Articles about Anomaly Intrusion Detection Techniques (2023)

Jacob Graham 1141178

Branden Yoshaev 1137913

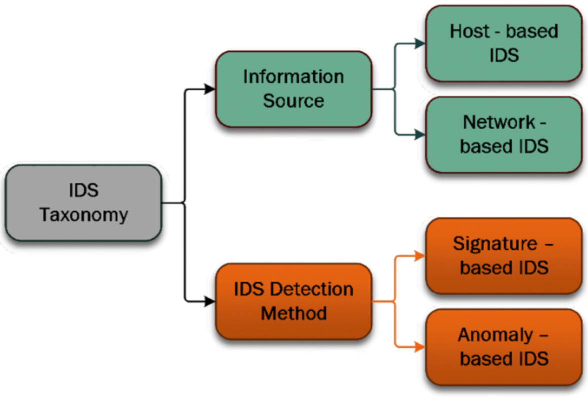
Abstract — **Anomaly intrusion techniques have become an essential area of study in the field of computer security. This is because traditional security mechanisms have become insufficient in detecting and preventing sophisticated attacks that are capable of bypassing static security mechanisms. Anomaly intrusion techniques are focused on the identification of anomalous behaviour that deviates from the expected or normal behaviour. These techniques use machine learning algorithms and statistical methods to detect intrusions and identify previously unknown or novel attacks. The primary goal of anomaly intrusion detection is to identify malicious activity that might otherwise go undetected. Unlike signature-based intrusion detection systems that rely on a pre-existing database of known signatures, anomaly detection algorithms identify malicious activity based on its deviation from normal system behavior. The process of identifying anomalies can be challenging because many factors can influence system behavior, including software updates, network traffic, and changes in user behavior. However, with advancements in machine learning and statistical analysis, anomaly intrusion techniques have become more effective at detecting previously unknown attacks. This article will provide an in-depth analysis of anomaly intrusion techniques. We will examine the fundamental concepts, machine learning algorithms, and statistical methods used in anomaly detection systems. Additionally, we will review the strengths and weaknesses of these techniques and explore how they can be used in real-world applications. Finally, we will discuss current research and future directions in the field of anomaly intrusion detection.**

I. SECURITY THREATS AND APPROACHES

Anomaly Intrusion Detection has various different types of techniques, security threats and intrusion detection techniques for wireless sensor networks (WSN), which are autonomous nodes communicating in a decentralized way through multi-hop routing. WSNs have the self-organizing capability, limited resources, and use multi-hop routing due to short transmission range. the differences between WSNs and mobile ad hoc networks (MANET) and present various attacks that can compromise WSNs' security, such as misdirection, selective forwarding, sinkhole, Sybil, wormhole, and hello flood attacks. Two main intrusion detection techniques, signature-based and anomaly-based, are discussed, the anomaly-based detection technique and several existing approaches, such as intrusion detection based on OSI layers. The authors propose using Received Signal Strength Indicator (RSSI) value at the physical layer, TDMA at the Mac layer, and forwarding tables generated by the routing protocol at the routing layer to detect anomalies. Many surveys have been conducted with different focuses, In the modern world, there is an ever-growing number of companies offering services such as e-commerce, social media applications, and other platforms which require users to share personal information to utilize them. For example, suppose a user wishes to purchase a subscription, in which they must enter their personal data into a website and trust their information is secure. This opens up the possibility of security issues like phishing, dos (denial of service), and xss (cross-site scripting) attacks. As we provide details on how these attacks and their severity are countered.

