International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 2, Mar-Apr 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

IOT WSNID Selection Based on Performance Metrics User Requirements Weight Approach

Dr. Rupinder Singh† and Dr. Rachhpal Singh†
†Khalsa College, Amritsar, Punjab. E-mail: rupi_singh76@yahoo.com

Abstract:

The Internet of Things (IoT)–based Wireless Sensor Network Intrusion Detection System (WSNIDS) is an essential security mechanism used to detect vulnerabilities and defend against malicious activities in sensor networks. The selection of an appropriate WSNIDS depends largely on the underlying IoT architecture and specific application requirements. Since no single solution is universally suitable, administrators must carefully analyze available options by considering system capabilities, cost, available information, and user preferences. This study proposes a selection framework based on a weighted evaluation of user requirements for IoT WSNIDS. Initially, user needs and relevant performance metrics are identified. Each requirement is then associated with one or more corresponding metrics. The requirements are ranked in order of importance, typically expressed in a positive manner, and assigned weights accordingly. The least important requirement is given the lowest weight, while more critical requirements receive proportionally higher values. Subsequently, each metric is assigned a cumulative weight derived from the requirements it supports. Finally, the metrics are ranked in descending order, enabling the identification of the most suitable WSNIDS solution based on alignment between system features and prioritized metrics.

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

I. INTRODUCTION

Organizational policies play a crucial role in defining user requirements, meaning that security considerations are largely influenced by internal strategies rather than being entirely objective. These policies establish system goals, permissible usage, and operational constraints. They also determine what activities should be monitored, when monitoring should occur, who should be informed, and how potential threats are evaluated in terms of risk. With the rapid expansion of networking technologies, concerns related to network security have increased significantly. As a result, Wireless Sensor Network Intrusion Detection Systems (WSNIDS) have emerged as essential tools for ensuring system protection. A WSNIDS may be implemented as either hardware or software, continuously monitoring system and network activities to detect malicious behavior or violations of established policies, while generating alerts and reports for administrative review.

The Internet of Things (IoT) represents a modern technological paradigm that integrates multiple wireless sensor networks, thereby introducing additional security vulnerabilities. These challenges are often addressed through the deployment of WSNIDS solutions. However, selecting and implementing an appropriate system from the wide range of available options is a complex and time-intensive task. The difficulty is further increased when organizations lack a well-defined security framework. Therefore, decisions regarding the selection of WSNIDS should be made carefully, with a comprehensive understanding of available technologies, system capabilities, and their potential impact.

In this work, a user requirement–driven weighted approach is proposed for selecting an appropriate IoT WSNIDS. The method begins with the identification of user requirements and relevant evaluation metrics. Each requirement is then associated with one or more corresponding metrics. The requirements are ordered based on their importance, typically expressed in a positive form. The least significant requirement is assigned the lowest weight (for example, one), while more important requirements are assigned proportionally higher weights. After assigning weights, each metric

is given a cumulative score based on the requirements it supports.

Finally, the metrics are arranged in descending order according to their calculated weights, with the most significant metrics appearing at the top. By aligning these weighted metrics with the features of available WSNIDS solutions, an appropriate system can be selected effectively.

II. WIRELESS SENSOR NETWORK AND INTRUSION DETECTION SYSTEM

The Internet of Things (IoT) refers to a network of interconnected physical objects, commonly known as "things," which are embedded with sensors, software, and communication technologies that enable them to collect and exchange data over the internet. These devices can include everyday household items, industrial equipment, and various smart systems. IoT is supported by advancements in low-power sensor technologies, network connectivity, cloud computing, machine learning, and artificial intelligence. Its operation relies on continuous data collection and real-time communication among devices, often facilitated through user interfaces, applications, and intelligent systems.

