International Journal of Research Publication and Reviews

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

Picking IOT WSNIDS Founded on Architectural Metrics Customer Requirements Load Method

Dr. Rupinder Singh

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

ABSTRACT –

Wireless Sensor Network (WSN) is internal part of Internet of Things (IoT) which is openly exposed to a large number of attacks. Wireless Sensor Network Intrusion Detection System (WSNIDS) is a software system that is used for detecting susceptibility of sensor network to attacks in IoT. It is the architecture of IoT WSN along with its application that decides the select of IOT WSNIDS. The architectural metrics play an important role in making this decision. The administrator of IoT WSN is responsible for choosing the right IOT WSNIDS in order to provide the top way out for the WSN. The one solution is not going to work for the WSNs, therefore the administrator is responsible for the comparison of the capabilities of exclusively IOT WSNIDS along with cost-effective, facts and needs to find single that works topmost for them. This paper offers an architectural metrics customer requirements load method for IOT WSNIDS selection. The paper focuses the discussion on collecting customer IOT WSNIDS requirements and IOT WSNIDS architectural metrics. After this each architectural metrics is matched with IOT WSNIDS necessity. Administrator of the sensor network lists their IOT WSNIDS needs in a restricted collection raging from minimum to maximum significant. Customer desires are regularly specified in a positive form or converted to the optimistic form. The lowest important requirement is assigned the lowest load i.e. one whereas the left over necessities are given rising loads in fraction to their relative significance. When all the necessities are loaded, every IOT WSNIDS metric is assigned a load which is equal to the total of the loads of the necessities it pays to. IOT WSNIDS metrics are arranged in descending order so that the metric with the supreme load is at the highest point. Suitable IOT WSNIDS may be nominated after matching the metrics load and IOT WSNIDS features.

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

I. INTRODUCTION

It is not completely possible to provide security of WSN practically, it dependents on the organization security policy choices which is further dependent on customer’s requirements. The security goals, appropriate uses, and constraints on the Wireless Sensor Network (WSN) are defined by organizations strategy about protection. It is the policy of organization that is going to pick what to observe, when to be watchful and whom to aware, or up to what mark of threat a likely intrusion presents. Matter of WSN security is an outcome of networking security due to its wide use. Internet of Things Wireless Sensor Network Intrusion Detection Systems (IOT WSNIDS) has appeared as an important security product. IOT WSNIDS is a software application or hardware device that is going to monitor WSN network along with system movements for mean happenings or WSN security strategy violations and provides reports to a WSN station.

As Internet of Things (IoT) is a fresh knowledge, it is frequently applied by relating a quantity of wireless sensor networks (WSNs) and simultaneously it is exposed to a number of attacks. Systems like Wireless Sensor Network Intrusion Detection Systems (IOT WSNIDS) are developed with the aim to deal several of these. As range of IOT WSNIDS products are projected in the research works, it turns out to be challenging to select and implement one of them as it’s a difficult and laborious procedure. This develops to be more challenging if the organization implementing the IoT is not supposed to aware of business security program. IOT WSNIDS selection would not be finished hurriedly, carelessly, or short of having a strong thoughtful of the technology, selections, or the likely impacts.

This paper is concern with a technique that can be used to for proper selection of IoT WSNIDS. The technique is a customer requirements load-based process for IOT WSNIDS selection. Herein, process first list expected customer IOT WSNIDS necessities and IOT WSNIDS metrics. Next, for discrete IOT WSNIDS necessity the concept match the concern metric(s). Customers, usually provide their necessities in a fractional assembling from minimum important to maximum. Requirements are frequently specified in optimistic arrangement or altered to the optimistic form. Subsequently, the minor necessity (i.e. slightest significant) is assigned the bottommost load (e.g., one). Remaining necessities may be allotted growing loads in fraction to their relative position. After all the requirements are loaded, every IOT WSNIDS metric is assigned a load that is matching to the totality of the loads of the necessities it pays to. IOT WSNIDS metrics are prearranged in downward order where metric with the uppermost load is at the uppermost. Proper IOT WSNIDS product or software may be a selection of after equating the metrics load and IOT WSNIDS properties.

