*International Journal of Latest Trends in Engineering and Technology*
*Vol.(9)Issue(3), pp.258-267*
*DOI: http://dx.doi.org/10.21172/1.93.43*
*e-ISSN:2278-621X*

# AN ANALYTICAL APPROACH TO ENHANCE THE INTRUSION DETECTION IN INTERNET OF THINGS NETWORK

RaviTeja Gaddam[1] & Dr. M. Nandhini[2]

**Abstract: Advancement in technology promising the future by connecting everything. The Internet of Things (IoT) makes it possible to connect and access every device through the Internet. Billions of devices are connecting and the count is increasing. IoT essentially constitutes several smart devices that widely vary in size, complexity, and usage. IoT is driving the world towards a new era and it is changing the way of our lives. Even though this superior connectivity will certainly improve our quality of life, it also nurtures severe security and fidelity problems. IoT objects have limited resources which complicates in applying conventional security practices and they are more vulnerable to critical attacks like Denial-of-Service attack, eavesdropping, sinkhole attack, etc. This paper surveys on latest security features and solutions of IoT and also analyses several security challenges that are to be taken into consideration while enhancing the security of IoT. In the coming future, IoT will be the key hub to connect several smart objects that are with different technologies and allowing various applications to interact with them in a safe manner is the main focus of researchers. To enhance the security and to provide efficient intrusion detection in IoT network, we propose an architecture with a possible usage of single board computer like Raspberry Pi and Snort, an open-source intrusion detection tool. We also discuss some potential directions to deploy the enhanced Snort on Raspberry Pi device.**
**Keywords: Internet of Things, security, attacks, intrusion detection, Snort, Raspberry Pi**

## 1. INTRODUCTION

Technological advancements in networking make the Internet to connect everything. Internet of Things (IoT) can be treated as the future Internet. IoT systems interconnect real-world sensors, small devices and systems to attain deeper automation, exploration, and integration in a system.

Also, the energy capacity, computing power, and storage capabilities of small sensing devices have considerably enhanced whereas their sizes have reduced significantly. These technological developments have led to an exponential growth in the count of Internet associated devices that can provide enormous services.

According to CISCO IBSG projections as shown in Figure 1, by 2020, the total of Internet-connected devices is likely to grow to 50 billion [1]. This growth is not because of the population rather the usage of devices and their technologies in everyday life.

Even though this superior connectivity will certainly improve our quality of life, it also raises severe security problems. The recent report of Akamai Technologies depicts that the most vulnerable attacks target the IoT devices [2]. Mirai malware created chaos recording the largest attack at 109Gbps. McKeay, the senior security advocate at Akamai Technologies, explained that these devices use open source codes which makes them more vulnerable to Mirai-based attacks.

IoT devices can share the data through the Internet by accessing different devices. This transmission of sensitive data can attract the attackers and makes the IoT networks as their primary target for cyber-attacks. In general, IoT devices communicate using wireless technology and makes them more vulnerable to several attacks like tampering, man-in-the-middle attack, sinkhole attack, Denial of Service attack, eavesdropping, etc.

Besides, conventional security mechanisms are not preferable due to the resource-constrained nature of IoT nodes. Other types of security enforcement approaches, such as intrusion detection system must be considered to safeguard the IoT networks. Intrusion Detection System (IDS) detects malicious actions or policy violations by monitoring the system actives or network traffic. IDS is generally a hardware or software which can be integrated into the current system. It is suitable for the resource constrained or inherited systems to protect their network security.

[1] Research Scholar, Dept. of Computer Science, Pondicherry University, Puducherry, Tamil Nadu, India
[2] Assistant Professor, Dept. of Computer Science, Pondicherry University, Puducherry, Tamil Nadu, India

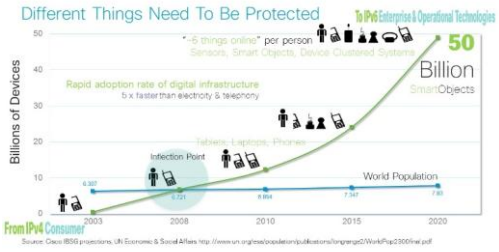


Figure 1. CISCO IBSG Projections

.

Currently, security in IoT network is attracting researchers and academicians as many worldwide organizations are involved in the development of IoT based systems. A number of IDS methods were proposed and developed by several recent works but they are not incomplete as the research efforts are presently trying to discover possible threats and provide countermeasures against them.