In general, a computer network is a collection of computers where information exchange occurs, and there is a main computer that acts like an agent controlling the tasks like load balancing and routing the packets to are correct locations. This network can be augmented by integrating a *secure controlling agent*, an intelligent entity which is responsible for controlling and managing a network's tasks, such as load balancing and routing packets. Additionally, the agent's algorithm is also capable of preventing denial of service (DoS) or distributed denial of service (DDoS) attacks on the network. Essentially, the agent analyzes all data flow in and out of the system, flagging and performing some action on malicious or illegal network activity (blocking IP addresses, configuring a firewall, limiting data flow from a specific location, or even shutting down the network). Like all computer systems, the agent is driven by a carefully-designed algorithm, called a *Secure Controller* algorithm, to function optimally. Among the most important features of the algorithm, it must be designed to be flexible and compatible, with the ability to adapt to new attack methods as they emerge and be able to integrate well with changing network infrastructure. The use of a secure controlling agent, when combined with a strong Secure Controller algorithm, provides an effective defence mechanism against network attacks and other intrusions which could compromise the integrity of system data. Better yet, when combined with other anomaly intrusion detection techniques such as signature-based intrusion detection, ensures that a network remains secure and reliable when faced with sophisticated attacks. We here see that the increasing number of companies offering online services that require users to share personal information opens up the possibility of security issues like phishing, dos, and XSS attacks. To counter these attacks, a secure controlling agent can be integrated into a computer network to control and manage tasks such as load balancing and routing packets. The agent's algorithm must be flexible and compatible to adapt to new attack methods as they emerge and integrate well with changing network infrastructure. The use of a secure controlling agent, along with a strong Secure Controller algorithm, provides an effective defence mechanism against network attacks and other intrusions that could compromise the integrity of system data. Combining with other anomaly intrusion detection techniques such as signature-based intrusion detection can ensure that a network remains secure and reliable against sophisticated attacks.

The need for intrusion detection systems (IDS) to secure information system resources and ensure business continuity, with a focus on anomaly-based IDS using the Local Outlier Factor (LOF) algorithm. The LOF algorithm evaluates each event's uniqueness based on distance from the nearest neighbours and is able to detect outliers regardless of data distribution. The article outlines related works in the area, discusses the proposed methodology, and presents experimental results of different threshold values' influence on anomaly detection accuracy using the data set. The LOF model based on normal data has been used for training, and the results show the importance of parameter selection for the LOF algorithm.



Intrusion Detection Systems (IDS), are used to monitor and investigate network activity data in real-time to identify potential security breaches. IDS can identify two types of intruders: external and internal, with external intruders being unauthorized users from outside the network and internal intruders being authorized users who try to access unauthorized data resources. There are two types of IDS: Active IDS, also known as Intrusion Detection and Prevention System (IDPS), which is designed to block attacks automatically and provide real-time action, and Passive IDS, which only monitors and alerts an operator of potential vulnerabilities and attacks. IDS identifies several types of intrusions, including attempted break-ins, probing, denial-of-service (DOS) attacks, masquerade identity intrusions, penetration, user-to-root (U2R), and remote-to-user (R2L).

Attempted break-ins involve unauthorized access to a system with the least amount of force, usually for financial gain, revenge, or competition. Masquerade identity intrusions involve an attacker pretending to be someone they're not to gain unauthorized access. Penetration is the ability to gain access to a system, while DOS attacks involve flooding a network or system with useless traffic to bring it down. DOS attacks have several types, such as SYN Flood, UDP flood, HTTP flood, NTP amplification, ICMP (Ping flood), Ping of Death, Slowloris, and zero-day attacks. An emphasis is made that IDS is crucial in identifying potential security breaches and intrusions, and it is essential to have a strong IDS in place to protect the network and data resources from both internal and external attacks. IDS can help in identifying the type of intrusion and taking appropriate action in real time, preventing significant data breaches and other security incidents.

II. Surveys

Intrusion detection systems, are based on two general approaches: detecting anomalous behaviour and monitoring is known malicious attacks and system vulnerabilities. Anomaly-based intrusion detection systems assume that normal activities will deviate under attacks and detect abnormalities compared to predefined behaviour models.a survey of anomaly intrusion detection techniques and the evolution of intrusion detection systems over the past two decades, focusing on recent advances in statistics, machine learning, neural networks, computer immunology, and data mining techniques. Specifically the focus on the advancements of intrusion detection for machine learning. Machine learning can be used to build a user profile. For example, Lane, T., Brodley, C. E. used instance-based learning to determine a similarity measure between the 10 most recent commands of an unknown user and his profile. Based on sequences of user commands in a certain time frame, the similarity measure is computed by calculating the differences in the sequences' characters, which is used to distinguish a real user from a masquerader. Balajinath, B., Raghavan, S.V. constructed a GBID (Genetic Based Intrusion Detector) to learn individual user behaviour. Using a behaviour model built from a 3-tuple learnt using a genetic algorithm, a numeric value was calculated for a fixed block size of commands in a user session. Then, that value is compared with existing non-intrusive thresholds for block sizes to determine the possibility of potential intrusions. Sinclair, C.

developed rules from existing machine learning applications.

