WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

IOT WSNIDS SELECTION ON THE BASIS OF LOGISTIC METRICS USER REQUIREMENTS WEIGHT APPROACH

Dr. Rupinder Singh[1], Dr. Rachhpal Singh[2], and Prabhjot Kaur[3]

[123]Khalsa College, Amritsar, Punjab. E-mail: singhrupi76@gmail.com

ABSTRACT –

The Internet of Things (IoT) Wireless Sensor Network Intrusion Detection System (IOT WSNIDS) is a network security software designed to identify vulnerabilities and prevent attacks. The selection of IOT WSNIDS depends on the architecture and application of the IoT. It falls upon the administrator to decide which IOT WSNIDS is the most suitable solution for the sensor network. There isn't a one-size-fits-all solution; thus, administrators must evaluate the capabilities of different IOT WSNIDS along with costs, information, and specific needs to identify the one that best meets their requirements. This research proposes a user requirement weight-based approach for selecting IOT WSNIDS in IoT. We primarily discuss the user's requirements for IOT WSNIDS and the related metrics, matching relevant metric(s) to each requirement. Users rank their IOT WSNIDS needs in a limited set from least to most important. These requirements are typically expressed in a positive context or adapted to a positive format. The first requirement (i.e., least important) receives the lowest weight (for example, one), while subsequent requirements are assigned increasing weights corresponding to their relative significance. After the needs are weighted, each IOT WSNIDS metric is given a weight equal to the total of the weights of the requirements it addresses. The metrics for IOT WSNIDS are organized in descending order, with the metric carrying the highest weight at the top. An appropriate IOT WSNIDS tool may be selected by aligning the weights of the metrics with the features of the IOT WSNIDS.

Keywords: Intrusion detection system; Internet of Things; metrics; Wireless sensor network; weight.

I. INTRODUCTION

Concerns related to safety are not solely practical; choices about user requirements are influenced by organizational policies. The organization's safety policies establish the goals, suitable applications, and constraints of the system. It is the consensus within the organization that will determine what to monitor, when to be cautious, whom to inform, and how severe a threat a possible intrusion may be. The expansion of networking has underscored the significance of network security. Wireless Sensor Network Intrusion Detection Systems (IOT WSNIDS) have become an essential security measure. An IOT WSNIDS can be a software program or a device that monitors network and/or system activities for suspicious actions or violations of policy and sends reports to a central location within the organization.

Given that the Internet of Things (IoT) is an emerging technology, it is often deployed by linking multiple wireless sensor networks (WSN), while also presenting several vulnerabilities. Solutions like Wireless Sensor Network Intrusion Detection Systems (IOT WSNIDS) have been developed to tackle many of these issues. As various IOT WSNIDS options are suggested in the literature, choosing and implementing one can become challenging and requires significant time and effort. This challenge is amplified if the organization lacks a formal business security program. The decision regarding which IOT WSNIDS to select should not be made hastily, casually, or without a solid comprehension of the technology, the available options, or the potential consequences.

Logistics metrics scorecards serve as effective instruments for evaluating a company's performance in relation to industry standards, and they can assist in pinpointing areas where logistics operations, safety, and customer service can be enhanced. Logistics can be understood as the management of material flow within a company, transitioning from suppliers to customers, ensuring that the customer is served in a timely manner and at the lowest possible expense. As a result, logistics is tasked with the planning, execution, and oversight of the storage and movement of goods and services, as well as the associated information about their origin and destination, all tailored to meet customer requirements. In logistics, as with many other domains, it is crucial to assess our processes, as this is the only means to understand our current status and identify opportunities for improvement.

When considering that logistics follows the product or service throughout its journey, understanding how to measure it becomes a vital aspect. In fact, one of the biggest challenges for businesses is to establish metrics that facilitate an efficient and effective assessment: genuine, actionable data that can be easily understood. Only in this way can we make informed decisions that contribute to the on-going enhancement of the service we offer to our customers. Besides employing the data for comparisons, both internally and against competitors, it is also crucial for shaping organizational strategies. Additionally, emerging technologies are instrumental in measuring logistics performance. Due to these technologies, connections and communications with suppliers and customers have become tighter, processes are significantly more adaptable and responsive, the information is more current and precise, and most crucially – we substantially lessen the effort required to attain it. Undoubtedly, regarding logistics performance, the companies that

excel in performance measurement are those dedicated to innovation and equipped with the appropriate indicators aligned with their corporate strategies.