This paper tries to analyze several attacks that are targeting the IoT network and discusses the recent works to provide security for IoT. We also propose an architecture for efficient IDS in IoT network.

The organization of the paper is as follows: In Section II, we discuss a general IoT architecture followed by discussing various attacks on IoT networks in Section III. In Section IV, authors deliberate the security in IoT followed by discussing several recent works in IoT in Section V. Section VI discusses various IoT challenges followed by proposing an architecture for better intrusion detection in IoT in Section VII. In Section VIII, we make a conclusion and discuss future work

## 2. GENERAL IOT ARCHITECTURE

The main purpose of IoT is to enable the objects to be connected using any network from anyplace. So the main focus of IoT is to identify suitable policies about configuration and interconnection of various sensors and devices [3]. CISCO proposed an IoT reference model to describe the functions of IoT elements.

The IoT Reference Model standardizes the terminology of IoT. As shown in Figure 2. Level 1 to Level 7 specifies the physical devices and their association for information processing and applications.

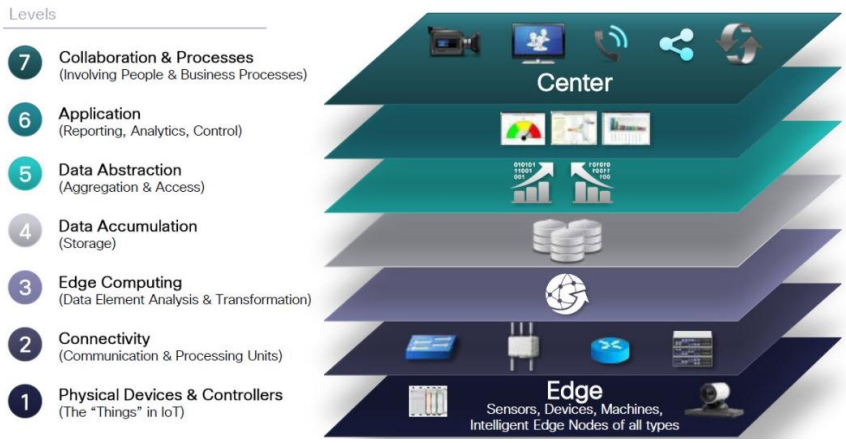


Figure 2. IoT World Forum Reference Model

By considering this model along with some recent studies like [4], a simplified model can be derived as shown in Figure 3.

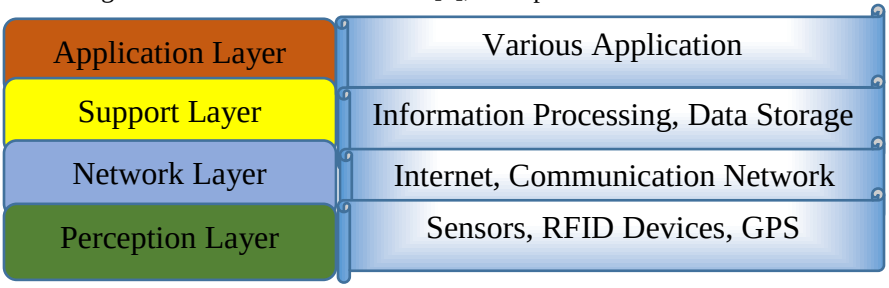


Figure 3. Simplified IoT Model

*Layer 1 - Perception Layer:*
The main purpose of this layer is to identify the objects and collecting information using their sensors. This layer contains technologies that are related to sensors, embedded devices, and tagging.

*Layer 2 - Network Layer:*
This layer reasonability is to transfer the collected data to the processing system. For this purpose, it contains the communication networks like the Internet, mobile communication, and Wireless Sensor Networks.

*Layer 3 - Support Layer:*
The main purpose of this layer is to process the data, analyze it and store in a database. This data can be used on demand because it is available all the time. For this purpose, this layer contains information processing systems and data storage systems.

*Layer 4 - Application Layer:*
All the useful applications that are specific to users or industry are available in this layer. Applications like Smart Home and Smart Traffic are some of them.
After discussing the IoT model and its layer-wise functionalities, next section discusses various possible attacks on the IoT devices.

