Phoenix: International Multidisciplinary Research Journal
Vol 3, No. 4, Oct-Dec, 2025
ISSN:2583-6897

TRANSFORMER BASED NETWORK INTRUSION DETECTION SYSTEM: A REVIEW

Dr Syed Umar
Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad, syedumar@mrec.ac.in
Goli Madhuri
Assistant Professor, Department of computer science and engineering, Malla Reddy (MR) Deemed to be University, Hyderabad, golimadhurireddy120@gmail.com
Dikshendra Daulat Sarpate
Professor, Department of Artificial Intelligence & Data Science, ZEAL College of Engineering & Research, Pune, Email id -dikshendra@gmail.com
Gopala Soujanya
Assistant Professor, Department of computer science and engineering, Malla Reddy (MR) Deemed to be University, Hyderabad, Soujanyachiluka52@gmail.com
B.Rani
Assistant Professor, Department of computer science and engineering, Malla Reddy (MR) Deemed to be University, Hyderabad, rani@mrec.ac.in

Abstract—**The paper's main aim, which is to observethe foundations of intrusion detection systems and their contributions to network security, will be made crystal obvious in the introduction. It will outline the precise facets of IDS—such as classifications, detection strategies, and best practices—that the paper will discuss. It will draw attention to the main points that will be explored and the paper's logical progression. The importance of researching intrusion detection systems will be emphasised in the introduction, particularly considering the always changing cyberthreats. It will highlight the possible effects on organisational resilience and data security of using efficient IDS systems. The introduction will provide the groundwork for a thorough examination of intrusion detection systems while highlighting their significance in the state of cybersecurity today. This article intends to provide readers with essential information to improve their network security policies and defend against the persistent and ever-evolving cyber threats by providing insights into the intricacies of IDS and their capabilities.**

Index Terms—Wireless Sensor Network, Intrusion Detection System, Energy Efficiency.

I. INTRODUCTION

The security of computer networks has emerged as a critical issue in the current digital era, as information is readily shared, and connection is pervasive. Organisations, governments, and people are all at danger from the enhancing frequency as well as complexity of cyber assaults. The need for reliable cybersecurity solutions has never been more pressing as criminal actors attempt to infiltrate sensitive data and exploit vulnerabilities on a constant basis. Network security leaders and a key line of defence against cyberattacks are intrusion detection systems (IDS). These advanced tools are designed to continuously scan for any indications of suspect or unauthorised behaviour while keeping a close eye on system operations and network traffic in real time. IDS are important for stopping unauthorized access attempts, service outages, and data breaches by quickly identifying and reacting to possible threats. The field of intrusion detection systems is observed in this study along with its underlying theories, methodology, and real-world uses. We'll examine how IDS may assistorganizations in safeguarding their digital assets and maintaining network integrity by promptly detecting and addressing various cyberattacks. The introduction will provide a general overview of the growing cybersecurity problems that organisations and people throughout the globe are facing [1]. It will draw attention to the rising number of cyberattacks, the financial and reputational costs associated with data breaches, and the developing strategies used by bad actors. The crucial part that IDS plays in enhancing network security will be described in this section. IDS provide organisations a proactive defence mechanism to combat potential threats before they develop into significant security events by offering real-time threat detection and timely alarms.

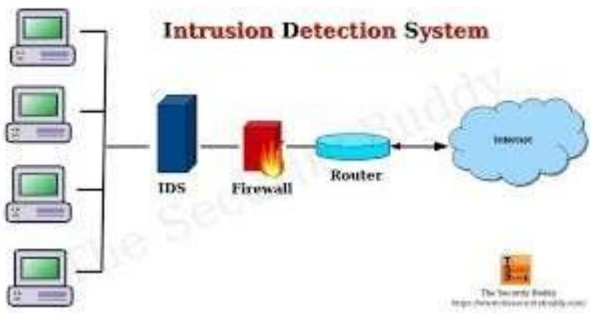

Figure 1: Intrusion Detection System's [2]

II. RELATED WORK

The literature study for an intrusion detection system, will concentrate on scholarly works, articles, and important research studies that examine several elements of IDS, such as its guiding principles, methodologies, effectiveness, problems, and developments. These topics will be covered in the review. These studies will be the primary area of concentration moving forward. The following is a condensed summary of the most pertinent topics that might possibly be included in the literature review of a research paper on IDS.