Wireless Sensor Networks (WSNs) form an integral part of IoT ecosystems. These networks consist of autonomous sensor nodes that operate without fixed infrastructure and are used to monitor environmental or system conditions. The data gathered by these sensors is transmitted through the network to a central point, commonly referred to as a base station, where it undergoes further processing. In many IoT implementations, this information is ultimately forwarded to centralized cloud servers for storage, analysis, and decision-making.

Despite their advantages, WSNs face several inherent limitations that introduce additional challenges. The deployment of robust security mechanisms is particularly difficult due to constraints such as limited processing power, restricted energy resources, and unreliable wireless communication channels. Earlier WSN protocols often assumed that all nodes within the network were trustworthy and cooperative. However, this assumption is no longer valid in modern applications, where sensor networks are increasingly exposed to various types of security threats and attacks.

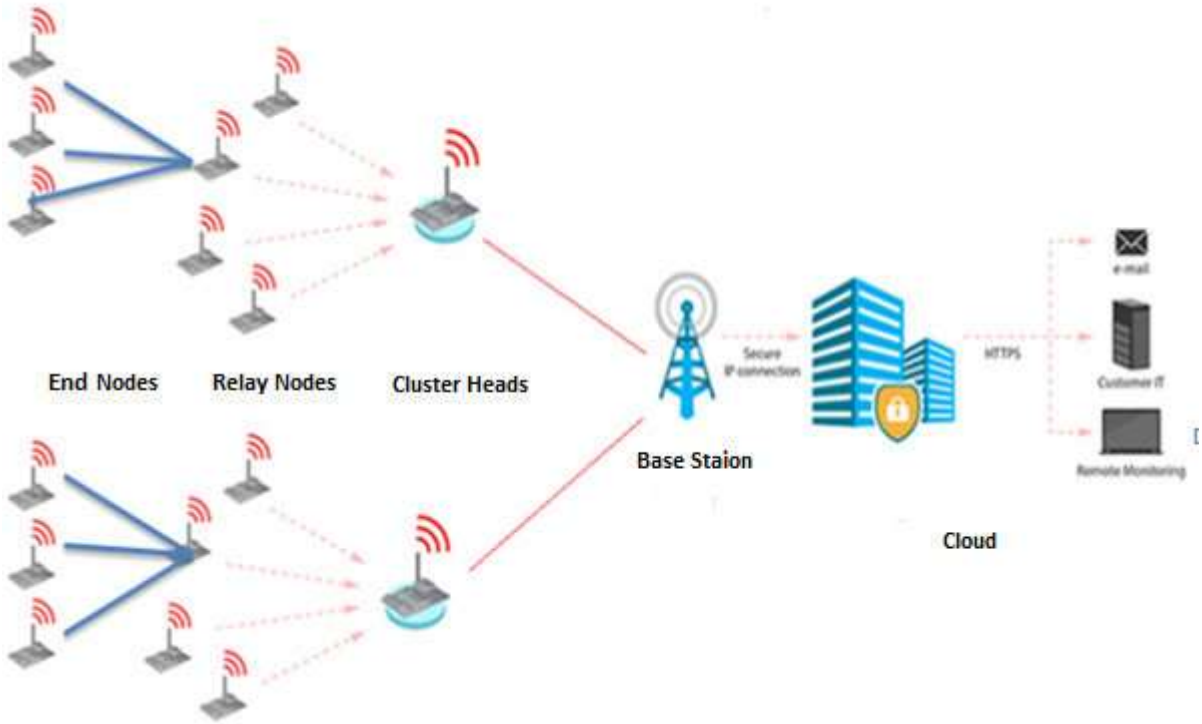


Figure 1: A typical IoT WSN

Intrusion detection refers to the process of identifying unauthorized or suspicious activities within a network or device. An IoT-based Wireless Sensor Network Intrusion Detection System (WSNIDS) may be implemented as either hardware or software that continuously monitors network traffic to detect abnormal behavior. In addition to analyzing traffic generated within the wireless sensor network, a WSNIDS also observes attempts by external entities to access the network through wireless access points (APs). As wireless sensor technologies become increasingly integrated into different parts of network infrastructures, WSNIDS solutions play a vital role in maintaining system security.

