Grenze International Journal of Engineering and Technology, Jan Issue

Wireless Network Intrusion Detection System: Techniques, Systems and Future Challenges

Ch Swathi[1] and K Suresh Babu[2]
[1]G Narayanamma Institute of Technology and Science, Assistant Professor, Department of CSE, Hyderabad, India
Email: chswathi0508@gmail.com
[2]Associate Professor of CSE at School of Information Technology, JNT University Hyderabad Hyderabad, India

***Abstract*—Our daily lives are gradually getting more and more permeated by information technology. It becomes more crucial to protect these systems as their interconnectedness expands. Most of these systems are now networked wirelessly since doing so reduces the time and money required for both installation and maintenance. We conduct a literature review to locate knowledge gaps and suggest future research objectives in the field of wireless network intrusion detection. We take a methodical approach to categorising current wireless IDS methods according to their respective levels of sophistication, scope of coverage, target wireless network, data gathering procedure, trust model, and analysis method. In this article, we provide a concise overview of the benefits and drawbacks of various approaches to wireless intrusion detection, taking into account the unique characteristics of various wireless networks like WLANs, WPANs, WSNs, ad hoc networks, mobile telephony, WMNs, and cyber physical systems (CPSs). We then provide a brief overview of the most and least explored wireless IDS strategies, highlight the gaps in the current research, and critically examine the reasoning behind the varying levels of attention paid to each. We conclude by pointing out areas deserving of further study that have received relatively little attention and offering suggestions for doing so.**

***Index Terms*— IDS Techniques, Wireless Networks, Classification, , MANETs; Intrusion Detection Security Attacks and IDS architectures.**

I. INTRODUCTION

Intrusion detection systems aid in the protection and defence of computer networks. They do this by gathering data from numerous systems and networks, and then analysing that data to look for vulnerabilities in the system's defences.

A. The benefits of intrusion detection include:

- Keep an eye on user and system behaviour and analyse it
- Configuration and security auditing
- Verifying the safety of vital data and system files
- Comparison of observed behaviour to previously recorded attacks for statistical analysis
- Detection and Analysis of Abnormal Behavior
- Verification of the Operating System

The core of an intrusion detection system consists of three parts.

Grenze ID: 01.GIJET.9.1.750

A Network Intrusion Detection System (NIDS) monitors all traffic in and out of a network for signs of intrusion. Promiscuous mode operation that compares subnet-passed traffic to a database of known threats. The alert is sent to the administrator after the assault is detected or unusual behaviour is noticed. A common use case for NIDS is to monitor the subnet where firewalls are located for intrusion attempts.
An NNIDS, or network-based intrusion-detection system, examines data travelling between a network and a certain host in order to spot potential security breaches. When comparing NIDS with NNIDS, it's important to note that the former simply monitors traffic on a single host, while the latter does so for an entire subnet. By way of illustration, the NNIDS might be set up on a VPN endpoint so that the decrypted traffic could be inspected. Observing whether or not a person istrying to access your virtual private network
With a Host Intrusion Detection System (HIDS), a snapshot of your current system files is taken and compared to a previous snapshot. The alert is delivered to the administrator in case any of the essential system files were altered or removed. Mission-critical computers, which are not supposed to malfunction, are a prime example of a system that uses HIDS.