II. INTRUSION DETECTION SYSTEM AND WIRELESS SENSOR NETWORK

The Internet of Things (IoT) is a system of physical items called “things” typically fixed with sensors, software, and supplementary tools for joining and swapping data over the internet. These devices variety comprises domestic objects, engineering tools, and every other compatible item. IoT offer access to low-cost, low-power sensor expertise, connectivity, cloud calculating platforms, artificial intelligence (AI), Machine learning. IoT works over the real-time gathering and exchange of data. An IoT system makes use of IoT application, Smart devices, and a graphical customer interface.

IoT encompasses WSNs are own configuring and infrastructure-less wireless networks that are basically used for observing the surroundings or devices. WSNs on their own will passes their data assembled through the sensor net to a vital locality termed base station for additional treating. Unlike WSNs distribute the composed data to a IoT cloud with a federal server.

WSN has a vast amount of limits from which consequences fresh troubles. The nodes having sensor untrustworthy message intermediate and risky resource constraints which make it very hard to install safety tool. Figure 1 illustrates the assembly of a typical IoT WSN. Maximum of the protocols for WSNs in the earlier supposed that all nodes are truthful and helpful. On the other hand, this is not the condition for numerous sensor network implementation currently and a diversity of attacks is likely in WSN.

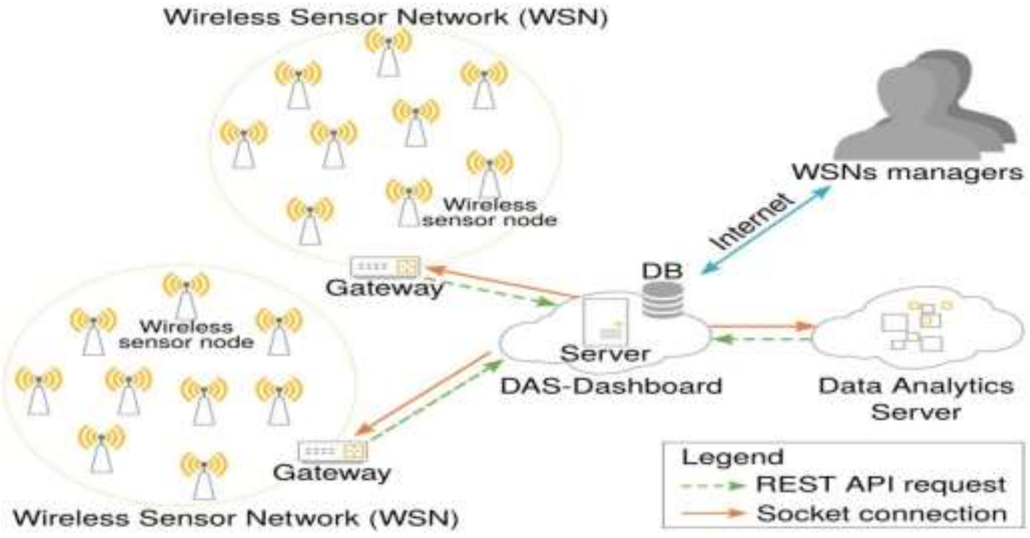


Figure 1: A typical IoT WSN

Intrusion recognition is the technique of spotting unwelcome stream of traffic on a WSN or a device. IOT WSNIDS can be hardware or software that observers network traffic in order to find out unwelcome movement. An IOT WSNIDS can watch WSN precise traffic; it also comprises scanning for outside customers annoying to attach to the network over access points (AP). IOT WSNIDS play vital character in safeguarding as networks progressively support WSN tools at numerous points of a topology. An IOT WSNIDS carrying out key is that sensors must be connected everywhere a WAP is organized so that the majority of tried attacks can be detected. Identifying the place of an attack is a thoughtful feature of an IOT WSNIDS where attackers are in nearby closeness to the WAP, and are really situated in the local areas. IOT WSNIDS can be federal or distributed. In federal IOT WSNIDS network sensors gather and pass occurrence data to a federal administration system, where the IOT WSNIDS data are kept and treated for sensing intrusion. Alternatively, a discrete IOT WSNIDS typically accomplish actions which are completed by both the sensors and the console. Distributed one is superior for WSN that are minor in size, and it is also more cost-effective. When WSNs are greater, a federal IOT WSNIDS is used for at ease controlling and real data treating.

