Privacy Inferences and Performance Analysis of Open Source IPS/IDS to Secure IoT-Based WBAN

Amjad Ali,[1] Dr. Maruf Pasha,[1] Rabbiah Zaheer,[2] Faiz Jillani,[1] Urooj Pasha[3]
Corresponding: Maruf.pasha@bzu.edu.pk
[1]Department of Information Technology, Bhauddin Zakariya University, Multan, Pakistan.
[2]Department of Physics, Bhauddin Zakariya University, Multan, Pakistan.
[3]Institue of Management Sciences, Bhauddin Zakariya University, Multan, Pakistan.

Abstract
Besides unexpected growth perceived by IoT's, the variety and volume of threats have increased tremendously, making it a necessity to introduce intrusion detections systems for prevention and detection of such threats. But Intrusion Detection and Prevention System (IDPS) inside the IoT network yet introduces some unique challenges due to their unique characteristics, such as privacy inference, performance, and detection rate and their frequency in the dynamic networks. Our research is focused on the privacy inferences of existing intrusion prevention and detection system approaches. We also tackle the problem of providing unified a solution to implement the open-source IDPS in the IoT architecture for assessing the performance of IDS by calculating; usage consumption and detection rate. The proposed scheme is considered to help implement the human health monitoring system in IoT networks

Keywords:
Privacy Inferences, IDS, IPS, IDS tools, WBAN, IoT Security, Performance assessment

1. Introduction

The (CPSs) Cyber-physical systems are usually the extremely interconnected system that is integrated to deliver and respond to the innovative functionalities in the discipline of diverse, including manufacturing, defense, healthcare, and energy. The advancement of technologies like Internet of Things (IoT), and 5th generation (5G) are major players in this research domain. This emerging technologies and advancement led to the expansion of IoT architecture including smart grids, smart cities, smart environment and factories, which has contribution concern to improve the quality of life to live with a cost-effective and components, effective manner.

The IoT lays the backbone of infrastructure for the next generation, enabling future, necessarily urban areas to develop. For such paradigms, Intrusion Prevention Detection System is a nontrivial problem that has attracted many researchers due to a drastic increase of various security threats in such systems[1]. The use of IoT networks has in smart environments has further posed many challenege in terms of security and vulnaerabilities issues caused by malicious entitites[2]. Additionally, the recent theory of Gartner's [3] has also identified the IoT-based attacks as the major reason for various enterprise attacks in 2020, emphasizing the requirement for novel defense strategies. The threats raised due to their insufficient protection are special because of the abundance of such devices in almost every aspect of our lives, devices with minimum or no security mechanisms expose end-users to various security risks. Considering an example, where an intruder somehow gains access to a vehicles devices/sensors then their data would be at highl risk. Once the intruder is inside the vehicles network he can easily spoof the sensors and devices for stealing personal information like GPRS and credit cards information as presented by Geer,D. [4].

Moreover the unexpected development perceived by "Internet of Things" network and sensor technology which are used for cybersecurity and healthcare, has to develop the most challenging features principally by the important increase of vulnerabilities and threads. Despite all the steps taken to defend the IoT devices from potential threats, security risk and their problems will remain apparent due to connecting objects and configuration errors, weak design of network security, including inefficient and inappropriate cryptographic techniques, updates, and poor maintenance.

In the above said emerging threats, to address the required security challenges for substructures behind the smart Environments is dominant [5]. Many researches are being carried out to deal with various aspects of IoT security challenges including the secure frameworks [6, 7], privacy inferences, [8] and authentication mechanisms [9].

There are several possible solutions to detect the abnormalities and intrusion in the real-time network, but such tools and techniques are not appropriate to secure the IoT networks owing to their various kind of restrictions including resource constraint devices, low power consumption. To protect and secure the IoT networks IPDS are utilized for monitoring the network traffic and to observe any single host for preventing malicious activities. Consequently, to reduce and detect the effects of cybercrime, the security system essential to be enforced by conducting real-time surveillance over the WBAN network for intrusion prevention and detection [10].

Manuscript received December 5, 2022
Manuscript revised December 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.12.1

IDPS is an integral part of a typical network security architecture that provides the reflectivity addicted to all activities of the system, permitting sensible prevention and detection to any incident such as malicious activities, undesired events, and all kind of attack which disturb the network services. Following Intrusion prevention and detection system are consider:

In this research paper, we have discussed and highlight the privacy inferences from existing approaches and also proposed the IoT WBAN architecture to implement the Intrusion detection and prevention system which are based on performance evaluation from the current Open source IDS/IPS. We deliberated the most popular IDS/IPS and then measure the performance and proposed the best open source IDS/IPS for IoT architecture. The selection of such three IDS/IPS Snort, Bro, Suricata is validated through the literature review which has considered earlier studies in the domain, as well as the requirement and characteristics of each IDS/IPS. An extended IDS taxonomy can be seen in Figure 1 that include a number of factors in taxonomy including, IDS architecture, usage frequency, Detection method, Response to IDS, Audit source data, and characteristics of Attacks [11]

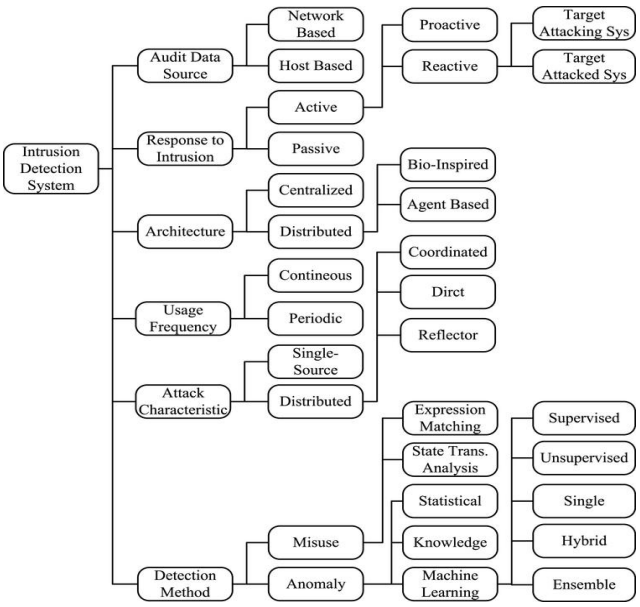

Figure 1 Intrusion detection taxonomy

2. Related work

As per experiments performed by Alhomoud, Adeeb (2011) the assessment on Suricata and Snort by three kinds of different situations on the high-speed traffic. The result in table 1.1 shows clearly that the Suricata performance is much better then snort using FreeBSD and Linux 2.6 when we compare with the virtual Linux in the case of packet drops. Conversely, the Snort results in table 1.2 are much better than Suricata in FreeBSD, the comparison shows the CPU usage which Suricata is high utilization than as compared to Snort. The authors recommend Snort is the best tool in detection rate as compare to Suricata [12].

