ISSN 2347 - 3983
Volume 11. No.5, May 2023
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter101152023.pdf
https://doi.org/10.30534/ijeter/2023/101152023

Selecting IOT WSNIDS Based on Metrics User Necessity Weight Approach

Rupinder Singh[1], Rachhpal Singh[2], Prabhjot Kaur[3]
[1]Dept. of Computer Science, Khalsa College, Amritsar, Punjab, India. E-mail: singhrupi76@gmail.com
[2]Dept. of Computer Science, Khalsa College, Amritsar, Punjab, India. E-mail: rachhpal_kca@yahoo.co.in
[3]Dept. of Computer Science, Khalsa College, Amritsar, Punjab, India. E-mail: prabhjotkaur@khalsacollege.edu.in

Received Date: March 30, 2023 Accepted Date: April 25, 2023 Published Date : May 07, 2023

ABSTRACT

Internet of Things (IoT) WSNIDS is a network security software that is built for detection of vulnerability exploits against attacks. The choice of WSNIDS depends on the IoT architecture and application. The administrator is the one who will decide which WSNIDS will be the best solution for the sensor network. Not one solution is possible that is going to work for all, so administrator has to equate the abilities that individual WSNIDS provide along with economical, information and desires to find one that works top for them. The concept in this paper offers a user requirement weight-based method to WSNIDS choice for IoT. We primary discuss user WSNIDS requirements and WSNIDS metrics, after that for each WSNIDS necessity we match the metric(s) that are concerned. User are required to lists their WSNIDS necessities in a limited collection that are significant ranging from least to most. User necessities are frequently indicated in a positive form or transformed to the optimistic form. The initial requisite (i.e., minimum significant) is allocated the lowest weight (e.g., one) while the remaining requirements are allocated growing weights in proportion to their relative importance. Once the necessities are weighted, each WSNIDS metric is allocated a weight that is identical to the totality of the weights of the necessities it is going to contribute. WSNIDS metrics are organized in downward sequence where metric having maximum weight is at the topmost position. Suitable WSNIDS means may be selected after match is done between the metrics weight and WSNIDS features.

Key words: Wireless sensor network, Internet of Things, Intrusion detection system, metrics, weight.

1. INTRODUCTION

Safety problems are not completely practical, organization policy choices decide about the user's necessities. The goals, suitable uses, and restrictions on the system are dependent on organizational plan concerning safety. It is organizational contract that is going to choose what to observe, when to be vigilant and whom to aware, or up to what mark of risk a potential intrusion presents. Networking has given growth to the matter of network security. Wireless Sensor Network Intrusion Detection Systems (WSNIDS) has developed as a vital security product. A WSNIDS is a software application or device that observe network and/or system actions for mean events or policy violations and produces reports to an organization station.

Since Internet of Things (IoT) is a new technology, it is usually implemented by connecting a number of wireless sensor networks (WSN) and at the same time it also has numerous exposures. Products like Wireless Sensor Network Intrusion Detection Systems (WSNIDS) is a solution that address many of these. As variety of WSNIDS are proposed in the works, it becomes problematic to select and implement one of them as it's a complicated and time-consuming process. This becomes more problematic if the organization does not have a business security program. WSNIDS choice should not be made speedily, casually, or without having a strong understanding of the technology, choices, or the possible influences.

This research paper, offer a user necessity weight-based method to WSNIDS selection for IoT. In this method first entirely likely user WSNIDS necessities and WSNIDS metrics are listed. Then, for individual WSNIDS necessity we find the concern metric(s). User lists their necessities in a limited collection from least significant to most. Requirements are regularly stated in positive form or changed to the positive form. Subsequent, the first requirement (i.e., least significant) is allotted the lowest weight (e.g., one). Further requirements may be allotted growing weights in percentage to their relation rank. When the requirements are weighted, each WSNIDS metric is allocated a weight that is identical to the amount of the weights of the requirements it contributes to. WSNIDS metrics are organized in downward order where metric with the maximum weight is at the topmost position. Suitable WSNIDS device or software may be selected after similar metrics weight and WSNIDS features.