The first few lines of the literature review need to be dedicated to tracing the historical past of IDS, starting with its founding concepts and going all the way up to most the state of the art at the moment in the field. This should be done in chronological order, beginning with its founding conceptions and ending with the most recent state of art in field. During the review, this task should be completed as quickly as feasible. This need to be done in the order that historical events occurred, beginning with the earliest conceptions and ending using the most latest technological advancements. The order need to proceed from the most recent to the oldest. It's probable that this section may look at some of the important publications that were crucial in the development of IDS and how it's used now. In addition to this, it may place a focus on major events and circumstances that constituted a turning point. A part of the study that is carried out on earlier written work should unquestionably be included into the process of classifying and analysing the several varieties of IDS that are now in use. It is required that this specific piece be finished [3,4]. This encompasses, in its own right, intrusion detection systems that are network-based as well as host-based. Each of these categories is important in their own right. In the scope of this category, hybrid tactics are also considered to be valid options. During the course of the investigation, we are needed to take into account not only the positives and negatives associated with each category but also the particular uses to which each one is best suited. It is vital to explore the different IDS detection methodologies over the course of the literature review.

These techniques may include signaturebased, anomalybased, and behavior-based approaches. Not only is it necessary to share any comparison studies that have been carried out, but it is also vital to emphasise how successful each method is in detecting known and hidden dangers. Not only is it vital to expose any comparison studies that have been carried out, but it is also vital to highlight how effective each strategy is. In addition to this, it is essential to specify whether comparative study has been carried out. It is quite probable that a significant portion of the overall amount of time spent on the literature review will be taken up by the study of studies that evaluate the effectiveness of IDS. This article provides an overview of studies that explore the influence that intrusion detection systems, which are more often referred to as IDS, have on the overall performance of networks, as well as detection rates, false positives, and false negatives. Additionally, detection rates are discussed in this article. When confronted with a situation like this one, it may be good to do research that compares the various IDS systems that are presently available on the market. The literature study needs to explore studies within the application of artificial intelligence and machine learningfor intrusion detection systems (also known as IDS). This is necessary since the use of these two types of technology in the area of cybersecurity is becoming increasingly prevalent. This subject of research absolutely has to include studies into the utilize of machine learning techniques for greater threat detection and mitigation, and these kinds of inquiries need to be brought into the field as a whole as well. It is vital, in order for the literature review to be exhaustive, to examine both the challenges that are generated by IDS as well as its constraints. This is because IDS can only be employed in certain situations.[5-8]

This tackles topics such as the evasion techniques that attackers use to get through IDS, as well as possible problems relating to privacy and resource limits. Additionally, this discusses a number of other potential concerns. The literature study requires to look at research that analyses the integration of IDS and IPS, which are abbreviated as IDS and IPS respectively. This is due to the fact that it is quite important to be able to react swiftly to attacks. In this regard, a particular emphasis must to be placed on studies that illustrate how the implementation of a number of different safeguards may, together, make the network a more secure site from which to carry out activities. Ourshould be able to locate studies on the most effective techniques to develop and put into operation IDS if our look it up in the review that was just recently done. As a part of this task, our will be needed to give suggestions for system's fine-tuning, improve the effectiveness of rule sets, and make sure that the system interacts seamlessly with the current security architecture. There is a possibility that the case studies from the actual world will be incorporated alongside stories of successful IDS installations in a number of different sectors in the research paper that is being done on the actual world's literature. These case studies may provide important information on the use of IDS in the real world as well as the difficulties that are encountered in a range of scenarios. After determining whether or not there are any holes in the existing body of knowledge, the next step of the review should be to identify possible new paths that IDS may go in the future. This may include individual pieces of forward-thinking technology, fields of research that need more exploration, and prospective remedies to problems created by the status quo. In general, it is anticipated that the section of the report that analyses the literature review would include a complete analysis of the body of information that is presently available on IDS. This will not only serve as evidence of an in-depth knowledge of the subject matter, but it will also provide the framework for an innovative contribution that the research will make to the industry as a whole.

III. IDS Components

We will investigate the primary elements that constitute an IntrusionDetection System (also known as IDS). An IntrusionDetection System (IDS) is a sophisticated security instrument that, to work properly, needs a variety of interrelated components. Typically, the following components are included:

Sensors: Sensors are the components of a monitoring system that oversee gathering and collecting data from the host or network that is being monitored. In network-based IntrusionDetection Systems, also known as NIDS, sensors are strategically positioned inside the network at important locations to monitor traffic. The Host-based Intrusion DetectionSystem, often termed as HIDS, employs sensors that are put on individual hosts to monitor system behaviours and events [9].