Table 1.1 Suricata and Snort on different platforms in Packet drops rate

Platform	Suricata	Snort	Ref#
FreeBSD	43.6%	3.24%	[12]
Linux	8.9%	31.43%	[12]

Table 1.2 Suricata and Snort on different platforms CPU usage rate

Platform	Suricata	Snort	Ref#
Linux	68%	27%	[12]
FreeBSD	24.5%	21%	[12]

P. Mehra, et al. [13] proposed the comparison study on the Bro and Snort. He presenting by starting the common evaluation on Snort and Bro and their overall structure, his proposed comparison based on some parameters including Flexibility, Capability, and Speed. The Bro tool is much better to run in the high-speed network as paralleled to Snort, however, Snort can be run and use in all kinds of OS due to GUI interface, as it is very easy to deploy. The authors did not include the detection rate and CPU usage consumption comparison because it is limited to requirements on each intrusion detection and prevention system.

Sforzin, A., et al. [14] (2016). Proposed another IDS for IoT architecture using Snort IDS and Raspberry Pi, by using this approach named RPiDS, the authors perform a report on the memory usage and CPU consumption rate via Snort upon this Raspberry Pi with various snort configurations, the results indicate that Snort has never achieved 100 percent usage, so a Raspberry Pi will host Snort IDS and make the technique conceivable. The results suggest that Snort has never achieved 100% usage, since a Raspberry Pi can host Snort IDS and make the strategy feasible to build a new IoT IDS architecture based on the existing resources, but the authors did not equate snort to those other open-source IDSs such as Suricata or Bro.

Sheikh, N. U., et al. (2018) Proposed another lightweight signature-based IDS which is inspired by the current Open-source Snort, Suricata, and Bro for IoT. [15] The new proposed IDS principle is to link strings with signatures that are configured in the IDS repository. The author suggests four-layer architecture; Pattern Generator, Signature Generator, Intrusion Detection Engine, and Output Engine. The above-said module testing performed

using the offline KDD cup 99 datasets. It remains resigned for the lightweight, but still, the result indicated that the output of IDS is high rate False-positive owing to the signatures with mismatching.

[16] Nam, K. and K. Kim (2018), proposed the SDN based IDS using Suricata, the authors first present the requirement of SDN security, and Suricata marked as a necessity for SDN based IDS, the methodology depends on Suricata integration and analysis using traffic replication, this process copies and transfers all packets that go through the networking devices to a particular server on which Suricata is mounted. As proposed nam, k. and k. Kim (2018) show through Suricata are sent to the OpenFlow tool that blocks the intrusion automatically. Compared to the other current ones, the paper did not state any justification for Suricata IDS' selection.

As proposed by [17] Bouziani, O., et al. (2019). A comparative study in duration attack detection using open-source IDSs such as Snort, Bro, and Suricata, the research approach was based on detailed simulation of such attacks and against three IDSs. Including (Simple LFI, Ping of death, packet Splitting, malicious traffic using Payload and Nmap), The results indicated that each IDS seems to have its detection feature, neither of the 3 Intrusion Detection system is regarded as the best because each has different detection capabilities. Conversely, Bro has measured an important tool for administrators because he gives an overview of network operations, it does not assume it has a high detection rate, it just displays the network traffic better in a logical manner while analyzing them.

3. Privacy implications of IDS

It has been observed that information sensitivity and privacy in the Intrusion Detection System can originate into three kinds of sources in data sensitivity or privacy; input of IDS data, data build in IDS, and data generated by IDS. Salman Niksefat, et al. (2017) [21] discuss the possible privacy issue and also their sensitive fields in individual sources. The fields of privacy conclude by-laws, the demands, and policies of privacy. Furthermore, the requirement of privacy fields can also have been divided into central classes: privacy-preserving identifier fields including IP address, user-name, and other non-identifiers data, including; hostname, URLs, Time-Stamp, Payloads, normal profiles, attack signatures, other non-identifiers. Perception concerning these two groups is expedient in our classification, as different kinds of techniques are mandatory to fulfill them, The Source of Privacy and Sensitive of data is define in following Figure 2.