One of the most apparent advantages is that these measures enable us to visualize the condition of the supply chain, streamlining the time needed to assess its health. Additionally, it aids in making informed decisions that can lead to quicker improvements; it enhances service quality, positively influencing customer relationships; and it provides the involved departments with the necessary time to concentrate on decisions that have a broader impact and act accordingly. In these times of ongoing change and persistent crises, optimizing our resources and prioritizing what is essential for our customers and our business is more crucial than ever, where defining indicators, monitoring, and ongoing improvement are vital aspects to achieve this. Let's move forward!

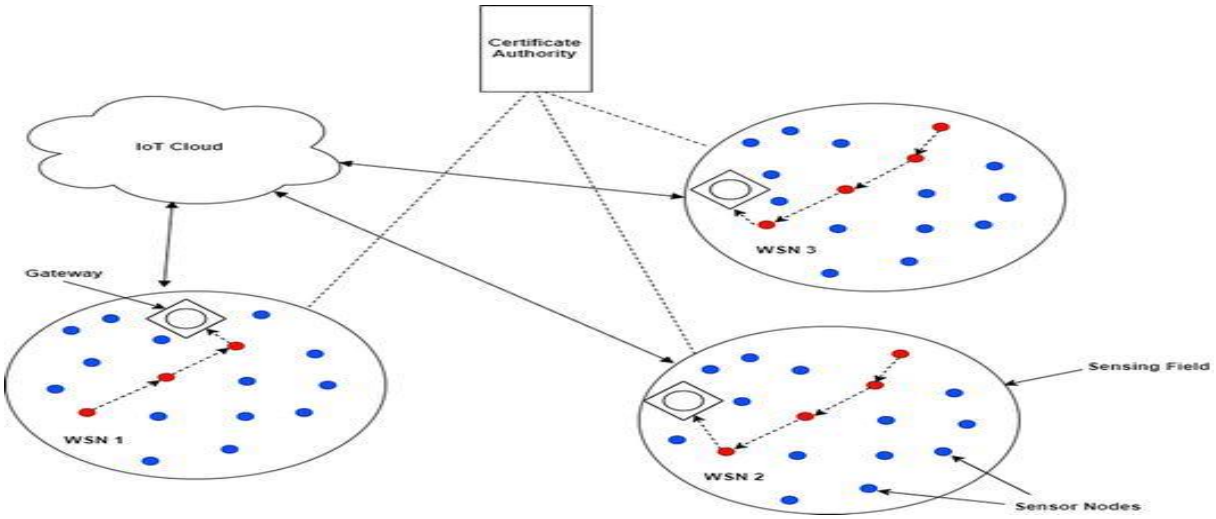
Metrics for logistic support performance are crucial for assessing and enhancing logistics processes. By utilizing these metrics, you can establish achievable objectives for minimizing costs, boosting quality, reducing time, and enhancing service. Moreover, they enable you to monitor and assess the progress and performance of your logistics operations, helping to pinpoint gaps, strengths, weaknesses, and potential opportunities. In addition, these metrics can be leveraged to implement corrective and preventive measures aimed at refining your logistics operations through adjustments in resources, processes, policies, and strategies. Lastly, you can utilize logistic support performance metrics to convey the outcomes and effects of your logistics operations to customers and stakeholders, illustrating value, efficiency, effectiveness, and competitiveness.

In this paper, we propose a method for selecting IoT WSNIDS based on user requirements and their respective weights. Initially, a comprehensive list of user IoT WSNIDS requirements and relevant metrics is created. Then, for each IoT WSNIDS requirement, we identify the corresponding metrics of concern. Users rank their requirements in a limited sequence from least important to most important. Requirements are typically expressed positively or rephrased to be in positive form. Subsequently, the first requirement (the least important) is assigned the lowest weight (for example, a weight of one). Other requirements are given increasing weights in percentage terms according to their relative significance. Once the requirements have been weighted, each IoT WSNIDS metric receives a weight that corresponds to the total of the weights of the requirements it supports. IoT WSNIDS metrics are then arranged in descending order, with the metric carrying the highest weight placed at the top. An appropriate IoT WSNIDS device or software can be selected after aligning the metrics' weights with the features of the IoT WSNIDS.

II. INTRUSION DETECTION SYSTEM AND WIRELESS SENSOR NETWORK

The Internet of Things (IoT) refers to a network of tangible items known as "things," typically equipped with sensors, software, and other technologies to facilitate data sharing and communication over the internet. These devices encompass a variety of items, including household appliances, industrial equipment, and any other compatible devices. IoT offers access to affordable, energy-efficient sensor technology, along with connectivity, cloud computing resources, artificial intelligence (AI) and machine learning. The functioning of IoT involves the real-time gathering and sharing of data. An IoT system incorporates smart devices, an IoT application, and a user-friendly graphical interface.

