUCTION :

Cyber security is a major concern for a wide range of businesses, agencies, government entities, and individuals all around the world. According to Buczak and given in [1], cyber security is the total of all technology and methods for tracking and preventing unauthorized access, modification, misuse, and denial of service to computer networks and assets. This also involves inclinations to give access to labeled content, as well as community-on-hand infrastructure. Most networks are connected via the internet and provide a means of replacing information, intelligence, software, and hardware. Computer infrastructure attacks are becoming a more serious threat [2]. Cyber detection on a network is a critical component of system security. Although the computer networking paradigm has been important in terms of the exchange of valuable property for improved operational efficiency, it has also been a constant source of malware transmission, increasing cyber-attacks in the online world.

Computer security refers to the protection of computer systems from risks to their confidentiality, integrity, and availability. Confidentiality means that records are disclosed in the most honest way feasibility policy; integrity means that records aren't lost or damaged, and the device functions properly; and availability means that device offerings are available when they're needed. Computer structures, computer networks, and the data they carry are all checked using computing structures. The improvement and augmentation of cyber-attack detection structures have been stimulated by these dangers, as well as others that are expected to emerge in the future [3].

This shift in the risk landscape is the result of the increased threat of cyber-attacks, which are regularly gaining control of all household, organizational, and business capacities. Because of the impact of cyber strain, akyazi [4] says in work that cyber-assault risks are linked to the ability to change device or database parameters, which is a good way to create a kinetic effect for escalating attacks, as well as the proclivity to disrupt labeled contents. Preventive and reactive tactics are included in cyber-attack defense. Those approaches, which can be classified as active or passive, are utilized in the context of usage – they could be direct countermeasures or cyber-attack mitigation processes. Denning [3] noted in his work that the value of cyber defense measures is rooted in the ability to address both active and passive threats, which have become the standard in the cyber world.

Cybercriminals regularly target Industrial control systems as a target. The majority of the people who work in these areas exhibit intricate business techniques and vital infrastructures that provide power, water, shipping, production, and other crucial services [5]. There was a period when those systems were essentially dumb, and those who were automated employed protocols that were exclusive to the device and resided on networks that included the outdoors. The landscape has shifted, and as a result, the majority of business management systems in use today connect to the internet either directly or indirectly. As with any other linked device, this exposes them to vulnerabilities. Downtime or invasion of an ICS network, on the other hand, might result in massive outages, hundreds of impacted consumers, or even a national tragedy. ICS protection is a framework for defending structures against both incidental and purposeful threats. A complex network of interactive manipulation structures or a limited number of controllers can make up a business control system. These structures collect data from far-flung sensors that measure and show process factors [6]. An ICS sends commands and receives signals from a variety of unique components, ranging from control valves to stress gauges.

Several anomaly detection techniques are then incorporated to tackle the problems and hazards encountered throughout the assault detection process. These strategies are combined and used through the use of a variety of machine learning algorithms [7]. However, the bulk of existing algorithms overlooks the unbalanced structure of ICS datasets, resulting in a low detection rate or large false-positive rate in real-world scenarios [8]. Several of the current strategies would be rendered ineffective if the entire physical device was assaulted at the same time [9]. Many studies on fault-tolerant management have been undertaken, and the results of these studies can be used to develop equipment for assault-resistant management [10]. There are several factors to keep in mind when it comes to escaping surveillance and isolation, there are numerous variations between fault-tolerant controls and assault-resistant controls, necessitating the employment of exact ways to tackle protection difficulties in ICSs [11]. To address the aforementioned issue, the work proposes a framework known as a unique approach of BRELU-RESNET principally based cyber-assault detection device with BAIT-based strategy for mitigation, which ensures accurate detection of cyber-assaults while maintaining better community authenticity.