Both the generic algorithm and decision tree are used to automatically generate rules for classifying network connections, and filtering out potentially anonymous ones. As you might expect, these rules are layered on top of an existing system's IDS (Intrusion Detection System) and greatly enhances it. intrusion detection systems, which can detect anomalous behaviour and known malicious attacks. Anomaly-based intrusion detection systems detect abnormal activities compared to predefined behaviour models. A survey of anomaly intrusion detection techniques and reviews the evolution of intrusion detection systems over the past two decades. Machine learning can be used to build user profiles to distinguish between real users and masqueraders. Discussion of various machine learning techniques, including instance-based learning, genetic-based intrusion detectors, and rules generated from machine learning applications. These techniques can enhance existing intrusion detection systems.

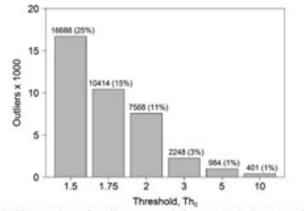


Fig. 2. The number of outliers removed from normal data set using corresponding Th_c values.

The importance of Intrusion Detection Systems (IDS) in organizations and the need for enhancing IDS technology. IDS technology has become highly automated, and the logs are monitored regularly for analyzing activities. To decrease the false alarm rate, it is mandatory to define baseline policy strategies. Research is ongoing for the development of real-time IDS with virtualization technologies, which can handle various aspects of the intrusion detection system. Host-based IDS (HIDS) is considered an important part of IDSs, which can detect attacks, prevent malicious activities, and restore the system to a secure state. reducing the false positive alarm rate requires more manual input in HIDS, unless the inputs are semantically balanced. The article also highlights the challenges of developing IDS for smartphones and tablets and the need for research to develop HIDS that utilizes trusted platform modules and cryptographic technologies. The ability of a HIDS to recover quickly from attacks is dependent on the attacks, and the monitoring of various events and processes is performed in a virtual machine.

III. Technology and Networks

Technology and networks are factors all about Intrusion Detection. There are various types that are used wireless Sensor Networks (WSNs) have become increasingly popular due to their ability to operate in challenging environments and the variety of applications they support. However, their characteristics, such as self-organizing nature, limited battery power, and distributed operations, make them vulnerable to various security attacks at all layers of the Open System Interconnections (OSI) model, which is several layers of a way for computer systems to communicate with each other over a network. Although several security solutions, such as authentication and secure routing, have been proposed to address these attacks, they are not sufficient to eliminate most of them. An Intrusion Detection System (IDS) is an alternative solution to address a wide range of security attacks in WSNs. There are several existing IDS techniques, including anomaly-based IDSs, signature-based IDSs, and hybrid IDS, and propose a new cross-layer IDS for detecting multi-layer attacks in WSNs. The proposed work is divided into four modules, including the chain cluster topology and the hybrid energy efficiency protocol (HEEP).

There are many challenges that networks and technology face, challenges posed by big and high-dimensional data and the use of feature selection (FS) as a preprocessing technique to address these challenges. It proposes a new approach for FS in intrusion detection systems that use fuzzy numbers and a correlation-based scoring method to reduce the size of the dataset while controlling the number of selected features. It also provides background information on FS algorithms, fuzzy concepts, genetic algorithms, and intrusion detection systems. The proposed method is shown to reduce the false alarm rate and control the number of features in network intrusion detection systems.

Comparing the proposed method with other approaches and discussing its potential benefits. Various feature selection methods for Intrusion Detection Systems (IDSs) help in identifying network attacks. The methods reviewed include DNA encoding, Information Gain-based algorithms, filtering algorithms, and hybrid algorithms. Each method has its advantages and disadvantages in selecting features. The article suggests that combining filtering algorithms with meta-heuristic search algorithms can improve the performance of IDSs. The need for effective systems to classify network traffic as an attack or normal is emphasized due to the increasing requirement for network security. A proposed method for feature selection in intrusion detection systems. The method uses a heuristic function algorithm and a fuzzy triangular number parameter to control the number of selected features. The results of applying the method to the NSL and CICIDS datasets (types of datasets) show that it outperforms other feature selection methods in terms of classification accuracy and false alarm rates. The proposed method selects fewer features than other methods while achieving similar or better accuracy. The article concludes that feature selection is an important pre-processing step to improve the performance of intrusion detection systems.