IoT incorporates Wireless Sensor Networks (WSNs), which are self-configuring and infrastructure-free wireless networks utilized for monitoring environmental conditions or devices. WSNs transmit the data they collect through the sensor network to a significant location known as the base station for further analysis. Various WSNs transfer the gathered information to a centralized server in the IoT cloud. WSNs face a significant number of restrictions that result in new challenges. The sensor nodes operate over an unreliable communication medium and have severe resource limitations, making it difficult to implement security measures. Figure 1 illustrates the framework of a typical IoT WSN. Most previous WSN protocols assumed that all nodes were trustworthy and cooperative. However, this is not the case for many current sensor network applications, and a range of attacks is possible in WSNs.



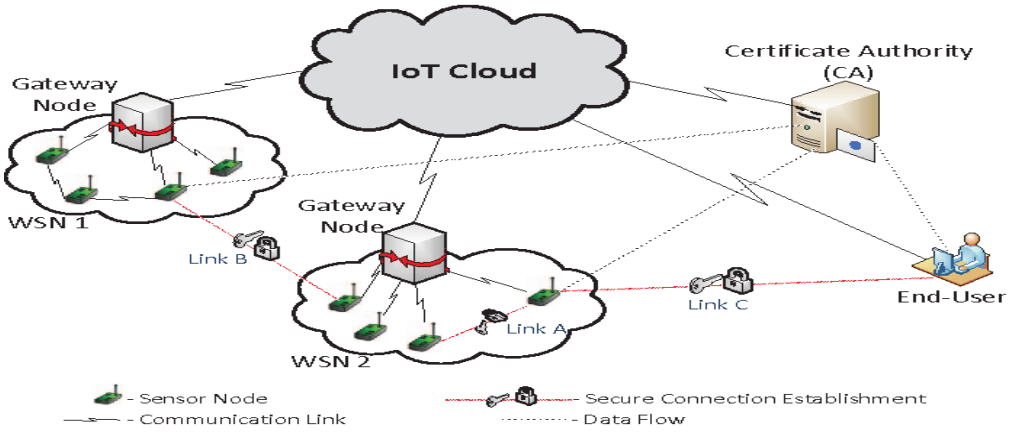


Figure 1: A classic IoT WSN

Intrusion detection involves identifying unauthorized traffic within a network or device. An IoT WSNIDS may consist of hardware or software that observes network traffic to identify unwanted activities. This type of IoT WSNIDS is designed to analyze specific traffic within a WSN and includes searching for external users attempting to connect to the network through AP (access points). IoT WSNIDS are essential for securing networks as they increasingly implement WSN technologies throughout various topology points. A practical approach for implementing an IoT WSNIDS is to position sensors at every location where a WAP is set up to ensure the detection of most attempted attacks. Identifying the position of an attack is a critical component of an IoT WSNIDS, particularly when attackers are near the WAP and physically situated within local areas. IoT WSNIDS can either be decentralized or centralized. In a centralized IoT WSNIDS, network sensors gather and transmit occurrence data to a chief management console, where the data is stored and processed to identify intrusions. Conversely, a decentralized IoT WSNIDS typically carries out functions performed by both the sensors and the console. The decentralized model is more suitable for smaller WSNs and offers greater cost-effectiveness. For larger WSNs, a centralized IoT WSNIDS is preferred for better management and more efficient data processing.

The elements of a Wireless Sensor Network (WSN), which plays a role in the Internet of Things (IoT), consist of sensors, servers, management logging databases, and user interfaces. WSN can operate in either a centralized or a distributed manner. In centralized architectures, data is aggregated in one location, enabling choices and activities to be made based on this collected information. In distributed architectures, decisions are made at the individual sensor node level. The IOT WSNIDS software can identify attacks occurring within the WSN's vicinity. It also offers tools for detecting sensor node misconfigurations and offers resources for server management. The IOT WSNIDS utilized in sensors may aid in enforcing security measures on the sensor nodes, like restricting access to certain WSN interfaces. Numerous components of the WSN are interconnected through a wired network. Communication between WSN components can occur over the organization’s typical networks or a separate management network. A management network or a conventional network can be employed for overseeing and governing the interface between the wired and non-wired wired networks.

IOT WSNIDS represents a novel technology, which brings with it several drawbacks that must be considered before implementing it in an existing sensor network. Being a recent development, it may contain bugs and vulnerabilities. The IOT WSNIDS technology could potentially undermine the safety of the sensor network or, in the worst-case scenario, increase its exposure. Another disadvantage of IOT WSNIDS is that the cost can be prohibitively high, especially when managing a large number of sensor networks that may require additional sensors for comprehensive management. The effectiveness of IOT WSNIDS is largely influenced by how the network administrator configures it. If properly set up or pre-configured to identify relevant elements within the sensor network, they can operate at optimal efficiency. Conversely, if not configured well, an IOT WSNIDS can be somewhat ineffective.