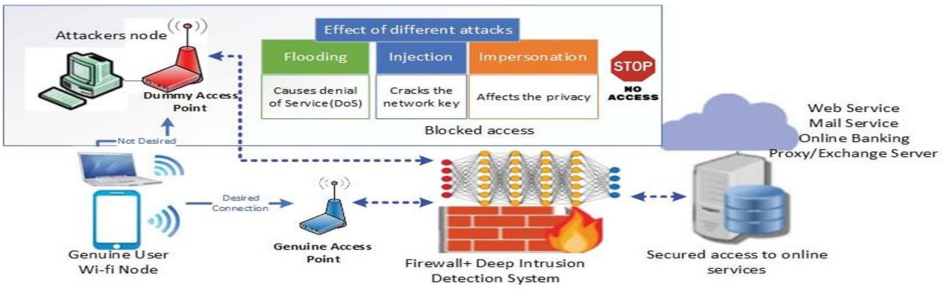

Figure 1: Network Intrusion Detection System

B. What Can and Cannot Be Expected from an Intrusion Detection System

However, the IDS is not the solution to all of our security concerns.
We need to know the limits of your IDS so that we know what to expect from it. Each network environment is unique, and so each Intrusion Detection System must be customised to match the requirements of our organisational environment. I will provide some instances of what these systems are capable of in the following sections.
The IDS can give these things:
Identify instances in which your system is being attacked; Find any mistakes in the configuration of your system; Assist the system administrator in completing the crucial step of formulating a policy for our computer resources; Reduce the complexity of managing security.Unfortunately, the IDS is unable to supply:
Deal with some of the modern hardware and features of networks; Analyze all of the traffic on a busy network; Handle problems involving packet-level attacks; Compensate for weaknesses in identification and authentication mechanisms; Investigate attacks without human intervention; Deal with weaknesses in network protocols; Deal with problems in the quality or integrity of the information the system provides.

II. Related Work

This chapter provides an overview of the research done on the hybrid network IDS that has been published so far. In addition, this section explains why a hybrid intrusion detection system is preferable to a more conventional one.
Based on vectors, Ijaz et al. [9] present a genetic algorithm. Vector chromosomes are used in this method. This technique is novel in that it displays training data as metrics and chromosomes as a vector. It paves the way for a fitness function to be attained in a variety of ways. In this study, we compare and contrast three different feature selection methods: the forward feature selector algorithm (FFSA), the linear correlation feature selector (LCFS), and the modified mutual information feature selector (MMIFS). Two datasets, CDU-13 and KDD-Cup '99, are used to evaluate the proposed approach. Metrics show that the vector genetic algorithm has a very low false positive rate of 0.17% and a very high detection ratio of 99.8% when it comes to DoS attacks. Important metrics in the IDS, such as U2R, Probe, and R2L assaults, are not evaluated by the authors.
To aid the DT, Alauthaman et al. [4] suggested a P2P bot identification method based on a feed-forward neural network. After that, we use CART as a feature selection technique to pick out the most important ones. Six rules

were used to determine which characteristics were most important, resulting in network traffic reduction measures being used. A total of 29 characteristics are chosen based on adherence to 6 criteria. Because of this, the proposed method was able to
99.20% precision and 99.08% detection rate. One drawback of using a CART is that it divides the variables one by one, which could make the decision tree unstable.
In [6], Kumar and Kumar present a hybrid NIDS model that relies on artificial intelligence. The model incorporates a neurofuzzy genetic algorithm, an adaptive neurofuzzy interference system, a fuzzy logic controller, and multilayer perception. The use of fuzzy logic for selecting relevant features was employed by the writer. In order to collect and sort network traffic, classify the data, and get ready to make the final decision based on an assumption of the correct assault, the suggested system relies on three main components: an analyzer, a collector, and a prediction module. As for the experiment itself,
is evaluated using the KDD-Cup '99 data set, and it increases the rate at which genuine attacks are detected while decreasing the rate at which false alarms are generated to within 1%. Results in fuzzy logic are observed based on assumptions, which might lead to inaccuracies in the results.
In a wireless sensor network IDS, Safaldin et al. [24] used the enhanced binary grey wolf optimizer as a feature selection approach and support vector machine for classification. The suggested method has a 0.96 accuracy rate, an FPR of 0.03, a detection rate of 0.96, and an execution time of 69.6 hours. The most significant drawback of the SVM classifier is how difficult it is to select a suitable kernel function. As a result of needing more space for the many support vectors generated by SVM, training on large datasets might take significantly longer.
In an Internet of Things (IoT) setting, Vallathan et al. [46] provide a deep learning-based method for dubious action detection. Deep learning methods and RFKD are used to make predictions about anomalous behaviour observed in footage collected by N/W surveillance tools. In order to categorise
purposes, while DNN is utilised for training and learning from data. In addition, the kernel density method is used for both predictive and cluster analysis purposes. The suggested method selects subsets of features using a standard merge-sort tree. The HHAR data sets are utilised for testing and grading. There was a 98.4 percent success rate and a specificity of
On the HHAR data set, the accuracy was 99.8%, while the sensitivity was 96.02%. One major limitation of neural networks is the length of time it takes to train a model because of how many hyperparameters must be tuned.

