Intrusion Detection System Techniques: A Review

Noor Suhana Sulaiman¹, Akhyari Nasir¹, Wan Roslina Wan Othman¹, Syahrul Fahmy Abdul Wahab¹, Nur Sukinah Aziz¹, Azliza Yacob¹, Nooraida Samsudin¹
¹Faculty of Computer, Media and Technology Management, University College TATI (UC TATI), Kemaman, Terengganu, Malaysia
suhana@uctati.edu.my

Abstract: Nowadays, Internet attacks are increasing rapidly. As a result, information security is a serious global concern among Information Technology users. Intrusion Detection System (IDS) is capable to detect unauthorized intrusions into computer systems and networks by looking for signatures of known attacks or deviations of normal activity. IDS is such as a detective control, the main function is to warn the user of any suspicious activity taking place. Active IDS research are still ongoing with remarkable techniques to detect attacks with significant accurate result. This paper deliver a brief overview on types of IDS and a types of techniques employed to detect intrusion.

1. Introduction

With the ever increasing users, object and device connected to each other through the Internet, like Internet of Things (IoT), have seen a steady increase of cloud systems to store data including credential data and paperless transaction as a result of online transactions. All these online technological dependencies expose users to high risk of public network / Internet breach of trusts such as compromised online credential data, unsafe communication between senders and receivers, and unauthorized access to communication session. In fact, given current rate of online technological growth, IoT based technologies are increasingly prone to vulnerabilities.

Different approaches are taken to deal with these vulnerabilities including the use of firewalls, adoption of cryptography techniques and introduction of secure protocols (named as https, SSL/TLS, IpSec, etc). Several protective techniques have been proposed and implemented to secure PC framework against cybercrime such as antivirus, firewall, encryption techniques and different protective measurements. Intrusions into a computing system can be defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a computer system resource. Intrusions into a computer system can be defined as any collection of acts that attempt to compromise the integrity, confidentiality or availability of resources of a computer system [1]. Thus, Intrusion Detection System (IDS) is by no mean replacing all of these approaches but complementing them. Even with all the techniques carried out, it could not guarantee full protection of the system. Therefore, the protective domain needs more efficient mechanism like Intrusion Detection System (IDS) as the next track of defense [2]. IDS is capable to detect unauthorized intrusions into computer systems and networks by looking for signatures of known attacks or deviations of normal activity. IDS
attempts to detect the attacks of computer by examining different information records observed in network processes [3]

2. Intrusion Detection System Overview
Starting in 1980, Intrusion Detection System (IDS) is an active research area [4]. Six categories of intrusive activities and how these activities might be detected were recommended [4]. These recommendations led to the development of anomaly and misuse detection. IDS attempts to detect intrusion such as illegitimate uses, misuses and abuses of computer systems by using authorized user or external perpetrator [3]. Intrusion evaluation method is important in securing the networks. The method can be divided into four phases including preprocessing, analysis, response and refinement as depicted in Figure 1. Initially, IDS dataset undergoes preprocessing phase; next, the information from preprocessing phases is analyzed to determine the intrusion or normal event occurrence. Then, the response phase determines suitable action should be taken to match the event triggered. Finally, the refinement phase fine tunes the utilization and intrusion detected to have better IDS tool.

![Diagram of Intrusion Detection System Basic Phases](image)

**Figure 1.** Intrusion Detection System Basic Phases

In **Preprocessing** stage, the data is taken from IDS or IPS sensors. Statistics are sorted to form a pattern to be used in classification. Information is formatted and classified depending on schemas of analysis used. In **Analysis**, information file is contrasted with the base of know-how. The facts files are to be logged as an event of intrusion; otherwise, the information file is dropped. The next record document is analyzed. In **Response**, the information is received inactively so caution is needed afterwards. The response can be performed to either automatically or manually after person-in-charge has manually analyzed the situation occurred. In **Refinement** stage, fine tuning is finished in light of previous utilization and intrusion detected. This helps in decreasing false advantageous ranges and to have greater security tool like Cisco Threat Response (CTR). It assists the refining stage to ensure that the alert is valid via checking the inclination of the user to the attack. The rules are based on the detection such as signature detection, sample matching and misuse detection [5].