The generation of multiple false positives or negatives can create further mix-up for the administrator. In general, IoT Wireless Sensor Network Intrusion Detection Systems (WSNIDS) are highly prone to false alarms, making on-going adjustments essential for effective intrusion detection. The effectiveness of an IoT WSNIDS relies on the administrators who respond after thoroughly analyzing the data gathered by the system. An IoT WSNIDS may require more resources than a wired IoT WSNIDS, as it must manage both alert data and the responsibility of identifying attackers detected by the system. The technology behind Wireless Sensor Networks (WSN) has vulnerabilities that wired networks typically do not encounter, including the need to validate each network sensor. For the security of the sensor network to be ensured, an IoT WSNIDS must provide features such as Authenticity, Confidentiality, Integrity, and Availability. Despite the various limitations associated with IoT WSNIDS, they can deliver a robust safety resolution for a Wireless Sensor Network when implemented effectively and properly configured.

III. PICKING CORRECT IOT WSNIDS

A diversity of IOT WSNIDS concepts are offered in the writings having various types and abilities. The judgment procedure for picking IOT WSNIDS can be distributed into the subsequent phases:

1). Recognize the compulsion for IOT WSNIDS by carrying out risk calculation of the institute.

2). Studying methodological atmosphere of organizations WSN.

3). Implement cost income inspection.
4). Apply user necessities weight-based scheme to choice and implement correct IOT WSNIDS.
5). Accomplish planned positioning of IOT WSNIDS.
6). Observing and looking after of IOT WSNIDS.

In this research, we will focus merely on step 4 of the said procedure. The choice of picking finest WSN IOT WSNIDS result for the WSN entirely rest on its users. Unique resolution is not ever successful to work for the entire mechanism, so the user has to associate the abilities of every IOT WSNIDS creation along with the inexpensive and material which in term will service them in discovering the requirements for the topmost way out. User necessities weight-based technique contains subsequent phases:

1) Gather user IOT WSNIDS necessities.
2) Allocate bottommost weight (e.g., one) to smallest vital necessity.
3) Supplementary necessities are assigned growing weights in magnitude to their comparative position. There is similarly possibility of matching weights.
4) Organize these necessities as of minimum significant to maximum one.
5) As soon as the necessities are weighted, every one IOT WSNIDS metric is allotted a weight that is the same to the amount of the weights of the necessities it pays to.
6) Organize IOT WSNIDS metrics in descendant order.
7) Choose appropriate IOT WSNIDS corresponding the necessities.

User necessities for IOT WSNIDS might be composed by inquiring subsequent investigations to the user:
1) What is the WSN extent of the organizations?
2) Whether there is essential for entire hardware creation, or whole software creation, or a joint hardware and software invention?
3) Whether the IOT WSNIDS invention necessary is to be profit-making system or open-source structure?
4) What would be the IOT WSNIDS approach on background for intrusion detection?
5) What would be the attack discovery capability of IOT WSNIDS?
6) How greatly it would be hard-hitting to install, organize, and control IOT WSNIDS product?
7) What stage and additional resources could be providing for suitable working of IOT WSNIDS?
8) How much performance of IOT WSNIDS is likely?
9) How much failing of IOT WSNIDS is tolerable?
10) How much accurate reportage and recapture is likely from IOT WSNIDS product?
11) What should be the teamwork of IOT WSNIDS product with the router and firewall?
12) What would be IOT WSNIDS pre-setting as per user situation?
13) How certification Organization is likely?
14) What and at what time updates are probable?
15) How memory might be providing to store logs and additional application records?
16) How greatly IOT WSNIDS pressure acceptance is possible?
17) What type of wireless networking cards are used in the system?
18) What network IP series is available?
19) What products and IOT WSNIDS compatibility is likely?
20) What would be the difficulty level of supervision for IOT WSNIDS?
21) What would be the lifetime of IOT WSNIDS product?
22) What kind of technical facility is predictable?
23) How much unambiguousness of reports is anticipated?
24) Is data going to be shared?
25) How prior session information is to be documented?
26) Is there necessity to spread the system in the forthcoming?
27) What would be the greatest input data treating proportion of IOT WSNIDS product?

Once collecting IOT WSNIDS user necessities by wishing above query, user may be invited to organize these necessities in an order as per necessity so that proper weights may be allotted to the necessities. Depending on the necessities user might not consider some of the above queries or may enhance to the list. After the necessities are stationary, method discussed in the paper might be practical for choosing suitable IOT WSNIDS product.