## 3. ATTACKS ON IOT NETWORKS

IoT systems collect and process an enormous amount of data that can be used by normal users or industries. This makes the IoT as a primary target for many hackers [5]. Sensitive information from IoT systems like location data, financial data, credit card numbers, etc. can be hacked by the potential attackers. In addition, they may compromise IoT elements like nodes, to attack the third party entities [6]. For the better understanding the security threats in IoT, we briefly discuss some potential cyber-attacks on IoT applications as shown in Figure 4.

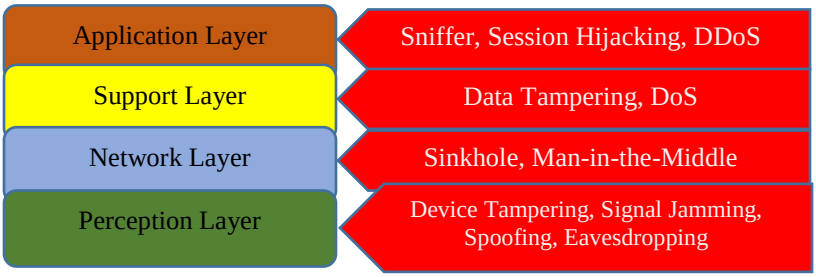


Figure 4. Layerwise Attacks on Simplified IoT Model

Device Tampering: In this attack, attacker physically swaps the original sensor node with malicious node. With this attacker can harm the network by getting total control of it.
Signal Jamming: Obstructing the communication channel among the nodes is the main target of this attack.
Spoofing: A fake broadcast message will be sent to the network by the attackers and they make it assume as from the original node. It may lead the attacker to gain full control of the system making it vulnerable.
Eavesdropping: Being wireless, RFID system may give the possible situation that Sensitive information like a password can be snooped by the attacker while the data is flowing.
Sinkhole Attack: This attack tries to congest the network and increases the energy consumption of nodes. The sinkhole creates conflict among malicious node and neighboring nodes to gain the communication channel access. This may lead to other critical attacks like denial of service attacks.
Man-in-the-Middle Attack: It is like eavesdropping in which the hacker can observe or control the communication between the two parties. To get more information, a hacker may falsify the identity and communicate without any doubt.
Data Tampering: To attain the personal benefits, one of the insiders tampers the data by extracting or modifying the IoT objects data.
Denial of Service Attack: This attack targets the availability feature and tries to shut down the system to make it unavailable.
Sniffer: To take sensitive information from the traffic, an attacker can implant sniffer or logger programs. It mainly tries to steal files, passwords and message texts.
Session Hijacking: To exploit the defects in session management, this attack discloses the user identities. Taking identity of others, an attacker can do whatever he wants.
Distributed Denial of Service (DDoS) Attack: This attack is same as DoS attack except that it can be done by taking control of multiple victims and making them as attackers.

As the technology is developing rapidly, so as the sophistication in attacks. Above discussed attacks are few and more novel attacks may target the IoT networks. In order to provide more security for IoT devices, next section discusses major requirements of IoT security.

## 4. IOT SECURITY REQUIREMENTS

Exponential growth in versatile devices that are interconnecting will be an affecting factor while providing the security in practical benefits of IoT [7]. After discussing various recent studies in IoT, this section describes the major security requirements in IoT [8].

While designing security mechanism in IoT network, the major security requirements that are to be focused are

- ✓ Confidentiality: Protecting the data transmissions from the third party
- ✓ Integrity: Providing the data without tampering
- ✓ Availability: IoT services should be available and should withstand operational failures.
- ✓ Authentication: Sensitive information must be accessed by legal users.
- ✓ Authorization: Granting privileges to devices in only accessing the necessary resources.

## 5. RECENT WORKS IN IOT

For a better understanding of the security requirements and solutions to IoT related problems, this section discusses various recent studies in IoT.

Martha Daniel discussed some real-world challenges in IoT in [9]. The author insisted how the daily life devices are communicating using current technology. While discussing security risks, the author mentioned two situations where the smart devices were under third-party control. One was car hijacking and other was malware attack on National Health Service network. Author briefed some techniques to protect the IoT from cyber-attacks. Techniques like protecting identities using cryptographic algorithms, alerting the intrusion automatically, and regularly updating the firmware will protect the IoT smart devices.

In [10], authors made some recommendations to minimize the security risks in IoT network. They suggested to use separate networks for different segments and the whole communication process must be monitored. All the IoT smart devices must go through initial configuration where their default passwords must be changed and better to use unique passwords. Regularly updating the firmware and implementing proper security policies will thwart the attackers.