IDS is classified into five categories which are Misuse, Anomaly, Host Based IDS, Network IDS and Hybrid IDS and described in Figure 2. The elaboration for each type is explained in the following sections.
2.1 Misuse Detection

The principle of detection of misuse is to reflect attacks in the form of a pattern or a signature so that in the future the same attack can be identified and avoided. These systems can detect several or all known patterns of attack, but they are of little use in detecting naive methods of attack [6]. Misuse detection usually detects intrusion signatures based on the rules set. A massive numbers of rule sets can be used to look for activities that maybe considered as intrusion state. The rules can be “If-then,” guidelines or certain based rules model. The activities might also be monitored live via monitoring device calls or later the usage of audit data [5].

2.2 Anomaly Detection

Anomaly detection defines variety of patterns of regular behaviours. Any abnormal elements observed from regular profiles are viewed as anomalies. Anomaly detection is tough to determine precisely from everyday profile. The key benefit of anomaly intrusion algorithms is that new types of attacks can be identified, since these new intrusions are likely to deviate from the standard [7] [8]. Thus, the detection generally suffers with higher false rate. Anomaly detection is divided to static and dynamic detections. In static detection, it is based on the assumption that there is an element of monitored device that does not change. If static portion of the device differs from its unique form, an error has occurred or an intruder has altered static portion of the system. Dynamic detection operates on audit archives or on monitored network traffic data. [9].

2.3 Host Based IDS

Host based IDS (HIDS) alludes to realize intrusions analyzed from information gathered from a single/individual host system. HIDS operator monitors the activities; for example, system integrity, utility activity, document changes, host based community traffic and machine logs. By utilizing frequent hashing tools, file timestamps, device logs, and video display units machine calls; local community interface offers the agent an understanding towards the present nation of nearby host. If unauthorized adjustments or activities detected, the user is alerted by a pop-up, additionally alerting the central management server, blocking off the activity, or a mixture of three mentioned. The option is primarily based on the policy installed in the local system. These host-based tactics are regarded as passive component. [5].
2.4 Network Intrusion Detection Systems

Network based totally IDS (NIDS) is utilized for monitoring and examining community site visitors to defend a machine from community’s primarily based assaults where the statistics is going over the network. NIDS is capable to distinguish malicious actions and display the visitor’s attacks network. NIDS comprises a variety of sensors to monitor packet movement. NIDS appears progressively at pastime packet, or close to actual time, to recognize intrusion patterns. The investigation of visitor’s pattern in intrusion detection may be accomplished at the sensor, administration servers, or combination of both. NIDS tactic is regarded as e active component [5].

2.5 Hybrid IDS

Previous researches in IDS counselled that the intrusion detection competencies are elevated through a hybrid method involving signature (misuse) detection in anomaly detection. In hybrid approach, the signature detection method detects an acknowledged attack and the anomaly detection method detects a novel/unknown attack.

3.0 Intrusion Detection System Technique

Techniques of data mining deal with knowledge or interesting patterns search from the massive data. Data mining turns large data into knowledge; then analyzes and generates the knowledge into information which is an important step in knowledge discovery process (Lakshmi & Raghunandhan, 2011). Data mining has been applied widely in the areas of IDS application, education, medical diagnosis, fraud detection and banking [6].

Knowledge Discovery in Databases (KDD) is a domain which encompasses theory, method and technique to make sense of data and extract useful knowledge from dataset. A set of standard is employed including selection, preprocessing, transformation, data mining and interpretation or evaluation to generate the knowledge, as depicted in Figure 3. In KDD data analyzing, data mining is the most important step in data processing [10].

![Figure 3. Standard Steps of Process in Knowledge Discovery Database (KDD). Kavakiotis](image)
Technique for data mining [11] capable of solving IDS problems such as;

- Discard normal operations from the alarm dataset in order to provide actual attack operations that are important.
- Evaluate the false alarm signature of a "bad" sensor generator.
- Look for unusual behaviours that show a real attack.
- Identify long, ongoing/continuous patterns

Three techniques of data mining applied to generate knowledge discovery are as follow; [12]

i) **Classification**: is a process of classifying data based on class label, by predicting group membership for instances of data;

ii) **Clustering**: is a process of partitioning dataset or object into meaningful subclasses (clusters), by separating set of unlabeled data into hidden data and natural discrete set;

iii) **Regression**: is the process of finding function or model to distinguish data into continuous real value instead of using classes. This technique estimates value by comparing between already known value and predicted value.