IV. WSNIDS METRICS

This segment of the paper, we will delve deeper into the metrics that are highly relevant to WSNIDS. The metrics are categorized into classes, each accompanied by a common metric that includes examples of low, average, and high scores. To maintain brevity, we will refrain from providing examples for every metric. The set of metrics for IoT WSNIDS will be divided into three categories: Logistical (class 1), Architectural (class 2), and Performance (class 3), as illustrated in figure 2 and defined in detail below.

A. Logistical Metrics (Class 1): These metrics serve to assess the costs, maintainability, and ease of management of a WSNIDS. The metrics relevant to WSNIDS in this domain are illustrated in Table 1. Table 1 presents only a selection of specific logistical metrics. Additional logistical metrics that could be considered include: level of administration, quality of documentation, standard of technical support, evaluation of available copies, product lifespan, and more.

An exemplary case of logistical metrics for WSNIDS is Distributed Management:
• Low Score: Each sensor must be operated independently at its own location.
• Average Score: Sensors can be controlled remotely, but there may be some limitations or variations in organizational oversight.
• High Score: Complete management of all sensors can be executed from any sensor or remotely, utilizing suitable encryption and validation methods.

Metrics such as Policy maintenance, Configuration difficulty, and License management are relevant, as products with low scores in these domains would pose challenges for use in a distributed setting with numerous sensors. Platform requirements indicate the system resources that will be utilized by the WSNIDS in resource-critical WSN scenarios.

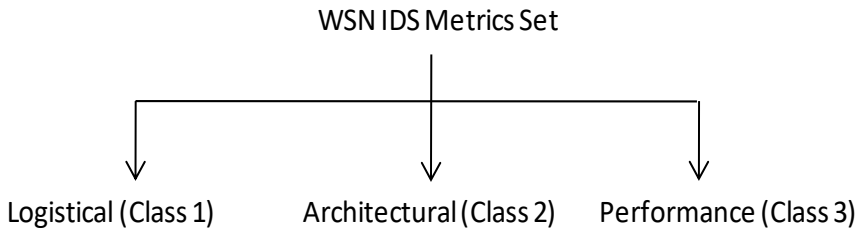


Figure 2: Classification of WSNIDS metrics

Table 1: Selected Logistical Metrics

Logistical Metrics	Description
Distributed Management	Assessing the distribution abilities of a WSN WSNIDS is essential. It helps identify the extent to which a WSN WSNIDS facilitates distributed management.
Configuration Difficulty	The challenges an administrator encounters during the installation and setup of a Wireless Sensor Network Intrusion Detection System.
Policy Management	The challenge of establishing security and intrusion detection regulations for a Wireless Sensor Network Intrusion Detection System (WSNIDS).
License Management	The challenges in acquiring, renewing, and expanding licenses for a WSN WSNIDS.
Availability of Updates	The accessibility of updates for behavior profiles and expenses related to product enhancements.
Platform Requirements	Resources required for deploying a WSN WSNIDS.

An example of an architectural metric for WSN WSNIDS is Policy Management:
- Low Score: Extremely challenging to establish intrusion detection and security policies for a WSNIDS.
- Average Score: Moderately challenging to establish security and intrusion detection policies for a WSNIDS.
- High Score: Very simple to establish intrusion detection and security policies for a WSNIDS.

B. Architectural Metrics (Class 2): These metrics are utilized to assess the alignment between the planned scope and design of the IoT WSNIDS and the actual positioning design. These metrics measure the effectiveness of the IDS's architecture. The metrics specified in this section are listed in Table 2. Additional architectural metrics that could be involved are: Misuse Based, Host/OS Security, Interoperability, Process Security, Package Contents Autonomous Learning, Signature Based, and Visibility, Anomaly Based among others.

Table 2: Selected Architectural Metrics

Architectural Metrics	Description
Adjustable Sensitivity	The challenge of adjusting the sensitivity of a Wireless Sensor Network Intrusion Detection System (WSNIDS) to find a balance between false positive and false negative error rates under various conditions and at different times.
Required Data Storage Capacity	The quantity of disk space required to save logs and additional application data.
Load Balancing Scalability	The quantity of disk space required to save logs and additional application data.
Multiple Sensor Support	The number of sensors that are supported.
Reordering and Stream Reassembly	It is utilized to detect an attack that has been intentionally fragmented and sent in a non-sequential order.
State Tracking	This metric is beneficial for strengthening WSNIDS against surges of random traffic aimed at misleading it.

Data Pool Selectability	This metric is utilized to establish the source data that will be examined for intrusions.
System Throughput	It is utilized to specify the maximum data input rate that can be effectively handled by the WSNIDS.