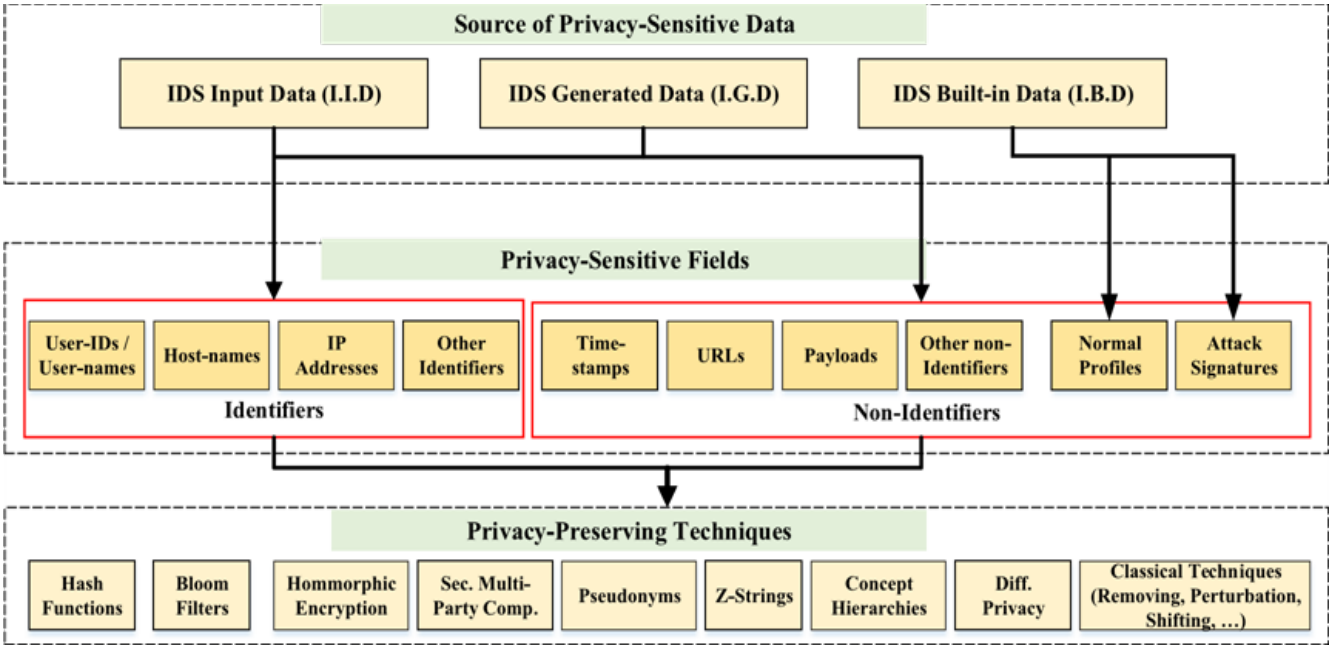

Figure 2. IDS/IPS privacy issues, Techniques

A. IDS input

The input to any IDS is any type of information including network traffic, log files that are identified or forwarded to the IDS for detection of intrusion. The data input of IDS might encompass identifying fields including, username, IP addresses, Hostname, or all kinds of credentials like passwords.

B. IDS built-in data Works and privacy issues

As proposed by Lundin et al. [7] anomaly-based intrusion detection system that could evaluate the data although maintaining the anonymity of regular profiles.The recommended techniques are restricted to pseudonymization of hostname, IP address, username only and, there is not any solution specified for other kinds of privacy-sensitive data.

Trousset et al. [22] introduced Secure Algorithm Execution ensuring (SAX) a secure technique, in which personal information and services are not exposed while intrusion detection. The objective is that IDS may exchange data to other IDSs for evaluation and at the same time maintain the privacy of both data and signatures of IDS. Many limitations exisit in this research, at least four parties are required to support private computing: two separate non-colliding agents, a processing site, and a monitoring site. This assumption limits the application of such a method throughout the absence of trust. To overcome these shortcominghs, Niksefat et al. [21] proposed a signature-based IDS for privacy-preserving that transform the signatures into DFA (Deterministic Finite Automata). The Private payloads were further evaluated against DFA in special secure two-party computing protocols in a quiet way that IDS client does not learn anything about input information and finding of the analysis. Conversely, as mentioned earlier, the technique is computational intensive due to the extremely low computational cost of the underlying cryptographic building blocks.

C. Evaluation Measure

Accuracy, False Alarms, detection rate were tabulated and considered to calculate the any model performance. As Table 1.3 depicts the comparison of IDS privacy tools and methods to evaluate the performance metrics in terms False positive (F.P) and False Negatives (F.N). FP means real attacks information is categorized equally normal. Similarly, false negative actual attacks information classified as normal.

Table 1.3: Privacy comparison False positive (F.P), False Negative (FN) computational and techniques

Method	Computational overhead	(F.P./F.N.?)
Hash functions:	Very Low	No
Bloom filters:	Medium	Yes
Z-strings:	Medium	Yes
Homomorphic Enc:	Very High	No
S.M.C protocols:	Very High	No
Pseudonyms:	Very Low	No
Concept hierarchies:	Low	YES
Differential privacy:	Depend	No

D. discussion and Analysis

The technique requires the provision of integrated data inside the IDSs, including signatures and normal profiles, making techniques more complicated and computational complexity.Table 1.4 presents a comprehsensive survey of recent researches.

Table.1.4 comprehensive survey and contribution of all papers published 2017-2020 in IoT security and privacy

Authors [Ref.]	Year	IoT privacy	IoT security	Block-chain
Kshetri et al. [29]	2017	✓	×	✓
Reyna et al. [35]	2018	×	✓	✓
Banerjee et al. [30]	2018	×	✓	✓
Sharmeen et al. [32]	2018	×	✓	×
Restuccia et al. [31]	2018	×	✓	×
Khan et al. [34]	2018	×	✓	✓
Panarello et al. [36]	2018	×	✓	✓
Kumar et al. [37]	2018	✓	✓	✓
Kouicem et al. [38]	2018	✓	✓	✓
Zhu et al. [39]	2018	✓	×	✓
Xiao et al. [33]	2018	✓	×	×
Hassija et al. [41]	2019	×	✓	✓
Chaabouni et al. [40]	2019	×	✓	×
Costa et al. [42]	2019	×	✓	×
Ali et al. [44]	2019	✓	✓	✓
Wang et al. [43]	2019	×	✓	✓
This Survey	2020	✓	✓	✓

IV. Proposed

A. Privacy-Preserving techniques in IDSs

Different methods may be employed to meet the data privacy needs of IDS, where each technique has its pros and cons. Some strategies can increase the false negative and false positive rate of IDS, or all others can affect the output of IDS

B. Type of Data

IDS can be categorized based on data and information being used for detecting malicious activities. Information gathering during the identification of the correct type of data not only impacts the network efficiency but also affects user privacy and personal information. For example, it is very easy to trace the owner of an IP-address if the system utilizes IP-addresses to evaluate the behaviors of devices. The following challenges identify in the above said.

1. The Information type that is used to identify the optimal performance in detection rate.
2. Privacy and protection of network users, there are two type of data used by current IDS to classify malicious actors
   I. Network trace data
   II. Data log of application layer

The Data log of the application layer is normally associated with the precise kind of information sets. The type of data would include device architecture details and could help for fingerprint in malicious devices. The Network traffic log is the second type of data, similarly IP address and traffic trace provides more details about device activities. Moreover, payload can be considered as another data type, which exchanges all information of user between the devices including, metadata, temperature reading, heart beat, web page.

C. Architecture of System

An IoT intrusion detection approach can perform in two modes: Standalone system, and collaborative system. The stand-alone detection systems are focused on observing traffic patterns in an ISP or a network domain. Such a system operates independently with a network service provider. The standalone system did not keep all the information about the user behaviors and domain consequently. IT could be completely circumvented using smart attacker and stealth method, i.e monitoring network traffic to another domain while targeting large numbers of domains at the same time. To encourage the creation of a collaborative network, an efficient IDS is required to recognize the collective actions of nodes across different domains.