Techniques of attack detection in IDS application are divided into seven categories as illustrated in Figure 4. The elaboration for each category is explained as follows:

![Figure 4. Categories of Techniques in IDS Application](image)

### 4.0 Statistical Approach

This approach includes statistical comparison of specific event criteria setting. Attributes set are considered as variable number and known as “user login, logout, number of files accessed in a period of time, usage of disk space, memory”, etc. [13]. Data collected is tested for intrusion analysis through the use of statistical models.

### 4.1 Data Mining

Data mining techniques are widely used in the community and are host to build mostly in misuse detection model. IDS is expressed as a statistics evaluation process. Statistics mining method is used to automatically examine user’s normal activity and intrusive behavior [14]. Data Mining is divided into four tasks [13] such as Classification, Clustering, Regression, and Association Rule Learning.
4.2 Pattern Matching
Pattern matching based IDS procedure is regularly used in network to model, match and recognize the intrusion pattern based totally on the packet head, packet content or both [14]. Referring to new types and variety of attacks, the number of signatures is growing as it increases computational cost in pattern matching. Additionally, this approach does not detect new attacks.

4.3 Expert System / Rule Based
The expert system is based on previous set of rules describing the intrusions. The security related to events in audit trail is translated to if-then-else rules [11]. This approach develops statistical profiles of entities (as user, workstation and application program) and use statistical abnormal activities in detecting intrusions. Unfortunately, approach requires updates from System Administrator in remaining up-to-date. Lack of maintenances or updates is the weakness of expert system [13].

4.4 State Machines
This model consists of set of states, transitions and actions. Intruders launch the intrusion portrayed with the arrangement of objectives and transition accomplished to conquer the system [15].

4.5 K-means Clustering
The algorithm uses input parameter k, then partitioning a set of n object into k cluster. The result of “intra-cluster” similarity is high; however, the “inter-cluster” similarity is low. The main purpose to employ this algorithm is to break up and crew statistics into normal and intrusion cases [12].

4.6 Learning Models
Learning model incorporates getting to know competencies in intrusion detection process and the usage of synthetic learning technique. Previously, mastering methods are extensively employed in anomaly detection when considering that self learning strategies can afford to routinely structure the conducted subjects and opinions [14]. Several learning models are discussed in the following.

Previous IDS adapts the use of neural network, which consists of two important elements. First element is a system which monitors audit trails in recognizing intrusion signature. Second element is to examine consumer behavior, if abnormal state occurs then alarm is alerted [14]. Neural network is a class of machine learning algorithms used to classify data. A neural network consists of node and edge. The weight value defines how a node impacts adjoining nodes. A subset of nodes in the model is referred to as input nodes. Detection the usage of neural networks is three steps process.

Fuzzy Logic is a structure of many-valued good and approximate judgment, a substitute to constant and genuine reasoning. Fuzzy set idea was introduced by Zadeh in 1965. Fuzzy Logic is designed mathematically to characterize uncertainty and vagueness using tools in dealing with real world problems. Fuzzy Logic based devices should be able to detect types of intrusive undertaking PC networks as the rule base holds higher set of policies [16]. A system based on fuzzy clustering and the ANN approach has been implemented. To address the problems of poor detection of stability as well as low accuracy detection, this approach may be applicable. In this process, the restore point was used for registry keys, roll back system files, project database and installed programs [17].

Genetic Algorithm (GA) makes use of biological evolution as a critical questioning system. The proposed IDS based on GA includes two modules; for every work in an alternate stage, a set of classification is generated from network audit facts in offline condition. In the stage to detect intrusion, the generated policy is used to classify real time network connections. GA makes use of evolution and natural resolution using a chromosome as record structure and evolves chromosomes in the use of selection, recombination and mutation operator. Every chromosome role is encoded as bit, character or number. These positions could be referred to as gene [16]. Unfortunately, GA limitation notes that improper threshold value might easily lead to high false alarm rate in new intrusion detection [14].
4.7 Biological Models

Previously, there is an anomaly detection models relating to biological principles named as Immune Based. IDS immune based is inspired by human immune system concept and is capable to perform similar tasks to innate and adaptive immunity. The normal behavior profile is generated by collecting services behavior gaining from audit data [14].