Data Storage: To store the data that has been gathered for analysis, IDS needs some kind of data storage method. This may require the use of databases or other repositories that store network traffic logs, system logs, and any other pertinent data.

Analysis Engine: The IntrusionDetection System's (IDS) essential component is the analysis engine. It is responsible for processing, analysing, and comparing data to known attack patterns (signatures) or baseline behaviour (anomalies). This component identifies possible threats by using various detection approaches, such as techniques focused on signatures, techniques based on anomalies, and strategies based on behaviours [10].

Rule Sets are collections of established rules and signatures that each describe a pattern of a known attack or suspicious activity. Rule sets are sometimes referred to as "rules." These rules provide the foundation for making comparisons against incoming data to spot any possible security breaches.

Alerting Mechanism: When the analysis engine determines that there has been either a possible incursion or suspicious behaviour based on the rule sets, it will immediately generate an alarm. An indication that there may have been a breach of security is sent to administrators or security workers via the alerting system.

A. *Sensor Placement and Data Collection*

In this part, we will discuss the method of data gathering in an IDS as well as the placement of sensors in an IDS strategically.

Positioning of Sensors in the NIDS: Typically, network-based intrusion detection system sensors are installed at strategic spots across the network, like at the network perimises, in the demilitarized zone (DMZ), or inside vital network segments. Because it is located in this position, the NIDS is able to properly monitor both incoming and departing traffic.

Positioning of Sensors in the HIDS: Individual hosts/endpoints are where host-based intrusion detection system sensors are deployed. They provide in-depth insights into the host's security by monitoring system-level actions such as file modifications, process execution, and login attempts by monitoring these activities [11].

Data Collection: Sensors are responsible for the continual collection of data from the monitored host or network. The data that is gathered in NIDS comprises network packets, which are then subjected to analysis in order to recognise harmful patterns or signatures. The data that is gathered by HIDS consists of system logs and audit trails, which together provide insight into host-level actions.

B. *Preprocessing and Data Normalization*

Preprocessing and data normalisation are two steps that are required to make the data that was acquired suitable for analysis. Both processes are very important [12,13].

Filtration and Cleaning of Data: One of the procedures in preprocessing is filtering and cleaning the received data to get rid of noise and information that isn't necessary. This is done to make the data more understandable [6]. Because of this phase, the analysis engine will only obtain data that is relevant to the inquiry, which will result in a greater degree of accuracy in the detections as well as fewer false positives.

The Process of Normalising Data: The process of normalising data entails standardising the format and size of the data to make it easier to compare and analyse the data in more efficientway. Normalisation is highly important when dealing with data that arrived from a range of sources or sensors because it assures that the results will be trustworthy and consistent. Normalisation is very important when working with data derived from multiple sources or sensors.

C. *Detection Engines and Rule Sets*

In this part of the article, we will investigate the detection engines and rule sets that make it possible for IDS to recognise possible dangers.

Signature-based Detection: This kind of detection is focused on a database of recognized attack patterns, which are sometimes referred to as signatures. Incoming data are compared to these signatures by the detection engine, which then identifies known hazards and generates an alert for those risks. Anomaly-based Detection: The baseline of typical activity for the network or host is established via anomaly-based detection. Any deviations from this baseline are logged as potential anomalies, which may indicate an attempt at unauthorised access or other peculiar goings-on [14].

Behaviour-based Detection: Behavior-based detection based on finding patterns of behaviour that might suggest malicious intent, even if attack signatures are not known. This is possible because behaviour-based detection does not rely on identifying specific attack signatures. In behaviour-based detection, It is standard procedure to utilize of machine learning algorithms to identify new or zero-day threats [15].

D. *Alerting and Response Mechanisms*

This section will discuss how intrusion detection system (IDS) alerts are created as well as the reaction mechanisms that are put into place after the discovery of possible intrusions.

Alert Generation: The intrusion detection system (IDS) will produce alerts if it identifies actions that are harmful or suspicious. The level of an alert may vary, and it will offer information about the discovered danger, the host or network segment that was impacted, and the kind of behaviour that was taking place [16]. Notifications of Alerts In most cases, intrusion detection system alerts are emailed, texted, or integrated with a Security Information and EventManagement (SIEM) system to be sent to security employees or administrators who have been specifically assigned to receive them.