Table 3: Selected Performance Metrics

Performance Metrics	**Description**
Observed False Positive Ratio	This represents the proportion of false alarms generated by the IDS in relation to the overall number of detection attempts.
False Negative Ratio	This refers to the proportion of real attacks that go undetected by the IDS compared to the total number of attempts at detection.
Cumulative False Alarm Rate	The weighted mean of the ratios for False Positives and False Negatives.
Induced Traffic Latency	It assesses the time taken for packets to reach the target network with and without the presence of a WSNIDS.
Stress Handling and Point of Breakdown	The breakdown threshold is identified as the amount of traffic from a sensor network or host that leads to a failure or breakdown of the IDS.
Throughput	This metric indicates the amount of traffic at which the IDS operates without losing any packets.
Depth of System's Detection Capability	It is characterized by the quantity of attack signature patterns and/or behavioral models that it recognizes.
Breadth of System's Detection Capability	The number of attacks and intrusions identified by the IDS that fall outside its knowledge domain is provided.
Reliability of Attack Detection	It is characterized as the proportion of false positives relative to the overall number of alarms triggered.
Possibility of Attack	It is described as the proportion of false negatives compared to true negatives.
Consistency	It refers to the differences in the effectiveness of a WSN IDS.
Error Reporting and Recovery	The capability of a WSNIDS to accurately detect and recover from incidents.
Firewall Interaction	The capability of a Wireless Sensor Network Intrusion Detection System (WSNIDS) to engage with Firewall systems.
User Friendliness	The capability of a WSNIDS to adapt based on the user's surroundings.
Router Interaction	Level of engagement of the IDS with the router.
Compromise Analysis	It is the capability to communicate the level of damage and breach resulting from intrusions.
Induced Traffic Latency	It refers to the extent to which the presence or functioning of the WSNIDS causes delays in traffic.
Distance	The range of the IDS within the sensor network.
Memory	The quantity of memory needed to process data captured by sensors.
Processing	The processing power of WSNIDS
Power	The energy usage of the WSN IDS for both data transmission and reception within the sensor network, as well as for data processing.

An illustration of an architectural metric for IoT Wireless Sensor Network Intrusion Detection Systems (WSNIDS) is Adjustable Sensitivity:

- Low Score: Lacks any adjustability
- Average Score: Adjustability achieved via static methods
- High Score: Smart, adaptive adjustability

C. Performance Metrics (Class 3): Performance metrics are employed to evaluate the ability of an IoT WSNIDS to carry out designated tasks while staying within performance constraints. These metrics assess and quantify the elements that impact the performance of the WSNIDS. The metrics described in this section are included in Table 3. Table 3 showcases just a subset of Performance metrics. Other Performance metrics that might be taken into account include: Evaluation of Intruder Intent, Clarity of Reports, Efficiency of Generated Filters, Collection of Evidence, Information Sharing, User Alerts, Program Interaction, Recording and Playback of Sessions, Threat Correlation, Analysis of Trends, among others.

An illustration of performance metrics for WSNIDS is the Observed False Positive Ratio:

- Low Score: WSNIDS exhibit a high Observed False Positive Ratio.
- Average Score: WSNIDS produce an average Observed False Positive Ratio.
- High Score: WSNIDS lead to a low or no Observed False Positive Ratio.

V. ALIGNING USER REQUIREMENTS WITH METRIC(S)

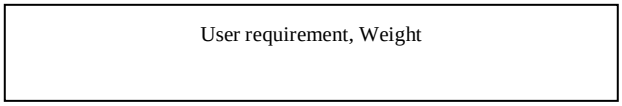
Table 4 presents the metrics associated with each potential user requirement. This table illustrates which metrics play a role in satisfying a specific requirement. For instance, the size of the user's wireless sensor network (WSN) is linked to the metrics of Distributed Management, Configuration Difficulty, Platform Requirements, Adjustable Sensitivity, Load Balancing, Scalability, and Multiple Sensor Support.