The collaborative solution further divided into two type of groups: (1) "centralized" which alert data from domain collaborators is communicate to a centralised system that identifies traffic sender activity by observing traffic patterns across multiple domains, in (2) the decentralized and distributed settings: here alert info of each service provider (SP) is shared and transmitted in a fully distributed manner without a centralized coordinator. The main challenge concerning the design of collaborative IDS/IPS is regarding information used for detection to protect the privacy. The ISP (Internet service provider) or domain are unwilling to share information of the users with each other while they risk the privacy of various customers. A trusted centralized authority can resolve privacy issues if the central authority guarantees that the data they generate cannot be misused or leaked. Moreover, usage of cryptographic approaches or noise data addition could reflected to anonymize user information; nevertheless, this will be expected to massively increase bandwidth requirements and computational time.

D. Analysis

Throughout this portion, we discussed the privacy inferences of IDS in IoT networks and open challenges in security and privacy as shown in table 1.5. The most important concerns are, the information type used for collaboration, and the architecture of the system. Firstly, the intrusion detection system architecture specifies whether an individual transfers the information in the detection system. The detection system must install on the end-user devices, such (IoT devices), and also install at the edge point router (smart home or network entry point) control locally using record information from a single source. The standalone system can only be used for information from a single source. Hence, it does not have high accuracy and performance. After all, the collaborative method operates on a centralized architecture, as mentioned in [18, 19, 20]. The protection of integrity and privacy of information envisioned in a centralized setup. Still, this might not be possible since an attacker may violate the privacy and integrity of all collaborators must breach only one device. Moreover, a centralized system presents other security challenges such as single-point-failure.

- The data transmission to other stakeholders is highly risky for privacy in a centralized system. Throughout this environment, four approaches may operate in the collaborating system. Transmission of raw information to a centralized system or further devices, which process all information to make significant decisions. There is no privacy preservation in this technique as information may be revealed to other individuals, thus increasing computational load.
- The transmission of processed data, such as exchange of host or IP address traffic statistics, often brings a privacy threat, however without demanding considerable additional resources
- Encryption on information exchange requires the privacy preservation, but on the other hand needs extensive computation for the transmission of encrypted data.

Table 1.5 Privacy and security open challenges.

Security Challenges	Privacy Challenges
Security in CIA triad in IoT system addresses	User information privacy addresses
Encryption/decryption both algorithms are being used in the security of IoT	Third-party restricted to use the data without user permission
Data confidentiality	Domain data confidentiality

Create assurance and full confidence in data	Choose, how, if, and what whom type of information is need to shared

A. IoT based WBAN

IoT 's primary objective is to make human life a little easier and conveniently facilitate the interactions between the environment and human health. Funding on IoT applications and also use cases is exponentially growing, with approximately 256 billion U.S. dollars divided into various areas by 2020.

According to Boujrad, M., et al. (2020) domains are characterized into 6 classes as shown in table 1.6.

Table 1.6 Domain and Classes

Sr #	Domains	Classes
1.	Mobile	Awareness about route, traffic, pollution, etc.
2.	Utilities	Saving cost and time
3.	Environmental monitoring	River height, Wind, Rainfall
4.	Smart City/Home	safety and security for the owners
5.	Smart Business	tracking goods and assets
6.	Healthcare	identification of patients and stuff

In this research paper we are going to proposed IoT WBAN through applying Open0Source IDS/IPS on WBAN architecture which is bases on Four layers attractive in to the consider the specification of individually layer.

B. Wireless Body Area Network (WBAN)

A WBAN is a singular kind of WSN that is related to the human body, where little sensor nodes were positioned on the body of the patient compared with the conventional wireless sensor network. A lightweight, low power, wearable, or implantable sensor node is the key requirement of any WBAN. A WBAN consists of a collection of non-homogenous sensors and medical equipment that play vital role in patient health monitoring. A radio frequency-based WBAN Technology for wireless networks that interconnect measuring devices (Sensors) that are applied on or in the human body. Continuously calculating biological systems including biological functions, Blood pressure ECG for heart rate, electrical activity, temperatures, and sensors of motion. To inform these sensors are used for better and quicker, health parameters for a remote service center Diagnostic medicine. It is important to help regulate the condition of the body across daily activities despite having to lie in bed by sending continuous data that can be analyzed by middleware. In this study, in this paper, we adopt four-layer architecture to reflect the IoT architecture

C. Open Source Intrusion Detection Systems:

We have presented various open source IDS as shown in figure 3 and performed in depth comparison of each.

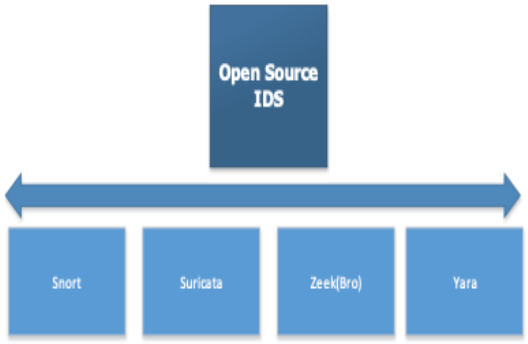

Figure 3. Open IDS

Snort:

Snort is a network intrusion detection tool that developed in 1998 by Martin Roesch. The Snort is a multi-platform, lightweight, and commonly used open-source that is a very fast intrusion detection tool that detects the attack and also prevents in real as well as a virtual environment. Snort is not only a rule base but also works as signature base IDS, which produces alarms on the base of a predefined set of rules, to preprocessing the network traffic after capturing. The Snort also provides an opportunity to download the signature of attack by their official source and also can be used by the network engineer to detect such kind of attacks. The Snort not only analyzes the network traffic can also be used for network packet sniffer, packet logger, content matching, analysis of protocols, and typically often used dynamically impassively detect or block the range of attacks, such as buffer overflows, Stealth Port-scan, web-application attack, SMB probes, the attempt of fingerprinting on OS (operating system). Figure 4 shows the basic building blocks of snort.