Massimo Alioto and Mohsen Shahghasemi reviewed various commercial IoT smart devices in [11]. Authors focused on hardware specifications of IoT nodes like size, lifetime, cost and energy consumption. Authors assessed several commercial devices used like discrete sensors, Micro Controller Units, Printed Circuit Boards. A good graphical comparison of stated specifications was done and it shows the usage of required devices for a specific purpose. Not only hardware specifications, authors also distinguished the communication of IoT nodes. The conclusion of authors was to improve the energy efficiency of the upcoming IoT smart devices.

Shruthi Jaiswal and Daya Gupta discussed several security challenges of IoT in [12] with a case study of Remote Patient Monitoring System. Authors compared network security with IoT based healthcare device security in various design aspects like memory constraints, speed, energy consumption, security updates, scalability, etc. Authors proposed a framework which first analyses security requirements and later evaluates the possible threats that are to be focused. The proposed framework was applied to the case study of Remote Patient Monitoring System and identified the need for device-specific security algorithms.

In [13], authors tried to differentiate the security and privacy in IoT networks. To classify the security threats, authors used an IoT reference model. Several works were surveyed to identify and classify various threats and controls of IoT network. Authors concluded that even though threats can target specific layers, some identical threats my effect more than one layer of IoT reference model.

Vipindev Adat and B.B.Gupta discussed the security risks and the related technologies to overcome them in [14]. After briefing the growth of IoT networks statistically, authors tried to analyze the IoT architecture by mainly focusing the security. They discussed security issues related to wireless communication, 6LowPAN topology, wireless sensor networks. Authors mentioned some common security measures and also briefed some existing IDS for IoT networks. SVELTE, RIDES and DEMO were few of them. Authors tried to find the limitations of these IDS as they were specific to certain types of attacks only.

Mangal Sain, Young Jin Kang and Hoon Jae Lee surveyed on current IoT technologies, models and approaches in [15]. Authors mainly focused on wireless communication technologies like NFC, RFID, Bluetooth, Wi-Fi, ZigBee, 6LoWPAN, etc. they analyzed these technologies in various aspects like network, topology, power, speed, application, range and cost. Authors also mentioned some available security projects that were related to IoT. Authors differentiate these projects based on their IoT targeted security features like authentication, privacy, access control, etc.

Authors of [16] discussed security-related best practices for the deployment of IoT devices. After discussing major security breaches of IoT like Target Corporation hack in 2013 and Mirai botnets DDoS attack in 2016, authors mentioned some general best practices to prevent threats to IoT network. To make the IoT network cyber-attack proof, authors suggested using two IoT database search engines Shodan and Censys instead of web-based search engines like Google and Bing.

Maurice Dawson in [17] discussed the policies to provide security in Hyperconnectivity and IoT. Authors briefed about how various standard organizations are framing several policies to provide security during communication. Regarding Hyperconnectivity, i.e. social streaming different data in a smart manner, blends IoT, Big Data, and social media to allow a vast amount of data transformation. This superior connectivity raised the number of cyber-attacks. To reduce the potential risks in IoT networks, authors mentioned that the security policies and frameworks must be compliance to a standard and their focus should be on reducing the number of vulnerabilities.

Mandrita Banerjee, Junghee Lee and Kim-Kwang Raymond Choo surveyed various security solution for IoT in [18]. Authors analyzed various existing IDS for IoT in various approaches like cryptography, adaptive, application specific IDS and they highlighted the importance of the public availability of IoT datasets in designing the security-related architectures to IoT. Authors proposed the usage of Blockchain technology in IoT to ensure the privacy and integrity of IoT related data sets. The real usage of Blockchain was in recording the financial transactions but authors proposed an approach in which the IoT datasets were maintained by a central hub. The main focus of this approach was to identify the compromised firmware and self-healing capability in IoT networks.

Authors of [19] had investigated the noise problem of sensor streaming data. They focused on various IoT network sensors characteristics and their data transmission issues. To reduce the noise during sensor data streaming, authors proposed a method based on Discrete Wavelet Transform (DWT). Experimental results showed that the applied method tried to reduce the noise during transmission by diminishing the data points. The comparison between errors caused by original signal and errors caused by denoised signal justified the usage of DWT during sensor data transmission.