The remaining portion of the paper is organized as follows: the second phase goes deeper into the problem. Studies that may be relevant to the method under consideration. The recommended methodology referred to as a single way of BRELU-RESNET principally based cyber-attack detection system with bait-based completely strategy for mitigation, is explained in Section three. Phase 4 depicts the suggested technique's outputs and dialogue based on overall performance criteria. Phase five is the final section of the report, and it concludes with suggestions for further research.

2. LITERATURE REVIEW :

Following the revelation of cyber-attacks on sensor data in 2020, Zhe et al [12] recommended an RNN-based completely state reconstruction approach for nonlinear tactic nation estimate. The recommended technique was used to locate cyber-assaults in closed-loop operations utilizing system-gaining knowledge-based detection structures, and an RNN version was built to replicate technique states using fictitious country metrics to assess manipulative behavior. Internal to LMPC and LEMPC, an RNN-based configuration re-constructor was used in real-time to provide precise stability evaluation and ensure closed-loop consistency of nonlinear procedures during cyber-assault detection. Through min-max, surge, and geometric cyber-assaults, the re-efficacy constructor's in reassembling process states for both LMPC and LEMPC was demonstrated using a chemical way context.

Georgios et al [13] 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 percentage. Obtained from experimental findings, a quantitative description of the considered classes were given and functionality was used in the suggested method to increase classification accuracy.

In the year 2020, Perez et al [14] presented a flexible modular structure for detecting and mitigating LR-DDoS attacks in SDN environments. The intrusion detection system (IDS) was trained in the framework using six machine learning models, and their overall performance was assessed using the DoS dataset from the Canadian Institute of Cybersecurity. Despite the difficulties of identifying LR-DoS attacks, the results of the study demonstrate that this technique has a 95 percent detection rate. The OS controller on the Mininet digital system is utilized to keep the simulated environment as close to real production networks as possible. All attacks experienced by employing the intrusion detection system inside the testing topology are mitigated by the intrusion prevention detection machine. This demonstrates how good the system is at recognizing and preventing LR-DDoS attacks.

The unattended detection of anomalies based on the statistical correlation between measurements was proposed by Karimipour et al [15] in 2019. The adopted version's goal was to create a configurable anomaly detection engine for large-scale intelligent networks that could distinguish between a real malfunction, attack and, a smart cyber-attack. The method suggested using symbolic dynamic filtering to reduce computing complexity while finding causal relationships between subsystems. The results of simulations of IEEE 39,118 and 2,848 bus systems show that the technique performs well under a variety of situations. The data shows that 99 percent of the high accuracy and false-high-quality rate are mean with less than 2 percent being substandard.

Behal et al [16] investigated energy robbery in the DG domain in the year 2020. Malicious clients breach the smart meter in this attack to reveal their renewable DG units and exploit their information, allowing you to claim extra energy from the grid. A deep learning system has been used to uncover such harmful behavior. The integration of DG smart meters, weather data, and SCADA metering elements in a deep co-evolutionary-neural network yielded the highest detection rate of 99.3 percent and the lowest false alarm rate of 0.22 percent, according to this study.

3. OBJECTIVES :

(1) To introduce the deep ensemble technique for detecting the presence of attack in the network.
(2) To process a SHP-ECC mechanism model for mitigating the attacker from the network.
(3) To assess the feasibility of the proposed system concerning certain performance metrics against other state-of-the-art frameworks.