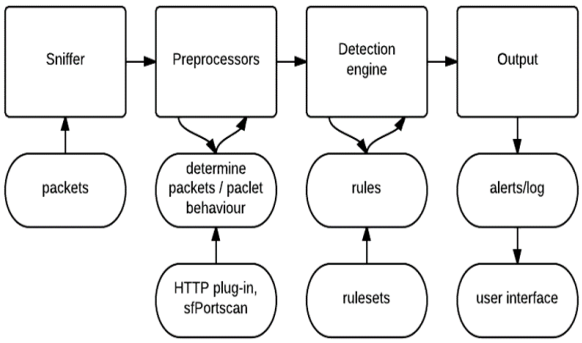

Figure 4. Working of Snort

***Suricata**:*
Suricata is also an open-source GUI tool developed in 2009 and released in 2010 by OISF (Open Information Security Foundations). It is the same as Snort but one of the main functions of Suricata is multithreading, which is extra efficient and scalable than Snort because Snort works on Single-thread. SIEMs, databases, and JOSN for the output and input files to ensure good integration with such tools, including as used by Suricata YAML. Due to its GPU acceleration and its multithreading competencies, Suricata's workload is often distributed. The multithreading function is scalable and more powerful than Snort. Since Snort only works with Single Thread, it is costly to have such powerful and strong capabilities because significant amounts are required to execute the project smoothly as shown in Figure 5.

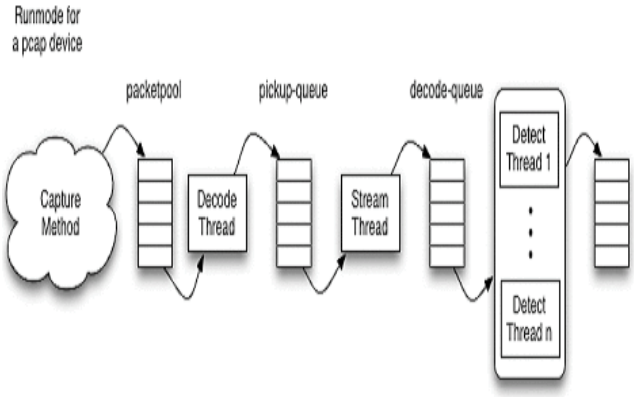

Figure 5. Suricata IDS/IPS workflow

***Zeek (Bro)**:*
Bro was develop by (Vern Paxson) in (NRGLBN) Laboratory, Bro IDS also can monitor network traffic as well as analyses; it can detect using the anomaly-based detection technique. Bro IDS is one of exclusively IDS only that has functioned as an Intrusion prevention system. Bro can also use to run on the UNIX operating system. Bro work on multi-layers' exploration by packet, captured matching with events and signatures for all kind of possible attacks, to produce logs the Bro performs rule-based scripts on stream events as represented in Figure 6.

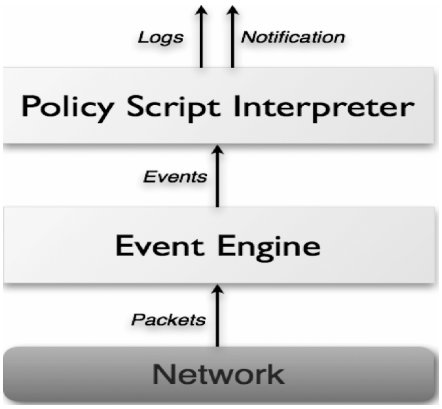

Figure 6. Zeek workflow

Yara
Yara is open-source, multi-platform and host-based IDS designed for malware researcher use to classify the samples of malware, misused recognition yara used as a detection method. This tool is use to write patterns in their own rules of language that are formerly examined for in a scanned file as discussed [23]. The rules of yara contain into two logical-parts, conditions and strings. The condition part guides how they're being paired and the String could be binary, regular expressions, text.

a. Security threats analysis:

Issues related to security are growing at multiple levels of different forms, including new threats and vulnerabilities. Due to rapid development of the IoT sector and increase in usage of IoT worldwide, the associated threats have also emerged [24]. As per a recent report by OWASP the IoT projects top level 10 security anxieties to avoid when creating, deploying, managing, or using in IoT environment, that security concerns are based on an investigation of all collected information provided via their experts and professional from the Security industry. The following list contains the major issues in the IoT environment depending on a different level of Internet of things architecture:

- Guessable, weak or hardcoded passwords
- Network services insecure
- Ecosystem interfaces insecure
- Shortage of secure mechanism update
- Outdated components or use of insecure
- Privacy protection insufficient
- Insecure Storage and data Transfer
- Shortage of device management
- Default setting Insecure
- Shortage of physical Hardening

Table 1.6. Assessment of three IDS Snort, Suricata and Zeek

Parameter	Intrusion Detection/Prevention System		
	Snort	**Suricata**	**Bro**
Multi-thread:	No	YES	YES
Operating System:	All	All	All
Developer:	Source-fire	Open information security foundations	NRGLBN lab
Rules:	SO rules, VRT Rules, Pre-processor Rules, Emerging Threats rules	Emerging threats rules, VRT Snort Rules	Emerging threats rules, Snort Rules,
Installation:	Using packages, or manual	Manual or using package	Manual or using package
User-friendly:	Provide solutions to common issues and More	Less	Less
Documentation:	Well-documented	Not well-documented	
Cost:	Commercial Version has a price	Free	Free
GUI:	Large number of compatible	Very-Few	
High-speed network support:	Not present	Present	Present

b. EXPERIMENTAL RESULTS:

Table 1.6 summarizes assessment of three open source IDS. Moreover, we use three metrics of performance to compare and calculate the performance of three IDS named (Snort, Suricata, and Bro) in different test circumstances. The following selected parameters are those metrics, which are purely base on the impact of the performance of any Intrusion Detection System. Following parameters are select for evaluation:

Packet drop: the total number of packets, which remain, dropped and not checked by IDS tools. It shows the less performance of IDS tools if they give more values of drop packets.

CPU utilization: It depicts total amount of processing cycles utilized used by the process.

Memory Utilization: it is the total quantity of physical memory consumed by the process.

In an attempt to validate the effectiveness of the open-source IDSs, selected two different experiments were perform:

1. **Detection Performance**:

It is also not sufficient to have robust intrusion detection to analyze the performance of the IDSs, bypassing infected and normal packets into them and see how many infected packets will be detected by each of the three IDSs to determine the message (Alert/ report) provided by each one, although that is not enough to detect without giving the true value of the intensity of the attacks as depicted in figure 7.