One common deployment strategy involves placing sensors near wireless access points, enabling the system to detect a wide range of intrusion attempts. When attackers are physically located near these access points, the ability to identify their presence and approximate location becomes an important feature of the system. WSNIDS architectures can generally be classified into centralized and distributed (decentralized) models. In centralized systems, sensors collect event data and transmit it to a central management console, where it is stored and analyzed for intrusion detection. In contrast, distributed systems perform detection tasks at both the sensor level and the management level. Distributed approaches are often more suitable for smaller networks due to cost efficiency, while centralized systems are preferred for larger networks because they simplify management and enable more efficient data processing.

A typical WSN, as part of an IoT environment, consists of sensor nodes, servers, logging databases, and management consoles. These networks may operate using either centralized or distributed architectures. In centralized configurations, decisions are made based on data aggregated at a single point, whereas in distributed systems, individual sensor nodes participate in decision-making processes. WSNIDS solutions are capable of detecting attacks within the coverage area of the network and also assist in system management by identifying configuration errors in sensor nodes. Furthermore, they support the implementation of security controls, such as regulated access to network interfaces. Communication among WSN components is often supported through wired infrastructure, which may use either the organization's primary network or a dedicated management network. This separation enables effective monitoring and control of interactions between the wireless sensor network and the broader wired environment.

IoT-based Wireless Sensor Network Intrusion Detection Systems (WSNIDS) are relatively recent developments, and therefore they present certain limitations that must be carefully considered before deployment in existing sensor networks. As an emerging technology, WSNIDS may still contain vulnerabilities, implementation flaws, or design weaknesses that could potentially impact overall network security. In some cases, improper deployment or immature system design may even increase the exposure of the network to security risks rather than reduce them.

Another significant concern is the cost associated with implementing WSNIDS solutions. The expense can become substantial, particularly in large-scale sensor network environments where additional sensors and infrastructure may be required to ensure complete coverage. Furthermore, the effectiveness of a WSNIDS largely depends on its configuration by the network administrator. When properly configured and tuned to match network requirements, the system can perform efficiently; however, incorrect or inadequate configuration can result in poor performance and reduced reliability.

A major challenge associated with WSNIDS is the occurrence of false positives and false negatives. Excessive false alarms can overwhelm administrators and make it difficult to distinguish between genuine threats and benign activities. Therefore, continuous monitoring, adjustment, and fine-tuning are necessary to maintain detection accuracy. The overall efficiency of the system also depends on how effectively administrators analyze the collected data and respond to detected threats.

Compared to traditional wired intrusion detection systems, WSNIDS solutions often require additional computational and energy resources, as they must process both network traffic and intrusion alerts while operating within resource-constrained environments. Moreover, wireless

sensor networks introduce unique security challenges, such as the need to authenticate individual sensor nodes and ensure secure communication across the network.

To achieve effective protection, a WSNIDS must support fundamental security principles, including authenticity, confidentiality, integrity, and availability. Despite the challenges and limitations, a well-configured and properly managed WSNIDS can provide a highly effective security mechanism for wireless sensor networks.

III. CHOOSING RIGHT IOT WSNIDS

The literature contains a wide range of IOT WSNIDS concepts with various features and functionalities. The following steps comprise the verdict procedure for selecting IOT WSNIDS:

1. Determine the need for IOT WSNIDS by evaluating the organization's execution risk.
2. Recognizing the technical environment of WSN organizations.
3. Conduct a cost-profit analysis.
4. To choose and implement the best IOT WSNIDS, utilize a weighted approach based on user requirements.
5. Implement IOT WSNIDS strategically.
6. IOT WSNIDS monitoring and upkeep.