4. METHEDOLOGY :

4.1 Proposed Model for Cyber-Attack Detection and Mitigation System:

In recent years, the increasing incidence of cyber-physical system attacks has raised the priority of industrial control system cybersecurity. The current state of ICS cybersecurity is based mostly on firewalls, and other intrusion prevention technologies, which will not be sufficient to combat escalating cyber threats from influenced attackers [17]. With the help of a deep learning method, the previous research effort built a framework for identifying attacks. Even though the network's attack nodes had been identified, they were not turned down. Earlier research suggested that a framework for cyber and physical systems had been devised. Cyber-attacks have been recognised and treated in the framework using ensemble deep learning algorithms that are specifically tailored for SGCS. A deep presentation-learning arrangement has also been developed for chance management employing a single symmetric presentation from the asymmetric dataset. The correctness of models was determined to be 91.62 percent [18]. As a solution to this difficulty, an enhanced and effective adversary version will be provided. As a result, developing a unique category and encryption technique, this research proposes a single architecture for attack node mitigation. To begin with, the input records are divided into two categories: Training records and testing information. The general training statistics are pre-processed in the beginning. Functions are extracted from this input training dataset in the second stage. The feature is optimized for deciding on the important capabilities when using TWMA in the third stage. The proposed BRELU-RESNET classifier is then used to train the characteristic. The classifier divides the records into two categories: attack and normal data. If the data is about an attack, use the BAIT method to save the source IP address into a safe log record. Following that, if the facts are ordinary, they are ready to be transmitted. The statistics are initially encrypted using the ESHP-ECC set of rules during record transmission. Following that, to calculate the shortest route distance Euclidean distance is used. The records are decrypted using the DSHP-ECC method at the destination node. The testing data are checked first in the security log report when checking out. If the information's source IP address is already known, the statistics will be prohibited or an attack will be detected. Figure 1 represents the proposed framework's block diagram.

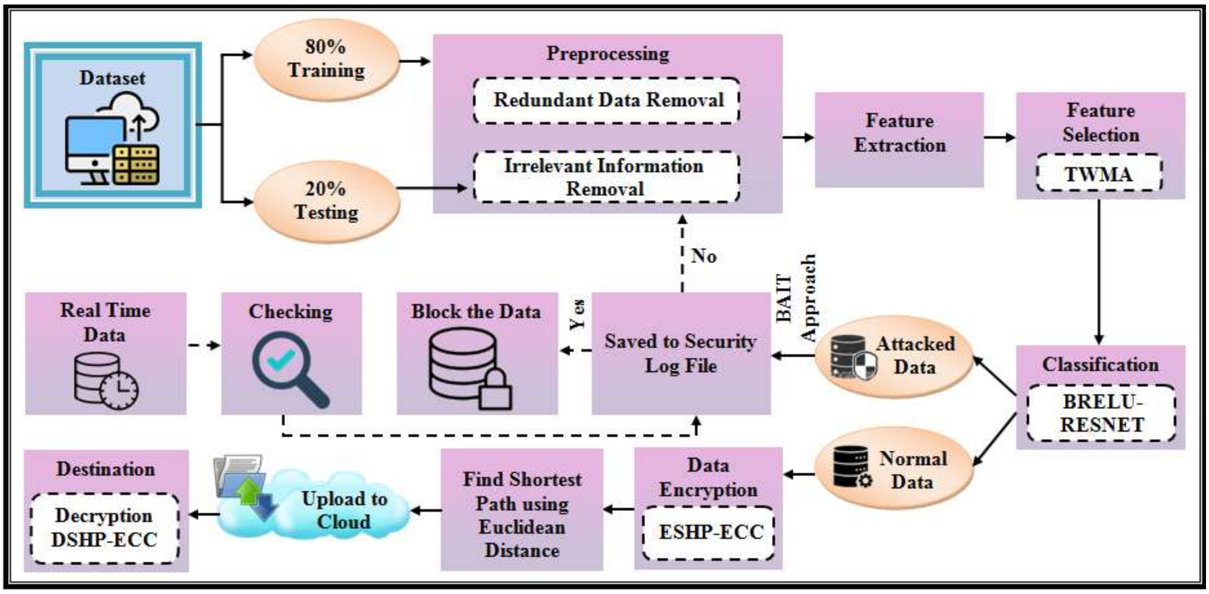

Fig. 1: The suggested cyber-attack detection and mitigation system's structural layout [19]