Yu et al. (2001) proposed IDS based on DNA sequence. This research defines sequences of DNA for a computer system. The knowledge includes DNA characterization of human body and any anomaly in tissues that can reflect in DNA sequence. Any changes of behavior patterns in the computer system are traced to the change of DNA sequences that can be either a normal or intrusion event. Standard Backpropagation Neural Network is employed to train normal DNA sequence in network traffic. The system successfully detects UDP Flood attack based on DNA sequence in normal network traffic. Although convincing, this preliminary result needs to be expanded to define more complete DNA scheme in computing system [14].

While investigating previous works conducted on Intrusion Detection System identified with machine learning methods, it comes to fore that there are three fundamental classifiers: Single classifiers, Hybrid classifiers and Ensemble classifiers.

(a) Single Classifiers

Single classifier approach uses one-class classification in classifying data known as unary classification or class modeling. Fuzzy Logic (Fuzzy Set Theory) is utilized in reasoning. Its esteem ranges from 0 to 1; for example, raining is characteristic occasion [19]. Fuzzy Logic is viable and has much potential as a method. It manages human basic leadership and thinking. Fuzzy Logic utilizes “if then else” rules. It is utilized as a part of many building applications [20], especially in anomaly detection. Fuzzy Logic is efficient in port scanning and probes; however, it consumes high resources (Kaur et al., 2013). Genetic Algorithms selection capability refers to criteria of performance [22]. GA is inspired by biologically heuristic search. IDS collecting traffic information employs GA; then, gathers information at normal state or intrusion state at present [23]. K-Nearest Neighbor (k-NN) is old and simple approach in sample classification [24]. Parameter k is essential to create k-NN classifier. The k value changes impact the different performances. k-NN calculates a rough distance between two different points; for instance, base learning and it difference from inductive approach. Support Vector Machine (SVM) is superior by setting up a hyper plan. This approach classifies the statistic into groups; then, divides the records into two portions to solve problem of vector and quadratic programming [21]. Artificial Neural Network (ANN) processes and classifies data inspired by the neurons of human brain. Multilayer Perceptron is basically used in neural community architecture. ANN is fast learning and capable to analyze “non-linear information set” with “multi variables” [22]. Decision Trees (DT) classifies a pattern generated from more than few decisions. The first selection helps the second selection; until it finally becomes a tree structure. The classification of sample starts with root node and ends with quit node which is additionally called leaf node. Each quit node (leaf node) presents a class of classification [23].

(b) Hybrid Classifiers

Hybrid architecture is designed with several heterogeneous methods, which complement each other in improving the performances. Hybrid classifiers are capable to enhance anomaly and misuse detection [25] to combine Host Based IDS (HIDS) and Network Based IDS (NIDS). Bahrainian & Dangel (2013) introduced a hybrid method of sentiment lexicons usage with a classifier of machine learning to detect opinions polarity in consumer and product area. Gautam & Yadav (2014) proposed machine learning technique analysis of semantic to classify sentences and reviews of product based on twitter data using WordNet to improve accuracy. Gokulakrishnan et al. (2012) examined different classifier performances such as Naïve Bayesian, Sequential Minimal Optimization (SMO), SVM and Random Forest in classifying Twitter data. Meanwhile, Chen et al. (2014) proposed a technique to
classify student’s Twitter data into several categories. However, the process of generation category is static. Furthermore, the static process results in the limitation of classifiers to improve accuracy performance.

(c) Ensemble Classifiers

Ensemble classifier is a group of individual classifiers which cooperate with each other to train the dataset in supervised classification. Ensembler classifier combines several single classifiers to generate an improved output [29]. Kumar et al. (2013) proposed a hybrid Intrusion Detection System. They used several classification techniques in their proposed method. They combined Bayes Theorem, Naive Bayes Classifier and K-Means Clustering to detect intrusions.