This study primarily concentrates on the fourth step of the previously outlined selection process. The responsibility for identifying the most appropriate IoT-based WSNIDS solution lies with the network users or administrators. Since no single system can address all possible scenarios, users must evaluate available WSNIDS options by carefully comparing their features, performance, cost, and supporting information. This comparative analysis helps in defining the specific requirements needed for selecting the most suitable solution. The user requirement–based weighted selection method involves the following steps:

1) Gather user IOT WSNIDS specifications.
2) Give the least important need the lowest weight, such as one.
3) Increasing weights are assigned to other requirements based on their respective positions. The possibility of similar weights also exists.
4) Sort these requirements in order of importance.
5) Each IOT WSNIDS metric is given a weight that is equal to the total of the weights of the requirements it contributes to after the requirements have been weighted.
6) Sort the IOT WSNIDS metrics in descending order.
7) Choose appropriate IOT WSNIDS that meet the specifications.

The following questions can be used to gather user needs for IOT WSNIDS:

1) How big is the WSN organization?
2) Is a complete hardware product, a complete software product, or a combined hardware and software product required?
3) Does the necessary IOT WSNIDS product need to be an open-source or commercial system?
4) How should intrusion detection be handled by IOT WSNIDS?
5) How well should IOT WSNIDS detect attacks?
6) To what extent might IOT WSNIDS product installation, configuration, and regulation be challenging?
7) What platform and other resources might be offered to ensure that IOT WSNIDS operate properly?
8) What level of IOT WSNIDS performance is anticipated?
9) How reliable should IOT WSNIDS be?
10) To what extent is accurate reporting and recovery from the IOT WSNIDS product predictable?
11) How should the firewall and router work with the IOT WSNIDS product?
12) What IOT WSNIDS configuration is appropriate for the user environment?
13) What is required of warrant management?
14) What upgrades are predictable and when?
15) How might logs and other application data be stored in memory?
16) What is the likelihood of IOT WSNIDS stress tolerance?
17) What sort of wireless cards does the network use?
18) What IP range is offered for the network?
19) How likely is it that IOT WSNIDS will work with other products?
20) How should IOT WSNIDS be administered?

21) How long should an IOT WSNIDS product last?
22) What type of technical support is anticipated?
23) To what extent are reports supposed to be clear?
24) Will information be disseminated?
25) How should data from prior sessions be recorded?
26) Will the network need to be expanded in the near future?
27) How fast should an IOT WSNIDS product handle input data?

After gathering user requirements for the IoT-based WSNIDS through the above set of questions, these requirements should be structured and prioritized to enable the assignment of appropriate weights. Users may modify the list by adding or removing questions depending on their specific needs and operational context. Once the requirements are clearly defined and remain consistent, the proposed weighted selection approach can be effectively applied to identify the most suitable WSNIDS solution.

IV. WSNIDS METRICS

This section presents the key metrics relevant to evaluating WSNIDS in greater detail. These metrics are organized into distinct categories, each including representative measures with indicative levels such as low, medium, and high. For brevity, examples are not provided for every individual metric. As shown in Figure 2, the evaluation criteria for IoT-based WSNIDS are classified into three primary groups: logistical (Class 1), architectural (Class 2), and performance (Class 3). Each of these categories is discussed in the following subsections.

A. Logistical Metrics (Class 1): A WSNIDS's cost, maintainability, and manageability are assessed using logistical metrics. Table 1 displays the metrics that are relevant to WSNIDS in this domain.
Only specific logistical parameters are included in Table 1. Additional logistical metrics that may be used include the following: product lifetime, available copy evaluation, technical support quality, administration level, and documentation quality.

Distributed Management is a comprehensive illustration of the logistical metrics for WSNIDS:
• Low Score: Every sensor must be operated directly at the sensor.
• Average Score: The sensor may have some organizational control, but it may also be operated remotely.
• High Score: All sensors can be completely supervised remotely or from any sensor. It is possible to use an
appropriate encryption and validation technique.