4.2 Data Encryption and Decryption Using SHP-ECC Mechanism:

Elliptic-Curve Cryptography (ECC) is a public-key cryptosystem based on the elliptic curve hypothesis, which is a secure unequal encryption strategy used for data security [20]. Using the elliptic curve residences, it produces public and private keys for each user. After that, the material is encrypted and decrypted using those keys. The keys are created at random in a normal ECC technique. As a result, the attackers may be able to hack the crucial information with ease. The probability of ones and zeros is generated mostly based on the randomly generated key fee in order to cope with the problem. Additionally, the relaxed hash technique is used to convert the key values into hash values. The proposed technique is referred to as encrypted because to changes inside the fashionable ECC. The relaxed hash technique is also used to turn the key values into a hash value. The recommended approach is known as Encrypted Comfortable Hash Possibility-Based Totally Elliptic-Curve Cryptography (ESHP-ECC) set of regulations due to the changes inside the current ECC. The keys are then decrypted using the Decrypted At Ease Hash Possibility-Based Elliptic-Curve Cryptography (DSHP-ECC) method.

5. RESULTS :

This section defines the precise evaluation of the proposed framework's very last outcome. The overall performance analysis, as well as the comparative analysis, are used to demonstrate the model's effectiveness. The proposed technique is implemented in Matlab, and the data are taken from the UNSW-NB 15 dataset, which is freely available on the internet.

5.1 Performance Evaluation of the Proposed SHP-ECC Mechanism:

The suggested SHP-ECC is compared to other current works such as Rivest, Shamir, Adleman, AES, and DES in terms of a variety of overall performance criteria, such as security stage, encryption time, and decryption time.

Table 1: Performance analysis of the proposed SHP-ECC based on the security level

Techniques	Security level (%)
Proposed SHP-ECC	93.75
RSA	6.25
AES	87.5
DES	12.5

Table 1 depicts the security rates achieved by the proposed SHP-ECC method and the existing works like RSA, AES, and DES.

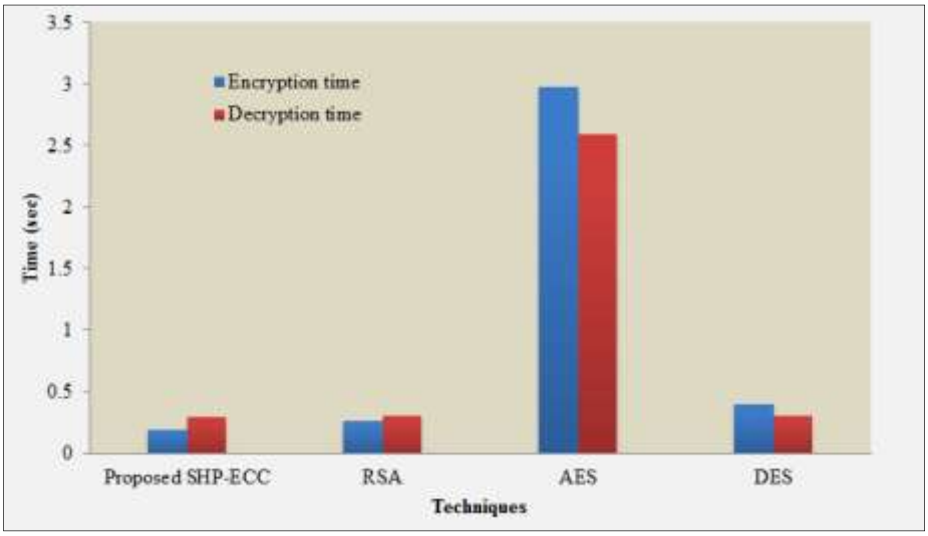

Fig. 2: Comparative analysis of the proposed SHP-ECC in terms of encryption and decryption time.

Figure 2 shows the comparison of encryption time and decryption time attained by the proposed SFP-ECC and the other exiting algorithms like RSA, AES, and DES. The efficiency of the model is determined by the low consumption of encryption and decryption time.