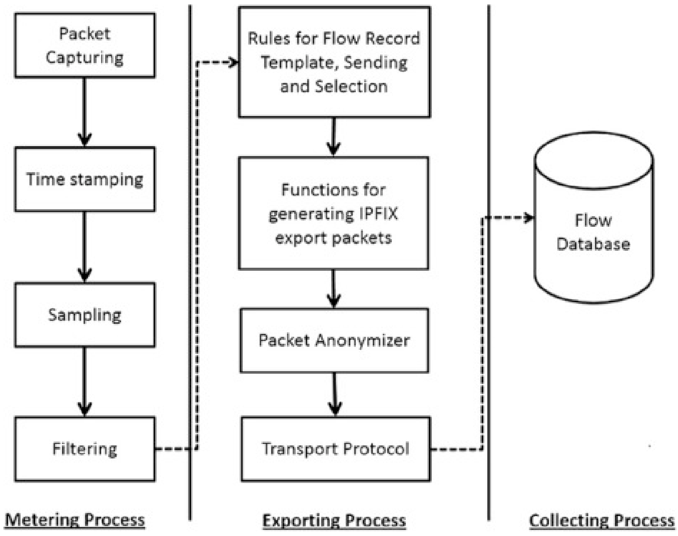
Biometrics has been a new part of our everyday lifestyle and is being used in many things around us. Our phones, computers, schools, transport, etc. It presents a new approach to user profiling in intrusion detection applications using behavioural biometrics, specifically keystroke and mouse dynamics. The proposed technique involves capturing mouse and keyboard actions, performing behavioural modelling and feature extraction to generate a unique signature for each user, and comparing it against the reference signature stored in a database. Also discusses the proposed algorithms and techniques used to generate the Keystroke Dynamics Signature (KDS) and Mouse Dynamics Signature (MDS) for user profiling. Overall, using biometrics in intrusion detection systems is seen as a promising way to enhance the detection process and improve accuracy.

Various proposals for intrusion detection systems (IDS) in virtual machines (VM) and cloud computing networks. Roschke et al. proposed a technique based on user configurations, but it requires multiple instances of IDS for each user. Bakshi and Yogesh proposed an IDS for the prevention of DDOS attacks, but it can only detect previously known attacks. Mazzariello et al. proposed integrating an IDS in open-source cloud computing but it fails to detect insider and unknown attacks. Sandar and Shenai proposed a scheme called EDoS for offering protection on the cloud using HTTP and XML but it is again unsuccessful in detecting previously unknown attacks. Dastjerdi et al. developed a framework called Cooperative Intrusion Detection System which is able to prevent single-point failures but is computationally intensive and does not block all forms of attacks. Lin et al. proposed the latest development in this field, which is a system deployed with respect to the virtual machine monitor (VMM) and dynamically updates detection rules as the system performs new operations.

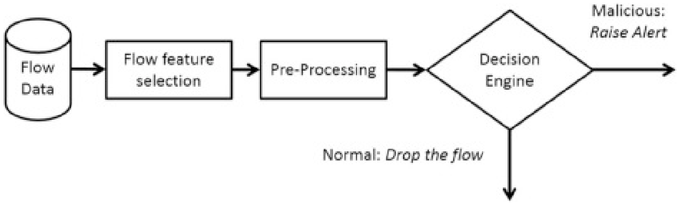
IV. Systems

There are different types of systems that use intrusion detection and use techniques to support them. advantages of using a hybrid approach for intrusion detection systems, which combines both anomaly and signature detection techniques. This approach helps in detecting both known and unknown attacks, and also reduces false alarm rates. The various approaches to hybrid intrusion detection systems, such as

EMERALD, NIDES, and random forests algorithm-based systems. These approaches use different techniques like statistical analysis engines and expert systems, subscription-based communication schemes, and correlation components to analyze both sets of reports of possible intrusive activity. As well as the challenge of getting different intrusion detection technologies to interoperate effectively and efficiently. Flow-based intrusion detection systems use network flow data for intrusion detection. Network flow data has multiple applications such as billing, traffic analysis, network visibility, congestion control, and intrusion detection. A network flow is a set of packets or frames passing through a network observation point during a specific time interval, and all packets belonging to a particular flow have a set of common properties. Observation points can be flow probes or flow-enabled network devices. The information of network flow is stored in a flow record, and the processing of flow records in a network is managed through a flow export and collection protocol. The explanation is that IPFIX is a flexible protocol adopted by the Internet Engineering Task Force (IETF) for the development of a standard flow export and collection protocol. The IPFIX architecture consists of observation points, an exporting process, and a collecting process, with each process serving a specific function in generating IPFIX flow records and storing them in a flow database.