Systems that receive low scores in these categories are generally unsuitable for deployment in distributed environments involving multiple sensor nodes. Therefore, factors such as policy management, configuration complexity, and license handling become important evaluation criteria. In addition, platform requirements indicate the level of system resources needed for the deployment and operation of a WSNIDS, which is particularly critical in resource-constrained wireless sensor network environments.

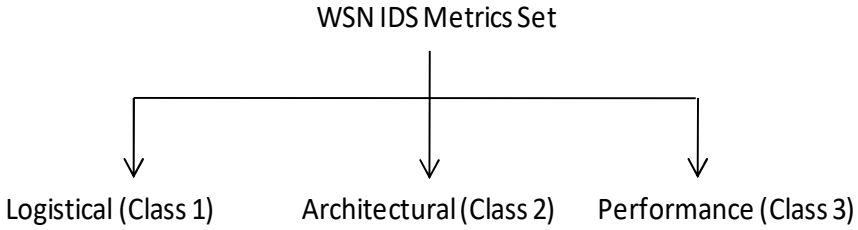


Figure 2: Classification of WSN WSNIDS metrics

Table 1: Selected Logistical Metrics

Logistical Metrics	**Description**
Distributed Management	Figuring out a WSN WSNIDS's distribution capability. It is used to assess how well distributed management is supported by a WSN WSNIDS.
Configuration Difficulty	The challenges an administrator encounters when setting up a WSN WSNIDS.
Policy Management	The challenge of establishing intrusion detection and security procedures for a WSN WSNIDS.
License Management	The challenge of acquiring, renewing, and extending licenses to a WSN WSNIDS.
Availability of Updates	The price of product upgrades and the availability of behavior profile updates.
Platform Requirements	System resources required for WSN WSNIDS implementation.

Policy Management serves as an example of an architectural metric for WSN WSNIDS.

- Low Score: Setting security and intrusion detection protocols for a WSNIDS is quite challenging.
- Average Score: Setting security and intrusion detection policies for a WSNIDS is less challenging.
- High Score: Setting security and intrusion detection rules for a WSNIDS is very simple.

B. Architectural Metrics (Class 2): In essence, architectural metrics are used to compare how the deployment architecture aligns with the anticipated scope and architecture of the IoT WSNIDS. These metrics assess the IDS's architectural effectiveness. Table 2 displays the metrics defined in this field. Anomaly Based, Misuse Based, Autonomous Learning, Host/OS Security, Interoperability, Package Contents, Process Security, Signature Based, and Visibility are some other architectural metrics that could be used.

Table 2: Selected Architectural Metrics

Architectural Metrics	**Description**
Adjustable Sensitivity	The challenge of adjusting a WSNIDS's sensitivity to strike a balance between false positive and false negative error rates for different situations and at different times.
Required Data Storage Capacity	How much disk space is required to keep logs and other application data?
Load Balancing Scalability	It gauges a WSNIDS's capacity to divide traffic into separate, balanced sensor loads.
Multiple Sensor Support	The number of sensors that are supported.
Reordering and Stream Reassembly	It is used to identify attacks that have been broadcast out of sequence and artificially fragmented.
State Tracking	In order to protect WSNIDS against random traffic storms that could mislead it, this statistic is helpful.
Data Pool Selectability	The source data to be examined for intrusions is defined by these metrics.
System Throughput	It serves to specify the highest data input rate that the WSNIDS is capable of processing.