III. Classification

The diagram depicts a tree structure for organising the many wireless network IDS methods now in use. We divide the research on intrusion detection into six categories, or "dimensions":
The first criterion is the system that will be monitored by the IDS, known as the "target system."
Secondly, the method used for detection is a key differentiator amongst IDSs;
Thirdly, the IDS's collection process is compared in this criterion, which distinguishes between traffic-based and behavior-based IDSs.
The fourth criterion, "Trust Model," differentiates between independent IDSs and those that collaborate on data collection and processing.
The fifth criterion is the method used for analysing data, which can differentiate between more basic methods like pattern matching and more complex methods like data mining. Analysis Technique specifies how an IDS performs its search, while Detection Technique describes the specific items for which the IDS will seek.
Considering both active and passive stances, this criterion compares and contrasts the two.

IV. Quantifying the Effectiveness of Intrusion Detection Systems

Researchers in the field of intrusion detection systems (IDS) typically utilise FPR, FNR, and DR to evaluate performance [11, 18]. Specificity is inverse of FPR, which occurs when an IDS incorrectly detects a trustworthy node as an invader. When an IDS incorrectly labels a hostile or selfish node as benign, this is known as a false negative, or in the literature as a failure to report [1,5]. Detection, on other hand, is achieved when an IDS accurately detects a malevolent or selfish node [6,7,8]. the true positive rate is equivalent to the sensitivity and recall. Accuracy, defined as 1 minus the difference between the false positive and negative rates, is one way that scientists evaluate performance.
Efforts are being made to improve IDS research by establishing new, more precise measures, and this is the subject of some current study. Detection delay is an underutilised yet crucial metric for evaluating IDS

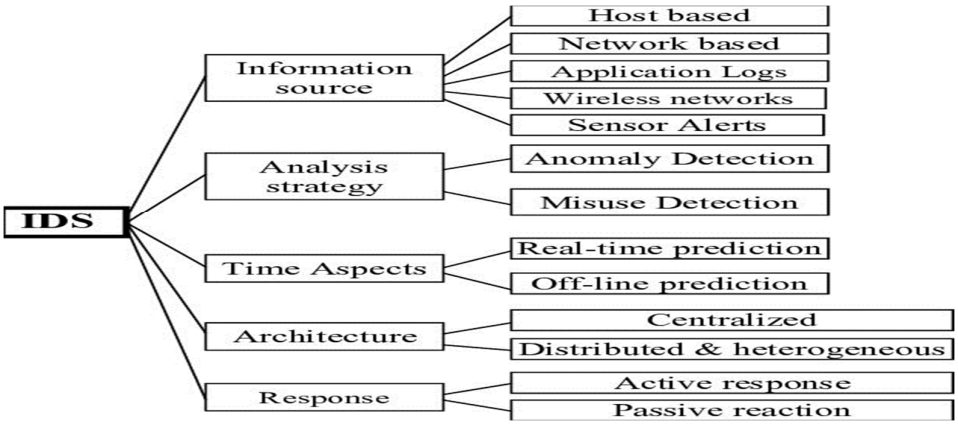

Figure 2 Classification of wireless network IDS

effectiveness [17, 18]. It doesn't matter if an attack is passive or aggressive; quicker detection means faster countermeasures.

Power consumption, communications overhead, and CPU load are also critical parameters for resource-constrained target systems. Many variants on this topic exist. Using a specific method, Ma et al. [25] calculate how long it takes for a particular number of nodes to run out of juice. Performance in packet sampling has been quantified by Misra et al. [26]. The effectiveness of a packet-sampling IDS is measured by the fraction of suspicious packets it correctly identifies after analysis.

The premise is that it is inefficient to sample many packets if only a small number of them actually cause an intrusion to be detected. The design by Misraet al. raises sampling rate if detection rate is higher than forfeit upper limit, and lowers it if it is lower. This means that the sampling efficiency of packets must be adjusted in relation to the detection rate. The detection rate is proportional to the inverse of the forfeit upper limit, but the efficiency of packet sampling is directly related to the threshold. It's preferable to have a high packet sampling efficiency, but that can't be at expense of a high detection rate. The main challenge is distinguishing between low detection rates caused by robust intrusion detection parameters in a peaceful environment and low detection rates caused by relaxed ID parameters in a hostile environment. Time spent on IDS training and test data analysis are quantified by Farid and Rahman [21]. However, there are studies that try to construct measures that are strong in theory but fall short in practise.