2. **Usage Consumption**:

The usage consumption test required if we have to implement the IDS on the Gateway level, it should not have required much, considering the limitations of all kinds of resources.

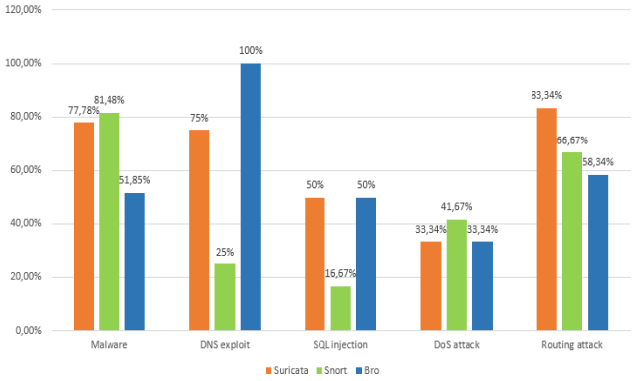

Figure 7. Summary of detection rate of Suricata, Snort and Bro on the different attacks.

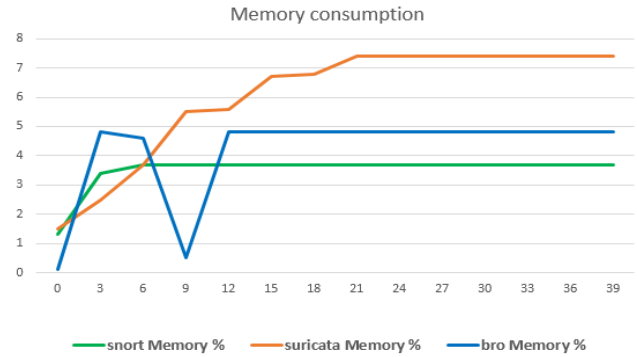

Figure 8. Memory Consumption

Table 1.7 list of Security attacks, issues and challenges in current IoT environment

IoT layers	Security Issues/Attacks	Security Parameters	REF #
Perception layer	Fake node, Node Capture, node mass authentication, key management and cryptographic algorithm	Integrity, Confidentiality, authentication	50
Middleware layer	Problems of cluster security, Spoofed and DoS attacks, replayed and altered routing information	integrity, Authentication	47,48, 49
Network Layer	Smart decision-making processing of large data, control suspicious information, attack using malicious code, multi-party authentication	Confidentiality ,Integrity	46
Application Layer	Issues in authentications and information access, recovery and protection of data, software vulnerabilities, spear-phishing, clone and reliability attack	access control, Information privacy	45

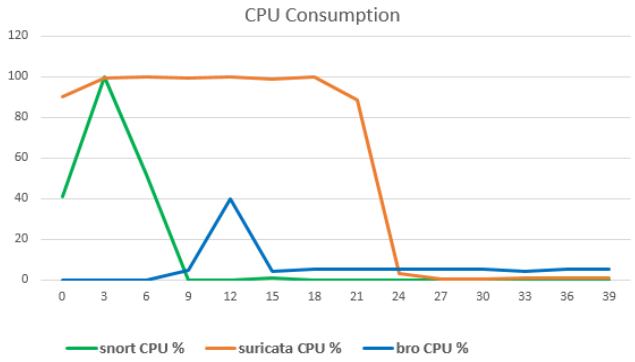

Figure 9 CPU consumption

In this experiment, we can see the result, Suricata is the best intrusion detection system between the above said IDS/IPS, given the fact that in certain vulnerabilities including DNS exploitation it reported less rate of detection, it is still the effective way to generate an alert message that best describes in this circumstance. We select Snort for the same purpose as the second one IDS, Bro is quite constrained to the response generated while discovering vulnerabilities. The Snort was a less consuming IDS among those in CPU with 0% when it became stabilized and 3 to 7% of memory. Suricata has been less intensive than Bro throughout CPU use at 1% when it became stable relative to Bro, which stayed at 5% as shown in Figure 9. Although at the preliminary step Suricata is almost overloaded by itself 1 core if CPU after passed the launching point. Suricata works with a multi-core that explains their low consumption. The usage of Memory; Bro was less consuming unlike Suricata at 4 to 8% especially in comparison to Suricata at 7 to 4% as represented in Figure 8. For even a resource-restricted platform that we might suggest using Snort, therefore Suricata would be the best alternative if there is no restriction of the resource.

c. WBAN Four layer Architecture

Table 1.7 summarizes list of Security attacks, issues and challenges in current IoT environment.

Perception layer:

The physical layer also called the Perception layer, this layer is composed of IoT devices such as actuators, sensors, and controller. This layer used the sensor sensors including, Bluetooth, RFID, 2-D barcode, and Near-Field communication the devices are made-up of different types including (smartphones, Mobile Devices, Tablets, Single-board computers, microcontroller units). This layer gathers environmental details including, vibration, location, humidity, temperature parameters.

Network layer:

Main connectivity layer that defines a different kind of protocols and communication network such as, Bluetooth, Lora, WiFi) used for the connectivity, playing a role as the edge where the data collected could be managed. The network layer's aims to expend communication far beyond BAN. The network layer allows WBAN to work by public network on the internet, including Wireless sensor network, data center, external servers, health monitoring system, etc. Through appropriate routing protocols, the WBAN data will sent efficiently to remote locations for health monitoring purposes [27]. The functioning and routing protocols of the network layer intends to take account of factors including data-centric technique, low-power consumption, data aggregation attributed-based addressing and fusion, etc. [26].

Cloud/ Middleware layer:

This layer implements a distributed architecture where IoT information is processed or analyzed before it could be transfer to the application layer. This layer exploits the development of technology such as data, cloud computing, and big data processing. The above-said layer has some advanced features of massive processing of data later it became difficult often to handle a large amount of data [52]. Moreover, filter the malicious data, dealing with suspicious information, and recognize valid information is one of the major problems in the middle layer [51]. The intruder could easily modify the information using malicious data and can acquire valid data lists or network information and ccan trigger system crash.