The constituents of a WSN which is portion of IoT comprise servers, Sensors, administration logging files, and system. WSN may be implemented either federal or dispersed. In federal systems, data are interconnected at a vital place so that the choices and actions are accomplished established on the data. In dispersed systems, judgments are accomplished at the sensor node level. The IOT WSNIDS software can be used to spot attacks in the area of the WSN. They also deal features to discovery out mis-configurations of the sensor nodes, and make available material to manage servers. The IOT WSNIDS that are used by sensors nodes might also assist to apply safety schemes on the sensor nodes, such as providing incomplete access to WSN boundaries. Frequent constituents of WSN are associated to each other over a network that is wired. The administration’s classic networks or discrete administration network can be applied for WSN module communications. An administration network or a regular network can be used for watching and governing the separation among the wired networks and WSN.

IDS for IOT WSN is not a common technology, therefore there are some obstacles associated with it. Some alertness must be put into concern before relating IOT WSNIDS to a present sensor network. Since it is a fresh tool, there may be errors and gaps in it. IOT WSNIDS skill, which may, worsen the safety level of the WSN, or grow its exposures at its wickedest case. Additional, shortcoming with the IOT WSNIDS is its price that may be also costly to pay for, mostly when we have a vast choice of networks consisting sensor, which might want extra sensors to succeed the entire network management.

IOT WSNIDS performance rest on how it is arranged by the network supervisor. If they are adjusted appropriately or are configured prior to find what precisely should be on the sensor network, then role to their best ability. Nevertheless, on the further hand, an IOT WSNIDS can be quite unproductive.

If a large number of false positives or false negatives are produced, then this will create further misunderstanding to the WSN administrator. Generally, IOT WSNIDSs are very subject to false alarms, therefore, consistent modification is compulsory for definite recognition of attack. IOT WSNIDS effectiveness rest on supervisors who reply after investigating WSN data composed by IOT WSNIDS. An IOT WSNIDS may prerequisite supplementary resources than wired IOT WSNIDS as it wishes to address in cooperation the alert data and the accountability to catch the attackers positioned by the IOT WSNIDS. The expertise of WSN comes with vulnerabilities that are not common with wired networks, for example authenticating each WSN sensor. It is essential for IOT WSNIDS to provide some common features for example Truthfulness, Privacy, Integrity, and Obtainability if the safety of the WSN is wanted. In spite of, these several faults IOT WSNIDS, can deliver a uncountable safety key for an IoT WSN once it is used professionally and organized properly.

III. PICKING CORRECT IOT WSNIDS

A range of IOT WSNIDS opinions are existing in the writings having various characteristics and abilities. The judgment process for picking IOT WSNIDS can be separated into the subsequent steps:

1). Recognize the need for IOT WSNIDS by implementation risk calculation of the organization.

2). Understanding practical atmosphere of organizations WSN.

3). Implement more profitable examination.

4). Implement the method in this paper to choose and apply correct IOT WSNIDS.

5). Accomplish planned placement of IOT WSNIDS.

6). Observing and upkeep of IOT WSNIDS.