The resilience of a system is quantified by Foo et al. [25] as its capacity to both meet consumer demand and withstand intrusion attempts. Both the analyses by Shin et al. [21] rely on trust or reputation that is unique to the application being studied. With these indicators, we can evaluate how well a network performs in accordance with the unique set of regulations governing any given application. In addition to this metric, Shin et al. [29] include the amount of incorrect content sent and the balance of workloads. These measures have been developed for specific purposes, and it is unclear how they may be generalised to the field as a whole. all claim that survival, application-specific trust, and reputation are important, they do not provide convincing arguments for doing so. Last but not least, some researches try to construct measures that have not yet proven beneficial. To quantify performance, Li et al. [23] adapt a metric from biometrics called EER, which is the rate at which false negatives (reject error) and false positives (accept error) are proportional to one another [22]. It is a bold assumption on the part of Li et al. to claim that these rates are inversely connected; if they are directly related, then EER is undefinable since there may be numerous instances in which false negative and positive rates are identical. Haddadi and Sarram [23] devised a test to see if a certain IDS method could identify a variety of different kinds of cyberattacks. Although this statistic is beautifully simplistic, it is incomplete without more information.

V. WIDE-OPEN PROBLEMS AND NEEDS

An extensive taxonomy and state-of-the-art survey of the most prominent intrusion detection techniques/systems suggested for MANETs is presented in this study. Detection methods and systems are typically sorted into groups according to the type of detection engine they use. There is a comparison of the various detection methods by highlighting their own strengths in each classification. We also covered their operational benefits and drawbacks. Existing intrusion detection systems (IDSs) are incapable of fending off the threats that will be

targeting networks in the future. IDS approach, then, necessitates an efficient adaptation to shifting networking technologies. Finally, we use the results of our survey to propose a number of avenues for further study into the development of an effective IDS for MANETs.

Metrics, First: Several intrusion detection methods and systems have been presented for MANETs over the years. But there is no universally agreed upon criterion or metric to evaluate detection system performance [9]. A crucial metric for judging an IDS is its detection latency [18,19]. The receiver operating characteristic (ROC) curve is extensively utilised by researchers for accurate evaluation of IDSs; nevertheless, the results may be deceptive or insufficient [15]. For the purpose of comparing and contrasting different IDSs for MANETs, measurements and standards related to resource utilisation, power consumption, communication overhead, and CPU processing load can be useful. Accordingly, researchers have some leeway in defining the criteria that will be used to assess the IDS.

IDS sensor nodes can be rendered ineffective by flooding attacks (in which a large number of non-attack packets are sent), which produce a flood of false positive alerts and hence crash the sensor nodes' alert processing functionalities. In order to carry out malicious actions, an adversary needs to breach the monitored host and then gain control of it. Therefore, the IDS needs to be able to protect itself from intrusion attempts. The IDS needs to be able to keep an eye on itself and defend itself.

As network topology and routing information available at each node is constantly evolving, accuracy and efficiency of detection procedures might be negatively impacted by anomaly-based detection engines' reliance on normal profiles of the nodes. Since traffic profiles are always shifting, and there is a lot of negative data (noise) in network traffic, it is important to identify the thresholds between "normaltraffic profile" and "abnormaltraffic profile." An adversary is able to adapt attack patterns to look like typical network activity. Finding "attack invariant" characteristics is thus essential for MANETs. High-velocity data in the network makes it difficult to maintain a flexible detection model that accurately reflects the typical operation of the system. A continual process to update the baseline model of behaviour is essential for any detection system to function properly.

The connection among attributes has a vital influence in the detection accuracy [27], making attribute selection one of the important elements that affect the performance of IDS. As a result, from a design perspective, picking the right atomic properties across the network and establishing a relationship between them that works with the detection model are crucial and difficult challenges. The decision-making process and the segregation process can be improved with the use of well chosen qualities.

Lack of a standardised dataset for evaluation purposes; currently, there is no data out there that can adequately mimic the conditions found in MANETs. Making a better dataset for testing IDS on MANETs is, thus, a difficult undertaking.

When it comes to application-level actions, a skilled hacker will always look for ways to make his or her assault look innocuous and evade detection by intrusion detection systems (IDSs). As a result, IDS audit data should place greater emphasis on application layer activities than on the lower layers because attacks tend to target the former.

The environment is always changing, making it difficult for intrusion detection methods [16,17] to keep up. As a result, the intrusion detection process's capacity to adjust to a constantly shifting context is a crucial characteristic. The malicious and harmless actions of users, systems, and networks are always evolving

Find the invaders' point of origin (9) Even if intruders are discovered, the majority of the proposed solutions [11,12,15] are unable to pinpoint where the intrusions originated. As a result, detection techniques need to be able to handle a broader variety of security assaults at a similar cost and pinpoint the origin of attacks.