Mechanisms for Responding: After receiving the warning, security analysts or administrators are tasked with analysing the issue and determining the most effective course of action. This reaction might entail blocking the IP address of the attacker, isolating a server that has been compromised, or initiating a more in-depth inquiry into the event.

Organisations can efficiently adopt intrusion detection systems to increase network security and defend themselves from possible cyber threats if they have a basic grasp of the components, data collecting, detection engines, and reaction mechanisms of IDS.

IV. Network-Based Intrusion Detection System (NIDS)

Architecture and Deployment Considerations

This section presents an comprehensive summary of the architecture of Network-based IntrusionDetection Systems (NIDS) as well as implementation concerns. It investigates the many components, such as sensors, analysis engines, and alerting systems, that are a part of the NIDS architecture [17]. In addition to this, it looks into the considerations that companies need to make before using NIDS, such as the location of sensors, the architecture of the network, and scalability.

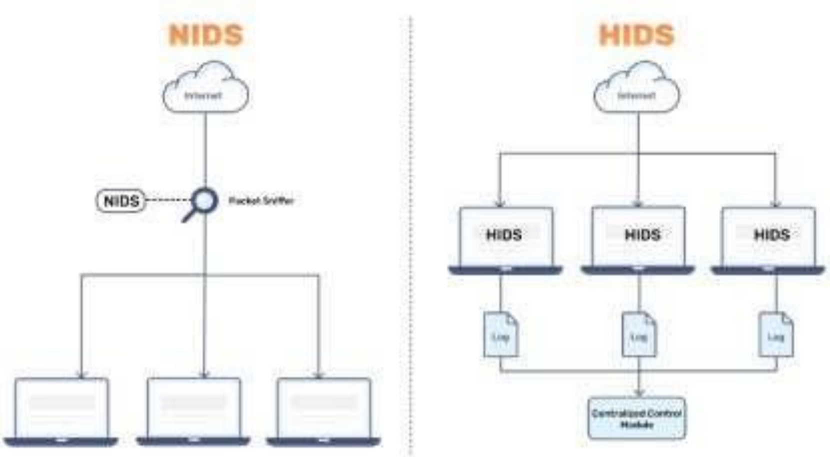

Figure 2: Architecture of network

Signature-based Detection in NIDS

In NIDS, among the most popular techniques for recognising known attack patterns or signatures is referred to as "signature-based detection." In this part, the mechanics of signature-based detection in NIDS, including the development and administration of signature databases, are dissected and analysed. In addition to this, it addresses the benefits and drawbacks of using this method, touching on topics such as false positives, signature changes, and evasion tactics that are used by malicious actors.

Anomaly-based Detection in NIDS

RegardingNetwork IntrusionDetection Systems (NIDS), anomaly-based detection focuses on finding anomalies in typical network behaviour. In this part, the approaches that are used to determine baseline behaviour, such as statistical methodologies and machine learning algorithms, are discussed. This article takes a look at how NIDS analyses network traffic for strange patterns and discusses the issues involved with selecting proper limits for anomaly detection.

Behavior-based Detection in NIDS

The machine learning and sophisticated approachesused in behaviour-based detection in NIDS go beyond known signatures and anomalies to discover suspicious behaviours suggestive of new or zero-day threats. This kind of detection goes beyond known signatures and abnormalities. This part digs further into the intricacies of behaviour-based detection, including topics such as the significance of training the data, the precision of models, and the flexibility of system to constantly changing threats.

Case Studies of NIDS Implementations

Real-world case studies of NIDS implementations in a number of organisations and areas are offered here for consideration. These case studies can be found in Part 3 of this article. Each case study provides useful insights into the challenges that were faced, the strategies that were employed for sensor positioning and rule building, and the entire performance of the NIDS in terms of recognising and mitigating risks. These insights may be used to improve the effectiveness of the NIDS. These case studies highlight how NIDS may be tailored to fit the one-of-a-kind needs of specific organisations, as well as the useful lessons that can be taken away from successful deployments of the system [18].

This section will deliver readers a in-depth overview of the capabilities and issues connected with Network-based IntrusionDetection Systems (NIDS) by delving into the architecture, detection methodologies, and real-world implementations of NIDS. This will allow readers to fully appreciate the capabilities and issues involved with NIDS. It is my hope that by the time our have finished reading this part, our will have an in-depth comprehension of NIDS. It provides important information that can be used to enhance network security and give protection against prospective intrusions and cyber threats, and it delivers this to businesses who are interested in including NIDS as a component of their cybersecurity strategy.

