MACHINE LEARNING-DRIVEN INTRUSION DETECTION SYSTEMS FOR REVOLUTIONIZING NETWORK SECURITY

Chikkalwar Sudha Rani [1], M. Vishnu Vardhana Rao [2]
Katakam Kusuma Kumari [3]
[1] Assistant Professor, Department of Computer science and Informatics,
University College of Engineering and Technology, Mahatma Gandhi University, Nalgonda,
Email: chsudharani.mgu@gmail.com
[2] Assistant Professor, Dept of CSE, Vignan's Group of institutions, Hyderabad, India
Email: mvvrao.mca31@gmail.com
[3] M Tech Scholar, Dept of CSE. ANUCET, Acharya Nagarjuna University, Guntur.

ABSTRACT

This article "Enhancement Network Security features through Intrusion Detection Systems" aims to improve the security posture of computer networks by researching and implementing state-of-the-art techniques. Implementing and thoroughly understanding anomaly- and signature-based intrusion detection systems is the primary objective of This article. It investigates the development of a robust system that can monitor network activity, identify familiar attack patterns, and identify anomalies in behavior. By combining these strategies, this article hopes to provide a more effective defense against a range of cyberthreats. Incorporating machine learning techniques into the IDS framework is another aspect of This article. By allowing the system to learn from and adapt to new threats, this improvement improves its ability to recognize complex and unique attacks. By reducing false positives and increasing overall accuracy, machine learning enhances an intelligent and dynamic intrusion detection system. The outcomes of the study will improve academics' understanding of network security and provide practical guidance on implementing state-of-the-art intrusion detection methods. By ensuring the availability, confidentiality, and integrity of their networked systems, this article's ultimate goal is to give businesses a greater defense against cyberattacks.

Keywords - Network Security, IDS, Signature based IDS, Anomaly based IDS, Machine learning

1. INTRODUCTION

Given the importance of information in today's technological world, safeguarding computer networks has become essential. To address the increasing problems associated with cyberattacks, this article "Enhancing Network Security through Intrusion Detection Systems" suggests and puts into practice advanced intrusion detection techniques. As a proactive defensive technology that may quickly identify and prevent potential security breaches, intrusion detection systems (IDS) are valued by the initiative. The confidentiality, availability, and integrity of data within computer networks are seriously threatened by the growing complexity and sophistication of cyberthreats. The dynamic nature of contemporary cyberthreats frequently renders traditional security solutions inadequate. An essential tool in the cybersecurity toolbox are intrusion detection systems, which can keep an eye on network activity and promptly send out alerts or react to questionable activity. This article's justification is the necessity of upgrading network security protocols in order to successfully counter a variety of dynamic cyberthreats. Organizations can increase their resistance to known and unforeseen threats by improving the capabilities of intrusion detection systems. By providing insights into the application of cutting-edge IDS techniques, the initiative aims to close the knowledge gap between theory and practice. This article has a wide range of applications, including anomaly-based and signature-based intrusion detection techniques. In order to recognize the significance of adaptive systems in the face of continuously changing cyberthreats, it also investigates the integration of machine learning algorithms. The construction of a strong and intelligent IDS architecture that can offer a dynamic protection mechanism is included in the scope. When using intrusion detection systems (IDS) to improve network security, it is important to recognize how crucial they are in protecting a network from potential threats and unwanted access. These systems work by keeping an eye on system or network activity, examining trends, and spotting any unusual activity that might point to a security breach. Organizations frequently use IDS to strengthen network security by quickly identifying and addressing a variety of cyberthreats. IDS can identify patterns linked to known attacks and anomalous activity by continually monitoring network traffic, allowing for a preemptive defense against possible intrusions. By continuously observing and examining network data for indications of malicious behavior, DS plays a crucial part in network security. Signature-based and anomaly-based detection techniques are examples of traditional IDS methodologies.

1.1 Intrusion Detection Using Signatures:

This method uses a database of recognized attack patterns or signatures. This method works well for spotting known dangers, but it might not be sufficient for new or tailored attacks. Enhancing signature databases, speeding up signature matching, and tackling false positive issues have been the main areas of research.

1.2 Anomaly-Based Intrusion Detection:

This method entails creating a baseline of typical network activity and sending out notifications when there are deviations. Although this approach is useful for identifying dangers that haven't been identified yet, it needs complex algorithms to differentiate between malicious and benign activity. Advances in anomaly detection algorithms and their practical applications are highlighted in the literature.