Theoretically, a more secure and dependable system can be created by combining different detection systems into a hybrid approach. While hybrid systems theoretically have the potential to outperform more traditional approaches, additional computing complexity means this isn't necessarily the case in practise. When looking for malicious activity, various detection technologies use various methods of monitoring and analysing system and/or network traffic. Some of the proposed detection strategies combine IDS's foundational capabilities with data privacy and authentication at the network node level, using preventative measures like cryptography and authentication. Researchers face a difficult trade-off when attempting to simultaneously build IDS that use prevention-based strategies to guarantee data security without compromising IDS capabilities. Instead of using two distinct security models, it would be preferable if these systems operated as a hybrid.

Scalability: In environments with many mobile nodes, the detection accuracy can suffer from some recommended techniques. MANET's key features are their portability and scalability. As a result, MANET IDS should be scalable to accommodate vast number of nodes, the dynamic nature of the networks, and to generate little communication and computation overhead.

Inter-layer IDS: While most of the proposed work addresses specific types of attacks (such as wormhole, black hole, rushing, and spoofing assaults), it fails to account for the full range of attacks that can occur at the application, transport, network, and data-link layers . However, most security assaults against the various layers of a communication protocol stack can be detected by using a cross-layer intrusion detection system. So, a potential topic of study is the implementation of a cross-layer mechanism capable of detecting attacks at lower layers.

IDS synchronisation . IDSs built on stand-alone architectures can be easily compromised by adversarial behaviour such as a Byzantine attack. When a malicious node is detected, these safeguards often initiate a local response system and punish it without alerting the rest of the network. Attacks such as "man in the middle" and "blackmail" can compromise IDSs based on distributed and cooperative design. To identify coordinated attacks on the network, it is necessary for the detection activities of separate IDSs to be properly synchronised with one another. So, it's a tough challenge for academics to figure out how to coordinate the detection operations of separate IDSs to spot coordinated attacks while keeping the communication load to a minimal.

For example, the genetic algorithms, hazard theory, artificial neural networks, and cutting-edge subjects in evolutionary computation are all examples of heuristic-based approaches to intrusion detection. Gaining a deeper knowledge of immunology allows for more precise data while developing new AIS models. Methods of detection based on heuristics are becoming increasingly useful in complicated systems. Therefore, the creation of IDSs inspired by cutting-edge findings in immunology and improved biological understanding could be a promising area of study.

In reaction to an intrusion, the local detection system reports an anomaly with low confidence due to the scarcity of relevant local data. Therefore, to attain high detection accuracy, global integrations of many local detection systems are required. A number of pieces of supporting evidence from local detection agents or from internationally collaborating detection agents are used to establish the alert's confidence level. As a result, it is recommended to implement a differentiated intrusion response mechanism that responds differently depending on the certainty of alerts, it's important to remember that the standard trade-offs between system security, performance, complexity, and so on, still apply.

VI. Conclusion

Network assaults are undeniably a major concern in the IT industry and question its rapid expansion and the widespread support it enjoys from the general population and official institutions. We aimed to provide a comprehensive picture of intrusion detection system (IDS) and attack in this research. We gain a more refined understanding of the issue, which aids in our search for workable solutions to IDS issues. There are attacks that can be employed against a network IDS because of these fundamental flaws. These attacks include insertion attacks, evasion attacks, and sophisticated assaults, all of which can trick the IDS into inaccurately reconstructing information from network packets. The development of IDS classifications has many benefits, one of which is the increased possibility of researchers working together to identify and address other gaps in the IDS area. In order to keep up with the ever-evolving nature of threats, it is essential that these categorizations be regularly revised and augmented.

References

[1] 1,L. Hung-Jen and C.-h. R. Lin, “Intrusion detection system a comprehensive review,” Journal of network and applications, vol. 36, no. 1, pp. 16–24, 2013.

[2] P. Fournier-Viger, J. C.-W. Lin, R. U. Kiran, Y. S. Koh, and R. Thomas, “A survey of sequential pattern mining,” Data Science and Pattern Recognition, vol. 1, no. 1, pp. 54–77, 2017.

[3] A. Smola and S. V. N. Vishwanathan, Introduction to Machine Learning, Cambridge University Press, 2008, ISBN-10:0521825830.