This paper focus only on step 4 of the provided process above. The customers of the WSN are going to decide the top IOT WSNIDS product for their network. One solution is able to work for all and complete concept, therefore, the user of the network should match the capacities of every IOT WSNIDS formation alongside the inexpensive which will support them in finding the desires for the maximum result. The process of Customer requirements load-based technique comprises subsequent phases:

1) Gather customer IOT WSNIDS necessities.

2) Allocate bottommost load (e.g., one) to smallest vital necessity.

3) Other necessities are chosen according to cumulative loads in amount to their comparative position. There is also possibility of matching loads.

4) Organize these necessities from minimum vital to highest one.

5) After the needs are loaded, every IOT WSNIDS metric is assigned a load namely correspondent to the whole of the loads of the necessities it pays to.

6) Position IOT WSNIDS metrics in descendent order.

7) Choose appropriate IOT WSNIDS identical to the necessities.

Customer necessities for IOT WSNIDS may be composed by questioning subsequent queries to the customer:

1) What is the size of IoT WSN organizations?

2) Specify the type of product required i.e. software, hardware, or combination of both.

3) Specify whether commercial or open-source product is required for IOT WSNIDS.

4) Specify the intrusion detection strategy to be used behind IOT WSNIDS.

5) Specify the level of intrusion detection ability of IOT WSNIDS.

6) Specify how convenient it should be for installing, configuring, and operating IOT WSNIDS product.

7) Specify the type of platform along with other resources is required for appropriate working of IOT WSNIDS.

8) Specify the percentage of performance is expected for IOT WSNIDS product.

9) Specify How much trustworthy should be IOT WSNIDS product.

10) Specify how much precise reporting and recovery is likely from IOT WSNIDS product?

11) Specify how cooperation of IOT WSNIDS system will be done with router and firewall is expected.

12) Specify the types and procedure of IOT WSNIDS product setting is required.

13) Specify the licence management procedure expected.

14) Specify the product updating time and procedure.

15) Specify the capacity and type of memory required for storing logs files along with other data.

16) Specify IOT WSNIDS load handling capability.

17) Specify the type of wireless cards to be used in the WSN.

18) Specify the range of network IP addresses is required.

19) Specify the compatibility of IOT WSNIDS product with the existing other products.

20) Specify the admin level control required for IOT WSNIDS product.

21) Specify the minimum lifetime of IOT WSNIDS product.

22) Specify the expectation regarding the technical facility.

23) Specify the types of reports along with the format.

24) Specify whether the data is to be shared on not.

25) Specify the process required for previous session data recording.

26) Specify whether there will be possibility of extending WSN in the future.

27) Specify the rate of IOT WSNIDS product input data processing.

After IOT WSNIDS client needs are composed by using the above questions, client will be in a position to arrange these desires in the order of necessities so as to allocate appropriate score to the necessities. As per the demand the customer may add new requirements to the above list. The customer is also given the provision of excluding any of the above questions. Once the customer finalize the requirements, the method discussed in this paper may be practical for picking suitable IOT WSNIDS creation.

IV. WSNIDS METRICS

This section of the paper, provide detailed list of Architectural metrics that are mostly relevant to IOT WSNIDS. The metrics are separated into three categories i.e. Logistical (class 1), Architectural (class 2), and Performance (class 3). This paper only discusses Architectural (class 2) metrics. As an example of Architectural metric, consider Multiple Sensor Support. The mentioned metrics score can be assigned by the criteria as follows:

Low Score (+): Sensors supported are very less.

Average Score (++): Sensors held is normal.

High Score (+++): Sensors held is very big.

IOT WSNIDS architectural Metrics are crucial to the architectural quality and maintainability of IOT WSNIDS software and hardware. These metrics can advise you around hazardous accumulations of architectural and technical debt initial in the IOT WSNIDS software process.