Marilyn Wolf in [20] discussed the issues related to security of Cyber-Physical Systems (CPS) in IoT. The author covered some security failed incidents like the DDoS attack on DNS in 2016, cyber-attack on the electrical facility in Ukraine in 2016 and hacking a United Airlines flight. He discussed challenges like traditional security techniques, untrusted designs and briefed the standards to be followed while designing reliable CPS. Author-specified various methodologies to reduce design time and run time of CPS-based IoT.

Seokjun Hong et.al in [21] discussed to improve a software called IoTCube, to interact with the IoT network through a web-based interface. To monitor and to assess the vulnerabilities in the IoT network, security experts use this software. As a part of requirement analysis, authors surveyed more than 50 IoTCube users and identified the need for improvement in it for effective risk assessment in IoT networks. Authors improvised the interface by modifying the perspective of IoT virtualization with the real world entities.

In [22], authors emphasized the importance of meeting the IoT requirements in the perspective of hardware. They insisted that the electronics, processors, and controllers must satisfy the resource-constrained environment of IoT. They discussed the importance of Edge Computing, Multicore Computing and Artificial Intelligence in providing the high-speed and low-cost smart nodes in IoT network. Authors analyzed various studies in IoT communication technologies and security mechanisms.

Yulong Fu et.al proposed an IDS for IoT based on the automata theory in [23]. After discussing various attacks and challenges in the existing IoT IDS, authors projected the various cases of IoT into algebra space. The proposed model based Input / Output Labelled Transition System like automata. Major parts of this model are to monitor, store, analyze, and respond to the unexpected events in the IoT network. Authors evaluated the proposed model on Raspberry Pi device with the help of an Android phone. Experimental results had shown the successful detection of false-attack, reply-attack, and jam-attack.

Laila Dahabiyeh in [24] emphasized the need for security of IoT through a social lens. The author discussed three case studies in securing the IoT networks. The first case study was regarding automotive industry. Cybersecurity challenges arose while making the cars connected. Various incidents were discussed and to enhance the security an attempt like CyberAuto Challenge hackathon was held to brought engineers, students, and white hat hackers to develop an awareness regarding auto-cyber security issues. The second case study was about wearable technologies. As the security in this area is at an initial stage more focus required to protect these devices and to ensure security. Smart Home was the third case study. After mentioning the vulnerabilities exploited by hackers in this technology, author briefed that the security must be to deal with a design approach. As a conclusion author discussed various IoT security challenges.

Authors of [25] discussed various issues regarding integration of IoT with Cloud Computing. After explaining the architectures of IoT and Cloud Computing networks, authors discussed some recent studies that mentioned the adoption of Cloud Computing for IoT integration. In order to integrate these two, various components like platform, infrastructure, and middleware technologies were deliberated. Authors explained the benefits of integrating these two by mentioning the applications in agriculture, healthcare, smart city, smart home, etc. At the end, authors discussed some open issues and security challenges for the integration of IoT and Cloud.

Shubhradeep Nandi explained the usage of Artificial Intelligence like IBM Watson and IBM IoT in providing cost-effective security hardware in [26]. The author described a security system based on Cognitive Premise. The main benefits of deploying this system were the usage of GPS without an active Internet connection, more data security and device security, precision calculations and customization. As a conclusion author expressed the significance of this project even though it is an emerging stage.

Authors of [27] discussed the possibilities of merging IoT, Cloud and Big Data. After explaining the protocols and standards of IoT, authors mentioned an IoT reference model where the stated three were integrated. The author explained the