[4] D. Tirtharaj, “A study on intrusion detection using neural networks trained with evolutionary algorithms,” Soft Computing, vol. 21, pp. 2687–2700, 2017.

[5] Y. Haipeng and W. Qiyi, “An intrusion detection framework based on hybrid multi-level data mining,” International Journal of Parallel Programming, vol. 47, pp. 740–758, 2017.

[6] M. Suad and M. Fadl, “Intrusion detection model using machine learning algorithm on Big Data environment,” Journal of big data, vol. 5, pp. 1–12, 2018.

[7] S. Ijaz, F. A. Hashmi, S. Asghar, and M. Alam, “Vector based genetic algorithm to optimize predictive analysis in network security,” Applied intelligence, vol. 48, no. 5, pp. 1086–1096, 2018.

[8] A. Mohammad and A. Nauman, “A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks,” Neural Computing & Applications, vol. 29, pp. 991–1004, 2018.

[9] V. Sivakumar and S. Rajalakshmi, "Optimal and novel hybrid feature selection framework for effective data classification," in Advances in Systems, Control and Automation, pp. 499–514, Springer, Singapore, 2018.
[10] K. Neeraj and K. Upendra, "Knowledge computational intelligence in network intrusion detection systems," in Knowledge Computing and Its Applications, pp. 161–176, Springer, Singapore,2018.
[11] C. Unal, "A new hybrid approach for intrusion detection using machine learning methods," Applied Intelligence, vol. 49,pp. 2735–2761, 2019.
[12] S. Akash and S. Khushboo, "Hybrid technique based on DBSCAN for selection of improved features for intrusion detection system," in Emerging Trends in Expert Applications and Security, pp. 365–377, Springer, Singapore, 2019.
[13] K. Rajesh and R. Manimegalai, "An effective intrusion detection system using flawless feature selection, outlier detection and classification," in Progress in Advanced Computing and Intelligent Engineering, pp. 203–213, Springer, Singapore,2019.
[14] P. Kar, S. Banerjee, K. C. Mondal, G. Mahapatra, and S. Chattopadhyay, "A hybrid intrusion detection system for hierarchical filtration of anomalies," in Information and Communication Technology for Intelligent Systems, vol. 106, pp. 417–426, Springer, Singapore, 2019.
[15] S. Mishra, C. Mahanty, S. Dash, and B. K. Mishra, "Implementation of BFS-NB hybrid model in intrusion detection system, recent developments in machine learning and data analytics," in Recent Developments in Machine Learning and Data Analytics, vol. 740, pp. 167–175, Springer, Singapore, 2019.
[16] V. Dutta, M. Choras, R. Kozik, and M. Pawlicki, "Hybrid model for improving the classification effectiveness on network intrusion detection system," in Conference on Complex, Intelligent, and Software Intensive, Cham, 2020.
[17] M. Latah and L. Toker, "An efficient flow-based multi-level hybrid intrusion detection system for software-defined networks,"CCF Transactions on Networking, vol. 3, pp. 26–271, 2020.
[18] I. Sumaiya Thaseen, J. Saira Banu, K. Lavanya, M. Rukunuddin Ghalib, and K. Abhishek, "An integrated intrusion detection system using correlation-based attribute selection and artificial neural network," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 2, article e4014, 2021.
[19] M. Safaldin, M. Qtair, and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 2, pp. 1559–1576,2021.
[20] G. Vallathan, A. John, and C. Thirumalai, "Suspicious activity detection using deep learning in secure assisted living IoT environments," The Journal of Supercomputing, vol. 77, pp. 3242–3260, 2021.
[21] Hackerpocalypse-cybercrime report, In Cybersecurity Ventures, 2016.
[22] A. AlEroud, G. Karabatis, P. Sharma, and P. He, "Context and semantics for detection of cyber attacks," International Journal of Information and Computer Security, vol. 6, no. 1, pp. 63–92, 2014.
[23] A. AlEroud and G. Karabatis, "Toward zero-day attack identification using linear data transformation techniques," in IEEE 7th international conference on software security and reliability, pp. 159–168, Washington, D.C., 2013.
[24] S. Axelsson, "Intrusion detection systems: a survey and taxonomy," 2000.
[25] R. M. Snort, "Lightweight intrusion detection for networks," in Proceedings of thirteenth USENIX conference on system administration, (LISA '99), pp. 229–238, Seattle, Washington, USA, 1999.