2. INTRUSION DETECTION SYSTEM AND WIRELESS SENSOR NETWORK

The Internet of Things (IoT) is the idea of joining any device to the Internet along with other connected devices. The IoT is a huge system of connected things and persons. These connected things and persons gather and share data

about the mode they are used and about the around environment. That contains a strange number of objects of all shapes and sizes ranging from smart microwave ovens automatically cooking your food for the exact time, to self-driving vehicles containing complex sensors to detect things in their route, to wearable fitness devices that measure the sum of steps taken along with heart rate, using this information for suggesting exercise plans [2].

IoT contains WSNs are self-organized and have less infrastructure wireless networks used for monitoring the situation or devices. WSNs willingly permits their data collected over the sensor network to a essential location called base station for further processing. Different WSNs pass the collected data to a centralized server at the IoT cloud. WSN has an enormous number of restraints from which upshots new challenges. The sensor nodes have untrustworthy communicating way and dangerous store of resources restrictions making it very tough to install secure system apparatus [1]. Figure 1 demonstrations the assembly of a distinctive IoT WSN. A large number of WSNs protocols in the earlier presumed reliable and supportive nodes. Although it is assumed but circumstances for a number of WSN applications is not the same and a large number of attacks are possible.

Intrusion detection is the method of detecting unwelcome traffic that can be present on a device and similarly on a network. WSNIDS may be either a software system or computer hardware that is going to monitor traffic over the computer network so as to spot undesirable movement. A WSNIDS analyses WSN precise data over the network; apart from this it contains system that scan for outside intruders that try to attack traffic over network over access points (AP). WSNIDS provide a vital part in safeguarding since networks progressively care WSN technologies at several points of a topology[9]10][11]. A WSNIDS execution key is installing sensors everyplace a WAP is arranged so that the common of tried attacks can be detected. Sensing the position of an intrusion occurrence is a serious piece of a WSNIDS where intruder is in near closeness to the WAP, and are really positioned in the limited areas. WSNIDS can be central or decentral. In central WSNIDS network devices gather and forward occurrence information to a central organization console, where WSNIDS information is kept and managed for noticing interference. At the same time, a dispersed WSNIDS regularly accomplish doings which are complete by both console and sensors. Decentral is better

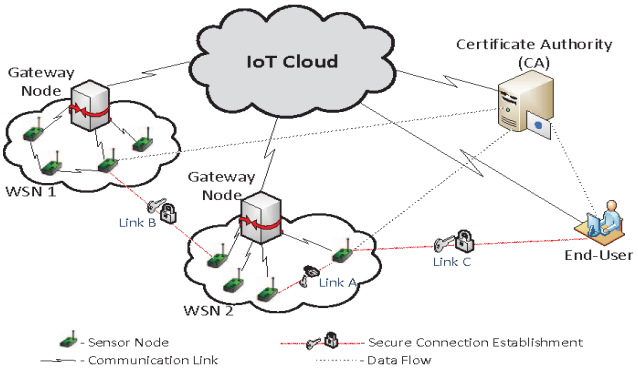


Figure 1: : A distinctive IoT WSN

meant for WSN that are lesser in magnitude, and is too additional profitable. Once WSNs are big, a central WSNIDS is used for easy organization and processing data effectively[4][13].

The composition of WSN which is part of IoT comprise consoles, Sensors, servers, logging databases of organization, etc. WSN can be executed either central or distributed. In central WSN, the information is interrelated at a common place in order to take conclusions and movements based on provided data. In decentral WSN, conclusions are finalized at the sensor node level. The software of WSNIDS can help in spotting intrusions in the area of a given WSN. They similarly provide capabilities in finding sensor node misconfigurations, and deliver material to be able to run servers. The WSNIDS might too support implementing security policies on the sensor nodes, for example giving partial access to WSN interfaces. Numerous parts of WSN are associated to each other over a wired network. The organization's typical networks or separate organization network can be used for WSN different parts communications. An organization network or a normal network can be used for monitoring and regulating the parting among the wired networks and WSN.