V. Host-Based Intrusion Detection System (HIDS)

Architecture and Deployment Considerations

This section examines the architecture of Host-based IntrusionDetection Systems (HIDS) as well as the factors that go into its adoption. It provides an overview of the essential elements that make up a HIDS, such as sensors, agents, and analysis engines, all of which are designed to be deployed on separate hosts in order to monitor and analyse actions at the system level. This section also highlights the considerations that organisations should take into consideration while installing HIDS. These variables include agent placement, resource utilisation, and interaction with preexisting host security systems.

Signature-based Detection in NIDS

Identifying known patterns or signatures of harmful actions on a host is the primary purpose of the signature-based detection technique, which is a core component of HIDS. In this part, the mechanics of signature-based detection in HIDS, including the generation and administration of signature databases, are dissected in depth. In addition to this, it covers the difficulties that are related with false positives, signature changes, and the need for rapid threat information to enhance the efficacy of HIDS [19].

Anomaly-based Detection in HIDS

Detecting anomalies in a host's normally functioning system is the primary emphasis of the anomaly-based detection method used by HIDS. This section examines how HIDS determines a baseline of normal activity and uses statistical analysis or machine learning approaches to determine whether or not certain behaviours are out of the ordinary. It covers the significance of dynamic baselines and the trade-offs that must be made in anomaly-based HIDS between the detection precision and the false alarms.

Behavior-based Detection in HIDS

Beyond known signatures and anomalies, behavior-based detection in HIDS focuses on finding abnormal behaviours that may suggest new or zero-day threats. This kind of detection extends beyond known signatures and anomalies. This part of the article digs further into the complexity of behavior-based detection, including the utilization of machine learning approachesand sophisticated heuristics to model typical host behaviour and identify deviations from the norm. Additionally, it tackles the issues of striking a balance between the host's resource overhead and the precision of the detection [20].

Case Studies of HIDS Implementations

This section offers real-world case studies of implementations of Host-based Intrusion Detection Systems (HIDS) across a variety of hosts in a variety of contexts. Each case study offers valuable insights into the problems that were encountered, the selection of detection techniques, the influence on host performance, as well as the efficacy of the HIDS in detecting and mitigating intrusions. These case studies illustrate how HIDS may be modified to accommodate particular host setups and security needs, while also providing useful insights gleaned from successful installations and serving as a repository of useful information [21].

This part intends to give readers with a complete knowledge of the advantages and problems associated with Host-based IntrusionDetection Systems (HIDS) by analysing the architecture, detection techniques, and real-world implementations of HIDS. In doing so, this part will explain the Host-based IntrusionDetection Systems (HIDS). It offers organisations that are interested in using HIDS helpful information that may improve their host security posture, detect prospective breaches, and effectively react to security events on specific hosts.

VI. Conclusion

Intrusion Detection Systems, often termed as IDS, are very important to maintaining the safety of computer networks since they provide real-time threat detection as well as proactive defence methods. Throughout the whole of this research study, we have investigated the basic concepts, methodology, problems, and future directions of IDS, illuminating the intricate terrain of cybersecurity in the process. The literature study based on development of IntrusionDetection Systems (IDS), from its earliest conceptions to its most recent breakthroughs, and it analysed the efficiency of various detection approaches. We studied the components, sensor location, and data collecting of both Network-based Intrusion DetectionSystems (NIDS) and Host-based IntrusionDetection Systems (HIDS). NIDS stands for Network-based IntrusionDetection System. HIDS is for Host-based Intrusion Detection System.

Reference

[1] D. M. Abdulqader, A. M. Abdulazeez and D. Q. Zeebaree, "Machine Learning Supervised Algorithms of Gene Selection: A Review, vol. 62, no. 03. pp. 13. 2020.

[2] Falcini GLami & Costanza, AM 2017, ‘Deep learning in automotive software’, IEEE Softw, vol. 34, no. 3, pp. 56–63. [Online]. Available: http://ieeexplore. ieee. org/document/7927925/

[3] Luckow M Cook, Ashcraft, N, Weill, E, Djerekarov, E & Vorster, B 2016, ‘Deep learning in the automotive industry: Applications andtools’, in Proc. IEEE Int. Conf. Big Data, pp. 3759–3768.

[4] Umar, Syed, Bommina Naveen Sai, Nagineni Sai Lasya,Doppalapudi Asutosh, and LohithaRani. "Machine Learning based Sentiment Analysis of Product Reviews Using DeepEmbedding." Journal of Optoelectronics Laser 41, no. 6(2022): 108-113.