Table 3: Selected Performance Metrics

Performance Metrics	Description
Observed False Positive Ratio	This is the proportion of incorrectly raised alerts by the IDS to all detection efforts.
False Negative Ratio	This is the proportion of real attacks that the IDS fails to identify to all detection attempts.
Cumulative False Alarm Rate	The False Positive and False Negative ratios' weighted average.
Induced Traffic Latency	It gauges how long it takes for packets to reach the target network both with and without a WSNIDS.
Stress Handling and Point of Breakdown	The amount of sensor network or host traffic that causes an IDS shutdown or malfunction is known as the point of breakdown.
Throughput	The amount of traffic that the IDS can handle without discarding any packets is defined by this measure.
Depth of System's Detection Capability	It is described as the quantity of behavior models and/or attack signature patterns that it is aware of.
Breadth of System's Detection Capability	It is determined by how many intrusions and attacks outside of the IDS's knowledge domain it detects.
Reliability of Attack Detection	The ratio of false positives to all alarms raised is its definition.
Possibility of Attack	The ratio of false negatives to real negatives is its definition.
Consistency	It is described as fluctuations in a WSN IDS's performance.
Error Reporting and Recovery	The accuracy with which a WSNIDS can report and recover.
Firewall Interaction	WSNIDS's capacity to communicate with firewall systems.
User Friendliness	The WSNIDS's capacity to adapt to the environment of the user.
Router Interaction	Degree to which the IDS and router interact.
Compromise Analysis	It is the capacity to document the degree of harm and compromise brought about by invasions.
Induced Traffic Latency	It is the extent to which the existence or operation of WSNIDS causes traffic to be delayed.
Distance	The IDS's coverage range within the sensor network.
Memory	The amount of memory needed to process sensor data that has been recorded.
Processing	The WSNIDS's processing power
Power	WSN IDS power usage for data processing and transmission within the sensor network.

Adjustable Sensitivity is an example of an architectural metric for IoT WSNIDS.

- Low Score: No Flexibility
- Average Score: Static approaches for adjustability
- High Score: Adaptability that is dynamic and intelligent

C. Performance Metrics (Class 3): The ability of an IoT WSNIDS to complete a certain task and adhere to performance limits is measured using performance metrics. These metrics quantify and assess the factors influencing the WSNIDS's performance. Table 3 displays the metrics defined in this field. Only the chosen performance measures are shown in Table 3. Analysis of Intruder Intent, Report Clarity, Efficiency of Generated Filters, Evidence Gathering, Information Exchange, User Alerts, Program Interaction, Session Recording and Playback, Threat Correlation, Trend Analysis, etc. are additional performance metrics that may be incorporated.

The Observed False Positive Ratio serves as an example of a WSNIDS performance metric.

- Low Score: WSNIDS produces a high number of observed false Ratio in the positive

• Average Score: WSNIDS produces an average of erroneous observations. Ratio in the positive
• High Score: WSNIDS produces little to no incorrect observations. Ratio in the positive

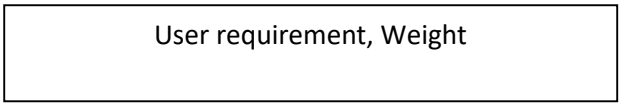
Numerous networked gadgets, sensors, and systems make up the Internet of Things (IoT). Performance indicators are crucial to ensuring these systems operate effectively and consistently. They aid in assessing an IoT system's performance. The main justifications for the significance of performance indicators in IoT are listed below.

1. System Efficiency: Performance measurements are used to gauge the effectiveness of IoT networks and devices. Metrics like latency, throughput, and bandwidth utilization indicate whether the system is operating at its best or whether it needs to be improved.
2. Reliability and Stability: IoT applications frequently operate in vital settings including smart homes, transportation, and healthcare. Performance metrics aid in keeping an eye on error rates, packet loss, and uptime to make sure the system is stable and dependable.
3. Energy Consumption: Batteries power all Internet of Things devices. Performance metrics aid in measuring energy efficiency and power consumption, which prolongs gadget life and lowers maintenance expenses.
4. Network Performance: Metrics like network latency, jitter, and data transmission speed aid in assessing the degree of connectivity between devices and servers because IoT is largely dependent on communication networks.
5. Scalability: Thousands or millions of devices could be a part of an IoT system. When more devices are added, performances metrics help determine whether the system can scale efficiently without experiencing performance degradation.
6. Security Monitoring: Strange performance trends may point to security risks or intrusions. Suspicious activity can be found by keeping an eye on measures like traffic volume and device response time.
7. Quality of Service (QoS): Performance measurements guarantee that IoT services fulfil necessary quality requirements. They support apps and users in maintaining steady performance.
8. System Optimization: Engineers and developers can find bottlenecks, enhance system architecture, and boost overall performance by examining performance indicators.