functionality and issues of each of the seven layers in the reference model. After mentioning the security challenges, the author discussed some examples of smart home, smart industry, precision agriculture, etc. to illustrate the capabilities of IoT.
Badis Hammi, et.al discussed the deployment of IoT technologies for enabling the smart cities projects in [28]. After briefing the communication standards in IoT, authors discussed some recent works in this application domain. To build large-scale networks with IoT devices, authors explained Semtech and SigFox's technology called LoRa ultra-narrowband (UNB). This wireless technology enabled the ease of building the smart city and to deploy IoT devices at more places in a cost-effective manner. Various smart city applications like navigation, environment monitoring, smart parking, smart health, waste management, etc. were discussed. Authors discussed various IoT security challenges and identified that the network, transportation, and platform issues were the major challenges for achieving smart cities.
Arsalan Shahid et.al illustrated the recent developments in making the cities smart in [29]. After specifying the applications of IoT, authors mentioned a survey on smart city components. Further discussed the recent works in smart grids, smart electronic meters, smart homes, surveillance cameras, and traffic controls. Authors discussed the main challenges for various IoT applications in smart cities are poor standardization and identification, resource constraints of sensor devices, and scalability energy constraints.
Hamideh Javdani and Hooman Kashanian discussed various issues regarding the usage of IoT in medical applications in [30]. Authors briefed the smart healthcare systems by explaining the architecture of IoT based smart rehabilitation system. Later discussed IoT based sensor devices that can be used in medical field to measure temperature, heart rate, breathing, skin, blood flow, etc. Authors analyzed various recent articles in the health field using IoT and summarized various challenges like security and privacy.
Authors of [31] emphasized the usage IoT networks in Mobile Commerce (M-Commerce). After discussing various attributes and applications of M-Commerce, author briefed the technology that enabling various devices to use it. Later, author briefed the importance of ubiquitous computing in IoT. Wearable gadgets like watches, smart glasses, and fitness trackers can be easily configured and monitored using IoT. Authors concluded by mentioning the main barriers to integrate M-Commerce with IoT are security and privacy.
D. Serpanos and M. Wolf illustrated the usage of IoT in an industrial environment in [32]. As an effort to build Smart Factories, authors discussed Industrie 4.0, a Germany initiative to bring the IoT technologies into production sector. Later, briefed the emerging IoT application in an industrial sector called Industrial Internet of Things (IIoT). After discussing the IIoT architecture and its technologies, authors mentioned its application in the field of manufacturing. Authors concluded by describing the challenges in IIoT like stability, incessant operation, fault tolerant, security and power optimization.
Cong Xie and Shu-Ting Deng discussed various issues related to the use of security applications in IIoT in [33]. After discussing the potential threats to IIoT like attacking the nodes and RFID systems, authors mentioned the security mechanism with the usage of biometrics especially fingerprint recognition. The RC4 algorithm was used for both encryption and decryption while transmitting the biometric data. As the IIoT requirements were at the initial stage, authors concluded by mentioning the requirement of new protective directions and policies to enable the effective use of IoT in industries.

Following table summarizes the above discussed recent works in various aspects.

Table I. Summary Of Iot Related Works

| Ref | Objective | Methodology | Achievements | Challenges |
|---|---|---|---|---|
| [9] | Real-World challenges in IoT | Cryptographic algorithms | Mitigation of security risks<br>Protecting devices<br>Securing smart devices | Cyber Attacks<br>Regularly updating the firmware |
| [10] | Minimize the security risks in IoT network | Corporate security policies | Identify rouge devices<br>Thwart potential IP traffic | Immature IoT devices<br>Monitoring and governing |
| [11] | Various commercial IoT smart devices | Assessed several commercial devices used like discrete sensors, Micro Controller Units, Printed Circuit Boards | Filling the gaps in terms of size, lifetime, and cost to trigger the expected exponential growth of the IoT | Quality<br>Energy efficiency in IoT nodes |
| [12] | Security challenges of IoT with a case study of Remote Patient Monitoring System | Framework which first analyses security requirements and later evaluates the possible threats that are to be focused | identified the need for device-specific security algorithms | Single algorithm is not sufficient |
| [13] | Differentiate the security and privacy in IoT networks | Used an IoT reference model | Provided layer based threats and controls | Identical threats may risk more than one layer |