Architectural metrics are fundamentally used to match the planned likelihood along with the IoT WSNIDS architecture. These metrics are used to match the positioning architecture. These metrics assess the architectural effectiveness of the WSNIDS. The metrics concerned with the architecture of IOT WSNIDS are presented in Table 1. Apart from this, additional Architectural metrics that might possibly be involved are: Signature Based, Host/OS Security, Misuse Based, Anomaly Based, Package Contents Autonomous Learning, Interoperability, Visibility, Process Security etc.

V. CUSTOMER REQUIREMENTS MAPPING WITH METRIC(S)

The metrics that are possibly linked with customer requirement are specified in table 2. This table specifies the metrics are fulfilling a particular requirement. For example question what should be the attack detection ability of IOT WSNIDS? is linked with the metrics state tracking, reordering and stream reassembly, data pool selectability, etc. as existing in the column corresponding to necessity digit 2.

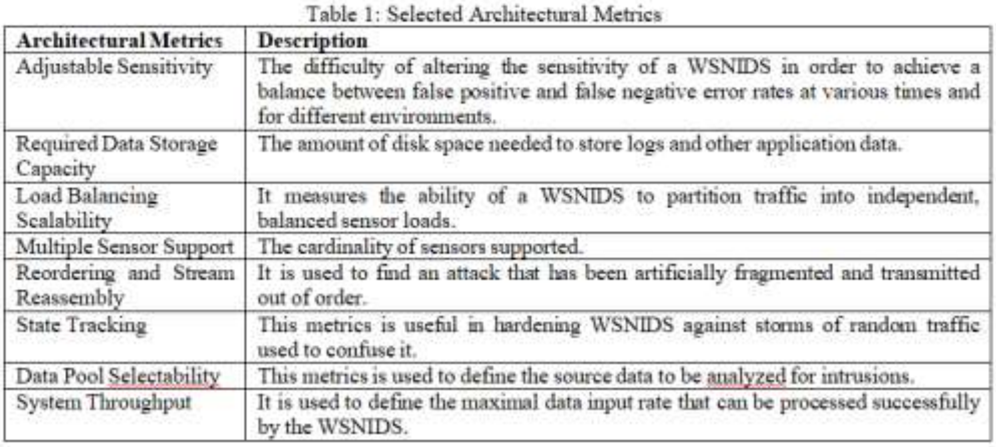
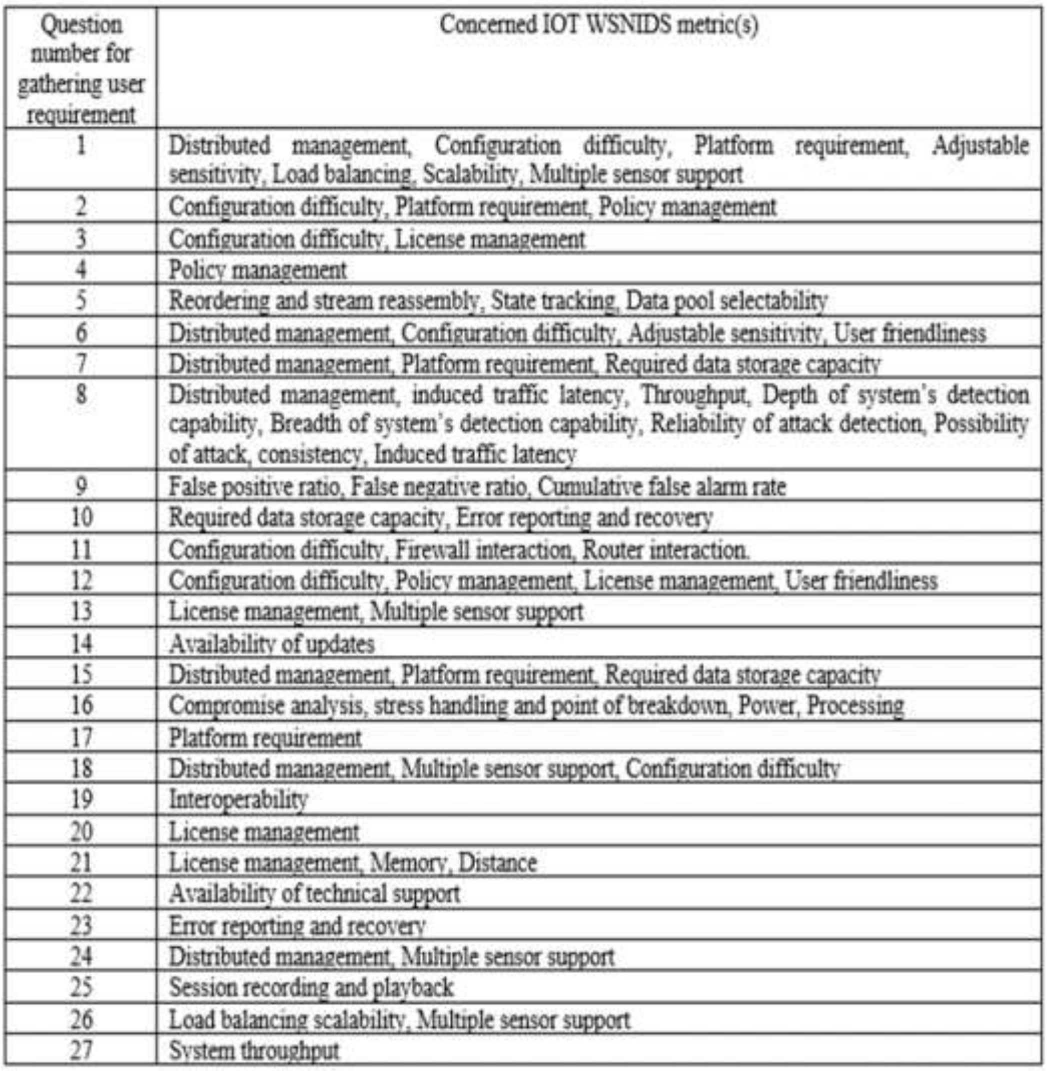