The architecture of a flow-based intrusion detection system that takes IPFIX/Netflow records as input. The flow records may have many attributes, but only relevant attributes are selected in the feature selection phase for attack detection. The flow records are then pre-processed in a specific format before being input into the detection algorithm. The algorithm then marks flow records as malicious or normal, with normal flows being dropped and malicious flows triggering alerts for further inspection.



The implementation of an intrusion detection system (IDS) using artificial neural networks (ANNs). The proposed system consists of two modules, namely the detection module and the classification module. The detection module captures incoming and outgoing packets in the network and uses ANNs for anomaly detection. The classification module uses ANNs to classify the data into normal or attack categories. The performance of the system was evaluated in three different scenarios, namely detection only, detection and classification, and detection and detailed classification. The results show that the system is effective in detecting and classifying network attacks. However, the training of the ANN requires a large amount of data and time, and there is a trade-off between increasing the classification levels and the percentage of detection. By emphasizing the importance of IDS as a complement to other security technologies, and how they work together to provide an integrated high level of security.

V. Algorithms

The importance of network security and intrusion detection technology in ensuring the privacy and security of personal and business activities carried out over the internet. The article introduces a new intrusion detection method based on a rough Fourier fast algorithm to improve detection accuracy and reduce false detection rates by optimizing the classification model. The requirements of network intrusion detection are analyzed, and the proposed intrusion detection model based on a rough Fourier fast algorithm reduces the average detection time by 0.04s and has an average improvement of 0.93% in the F-measure value. The information module includes technology, people, organization, and management components. Also the vulnerability model and the root causes of vulnerabilities, such as violations of software engineering techniques, software usage, and environmental assumptions. Additionally, the application of the rough Fourier fast algorithm in intrusion anomaly detection. The algorithm extracts knowledge and patterns useful to users from a large amount of data and determines whether abnormal behaviour occurs. The anomaly detection module has its advantages and disadvantages of the rough Fourier fast algorithm. Limitations of existing network security products, which are mainly based on passive defence and lack communication and cooperation with each other. The importance of situational element extraction technology in identifying attack types and improving the accuracy of situational information for network workers to conduct situational assessment and prediction. The rough Fourier fast algorithm is shown to have a better extraction effect of situational elements compared to other reduction algorithms. A situational element extraction method based on a rough Fourier fast algorithm to extract key information from massive situational element data and respond to the network situation in time. The method uses four classifiers to identify attack types and the relationship between attributes and classification modelling time. The proposed model improves the precision, accuracy rate, and recall rate. It also discusses the impact of attribute reduction on data analysis and mining. The rough Fourier fast algorithm has the best effect in reducing the dimension of network intrusion detection data, as the proposed method has both theoretical and practical value.

VI. Security

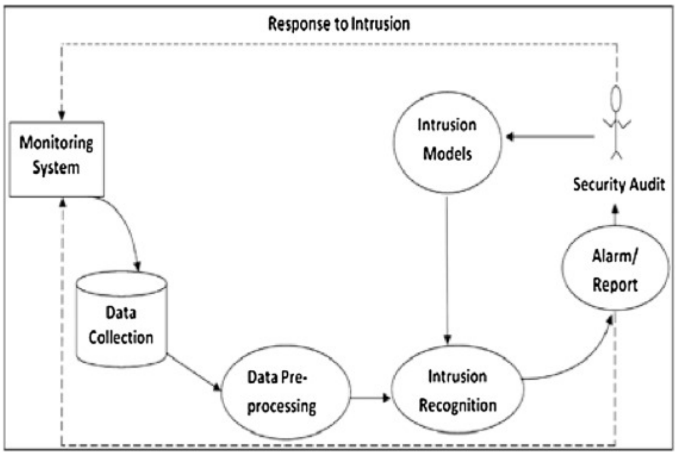
The security of computer information systems is crucial for national sovereignty, trade secrets, and personal privacy in the information age. Database intrusion detection technology is a widely used technology and management tool that provides real-time protection to internal and external attacks, and incorrect operations and gives an alarm promptly when detecting intrusions. Intrusion detection research can be traced back to 1980, and the field has undergone significant developments, including the design of autonomous agents for intrusion detection and an Agent-based distributed intrusion detection system model. There are two common methods of intrusion detection: misuse detection and anomaly detection. Misuse detection makes detection by using known attack methods based on defined intrusion patterns, while anomaly detection makes intrusion detection according to user behaviour or normal degree of resource use rather than by a specific behavior. There are several different types of methods some of which are: The Correlation Analysis Method is a data mining method that is widely used to find relationships between a group of objects in a database. This method is divided into two categories: association rules and sequential patterns. Association rules analyze a set of records and derive the relationship between items in a given collection of items and sets of records. On the other hand, sequential patterns analyze causality between data and find the relationship between database records in the time window.