V. MAPPING USER REQUIREMENTS TO METRIC(S)

Table 4 presents the relationship between user requirements and the corresponding evaluation metrics. It highlights the specific metrics that contribute to satisfying each requirement. For example, as shown for requirement number 1, factors such as distributed management, configuration complexity, platform requirements, adjustable sensitivity, load balancing scalability, and support for multiple sensors are directly related to the scale of the user's wireless sensor network. The primary purpose of this table is to guide users in selecting an appropriate IoT-based WSNIDS by clearly linking requirements with relevant metrics. Figure 3 illustrates the notation system used to represent the relationship between user requirements and WSNIDS evaluation metrics. It also demonstrates how user requirements are weighted and how these weights influence the overall importance of each metric.

The relationship between weighted user requirements and the corresponding weighted WSNIDS metrics is illustrated using the notations presented in this section. As depicted in Figure 3, configuration complexity receives the highest weight, indicating that a WSNIDS solution with minimal configuration effort is most suitable for the given user environment. It is also possible that certain metrics identified earlier may not correspond to any specific user requirement in a particular scenario. Furthermore, the proposed approach can be extended in the future by incorporating additional metrics and evaluation criteria as wireless sensor network technologies continue to evolve.



Represent each user requirement and its corresponding weight

IDS Metrics, Total weight

Represent each IOT WSNIDS metrics and total weight contributed by user requirement

Used to connect user requirements and IOT WSNIDS metrics

Table 4: User requirements and metrics 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

Question number for gathering user requirement	Concerned IOT WSNIDS metric(s)
1	Platform requirements, configuration challenges, and distributed management Scalability, load balancing, and adjustable sensitivity Support for multiple sensors
2	Platform requirements, policy management, and configuration challenges
3	Difficulties with configuration and license management
4	Management of policies
5	Data pool selectability, state tracking, and reordering and stream reassembly
6	Distributed administration, challenging configuration, modifiable sensitivity, and user-friendliness
7	Platform requirements, distributed administration, and necessary data storage capacity
8	dispersed administration, Throughput, reliability of attack detection, potential for attack, consistency, depth and breadth of the system's detection capability, and induced traffic latency
9	Ratios of false positives, false negatives, and cumulative false alarms
10	Data storage capacity requirements, error reporting, and recovery
11	Router interaction, firewall interaction, and configuration complexity.
12	User friendliness, policy management, license management, and configuration complexity
13	management of licenses, Support for multiple sensors
14	Updates' accessibility
15	Platform requirements, distributed administration, and necessary data storage capacity
16	Analysis of compromises, stress management and breakdown points, power, and processing
17	Platform prerequisite
18	Multiple sensor support, distributed management, and challenging configuration
19	Interoperability
20	Management of licenses
21	Memory, Distance, and License Management
22	Technical assistance is available.
23	Reporting and recovering errors
24	Multiple sensor support and distributed management
25	Recording and replaying sessions
26	System throughput, load balancing scalability, and support for multiple sensors
27	Management of licenses