Table 4: Metrics user requirements relation

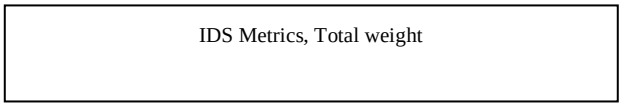
Question number for gathering user requirement	Concerned IOT WSNIDS metric(s)
1	Distributed management, Configuration difficulty, Platform requirement, Adjustable sensitivity, Load balancing, Scalability, Multiple sensor support
2	Configuration difficulty, Platform requirement, Policy management
3	Configuration difficulty, License management
4	Policy management
5	Reordering and stream reassembly, State tracking, Data pool selectability
6	Distributed management, Configuration difficulty, Adjustable sensitivity, User friendliness
7	Distributed management, Platform requirement, Required data storage capacity
8	Distributed management, induced traffic latency, Throughput, Depth of system's detection capability, Breadth of system's detection capability, Reliability of attack detection, Possibility of attack, consistency, Induced traffic latency
9	False positive ratio, False negative ratio, Cumulative false alarm rate
10	Required data storage capacity, Error reporting and recovery
11	Configuration difficulty, Firewall interaction, Router interaction.
12	Configuration difficulty, Policy management, License management, User friendliness
13	License management, Multiple sensor support
14	Availability of updates
15	Distributed management, Platform requirement, Required data storage capacity
16	Compromise analysis, stress handling and point of breakdown, Power, Processing
17	Platform requirement
18	Distributed management, Multiple sensor support, Configuration difficulty
19	Interoperability
20	License management
21	License management, Memory, Distance
22	Availability of technical support
23	Error reporting and recovery
24	Distributed management, Multiple sensor support
25	Session recording and playback
26	Load balancing scalability, Multiple sensor support
27	System throughput

User requirement gathering Question number	IOT WSNIDS metric(s) concerned
1	Distributed management, Configuration difficulty, Platform requirement, Adjustable sensitivity, Load balancing, Scalability, Multiple sensor support
2	Configuration difficulty, Platform requirement, Policy management
3	Configuration difficulty, License management
4	Policy management
5	Reordering and stream reassembly, State tracking, Data pool selectability
6	Distributed management, Configuration difficulty, Adjustable sensitivity, User friendliness
7	Distributed management, Platform requirement, Required data storage capacity
8	Distributed management, Induced traffic latency, Throughput, Depth of system's detection capability, Breadth of system's detection capability, Reliability of attack detection, Possibility of attack, consistency, Induced traffic latency
9	False positive ratio, False negative ratio, Cumulative false alarm rate
10	Required data storage capacity, Error reporting and recovery
11	Configuration difficulty, Firewall interaction, Router interaction.
12	Configuration difficulty, Policy management, License management, User friendliness
13	License management, Multiple sensor support
14	Availability of updates
15	Distributed management, Platform requirement, Required data storage capacity
16	Compromise analysis, stress handling and point of breakdown, Power, Processing
17	Platform requirement
18	Distributed management, Multiple sensor support, Configuration difficulty
19	Interoperability
20	License management
21	License management, Memory, Distance
22	Availability of technical support
23	Error reporting and recovery
24	Distributed management, Multiple sensor support
25	Session recording and playback
26	Load balancing scalability, Multiple sensor support
27	System throughput

The focus on Multiple Sensor Support and Balancing Scalability is outlined in the section corresponding to necessity number 1. The objective of the table is to assist users in selecting the appropriate IoT WSNIDS. Figure 3 illustrates the connections between user needs and IoT WSNIDS metrics. It presents the user requirements in relation to the weighting of IoT WSNIDS metrics. The following representations are employed to denote weighted user needs alongside the example of weighted IoT WSNIDS metrics association. In the arrangement shown in Figure 3, the metric difficulty receives the highest weight, indicating that the IoT WSNIDS product with the simplest configuration is the most suitable choice for the user in this scenario. It is also possible that some of the metrics mentioned earlier may not contribute to any user requirement. As WSN technology evolves, additional metrics and inquiries may be incorporated into this framework.



User requirement with weight



IOT WSNIDS metrics with total weight contribution

Connecting user requirements with IOT WSNIDS metrics

Illustration 3: Example of metric weight for user requirements in IoT WSNIDS.

VI. CONCLUSION AND FUTURE WORK

Wide range of IOT WSNIDS ideas are recommended for WSN, on the other hand it turn out to be problematic for the operator to choose among them that encounter their desires as these thoughts vary in structures and capabilities. This paper, offer a user necessity weight-based methodology to be used for picking an IOT WSNIDS model so as it can be applied for providing safety to WSN. We identify various steps that are favorable for selecting IoT WSNIDS and how the priorities of operators might be balanced. We discuss various metrics associated with the Internet of Things in wireless sensor networks, specifically WSNIDS, and how these metrics can be aligned with weighted user requirements. While, we tried our greatest to discovery out the user desires and metrics concerned with IOT WSNIDS, but a lot is to be done to find out new. The approach outlined in the paper can be extended by allocating negative and fractional weights to the operator requirements, thereby allowing for a more accurate selection of IOT WSNIDS.

REFERENCES

[1] Rama Prasad V Vaddella, "A Study on Intrusion Detection System in Wireless Sensor Networks", International journal of communication networks and information security, Vol. 12 No. 1, 2020.