WSNIDS is a novel concept, thus it also has some weaknesses related to it. So, carefulness should be considered into thought by previously implementing WSNIDS to a present sensor network. Since it is a novel concept, there might be errors along with loopholes in it. A number of WSNIDS techniques are proposed in the literature[12][14][15][16][17][18][19][20][21][22].

WSNIDS concept, which may, deteriorate the safety level of the sensor network, or rise its exposures at its weakest case. Additional, problem with the WSNIDS is its cost that may be also high to pay for, mainly when there are a huge series of sensor networks, may be needing extra sensors to for managing the complete network treatment. WSNIDS act depends on in what way settings are arranged by the network manager. If adjusted properly or are pre-configured to discovery what precisely should on the sensor network, then their role to their best ability. But, at the same time, a WSNIDS can be quite unsuccessful[6][7].

Generation of numerous false negatives or false positives would result in additional misunderstanding for the administrator. Overall, WSNIDSs are highly susceptible to false alarms, hence, regular fine-tuning is mandatory for actual detection of intrusion. WSNIDS efficiency rest on on administrators who reply subsequently analysing WSN data collected by WSNIDS. A WSNIDS may require additional components than wired WSNIDS as it desires to tackle both the watchful data and the duty to catch the invaders position by the WSNIDS. The system of WSN comes with susceptibilities what the wired networks repeatedly not tackle, for example validating each sensor on the network. WSNIDS essential property is to offer the features such as Integrity, Authenticity, Privacy, and Availability as far as the WSN security is desired. Apart from this, these numerous weaknesses with WSNIDS, it can offer a countless security system for a WSN with the condition that it is used efficiently and configured appropriately[5][8].

3. CHOOSING RIGHT WSNIDS

Step No.	Steps
1.	Identify the necessity for WSNIDS by execution risk assessment of the organization.
2.	Understanding technical environment of organizations WSN.
3.	Perform cost profit examination.
4.	Apply user requirements weight-based method to select and implement right WSNIDS.
5.	Perform strategic deployment of WSNIDS.
6.	Monitoring and maintenance of WSNIDS.

A variety of WSNIDS philosophies are available in the literature providing different types of features along with capabilities. Verdict process for picking WSNIDS may be divided according to the above steps:

In this paper, the main concentration is on step 4 as given in the procedure. The conclusion of picking finest WSNIDS answer entirely rest on the users. It is commonly known that one result is not ever working the whole thing, so the it is better to compare abilities of individually WSNIDS products and should also be economical. User necessity weight-based method includes the given below phases:

User necessity needed for WSNIDS are gathered by questioning following:

After gathering WSNIDS user necessity by requesting the questions as above, the next step is requesting the user to organize these necessities in a direction according to necessities with the purpose of allocating suitable weights to the necessities. According to the requirement the user is given the full liberty to leave any of the given questions.
The user is also given the full liberty to add a new question to the given ones. As soon as the necessities are static, method proposed may be used for picking proper WSNIDS.

4. WSNIDS METRICS

This unit of paper, discuss more information about the metrics extremely relevant to WSNIDS. The metrics are clustered collectively by classes that are further explained by a typical metric, and includes cases of high, average and low scores [3]. The paper does not contain instances for individually metrics. The proposed methodology used in this paper for metrics set will divide IoT WSNIDS into Logistical (class 1), Architectural (class 2), and Performance (class 3). The figure 2 shows the classification and is discussed in detail below.

Step no.	Steps
1.	Collect user WSNIDS requirements.
2.	Assign lowermost weight (e.g., one) to least vital requirement.
3.	Other requirements are allotted increasing weights in quantity to their relative position. There is also likelihood of identical weights.
4.	Arrange these requirements from smallest important to greatest one.
5.	Once the requirements are weighted, each WSNIDS metric is allocated a weight that is equivalent to the sum of the weights of the requirements it contributes to.
6.	Arrange WSNIDS metrics in descending order.
7.	Select suitable WSNIDS matching the requirements.