[5] Polishetty M Roopaei & Rad, P 2016, ‘A next-generation secure cloud based deep learning license plate recognition for smart cities’, in Proc. 15th IEEE Int. Conf. Mach. Learn. Appl, Anaheim, CA, USA, pp. 286–293.

[6] Fausto, A., Gaggero, G., Patrone, F., & Marchese, M. (2022). Reduction of the Delays Within an Intrusion Detection System (IDS) Based on Software Defined Networking (SDN). IEEE Access, 10, 109850-109862.

[7] Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2023). Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. Procedia Computer Science, 217, 1406-1415.

[8] Naveen Sai Bommina, Uppu Lokesh, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Optimized AI Models for Real-Time Cyberattack Detection in Smart Homes and Cities", International Journal of Applied Engineering & Technology, Vol. 4 No.1, June, 2022.

[9] Ullah, M. U., Hassan, A., Asif, M., Farooq, M. S., & Saleem, M. (2022). Intelligent Intrusion Detection System for Apache Web Server Empowered with Machine Learning Approaches. International Journal of Computational and Innovative Sciences, 1(1), 21-27.

[10] Adnan, A, Muhammed, A, Abd Ghani, AAA, Abdullah, A & Hakim, F2021, ‘An intrusion detection system for the internet of things based on machine learning: review and challenges. Symmetry’, vol. 13, no. 6, pp. 1-13.

[11] Kasongo, SM & Sun, Y 2021, ‘A Deep Gated Recurrent Unit based model for wireless intrusion detection system. ICT Express, vol. 7, no. 1, pp. 81-87.

[12] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Privacy-Preserving Federated Learning for IoT Devices with Secure Model Optimization", International Journal of Communication Networks and Information Security (IJCNIS), (2021), 13(2), 396–405.

[13] K Sankar, Divya Rohatgi, S Balakrishna Reddy, "COX Regressive Winsorized Correlated Convolutional Deep Belief Boltzmann Network for Covid-19 Prediction with Big Data", Grenze International Journal of Engineering & Technology (GIJET), Grenze ID: 01.GIJET.9.1.547, © Grenze Scientific Society, 2023.

[14] Usman, M., Zubair, M., Hussein, H. S., Wajid, M., Farrag, M., Ali, S. J., ... & Habeeb, M. S. (2021). Empirical mode decomposition for analysis and filtering of speech signals. IEEE Canadian Journal of Electrical and Computer Engineering, 44(3), 343-349.

[15] D Veerendra, BN Umesh, A Khandare, D Rohatgi, K Tiwari, S Datta, "ECA-MURE algorithm and CRB analysis for high-precision DOA estimation in coprime sensor arrays", IEEE Sensors Letters 7 (12), 1-4.

[16] HABEEB, M. S., & BABU, T. R. (2024). WOA-SA: OPTIMIZING NIDS WITH ENHANCED DEEP LEARNING FOR ZERO-DAY ATTACK DETECTION. Journal of Jilin University (Engineering and Technology Edition).

[17] RS Supriya Khaitan, Divya Rohatgi, Sana Nalband, Tejali Mhatre, Shweta Patil, "Enhancing Essay Grading Efficiency and Consistency through Two-Layer LSTM Models and Attention Mechanisms", Journal of Information Systems Engineering and Management 10 (2), 191-202.

[18] Uppu Lokesh, Naveen Sai Bommina, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Designing Energy-Efficient and Secure IoT Architectures Using Evolutionary Optimization Algorithms", International Journal of Applied Engineering & Technology, Vol. 4 No.2, September, 2022.

[19] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Multi-Objective Genetic Algorithms for Secure Routing and Data Privacy in IoT Networks", International Journal of Communication Networks and Information Security (IJCNIS), (2020), 12(3), 632–643.

[20] Nandipati Sai Akash, Naveen Sai Bommina, Uppu Lokesh, Hussain Syed, Syed Umar, "Optimized Block Chain-Enabled Security Mechanism for IoT Using Ant Colony Optimization", International Journal on Recent and Innovation Trends in Computing and Communication, (2023), 11(10), 1226–1233.

[21] Singh, A., Gupta, M., Raj, A., Gupta, S. K., & Habeeb, M. S. (2020, December). TWDM-PON: The Enhanced PON for Triple Play Services. In 2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE) (pp. 1-5). IEEE.