1.3 Machine Learning in Intrusion Detection:

There has been a lot of interest in incorporating machine learning methods into IDS. The flexibility and self-learning capabilities of machine learning models allow IDS to develop and recognize new threats. In order to improve the precision and effectiveness of intrusion detection, studies investigate the use of several machine learning methods, such as neural networks, decision trees, and clustering.

1.4 Network Segmentation:

In order to prevent attackers' lateral movement and contain possible breaches, networks are divided into smaller, isolated pieces as part of the current system. Although somewhat successful, it could not be enough to stop sophisticated threats that take advantage of weaknesses in several areas.

2. ITERATURE REVIEW

2.1 Overview of the Literature Survey:

Because leaked data can result in significant losses, protecting an organization's and an individual's computer and network information has become crucial. To stop this harm, an intrusion detection system is employed. Various machine learning techniques are created in order to improve the functionality of IDS. Addressing the issue of intrusion detection system (IDS) adaptability is the primary goal [1]. The suggested intrusion detection system is capable of identifying both known and unknown threats. The Clustering Manager (CM), Decision Maker (DM), and Update Manager (UM) are the three main components of the suggested IDS. The suggested IDS's functionality is estimated using the NSL-KDD dataset. There were both supervised and unsupervised methods used. The data entered into the system is based on the training of an agent who rejects the IDS-provided repair suggestions. This method is used in the supervised mode. When operating in unsupervised mode, the system can detect both known and unknown traffic. The system's functionality has been enhanced following the updating of recently received data from both supervised and unsupervised modes. When the system operates in unsupervised mode, its performance improves [2]. A hybrid model is created by combining machine learning methods such as Extreme Learning Machine (ELM) and Support Vector Machines (SVM) [3]. High-quality datasets are constructed using modified K-means. It creates little datasets that represent the entire set of original training data. This step cuts down on the classifier's training time. KDDCUP 1999 is applied in the implementation process. It displays an accuracy of almost 95.75 percent. To report this issue, a number of machine learning approaches are investigated, including SVM, Random Forest (RF), and ELM. In terms of accuracy, ELM performs better than other methods. Datasets are separated into three categories: whole datasets, half of the dataset, and one-fourth of the data samples. But in half of the data samples and one-fourth of the data samples, SVM yields superior results. The most effective way to manage the massive volume of data—roughly two lakh instances and more—is ELM [4]. A novel hybrid classification technique is put forth for Artificial Fish Swam (AFS) and Artificial Bee Colony (ABC) [5]. Due to the extensive use of the internet, computer systems are now vulnerable to many forms of information theft, which has led to the development of IDS. Correlation-based feature selection (CFS) and fuzzy

CMeans clustering (FCM) are used [6] to separate training datasets and remove superfluous features. The CART approach, which is used to distinguish between normal and anomalous records according on the chosen attributes, is used to construct if-then rues. The suggested solution makes use of a straightforward filter-based paradigm called correlation-based feature selection. Datasets having features that are uncorrelated with the other classes but substantially correlated with the class are used. This method achieved a 99 percent anomaly identification rate and a 0.01 percent false positive rate utilizing the NSL-KDD and UNSW-NB15 datasets. An artificial bee colony and AdaBoost algorithms are used in a hybrid approach for A-NIDS to achieve a high detection rate (DR) and low false positive rate (FPR) [7]. Understanding the core ideas of intrusion detection systems (IDS) forms the basis of this literature review. Because they actively monitor and analyze network data for indications of hostile activity, intrusion detection systems (IDS) are essential to network security. Signature-based and anomaly-based detection techniques are examples of traditional IDS methodologies. A database of recognized attack patterns, or signatures, is the foundation of signature-based detection. This method works well for spotting known dangers, but it might not be sufficient for new or tailored attacks. Enhancing signature databases, speeding up signature matching, and tackling false positive issues have been the main areas of research. Setting up a baseline of typical network behavior and sending out notifications when deviations happen are the two main components of anomaly-based detection. Although this approach is useful for identifying dangers that haven't been identified yet, it needs complex algorithms to differentiate between malicious and benign activity. Advances in anomaly detection algorithms and their practical applications are highlighted in the literature [8].