6. DISCUSSION :

According to the results obtained in the previous section, the tabulated data, it is known that the proposed method accomplishes a high-security rate of 93.75 percent. But the existing works exhibit the security level at an average of 35.41 percent. This is relatively low when compared to the proposed work. Hence it is concluded that the proposed work efficiently performed the encryption and decryption process and mitigates the external attack. Thus, the proposed SHP-ECC safeguards the cloud server against intruders. As per the statement, the proposed method encrypts and decrypts the data at the time of 0.1980606 seconds, and 0.3009068 seconds. But the existing works require an average of 1.218806 seconds to encrypt the data and 1.07358133 seconds to decrypt the data.

Therefore, the proposed SHP-ECC efficiently performs the encryption and decryption process with less consumption of energy and also ensures the security of the data access.

7. CONCLUSION :

The paper proposes a unique BRELU-ResNet-based Cyber-attack Detection system with a BAIT-based comprehensive mitigation mechanism. Several operations were concerned about the effectiveness of this technique in detecting cyber-attacks. Pre-processing, characteristic extraction, feature selection, and classification are all used to detect intrusions. The typing phase effectively determines whether the data are normal or malicious. The information transmission procedure commences if the records are normal. The encryption and decryption methods are implemented using the SHP-ECC set of rules to ensure security. The experimentation assessment is then completed, with an overall performance evaluation and comparative analysis of the offered methods in terms of some overall performance indicators to validate the effectiveness of the given set of rules. The improved method can deal with a wide range of uncertainty and produce even more promising results. The analysis is based on the UNSW-NB 15 dataset, which shows that the proposed approach achieves an excessive security level of 93.75 percent. The suggested cyber-attack detection methodology surpasses current state-of-the-art methodologies and remains more dependable and robust. In the future, the study will be expanded to include more advanced neural networks as well as different types of realistic attacks.

REFERENCES :

[1] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, *18*(2), 1153-1176. Google Scholar↗

[2] 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↗

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

[4] Akyazi, U., & Force, T. A. (2014). Possible scenarios and maneuvers for cyber operational area. *European Conference on Cyber Warfare and Security*, *1*(10), 1-7. Google Scholar↗

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

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

[7] Denning, D. E. (2014). Framework and principles for active cyber defense. *Computers & Security*, *40*(1), 108-113. Google Scholar↗

[8] Baldoni, S., Battisti, F., Carli, M., & Pascucci, F. (2021). On the Use of Fibonacci Sequences for Detecting Injection Attacks in Cyber Physical Systems. *IEEE Access*, *9*(1), 41787-41798. Google Scholar↗

[9] Sui, T., Mo, Y., Marelli, D., Sun, X., & Fu, M. (2020). The vulnerability of cyber-physical system under stealthy attacks. *IEEE Transactions on Automatic Control*, *66*(2), 637-650.
Google Scholar↗

[10] Jahromi, A. N., Karimipour, H., Dehghantanha, A., & Choo, K. K. R. (2021). Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems. *IEEE Internet of Things Journal*, *8*(17), 13712-13722.
Google Scholar↗

[11] Lv, Z., Han, Y., Singh, A. K., Manogaran, G., & Lv, H. (2020). Trustworthiness in industrial IoT systems based on artificial intelligence. *IEEE Transactions on Industrial Informatics*, *17*(2), 1496-1504.
Google Scholar↗

[12] 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↗

[13] 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↗

[14] Perez-Diaz, Jesus Arturo, Ismael Amezcua Valdovinos, Kim-Kwang Raymond Choo, and Dakai Zhu (2020). A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, *8*(2), 155859-155872.
Google Scholar↗

[15] Karimipour, Hadis, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo, and Henry Leung (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access* 7, 80778-80788.
Google Scholar↗

[16] 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↗

[17] 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↗

[18] Ibor, A. E., & Epiphaniou, G. (2015). A hybrid mitigation technique for malicious network traffic based on active response. *International Journal of Security and Its Applications*, *9*(4), 63-80.
Google Scholar↗

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

[20] 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↗

****