Question No.	Question
1.	What is the size of the organizations WSN?
2.	Whether there is need for whole hardware product, or whole software product, or a joint hardware and software product?
3.	Whether the WSNIDS product required is to be commercial system or open-source system?
4.	What should be the WSNIDS strategy behind intrusion detection?
5.	What should be the attack detection ability of WSNIDS?
6.	How much it should be tough to install, configure, and regulate WSNIDS product?
7.	What platform and other resources could be provided for appropriate functioning of WSNIDS?
8.	How much performance of WSNIDS is expected?
9.	How much unfailing should be WSNIDS?
10.	How much precise reporting and recovery is predictable from WSNIDS product?
11.	What should be the collaboration of WSNIDS product with the firewall and router?
12.	What should be WSNIDS setting as per user environment?
13.	How warrant Management is expected?
14.	What and when updates are predictable?
15.	How memory could be provided to store logs and other application data?
16.	How much WSNIDS stress tolerance is likely?
17.	What kind of wireless cards are used in the network?
18.	What network IP range is provided?
19.	What compatibility of WSNIDS with other products is likely?
20.	What should be the level of administration for WSNIDS?
21.	What should be the WSNIDS product lifetime?
22.	What kind of technical provision is expected?
23.	How much clearness of reports is expected?
24.	Is information going to be shared?
25.	How previous session data is to be recorded?
26.	Is there need to extend the network in the upcoming?
27.	What should be the best input data processing rate of WSNIDS product?

4.1 Logistical Metrics (Class 1): These metrics are used to calculate expenditure, maintain, and manage WSNIDS. Table 1 shows the metrics possible in this category of WSNIDS. Table 1 comprises the common logistical metrics. Other one that can be included are: Administration level, Document quality, Quality of technical support, Available copy evaluation, Product lifetime, etc.

A thorough case that can be discussed for the logistical metrics is Distributed Management:

- Low Score: Running of individual sensor essentially be completed at the sensor itself.
- Average Score: Sensor management can be done remotely but at the same time partial or degree of organizational control is allowed.
- High Score: Whole supervision of entire sensors is possible from any sensor or at faraway place. Suitable encoding and validation system may be used.

Metrics such as Policy maintenance, License management, Configuration difficulty, etc. are valid as IDS with low scores in these metrics in a distributed environment would not be easy to be used with several sensors. Platform requirements provide the system resources hint that will be used up by the WSNIDS in the resource-critical WSN situation.

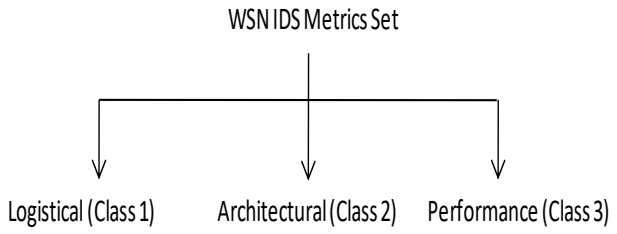


Figure 2: Organisation of WSNIDS metrics

An explanatory case of an architectural metric for WSNIDS is Policy Management is:

- Low Score: Very difficult to set safety and invasion discovery strategies for a WSNIDS.
- Average Score: Less difficult to set safety and invasion discovery strategies for a WSNIDS.
- High Score: Very easy to set security and intrusion detection policies for a WSNIDS.

4.2 Architectural Metrics (Class 2): These metrics are frequently used to evaluate the proposed possibility and architecture of the IoT WSNIDS and how they fulfil the placement architecture. The metrics assess the architectural effectiveness of the IDS. Table 2 shows the metrics used in this part. Additional metrics that may be involved are: Misuse Created, Interoperability, Variance Based, Based on Signatures, Independent Learning, Security, Set Contents, Procedure Security, and Visibility etc.

Table 1: Selected Logistical Metrics

Logistical Metrics	Description
Distributed Management	Determining the distribution capabilities of a WSN WSNIDS. It is used to determine up to what extent a WSN WSNIDS supports distributed management.
Configuration Difficulty	The difficulties an administrator faces while installing and configuring a WSN WSNIDS.
Policy Management	The difficulty in setting security and intrusion detection policies for a WSN WSNIDS.
License Management	The difficulty in obtaining, updating and extending licenses to a WSN WSNIDS.
Availability of Updates	The availability of updates of behaviour profiles and cost of product upgrades.
Platform Requirements	System resources needed to implement a WSN WSNIDS.