Table 1: Selected Architectural Metrics

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 2: Requirement and corresponding metrics.



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 table is prepared for the purpose of helping customer in making a precise choice to IOT WSNIDS. The figure 2 provides diagrams used for presenting IOT WSNIDS metrics and customer desires association. Weighing of customer requirement to IOT WSNIDS metric is shown in figure 3. Figure 3 provides example of loaded IOT WSNIDS metrics and loaded customer desires association. As shown in the example, the IOT WSNIDS metrics gets different scores depending upon the connectivity with the customer requirements. In this example metric configuration difficulty is having highest score (load), this indicates that the IOT WSNIDS solution having minimum effort related to software configuration seems to be the top result to the customer setting. In this illustration there is also possibility that few of the metrics represented above may not add to some of the customer necessity. Since the WSN information is altering additional metrics and queries may be added to the above methodology.

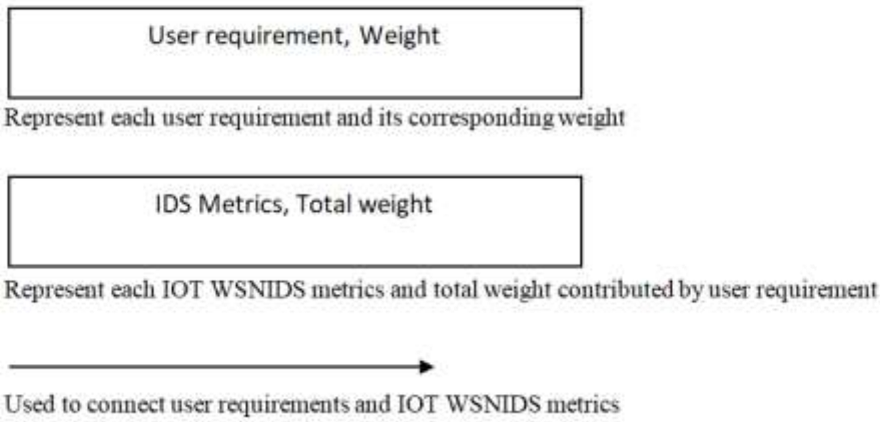

User requirement, Weight
Represent each user requirement and its corresponding weight
IDS Metrics, Total weight
Represent each IOT WSNIDS metrics and total weight contributed by user requirement
Used to connect user requirements and IOT WSNIDS metrics

Figure 2: Notations for mapping requirement and metrics.