The literature acknowledges a number of difficulties in implementing IDS. The necessity of updating signature databases on a regular basis, the problem of creating precise baselines for anomaly detection, and the possibility of false positives and negatives are some of these difficulties. For the creation of dependable and efficient intrusion detection systems, these issues must be resolved. The use of hybrid techniques, which blend anomaly-based and signature-based detection methods, has grown in popularity. In order to capitalize on each technique's advantages and minimize its disadvantages, research investigates how these approaches can work in concert[9]. The goal of hybrid models is to offer a more thorough and flexible defense against a variety of online dangers. Case studies and real-world IDS deployments in various organizational contexts are included in the literature study. These actual cases demonstrate how well intrusion detection systems identify and neutralize online threats. Case studies also provide insight into the difficulties encountered during implementation as well as solutions. An examination of upcoming developments and new technology in the intrusion detection space rounds off the analysis. This covers the possible effects of AI, how blockchain can improve IDS security, and how threat intelligence streams can be integrated to strengthen proactive defenses [10].

3. IMPLEMENTATION STUDY

In order to defend against known threats, the current network security system frequently depends on conventional security measures like firewalls and antivirus software. Although these solutions offer a minimum level of protection, they might not be sufficient to handle the complex and ever-changing nature of contemporary cyberthreats. To improve the capabilities of the current security architecture, intrusion detection systems (IDS) are frequently incorporated.

3.1 Antivirus and firewall software:

By permitting or prohibiting traffic according to preset security rules, traditional firewalls serve as a barrier between a private internal network and external networks. The purpose of antivirus software is to identify and eliminate known malware. These solutions may find it difficult to recognize and stop new or focused attacks, even while they are effective against conventional threats.

3.2 Systems for detecting intrusions (IDS):

One important development is the incorporation of IDS into the current system. To find known threats, signature-based intrusion detection systems use a database of established patterns, or signatures. IDSs that are based on anomalies create a baseline of typical network activity and sound an alarm when there are deviations. False positives and the requirement for regular signature database upgrades are two potential problems with these systems.

3.3 Network Segmentation:

In order to minimize attackers' ability to move laterally and contain possible breaches, networks are divided into smaller, isolated segments as part of the current system. Although somewhat successful, it could not be enough to stop sophisticated threats that take advantage of weaknesses in several areas.

3.4 User education and security policies:

To encourage employees to behave securely, the current system frequently includes security regulations and user training. Even if they are necessary, human mistake and changing attack methods can still be dangerous, which emphasizes the necessity for automated and intelligent security solutions.

3.5 Incident Response Plans:

To quickly handle security breaches, organizations usually have incident response plans in place. The speed and complexity of sophisticated cyberattacks, however, may be too much for these plans, which frequently rely on manual intervention.

3.6 Security Information and Event Management (SIEM):

To gather and examine log data from several network devices, some businesses implement SIEM systems. Although SIEM offers information about possible security events, it might not have the proactive real-time features of more sophisticated IDS solutions.

3.7 Vendor-Specific Security Solutions:

The integration of proprietary or vendor-specific security solutions into the current system may vary depending on the company. The efficacy of these solutions, which frequently concentrate on particular facets of security, is contingent upon how extensive their features are and how well they can adjust to new threats.

4. PROPOSED METHODOLOGY

By implementing cutting-edge Intrusion Detection Systems (IDS) that overcome the shortcomings of the current security infrastructure, the suggested system seeks to greatly improve network security. The following are the main elements and characteristics of the suggested system: The suggested system offers a thorough defense against a variety of cyberthreats by combining anomaly-based and signature-based intrusion detection methods. While anomaly-based detection creates a baseline of typical behavior and identifies variations suggestive of possible intrusions, signature-based detection assists in identifying established attack patterns.

4.1 Integration of Machine Learning:

The suggested solution integrates machine learning techniques into the IDS architecture to adjust to new and changing threats. Through machine learning, the system can gradually learn from novel patterns and behaviors, improving its capacity to identify attacks that were previously unknown. This adaptive method increases overall detection accuracy while lowering false positives.

4.2 Real-time Monitoring and Alerts:

Network traffic and system activity are monitored in real-time by the suggested IDS. Alerts are sent out instantly in the event of any suspicious activity or possible security breach, enabling prompt action and remediation. In order to prevent unwanted access and lessen the effect of security incidents, real-time warnings are essential.

4.3 Behavioral Analysis and Profiling:

To profile and comprehend typical user and network activity, the system has behavioral analysis capabilities. This lessens false positives by helping to distinguish between benign alterations and possibly harmful activity. A more precise and contextually aware intrusion detection system is facilitated by behavioral profiling.

4.4 Constant Updates and Integration of Threat Intelligence:

The significance of regular updates to threat intelligence feeds and signature databases is emphasized by the suggested system. By doing this, the IDS is kept up to date and equipped to recognize the most recent threats. By utilizing outside insights into new cyberthreats, integration with threat intelligence sources improves the system's proactive defense.