4.8 Metrics for IDS Evaluation

High detection rates and low false positive rates are key factors to consider in order for IDS to be considered successful. For an IDS assessment, various metrics may be used. Such metrics are then discussed, showing the meaning and function of each one. It is important to remember that IDS output is not expressed depending only on the detection rate as the only assessment metric [31]. Other significant assessment factors, including the overall system’s transparency and protection, memory requirements, power consumption and throughput, should be considered. In addition, [32] adds ease of use, interoperability, openness and collaboration to the aforementioned specifications. It is possible to describe IDS accuracy in terms of:

- True Positive (TP): Number of intrusions correctly detected
- True Negative (TN): Number of non-intrusions correctly detected
- False Positive (FP): Number of non-intrusions incorrectly detected
- False Negative (FN): Number of intrusions incorrectly detected

Hodo et al. [33], Buse et al. [34] and Aminanto et al. [35] address the key metrics to consider for assessment in their respective work. These include the overall accuracy, decision speeds, precision, recall, F1 and Mcc. In fact, true negatives and true positive ones correspond to the desired habits. Typically, however, an IDS is incomplete and results in the existence of two other unhealthy behaviors. Multiple IDS normally suffer from imperfections that contribute to the identification of these unhealthy habits. Other metrics and analysis, such as the ability to track new threats, are more or less used in the sense of IDS [36].

4.9 Limitation

In the following, the weaknesses and problems in datasets used in IDSs can be summarized:

Special Purpose Datasets: The number of usable datasets that serve special purpose IDSs is restricted. Publicly accessible datasets for the IoT, SCADA and Tor networks, for example, are currently inadequate.

Dataset Outlook: Fast developments in networking and related technology require a change in the paradigm of dataset generation. Accessible databases currently do not cover emerging technologies such as Blockchain, Software Defined Network (SDN), Network Function Virtualisation (NFV), Big Data, and their related risks [37] [38] [39].

Unavailability of systematic dataset: The current study highlighted the lack of an up-to-date dataset available that represents the emerging attacks on modern networks. Since these models were not trained with enough attack types and patterns, most of the proposed methodologies were unable to detect zero-day attacks. It needs to be checked and confirmed using the dataset of older and newer attacks to come up with an appropriate IDS model [40].
5.0 Conclusion

This paper reviews various types of Intrusion Detection System, and numerous techniques employed to detect attack. Researchers are looking into detail in the IDS domain, as cyber attacks are becoming more sophisticated and thereby presenting increasing challenges in accurately detecting intrusions. Failure to prevent the intrusions could degrade the credibility of security service, which are data confidentiality, integrity, and availability.

6.0 Acknowledgement

This research is fully supported by UC TATI Short Term Grant (STG), 9001-2006, which help in completing the research in a viable and efficient.