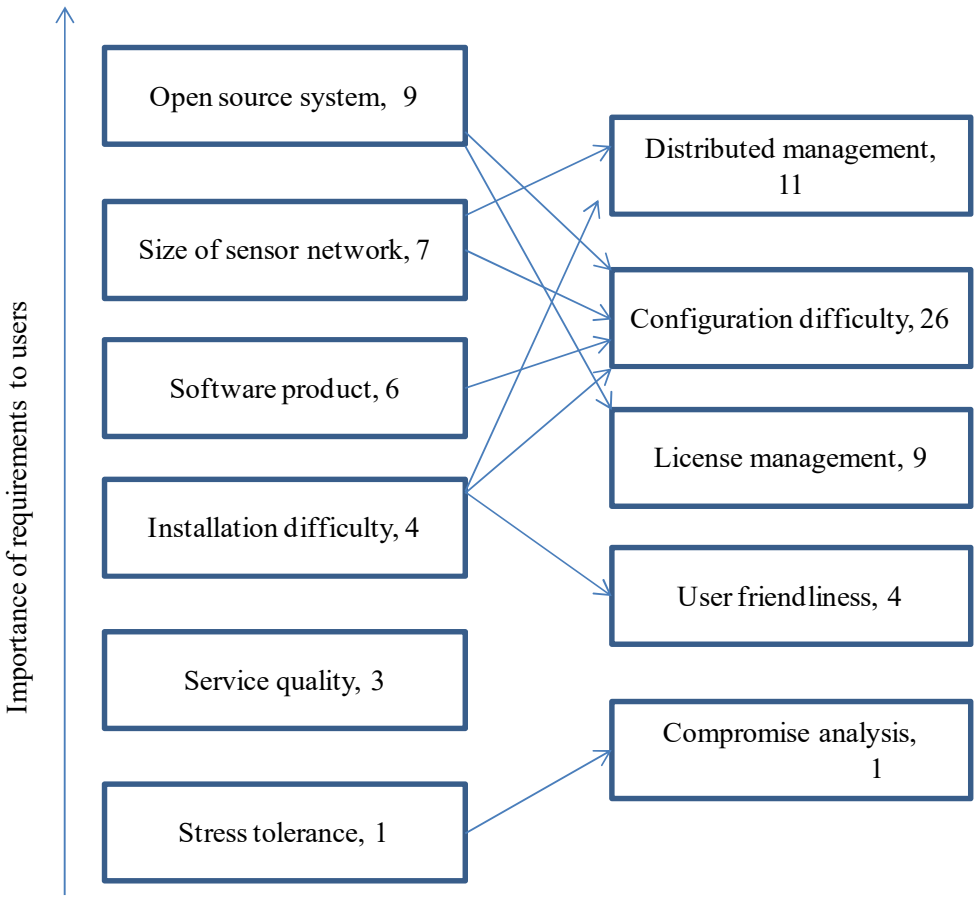


Figure 3: User requirement to IOT WSNIDS metric weight example

VI. CONCLUSION AND FUTURE WORK

A wide range of IoT-based WSNIDS solutions has been proposed for wireless sensor networks; however, the variation in their features and capabilities makes the selection process complex for users. To address this challenge, this study introduces a user requirement–driven weighted approach for selecting an appropriate WSNIDS solution. The paper outlines the key steps involved in the selection process, including the identification and prioritization of user requirements, as well as the assignment of weights based on their relative importance. Furthermore, a comprehensive set of evaluation metrics for WSNIDS is defined, and a systematic method is presented to map these metrics to user requirements. This mapping enables a structured comparison of available solutions and supports informed decision-making. Although significant effort has been made to identify relevant requirements and metrics, the domain continues to evolve, leaving scope for further research. Future enhancements to the proposed method may include the use of fractional or negative weighting schemes to achieve more refined and flexible selection outcomes.

REFERENCES

[1] Prabhjot Kaur, Rupinder Singh, Rachhpal Singh, "Evaluating Internet of Things Wireless Sensor Network Intrusion Detection System based on Architectural Metrics Scorecard Based Approach", International Journal of Computer Science Trends and Technology (IJCST), Vol.11, Issue 3, 2023.

[2] Samuel Mends & Kofi Sarpong Adu-Manu, "Evaluating Machine Learning Efficacy for DoS Intrusion Detection in Wireless Sensor Networks", International Journal of Computer Network and Information Security, IJCNIS Vol. 16, No. 6, 2024.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