4.5 Easy-to-use Dashboard and Reports:

The suggested solution includes an intuitive dashboard that gives managers clear visual representations of network activity, warnings, and possible dangers. Comprehensive analysis of security incidents is made possible by detailed reporting features, which aid in well-informed decision-making and ongoing security posture improvement.

4.6 Automated Reaction Systems:

An essential component of the suggested system's reaction to security events is automation. Isolating compromised systems, preventing hostile traffic, and starting pre-established security procedures are examples of automated reactions. This lessens the effect of security breaches while also speeding up reaction times.

5. MODULES & ALOGRITHAM

5.1 Signature-Based Detection: Synopsis:

This method uses pre-established patterns or signatures of known harmful activity to detect threats. These signs stand for particular traits or patterns connected to recognized dangers. Algorithm Description: The system looks for patterns in network traffic and compares them to the signature database. An alert is sent out in the event that a match is discovered, signalling the existence of a recognized threat.

5.2 Anomaly-Based Detection: Overview:

This method looks for actions that deviate from typical behaviour. With this method, a baseline of what is deemed normal is established, and when actions dramatically depart from this baseline, alerts are raised. Algorithm Explanation: The normal behaviour baseline is established using rule-based systems, statistical models, or machine learning algorithms. An alert is produced whenever network activity departs from this baseline.

5.3 Machine Learning Algorithms:

Synopsis: By facilitating intelligent and adaptive threat identification, machine learning algorithms improve intrusion detection systems. These algorithms continuously enhance their capacity to spot novel patterns by learning from past data.

5.4 Algorithm Description:

Typical machine learning algorithms consist of the following:

a. Neural Networks: Learn intricate patterns by imitating the structure of the human brain.

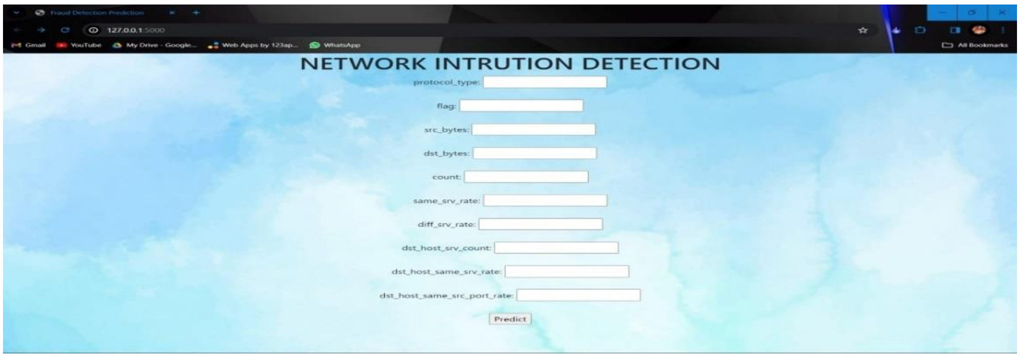
b. Decision trees are hierarchical structures that use input features to inform their decisions.

c. Clustering algorithms: These are helpful for detecting anomalies since they group data points according to commonalities.

5.5 Statistical Analysis: Synopsis:

Statistical techniques examine network data to find irregularities or trends suggestive of malevolent behaviour. The mean, median, standard deviation, and other statistical metrics are examples of these techniques. The algorithm Explanation: The system can identify departures from typical behaviours by setting statistical criteria. Alerts are triggered by unusual patterns that surpass predetermined thresholds.

6. RESULTS AND DISCUSSION SCREEN SHOTS



NETWORK INTRUTION DETECTION

protocol_type:

flag:

src_bytes:

dst_bytes:

count:

same_srv_rate:

diff_srv_rate:

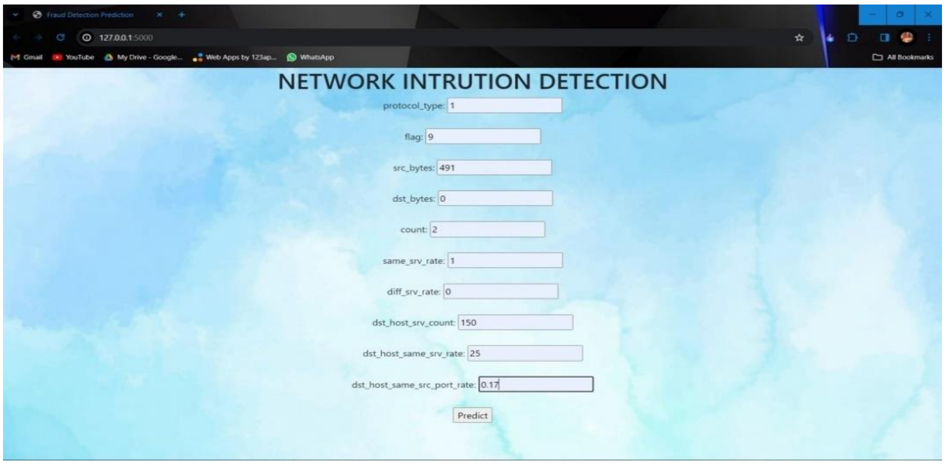
dst_host_srv_count:

dst_host_same_srv_rate:

dst_host_same_src_port_rate:

Predict

Fig 1: In this page the user can give the values that is parameters that says weather intrusion is happened or not



NETWORK INTRUTION DETECTION

protocol_type: 1

flag: 9

src_bytes: 491

dst_bytes: 0

count: 2

same_srv_rate: 1

diff_srv_rate: 0

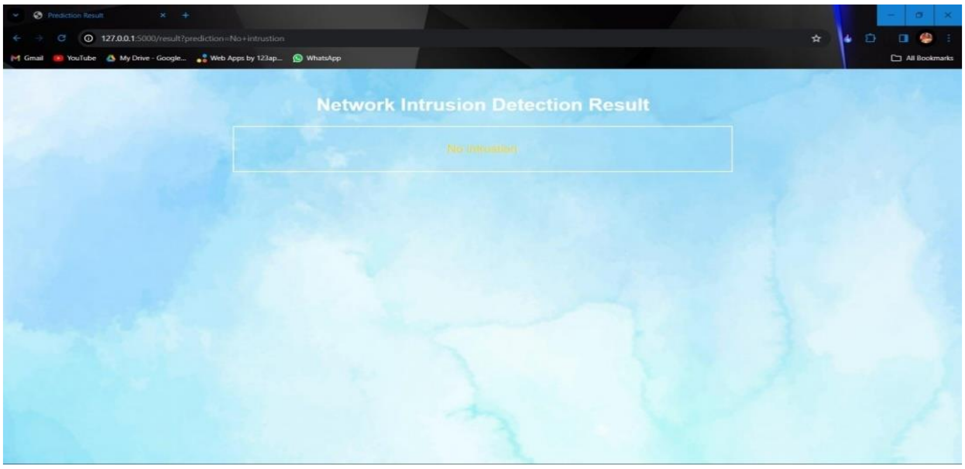
dst_host_srv_count: 150

dst_host_same_srv_rate: 25

dst_host_same_src_port_rate: 0.17

Predict

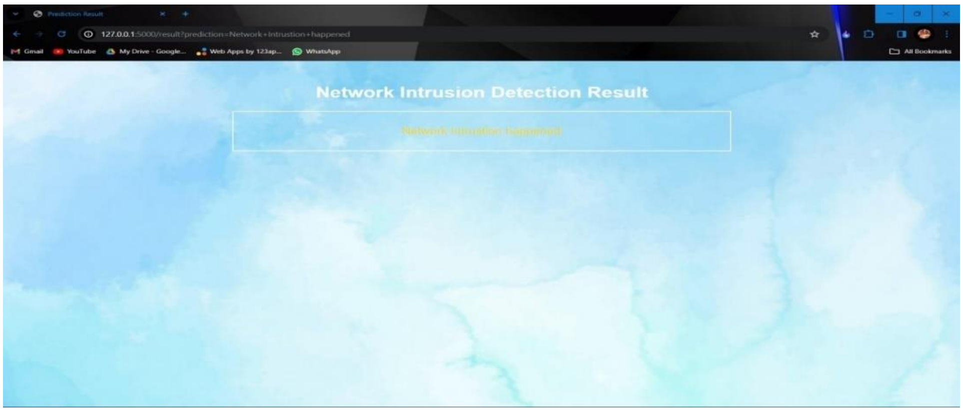
Fig 2: - After giving input in the dashboard



Network Intrusion Detection Result

No intrusion

Fig 3:- After entering the values we need to press the predict button which calls the trained machine and predict whether the intrusion is happened or not



Network Intrusion Detection Result

Network intrusion happened

Fig 4:- Protocol Type: The type of protocol used in a network communication can provide clues.