VII. Techniques

Intrusion Detection Systems (IDS) in computer security and the different techniques used for intrusion detection. The two main types of intrusion detection techniques are Misuse or Signature Based and Anomaly Based methods. The use of data mining and machine learning algorithms, including Fuzzy Logic based methods and clustering algorithms, have been widely used in automatic intrusion detection. The article also discusses various hybrid models that combine multiple techniques for better detection accuracy rates, including Weighted FCM and Immune Genetic Algorithm, Kernel Fuzzy C-Means and Bayesian Neural Networks, and fuzzy clustering with multilayer perceptron neural network. Methods based on fuzzy clustering to overcome the limitations of the traditional Fuzzy C-Means method. The proposed method involves three steps: pre-processing, feature selection, and clustering. To evaluate the proposed method, experiments were conducted on the KDD Cup 99 dataset, and the results were compared with other methods. The validation of the proposed method uses four cluster validity functions, accuracy, false alarm rate, and comparisons with contemporary methods.

Anomaly-based intrusion detection techniques are used to detect network security breaches. The advantages and limitations of these techniques, as various types of anomaly detection systems, including statistical, rule-based, and machine learning-based systems. The challenges associated with implementing these techniques, such as data preprocessing, feature selection, and evaluating the effectiveness of the detection system. While anomaly-based detection techniques are useful, they should be used in combination with other techniques to provide a more comprehensive approach to network security.

The process of identifying unexpected hidden patterns in data sets that do not match the normal flow of behaviour. Anomalies are also referred to as outliers, discordant observations or aberrations. An anomaly detection system monitors the behaviour of a system and flags deviations from usual activity as an anomaly. A machine learning-based approaches to detect anomalies in real-time weather datasets, particularly in predicting the significant signs of changing climate events for a specific region in the state. The proposed framework is designed to forecast changing climate problems for a decade weather dataset. We see various techniques for intrusion detection and the types of categories of intrusion detection systems. It also presents the advantages and disadvantages of different algorithms and techniques used in intrusion detection systems.



VIII. Conclusion

In conclusion, anomaly-based intrusion detection techniques are an essential aspect of network security, as they help detect potential security breaches and intrusions that may be missed by signature-based methods. Anomaly detection systems can use different approaches such as statistical, rule-based, or machine learning-based systems, to analyze and detect abnormal behaviour and identify possible security threats. However, these techniques come with their own set of limitations, including data preprocessing, feature selection, and evaluation of effectiveness, which can impact their accuracy and reliability. Therefore, anomaly detection techniques should be used in combination with other approaches to provide a comprehensive and effective approach to network security.

References

[1] Islam, S., & Rahman, S. A. (2011, November). *Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches*, from https://www.researchgate.net/profile/Syed-Ashiqur-Rahman/publication/309204365_Anomaly_Intrusion_Detection_System_in_Wireless_Sensor_Networks_Security_Threats_and_Existing_Approaches/links/5809866808ae993dc050a460/Anomaly-Intrusion-Detection-System-in-Wireless-Sensor-Networks-Security-Threats-and-Existing-Approaches.pdf?origin=publication_detail

[2] Chandran, Sharanya & Kumar, K. (2018). A survey of intrusion detection techniques. International Journal of Engineering & Technology. 7. 187. 10.14419/ijet.v7i2.4.13036.

[3] Alamiedy, T.A., Anbar, M., Alqattan, Z.N.M. *et al.* Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm. *J Ambient Intell Human Comput* **11**, 3735–3756 (2020). https://doi.org/10.1007/s12652-019-01569-8

[4] Yingbing Yu. 2012. A survey of anomaly intrusion detection techniques. J. Comput. Sci. Coll. 28, 1 (October 2012), 9–17

[5] Chandran, Sharanya & Kumar, K. (2018). A survey of intrusion detection techniques. International Journal of Engineering & Technology. 7. 187. 10.14419/ijet.v7i2.4.13036.