An explanatory architectural metric sample is Adjustable Sensitivity for IoT WSNIDS:

- Low Score: Not any Adjustability
- Average Score: Adjustability but through fixed means
- High Score: Adjustability is dynamic and Smart

4.3 Performance Metrics (Class 3): These metrics are basically involved in measuring the capability of an IoT WSNIDS to attain a specific predefined work. This work should be in accordance to the performance restrictions. The metrics involved in this class are used to evaluate and estimate the constraints that influence the performance of the WSNIDS. Table 3 represent the metrics defined in this

Table 2: Selected Architectural Metrics

Architectural Metrics	Description
Adjustable Sensitivity	The difficulty of altering the sensitivity of a WSNIDS in order to achieve a balance between false positive and false negative error rates at various times and for different environments.
Required Data Storage Capacity	The amount of disk space needed to store logs and other application data.
Load Balancing Scalability	It measures the ability of a WSNIDS to partition traffic into independent, balanced sensor loads.
Multiple Sensor Support	The cardinality of sensors supported.
Reordering and Stream Reassembly	It is used to find an attack that has been artificially fragmented and transmitted out of order.
State Tracking	This metrics is useful in hardening WSNIDS against storms of random traffic used to confuse it.
Data Pool Selectability	This metrics is used to define the source data to be analyzed for intrusions.
System Throughput	It is used to define the maximal data input rate that can be processed successfully by the WSNIDS.

Table 3: Selected Performance Metrics

Performance Metrics	Description
Observed False Positive Ratio	This is the ratio of alarms that are wrongly raised by the IDS to the total number of detection attempts.
False Negative Ratio	This is the ratio of actual attacks that are not detected by the IDS to the total number of detection attempts.
Cumulative False Alarm Rate	The weighted average of False Positive and False Negative ratios.
Induced Traffic Latency	It measures the delay in the arrival of packets at the target network in the presence and absence of a WSNIDS.
Stress Handling and Point of Breakdown	The point of breakdown is defined as the level of sensor network or host traffic that results in a shutdown or malfunction of IDS.
Throughput	This metrics defines the level of traffic up to which the IDS performs without dropping any packet.
Depth of System's Detection Capability	It is defined as the number of attack signature patterns and/or behavior models known to it.
Breadth of System's Detection Capability	It is given by the number of attacks and intrusions recognized by the IDS that lie outside its knowledge domain.
Reliability of Attack Detection	It is defined as the ratio of false positives to total alarms raised.
Possibility of Attack	It is defined as the ratio of false negatives to true negatives.
Consistency	It is defined as the variations in the performance of a WSN IDS.
Error Reporting and Recovery	The ability of a WSNIDS to correctly report and recover.
Firewall Interaction	The ability of a WSNIDS to interact with the Firewall systems.
User Friendliness	The ability of a WSNIDS to configure according to user's environment.
Router Interaction	Degree of interaction of the IDS with the router.
Compromise Analysis	It is the ability to report the extent of damage and compromise due to intrusions.
Induced Traffic Latency	It is the degree to which traffic is delayed by the WSNIDS presence or operation.
Distance	The distance coverage of the IDS in the sensor network.
Memory	The amount of memory required for processing of captured sensor data.
Processing	The processing capabilities of WSNIDS
Power	Power consumption of WSN IDS for transmission and reception of the data in the sensor network and for processing of data.

class. The table contains only the particular Performance metrics. Additional Performance metrics in this class that can be added are: Program Communication, Examination of Intruder Intent, Clearness of Reports, Usefulness of Generated Filters, Data Sharing, Evidence Collection, User Warnings, Session Recording and Playback, Threat Correlation, Trend Examination, etc.

Observed False Positive Ratio is an explanatory case of performance metrics for WSNIDS:

• Low Score: WSNIDS produce large number of Observed false Positive Ratio

• Average Score: WSNIDS produce normal Observed false Positive Ratio
• High Score: WSNIDS produce small or no Observed false Positive Ratio

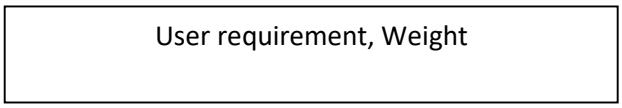
5. MAPPING USER NECESSITY TO METRIC(S)

The metrics connected by each of probable user requirement continue in table 4. It shows metrics that are contributing to achieve a definite condition. For example, performance of WSNIDS is concern with the metrics 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 etc. presented in the column corresponding to requirement number 8.