For example: An unexpected use of an uncommon protocol (e.g., ICMP tunneling) could indicate an intrusion. A sudden switch from a secure protocol (e.g., HTTPS) to an insecure one (e.g., HTTP) might raise suspicion.

7. CONCLUSION & FUTURE WORK

This article effectively tackles the pressing requirement for cutting-edge security measures to counteract growing cyberthreats. It offers a thorough examination of intrusion detection techniques, making a significant contribution to the cybersecurity community. This article has created a proactive, flexible, and strong network security defensive mechanism by utilizing a mix of signature-based, anomaly-based, and machine learning techniques.

This initiative is an important step in strengthening networks' resistance to changing cyberthreats. This article required the integration of cutting-edge intrusion detection techniques, technologies, and best practices.

This article is a thorough and proactive strategy for protecting networks from a wide range of online dangers. Although the current system provides a strong basis, This article's flexible and forward-thinking architecture puts it in a position to change with the constantly shifting network security environment. Maintaining the system's efficacy in the face of changing cybersecurity issues will need ongoing cooperation, threat monitoring, and system changes.

7. 1 Upcoming Improvements:

Although this article establishes the groundwork for strong network security, there are numerous opportunities for further development and extension. The following are some possible future article scopes: Form partnerships with outside threat intelligence communities to exchange knowledge and research results and support a team effort to counter cyberthreats. This can improve This article's capacity to remain ahead of new dangers. The intrusion detection system will continue to be efficient and flexible in the face of new threats thanks to these future scopes, which are in line with the changing cybersecurity environment and technological developments. This article's ongoing success will depend on regular updates, cooperation with the cybersecurity community, and a dedication to being up to date on the most recent threats.

REFERENCES

[1] H.Wang,J.Gu,andS.Wang,‘‘An effective intrusion detection framework based on SVM with feature augmentation,’’ Knowl.-Based Syst., vol. 136, pp. 130–139, Nov. 2017.

[2]Setareh Roshan, Yoan Miche, Anton Akusok, Amaury Lendasse; “Adaptive and Online Network Intrusion Detection System using Clustering and Extreme Learning Machines”, ELSEVIER, Journal of the Franklin Institute, Volume.355, Issue 4,March 2018,pp.1752-1779.

[3] Wathiq Laftah Al-Yaseen , Zulaiha Ali Othman , Mohd Zakree Ahmad Nazri; “Multi-Level Hybrid Support Vector Machine and Extreme Learning Machine Based on Modified K-means for Intrusion Detection System”, ELSEVIER, Expert System with Applications, Volume.66,Jan 2017,pp.296-303.

[4]Iftikhar Ahmad, Mohammad Basheri, Muhammad Javed Iqbal, Aneel Raheem; “Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection”, IEEE ACCESS, Survivability Strategies for Emerging Wireless Networks, Volume.6,May 2018,pp.33789-33795.

[5]BuseGulAtli1, YoanMiche,AapoKalliola, IanOliver, SilkeHoltmanns, AmauryLendasse; “Anomaly-Based Intrusion Detection Using Extreme Learning Machine and Aggregation of Network Traffic Statistics in Probability Space” SPRINGER, Cognitive Computation, June 2018,pp. 1-16

[6] Pinjia He, Jieming Zhu, Shilin He, Jian Li, and Michael R. Lyu; “A Feature Reduced Intrusion Detection System Using ANN Classifier”, ELSEVIER, Expert Systems with Applications, Vol.88, December 2017 pp.249-247.

[7] Vajiheh Hajisalem, Shahram Babaie; “A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection”, ELSEVIER, Department of Computer

Engineering, Vol. 136, pp. 37-50, May 2018.
[8] Karen A. Garcia, Raul Monroy , Luis A. Trejo, Carlos Mex-Perera and Eduardo Aguirre,“ Analyzing Log Files for Postmortem Intrusion Detection”, IEEE Transactions on Systems,Man, and Cybernetics, part C(Application and Reviews)42.6(2012),pp.1690-1704.
[9] R.M.Elbasiony,E.A.Sallam,T.E.Eltobely,andM.M.Fahmy,‘‘A hybrid network intrusion detection framework based on random forests and weighted k-means,’’ Ain Shams Eng. J.,vol. 4,no. 4,pp. 753–762, 2013.
[10] Hudan Studiawan, Christian Payne, Ferdous Sohel; “Graph Clustering and Anomaly Detection of Access Control log for Forensic Purposes”, ELSEVIER, Digital Investigation, Vol. 21, pp.76-87, June 2017.