[2] Snehal Boob and Priyanka Jadhav, "WSN Intrusion Detection System*",* International Journal of Computer, Volume 5, No. 8, August 2010.

[3] G. A. Fink, B. L. Chappell, T. G. Turner, and K. F. O'Donoghue, "A Metrics-Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems, WPDRTS, 15-17 April 2002, Ft. Lauderdale, Florida.

[4] Nikhil Kumar Mittal, "A survey on Wireless Sensor Network for Community Intrusion Detection Systems," 3rd International Conference on Recent Advances in Information Technology (RAIT), 2016, pp. 107 – 111.

[5] D. Udaya Suriya Rajkumar, Rajamani Vayanaperumal, "A leader based intrusion detection system for preventing intruder in heterogeneous Wireless sensor network," IEEE Bombay Section Symposium (IBSS), 2015, pp. 1 – 6.

[6] Zixin Zhou, Lei Liu, and Guijie Han, "Survival Continuity on Intrusion Detection System of Wireless Sensor Networks," 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015, pp. 775 – 779.

[7] Karen Medhat, Rabie A. Ramadan, and Ihab Talkhan, "Distributed Intrusion Detection System for Wiress Sensor Networks," 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, pp. 234 – 239.

[8] Prachi S. Moon and Piyush K. Ingole, "An overview on: Intrusion detection system with secure hybrid mechanism in ireless sensor network," International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015, pp. 272 – 277.

[9] Okan Can and Ozgur Koray Sahingoz, "A survey of intrusion detection systems in wireless sensor networks," 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), 2015, pp. 1 – 6.

[10] Yousef EL Mourabit, Ahmed Toumanari, Anouar Bouirden, Hicham Zougagh, and Rachid Latif, "Intrusion detection system in Wireless Sensor Network based on mobile agent," Second World Conference on Complex Systems (WCCS), 2014, pp. 248 – 251.

[11] Ting Sun and Xingchuan Liu, "Agent-based intrusion detection and self-recovery system for wireless sensor networks," 5th IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT), 2013, pp. 206 – 210.

[12] Aneel Rahim and Paul Malone, "Intrusion detection system for wireless Nano sensor Networks," 8th International Conference for Internet Technology and Secured Transactions (ICITST), 2013, pp. 327 – 330.

[13] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, 2014, Volume: 16, Issue: 1, pp. 266 – 282.

[14] Xue Deng, "An intrusion detection system for cluster based wireless sensor networks," 16th International Symposium on WSN Personal Multimedia Communications (WPMC), 2013, pp. 1 – 5.

[15] Keldor Gerrigagoitia, Roberto Uribeetxeberria, Urko Zurutuza, and Ignacio Arenaz, "Reputation-based Intrusion Detection System for wireless sensor networks," a Complexity in Engineering (COMPENG), 2012, pp. 1 – 5.

[16] Chia-Fen Hsieh, Yung-Fa Huang, and Rung-Ching Chen, " A Light-Weight Ranger Intrusion Detection System on Wireless Sensor Networks," Fifth International Conference on Genetic and Evolutionary Computing (ICGEC), 2011, pp. 49 – 52.

[17] Han Bin, "Research of Cluster-Based Intrusion Detection System in Wireless Sensor Networks," International Conference on Internet Technology and Applications (iTAP), 2011, pp. 1 – 4.

[18] Luigi Coppolino, Salvatore D'Antonio, Luigi Romano, and Gianluigi Spagnuolo, "An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies," 5th International Conference on Critical Infrastructure (CRIS), 2010, pp. 1 – 8.

[19] K. Q. Yan, S. C. Wang, S. S. Wang, and C. W. Liu, "Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network," 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010, Volume: 1, pp. 114 – 118.

[20] Abror Abduvaliyev, Sungyoung Lee, and Young-Koo Lee, "Energy efficient hybrid intrusion detection system for wireless sensor networks," International Conference On Electronics and Information Engineering (ICEIE), 2010, Volume: 2, pp. V2-25 - V2-29.

[21] Lionel Besson and Philippe Leleu, "A Distributed Intrusion Detection System for Ad-Hoc Wireless Sensor Networks: The AWISSENET Distributed Intrusion Detection System," 16th International Conference on Systems, Signals and Image Processing, 2009, pp. 1 – 3.

[22] P. J. Pramod S. V. Srikanth, N. Vivek, Mahesh U. Patil, and Chandra Babu N. Sarat, Intelligent Intrusion Detection System (In2DS) using Wireless Sensor Networks," International conference on Networking, Sensing and Control, 2009, pp. 587 – 591.