Manuscript received December 5, 2022
Manuscript revised December 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.12.1

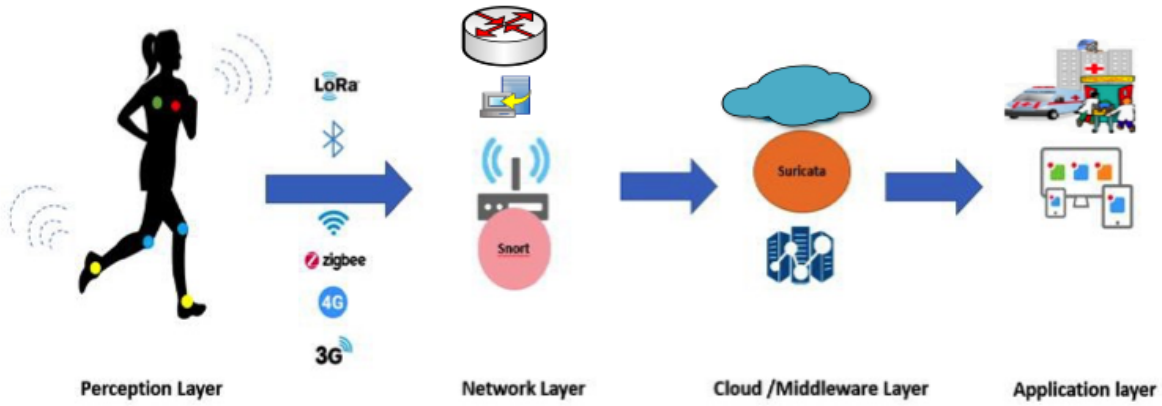

Figure 10. Secure WBAN Proposed architecture

Application layer:

The Application layer provided the facility of interface managing for WBAN data querying and managing. In furthermore, such a layer is also answerable for time synchronization and node localization. The application-specific is the implementation of the application layer in WBAN, but the most important feature of the application layer in the WBAN context is to ensure a secure environment for remote access to sensitive medical information [28]. Such a layer provides visualization of data given by IoT devices: essentially, this system includes personalized services that meet user needs.

Through, Suricata implementation on the Middleware layer, combined with Snort has been introduced on Gateway/network layer; we have introduced new approach that is based on current Open-source IDS/IPS, which would detect the intrusion on WBAN framework. Considering all requirement of IoT system and through performing a complete review of the most prominent but successful existing IDS/IPS: Snort, Suricata, and Bro, the very last one has been dropped because it has not shown any significant results as compare to other two IDSs. The decision of using such open-source IDSs were demonstrated by the fact that they are rules / signature-based which indicates that they can detect all current attacks and their signatures remain stored in the knowledge base, nor do they produce any false positive or true negative compared to other methods of IDS (anomaly-based, specification-based), that were very significant in WBAN frameworks.

V. Conclusion

This paper examined up to date intrusion detection system focused on memory usage, privacy concerns and

CPU of IoT metrics implementing suricata joined with Snort on the cloud layer which implement on gateway/network layer, manage to offer a new approach on existing (open source) IDSs, it can detect anomalies on WBAN system taking into consideration all specification of IoT system. By doing an extensive study on Open-source IDSs: Snort, Suricata, and Bro. Bro and Snort have different functions and, they behave differently in terms of architecture and functions. Suricata has a multi-threaded architecture that requires more memory and CPU resources than Snort. The purpose of thesis open-source IDSs was that they detect all the standing attacks because of their rule/Signature based nature. As compared to other IDSs they do not generate any false positive or true negative (anomaly-based, specification-based) and, a signature is stored in the knowledge base, which is vital criteria for WBAN systems. Figure 10 presents a secure WBAN architecture.

References

[1] Boujrad, M., et al. (2020). Performance Assessment of Open Source IDS for improving IoT Architecture Security implemented on WBANs. Proceedings of the 3rd International Conference on Networking, Information Systems & Security.

[2] Habibzadeh, H.; Nussbaum, B.H.; Anjomshoa, F.; Kantarci, B.; Soyata, T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustain. Cities Soc. 2019, 50, 101660.

[3] Gartner. Gartner's Top 10 Security Predictions 2016. Available online: https://gtnr.it/2vRorda (accessed on 1 February 2020).

[4] Geer, D. The Internet of Things: Top five threats to IoT devices.Available online: https://bit.ly/2UVixkF (accessed on 1 February 2020).

[5] Ande, R.; Adebisi, B.; Hammoudeh, M.; Saleem, J. Internet of Things: Evolution and technologies from a security perspective. Sustain. Cities Soc. 2019, 54, 101728, doi:10.1016/j.scs.2019.101728.

[6] Riahi, A.; Challal, Y.; Natalizio, E.; Chtourou, Z.; Bouabdallah, A. A Systemic Approach for IoT Security. In Proceedings of the 2013 IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), Cambridge, MA, USA, 20–23 May 2013

[7] Jesus Pacheco, S.H. IoT Security Framework for Smart Cyber Infrastructures. In Proceedings of the IEEE International Workshops on Foundations and Applications of Self* Systems, Augsburg, Germany, 12–16 September 2016.

[8] Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017.

[9] Yao, X.; Han, X.; Du, X.; Zhou, X. A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications. IEEE Sens. 2013, 13, 3693–3701.

[10] Sundararajan, T. and A. J. J. o. C. S. Shanmugam (2010). "A novel intrusion detection system for wireless body area network in health care monitoring." 6(11): 1355.

[11] Al-Utaibi, K. A., et al. (2018). "Intrusion detection taxonomy and data preprocessing mechanisms." 34(3): 1369-1383.

[12] Alhomoud, Adeeb & Munir, Rashid & Pagna Diss, Jules & Awan, Irfan & Al-Dhelaan, Abdullah. (2011). Performance Evaluation Study of Intrusion Detection Systems.Procedia CS. 5. December 2011, DOI: 173-180. 10.1016/j.procs.2011.07.024.

[13] P. Mehra, "A brief study and comparison of snort and bro open source network intrusion detection systems," International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 6, August 2012, ISSN : 2278 – 1021

[14] Sforzin, Alessandro & Gomez Marmol, Felix & Conti, Mauro & Bohli, Jens-Matthias. (2016). RPiDS: Raspberry Pi IDS — A Fruitful Intrusion Detection System for IoT. 440-448. July 2016, DOI: 10.1109/UICATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0080.