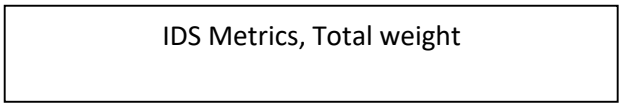
Table 4: user necessity and metrics relation

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

The work of the table is to assist users in for precise selection of WSNIDS. Figure 3, gives symbolizations to denote user necessity and WSNIDS metrics association. Figure 3 gives user requirement to WSNID metric weighting. The notations given below are used for representing weighted user necessity and weighted WSNIDS metrics association. In figure 3, metric configuration difficulty obtains maximum weight, so WSNIDS product with minimum effort in configuring looks to be the utmost product as per the need of the user system. WSN knowledge is altering additional metrics and requests may be further provided to tactic.



Represent each user requirement and its corresponding weight



Represent each WSNIDS metrics and total weight contributed by user requirement

Used to connect user necessity and WSNIDS metrics

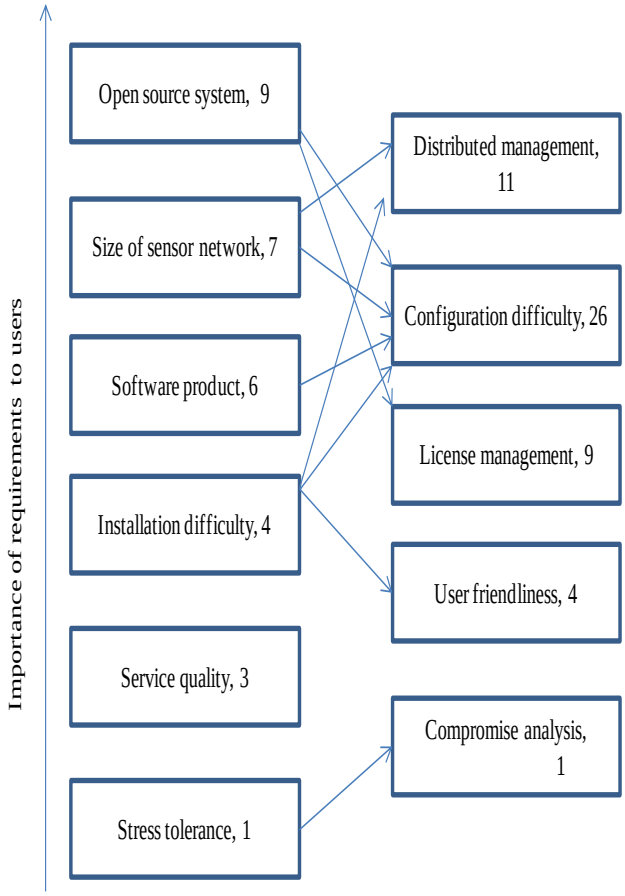


Figure 3: User necessity to WSNIDS metric weight sample

6. CONCLUSION AND FUTURE WORK

A large number of IoT WSNIDS concepts are projected for IoT containing wireless sensor networks, but it turns out to be difficult for the user to select one of them that fulfil their requirements as these ideas vary in structures and capabilities. This paper, offer a user necessity weight-based approach to be used for picking an IoT WSNIDS concept as it can be applied practically so that security to WSN attached with IoT can be provided. We define several steps required for the choice of WSNIDS and how user necessities may be weighted. We, also describe numerous metrics that are concern with IoT WSNIDS and how mapping of weighted user necessities to these metrics can be done. However, we tried our best to find out the user necessities and metrics concerned with IoT WSNIDS, but a more is to be done. The technique discussed in the paper may be applied by assigning fraction and negative weights to the user necessities so that additional exact selection of IoT WSNIDS can be done.

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 wireless 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**, ifth 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.