[6] Magdalene, A. H. S., & Kumar, P. (2014). Identifying security threats using signature based intrusion detection system in wireless sensor networks. *Advances in Natural and Applied Sciences*, *8*(16), 44+.

[7] Auskalnis, J., Paulauskas, N., & Baskys, A. (2018). Application of local outlier factor algorithm to detect anomalies in computer network. *Elektronika Ir Elektrotechnika*, *24*(3). https://doi.org/10.5755/j01.eie.24.3.20972

[8] Srinivasan, V., & Vidhya, M. (2015). Cross layer based anomaly intrusion detection in wireless sensor network. *Advances in Natural and Applied Sciences*, *9*(6 SE), 607+. https://link-gale-com.ezproxy.lakeheadu.ca/apps/doc/A420324572/AONE?u=ocul_lakehead&sid=bookmark-AONE&xid=13972e0

[9] Shiravani, A., Sadreddini, M. H., & Nahook, H. N. (2023). Network intrusion detection using data dimensions reduction techniques. *Journal of Big Data*, *10*(1), NA. https://link-gale-com.ezproxy.lakeheadu.ca/apps/oc/A739531322/AONE?u=ocul_lakehead&sid=bookmark-AONE&xid=f037df63

[10] Ranjan, R., & G, S. (2014). A new clutering approach for anomaly intrusion detection. *International Journal of Data Mining & Knowledge Management Process*, *4*(2), 29–38. https://doi.org/10.5121/ijdkp.2014.4203

[11] García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1-2), 18–28.

[12] A. A. E. Ahmed and I. Traore, "Anomaly intrusion detection based on biometrics," *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, West Point, NY, USA, 2005, pp. 452-453, https://doi.org/10.1109/iaw.2005.1495997

[13] Shijoe Jose *et al* 2018 *J. Phys.: Conf. Ser.* **1000** 012049 PDF link: https://iopscience.iop.org/article/10.1088/1742-6596/1000/1/012049/pdf

[14] Muhammad Fahad, U., Muhammad S., & Yaxin, B. (2017). Flow-based intrusion detection: Techniques and challenges. *Computers & security*. 70, 238-254. https://doi.org/10.1016/j.cose.2017.05.009

[15] Harish, B. S., & Kumar, S. V. A. (2017). Anomaly based Intrusion Detection using Modified Fuzzy Clustering. *International Journal of Interactive Multimedia and Artificial Intelligence*, *4*(6), 54+. https://link-gale-com.ezproxy.lakeheadu.ca/apps/d

oc/A587019692/AONE?u=ocul_lakehead&sid=bookmark-AONE&xid=15fa13cf

[16] Vaishnavi, P., Palanivel, G., & Duraiswamy, K. (2017). A novel framework for anomaly detection and prediction of significant signs of changing climate events using machine learning techniques. *Advances in Natural and Applied Sciences*, *11*(2), 14+. https://link-gale-com.ezproxy.lakeheadu.ca/apps/doc/A492465754/AONE?u=ocul_lakehead&sid=bookmark-AONE&xid=a3d46636

[17] Xiang-He, W., & Hong, Z. (2016). Explorations of computer database intrusion detection technology targeting at external forced entry. *RISTI* [Revista Iberica de Sistemas e Tecnologias de Informacao], (17B), 370+.

[18] Al-Janabi, S. T., & Saeed, H. A. (2011). A neural network based anomaly intrusion detection system. *2011 Developments in E-Systems Engineering*. https://doi.org/10.1109/dese.2011.19

[19] Duan, X. (2022). Computer Network Intrusion Anomaly Detection Based on Rough Fourier Fast Algorithm. *Mathematical Problems in Engineering*, *2022*. https://link-gale-com.ezproxy.lakeheadu.ca/apps/doc/A721691392/AONE?u=ocul_lakehead&sid=bookmark-AONE&xid=47ae0fca

[20] S. A. Maske and T. J. Parvat, "Advanced anomaly intrusion detection technique for host based system using system call patterns," *2016 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India, 2016, pp. 1-4, doi: 10.1109/INVENTIVE.2016.7824846.

[21] Aljawarneh, S., Aldwairi, M., & Yassein, B., M. (2018, April 14). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *ScienceDirect*. https://www.sciencedirect.com/science/article/abs/pii/S1877750316305099