References

[1] N. S. Sulaiman and R. A. Bakar, “Rough Set Discretize Classification of Intrusion Detection System,” Journal of Engineering and Applied Sciences, vol. 11, no. 3, pp. 488–496, 2016.
[2] M. Dhakar and A. Tiwari, “A novel Data mining based hybrid intrusion detection framework,” UK J. Inf. Comput., vol. 9, no. 1, pp. 037–048, 2014.
[3] J. Endorf, C., Schultz, E. and Mellander, Intrusion detection and prevention. 2004.
[4] J. Anderson, “Computer Security Threat Monitoring and Surveillance,” 1980.
[5] R. S. H. Rizvi and R. R. Keole, “A Review on Intrusion Detection System,” Int. J. Adv. Res. 1Computer Sci. Manag. Stud., vol. 3, no. 3, pp. 22–28, 2015.
[6] Y. Li, J. Wang, Z. Tian, T. Lu, and C. Young, “Building lightweight intrusion detection system using wrapper-based feature selection mechanisms,” Comput. Secur., vol. 28, no. 6, pp. 466–475, 2009, doi: 10.1016/j.cose.2009.01.001.
[7] D. Denning, “An intrusion-detection model,” IEEE Trans. Softw. Eng., 1987.
[8] S. Bouzida, Y., Cuppens, F., Cuppens-Boulahia, N., Gombault, “Efficient Intrusion Detection Using Principal Component Analysis,” 2004.
[9] S. V. Kale, S. R. Kale, R. A. Naphade, and P. A. A. Dande, “A Review of Various Intrusion Detection Approaches 1,” Int. J. Adv. Res. Eng. Comput. Sci. Softw., vol. 6, no. 3, pp. 261–262, 2016.
[10] I. Kavakiotis, O. Tsave, A. Salifoglou, N. Maglaveras, I. Vlahavas, and I. Chouvarda, “Machine Learning and Data Mining Methods in Diabetes Research,” Comput. Struct. Biotechnol. J. 15, pp. 104–116, 2017.
[11] N. S. Sulaiman, N. Aziz, and W. A. Alyani, “Overview of Network Dataset and Data Mining Technique,” International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 1, pp. 287–290, 2020.
[12] M. Gera and S. Goel, “Data Mining - Techniques, Methods and Algorithms: A Review on Tools and their Validity,” international J. Comput. Appl., vol. 113, no. 18, 2015.
[13] N. A. Elfeshawy and O. S. Faragallah, “Divided two part adaptive intrusion detection system,” Springer Sci. Media, 2012.
[14] Ghorbani, AA, Lu, W, Travallace, and M, “Network Intrusion Detection and Prevention Concepts and Techniques,” Springer, 2010.
[15] S. Akbar, D. K. N. Rao, and Dr.J.A.Chandula, “Intrusion Detection System Methodologies Based on Data Analysis,” Int. Journal Comput. Appl., vol. 5, no. 2, 2010.
[16] M. M. M. Hassan, “Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic,” Int. J. Innov. Res. Comput. Commun. Eng., vol. 1, no. 7, 2013.
[17] D. P. K. and V. B. Gaikwad, Sonali Jagtap, “Anomaly Based Intrusion Detection System Using Artificial Neural Network and fuzzy clustering,” Int. J. Eng. Res. Technol., 2012.
[18] B. Yu, E. Byres, and C. Howey, “Monitoring Controller’s” DNA Sequence” For System Security,” 2001.
[19] H. Zimmermann, “Fuzzy set theory and its applications,” 2001.
[20] A. A. Aburomman and M. B. I. Reaz, “Evolution of Intrusion Detection System Based on Machine Learning Methods”, "Aust. J. Basic Appl. Sci., 2013.
[21] H. Kaur, G. Singh, and J. Minhas, “A Review of Machine Learning Based Anomaly Detection Technique,” Int. J. Comput. Appl. Technol. an d Res., vol. 2, no. 2, 2013.
[22] Kamran, “An adaptive genetic based signature learning system for intrusion detection,” Expert Syst. w ith Appl., 2009.
[23] R. Borgohain, “FuGeIDS : Fuzzy Genetic paradigms in Intrusion Detection Systems,” Int. J. Adv. Netw. Appl., vol. 3, no. 6, 2012.
[24] S. Manocha and M. A. G. Irolami, “An empirical analysis of the probabilistic K-nearest neighbor classifier,” Pattern Recognit. Lett., 2007.
[25] M. Govindarajan and R. M. Chandrasekaran, “Intrusion detection using neural based hybrid classification methods,” Comput. Networks, 2011.
[26] X. Chen, M. Vorvoreanu, and K. Madhavan, “Mining Social Media Data to Understand Students’ Learning Experiences,” IEEE Trans., vol. 7, no. 3, pp. 246–259, 2014.
[27] A. Kumar, H. C. Maurya, and R. Mishra, “A Research Paper on Hybrid Intrusion Detection System,” Int. J. Adv. Technol., vol. 2, no. 4, 2013.
[28] X. B. Hanan Hindy, David Brosset, Ethan Bayne, Amar Seeam, Christos Tachtatzis, Robert Atkinson, “A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems,” arXiv, 2020.
[29] S. Axelson, “The base-rate fallacy and the difficulty of intrusion detection,” ACM Trans. Inf. Syst. Secur., vol. 3, no. 3, 2000.
[30] R. A. E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, “Shallow and deep networks intrusion detection system: A taxonomy and survey,” arXiv, 2017.
[31] B. Atli, “Anomaly-based intrusion detection by modeling probability distributions of flow characteristics,” 2017.
[32] K. K. M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, “Deep abstraction and weighted feature selection for Wi-Fi impersonation detection,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 3, 2018.
[33] N. Suhana, “Big Data Analytic of Intrusion Detection System,” International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 1, 2020.
[34] M. A. F. A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras and F. A. K. M. Mukherjee, “Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security,” Sensor, vol. 19, 2019.
[35] H. H. H. Li, F. Wei, “Enabling dynamic network access control with anomaly-based IDS and SDN,” 2019.
[36] J. H. W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, “When intrusion detection meets Blockchain technology: A review,” IEEE Access, vol. 6, 2018.
[37] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches,” Trans Emerg. Tel Tech, 2021.