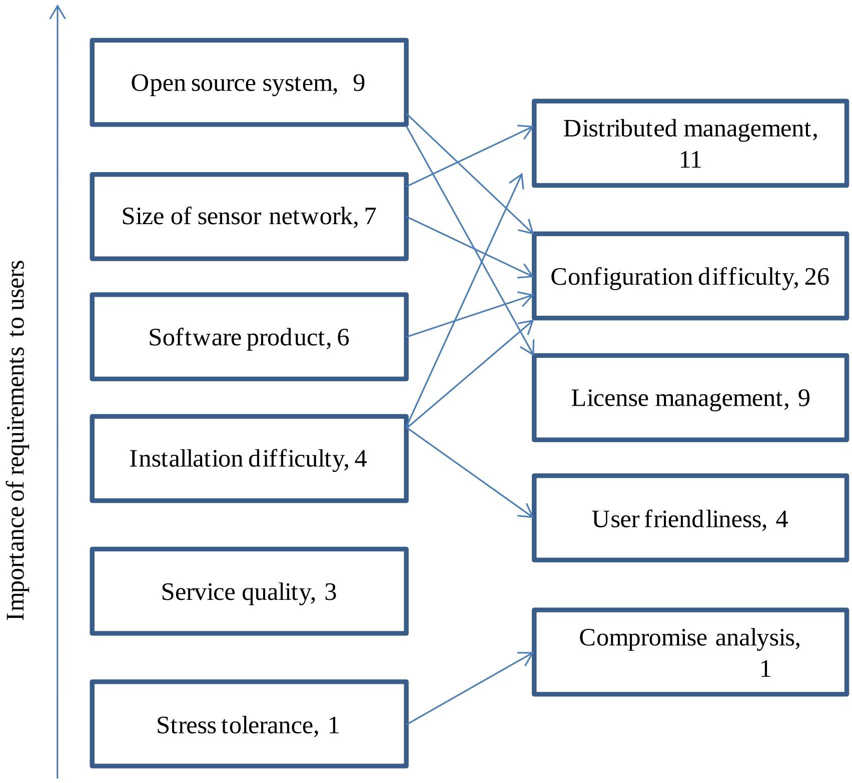

Importance of requirements to users
Open source system, 9
Size of sensor network, 7
Software product, 6
Installation difficulty, 4
Service quality, 3
Stress tolerance, 1
Distributed management, 11
Configuration difficulty, 26
License management, 9
User friendliness, 4
Compromise analysis, 1

Figure 3: Customer necessity to IOT WSNIDS metric load example

VI. CONCLUSION AND FUTURE WORK

A quantity of WSNIDS concepts for IoT are suggested for WSN in the literature, but it turn out to be tough for the customer to pick the among them that encounter their necessities as these concepts vary in types and abilities. In this research work, I suggest a customer essential load-based method to be used for choosing an IOT WSNIDS idea so that it can be realistic for providing safety to WSN. The paper defines numerous stages vital for the select of IOT WSNIDS and in what way customer needs may be loaded. The paper too describes numerous metrics concern with IOT WSNIDS and how to map of these loaded customer needs to these metrics may be completed. Though, I found a number of metrics concerned with IOT WSNIDS concern with customer necessities, but a lot is to be done. The methodology used in this paper may be drawn-out by passing on negative and fraction loads to the customer needs so as to further precise choice of IOT WSNIDS can be finished.

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-Load 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.