[15] Sheikh, N. U., et al. (2018). "A Lightweight Signature-Based IDS for IoT Environment."

[16] Nam, K. and K. Kim (2018). A study on sdn security enhancement using open source ids/ips suricata. 2018 International Conference on Information and Communication Technology Convergence (ICTC), IEEE.

[17] Bouziani, O., et al. (2019). A Comparative study of Open Source IDSs according to their Ability to Detect Attacks. Proceedings of the 2nd International Conference on Networking, Information Systems & Security.

[18] Haddad Pajouh, H.; Javidan, R.; Khayami, R.; Ali, D.; Choo, K. A Two-layer Dimension Reduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks. IEEE Trans. Emerg. Top. Comput. 2016, 7, 314–323.

[19] Chordia, A.S.; Gupta, S. An Effective Model for Anomaly IDS to Improve the Efficiency. In Proceedings of the International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, India, 8–10 October 2015.

[20] Wang, K.; Du, M.; Yang, D.; Zhu, C.; Sun, Y. Optimal Active Detection in Machine-to-Machine Mobile Networks: A Repeated Game Approach. In Proceedings of the IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016.

[21] Salman Niksefat a, Parisa Kaghazgaran b,*, Babak Sadeghiyan a Privacy issues in intrusion detection systems: A taxonomy, survey and future directions. APA Research Center, Amirkabir University of Technology, Tehran, Iran b Texas A & M University, TX, USA.

[22] François Trousset, Pascal Poncelet, Florent Masseglia, SAX: a privacy preserving general purpose method applied to detection of intrusions, in: First International Workshop on Privacy and Anonymity for Very Large Databases, ACM, 2009, pp. 17–24.

[23] (Accessed 5.7.2019), Yara documentation. URL: https://yara.= readthedocs.io/en/v3.5.0/index.html.

[24] Kozlov, D., et al. (2012). Security and privacy threats in IoT architectures. BODYNETS.

[25] D L. Filipe, F. Fdez-Riverola, N. Costa, A. Pereira, Wireless body area networks for healthcare applications: protocol stack review, Int. J. Distributed Sens. Netw. 11 (10) (2015).

[26] L. Filipe, F. Fdez-Riverola, N. Costa, A. Pereira, Wireless body area networks for healthcare applications: protocol stack review, Int. J. Distributed Sens. Netw. 11 (10) (2015).

[27] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Comput. Network. 38 (4) (2002) 393e422.

[28] T. Penzel, B. Kemp, G. Klosch, A. Schlögl, J. Hasan, A. Varri, I. Korhonen, Acquisition of biomedical signals databases, IEEE Eng. Med. Biol. Mag. 20 (3) (2001) 25e32.

[29] Kshetri, N. J. T. p. (2017). "Blockchain's roles in strengthening cybersecurity and protecting privacy." **41**(10): 1027-1038.

[30] Banerjee, M., et al. (2018). "A blockchain future for internet of things security: a position paper." **4**(3): 149-160.

[31] Restuccia, F., et al. (2018). "Securing the internet of things in the age of machine learning and software-defined networking." **5**(6): 4829-4842.

[32] Sharmeen, S., et al. (2018). "Malware threats and detection for industrial mobile-IoT networks." **6**: 15941-15957.

[33] Xiao, L., et al. (2018). "Secure mobile crowdsensing based on deep learning." **15**(10): 1-11.

Manuscript received December 5, 2022
Manuscript revised December 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.12.1

[34] Khan, M. A. and K. J. F. G. C. S. Salah (2018). "IoT security: Review, blockchain solutions, and open challenges." 82: 395-411.

[35] Reyna, A., et al. (2018). "On blockchain and its integration with IoT. Challenges and opportunities." 88: 173-190.

[36] Alfonso Panarello Id and Nachiket Tapas. 2018. Blockchain and IoT Integration : A Systematic Survey.

[37] Kumar, N. M. and P. K. J. P. C. S. Mallick (2018). "Blockchain technology for security issues and challenges in IoT." 132: 1815-1823.

[38] Kouicem, D. E., et al. (2018). "Internet of things security: A top-down survey." 141: 199-221.

[39] Xiaoyang Zhu and Youakim Badr. 2018. Identity management systems for the Internet of Things: A survey towards blockchain solutions. Sensors (Basel, Switzerland) 18, 12 (2018), 1–18

[40] Chaabouni, N., et al. (2019). "Network intrusion detection for IoT security based on learning techniques." 21(3): 2671-2701.

[41] Hassija, V., et al. (2019). "A survey on IoT security: application areas, security threats, and solution architectures." 7: 82721-82743.

[42] da Costa, K. A., et al. (2019). "Internet of Things: A survey on machine learning-based intrusion detection approaches." 151: 147-157.

[43] Lin, Y., et al. (2015). "Performance evaluation of remote display access for mobile cloud computing." 72: 17-25.

[44] Ali, M. S., et al. (2018). "Applications of blockchains in the Internet of Things: A comprehensive survey." 21(2): 1676-1717.

[45] Kumar, S. A., et al. (2016). Security in internet of things: Challenges, solutions and future directions. 2016 49th Hawaii International Conference on System Sciences (HICSS), IEEE.

[46] Razouk, W., et al. (2017). A new security middleware architecture based on fog computing and cloud to support IoT constrained devices. Proceedings of the 1st International Conference on Internet of Things and Machine Learning.

[47] Kraijak, S. and P. Tuwanut (2015). A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. 2015 IEEE 16th International Conference on Communication Technology (ICCT), IEEE.

[48] Turkanović, M., et al. (2014). "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion." 20: 96-112.

[49] Cárdenas-Haro, J. A. and M. Dawson Jr (2019). Detecting and Preventing File Alterations in the Cloud Using a Distributed Collaborative Approach. 16th International Conference on Information Technology-New Generations (ITNG 2019), Springer.

[50] Zhao, K. and L. Ge (2013). A survey on the internet of things security. 2013 Ninth international conference on computational intelligence and security, IEEE.

[51] Bouloukakis, G., et al. (2019). "Automated synthesis of mediators for middleware-layer protocol interoperability in the IoT." 101: 1271-1294.

[52] Kraijak, S. and P. Tuwanut (2015). A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. 2015 IEEE 16th International Conference on Communication Technology (ICCT), IEEE.