| | | | | |
|---|---|---|---|---|
| [14] | Security risks and the related technologies to overcome them | Used secure IoT architecture | Analysed layer based security challenges and discussed solutions | Authentication<br>DDoS attacks |
| [15 | Surveyed on current IoT technologies, models, and approaches | Differentiate these projects based on their IoT targeted security features like authentication, privacy, access control | Analysed device security, proper access control | Authentication<br>API security<br>Middleware support |
| [16] | Security-related best practices for the deployment of IoT devices | Using two IoT database search engines Shodan and Censys instead of web-based search engines like Google and Bing | Identifying genuine IoT devices in a huge network | Cyber-physical attacks |
| [17] | Policies to provide security in Hyperconnectivity and IoT | The security policies and frameworks must be compliance to a standard and their focus should be on reducing the number of vulnerabilities | Devices have the ability to perform checks as necessary as possible to remain securely attached | CWE database get updated daily to ensure that the device owner understands the appropriate risk |
| [18] | Importance of the public availability of IoT datasets in designing the security-related architectures to IoT | usage of Blockchain technology in IoT to ensure the privacy and integrity of IoT related data sets | Identifying the compromised firmware | Privacy of datasets<br>Lifetime of datasets |
| [19] | Investigate the noise problem of sensor streaming data | Method based on Discrete Wavelet Transform (DWT) | Applied method tried to reduce the noise during transmission by diminishing the data points | Incorrect information<br>Using time and resources to process useless data |
| [20] | Issues related to security of Cyber-Physical Systems (CPS) in IoT | Safety and security approaches at design time and runtime | Reduce design time and run time of CPS-based IoT | Traditional security techniques<br>Untrusted designs<br>Poor standards |
| [21] | Improve a software called IoTCube, to interact with the IoT network through a web-based interface | Surveyed more than 50 IoTCube users | Improvised the interface by modifying the perspective of IoT virtualization with the real world entities | Connectivity<br>Vulnerability status<br>Potential security problems |
| [22] | Importance of meeting the IoT requirements in the perspective of hardware | Edge Computing, Multicore Computing, and Artificial Intelligence | Providing high speed low-cost computations in the IoT framework | Reliability<br>Availability<br>Performance |
| [23] | IDS for IoT based on the automata theory | Model-based Input / Output Labelled Transition System like automata | Evaluated the proposed model on Raspberry Pi device with the help of an Android phone. Experimental results had shown the successful detection of false-attack, reply-attack, and jam-attack | State space explosion problem<br>Only for limited type of attacks |
| [24] | Need for security of IoT through a social lens | Three case studies in securing the IoT networks | Inferred security of IoT | Offshore development of IoT devices |
| [25] | Issues regarding integration of IoT with Cloud Computing | In order to integrate these two, various components like platform, infrastructure, and middleware technologies were deliberated | Applications in agriculture, healthcare, smart city, smart home, etc | Mobility<br>Context-based adjustments<br>Reliability<br>Quality of Service |
| [26] | Usage of Artificial | Security system based on | the usage of GPS without an | Cloud-based usage |

| | | | | |
|---|---|---|---|---|
| | Intelligence like IBM Watson and IBM IoT in providing cost-effective security hardware | Cognitive Premise | active Internet connection, more data security and device security, precision calculations and customization | Training the data<br>Requirement of Mobile |
| [27] | Possibilities of merging IoT, Cloud and Big Data | an IoT reference model | Discussed some examples of smart home, smart industry, precision agriculture | Integration<br>Scalability |
| [28] | Deployment of IoT technologies for enabling the smart cities projects | Semtech and SigFox's technology called LoRa ultra-narrowband (UNB) | Ease of building the smart city and to deploy IoT devices at more places in a cost-effective manner | Networking<br>Transportation<br>Platform issues |
| [29] | Recent developments in making the cities smart | Survey on smart city components | Application components in Smart Cities and Smart Homes | Poor standardization and identification<br>Resource constraints of sensor devices<br>Scalability energy constraints |
| [30] | Usage of IoT in medical applications | The architecture of IoT based smart rehabilitation system | Remote monitoring of Health Care System | Data security |
| [31] | Usage IoT networks in Mobile Commerce | Ubiquitous Computing in IoT | On-demand mobile enterprise solution via mobile apps | Security<br>Performance availability |
| [32] | Usage of IoT in industrial environment | Industrie 4.0, a Germany initiative to bring the IoT technologies into production sector | Operational technology<br>Industrial control systems | Stability<br>Incessant operation<br>Fault-tolerant<br>Security<br>Power optimization |
| [33] | Issues related to the use of security applications in IIoT | Usage of biometrics especially fingerprint recognition. The RC4 algorithm was used for both encryption and decryption while transmitting the biometric data | Connecting industrial objects to IoT network | Generating unique barcode for every fingerprint information |

After discussing various recent works in IoT, next section discusses some security challenges that are to be considered for securing IoT devices.

## 6. IOT SECURITY CHALLENGES

Being a multi-technology support network, IoT devices are more vulnerable to various security problems and researchers in this field face a lot of challenges while providing the security to IoT networked devices. This section mentions some challenges identified from the above recent works in IoT, which are to be considered while ensuring security in IoT networks.

Resource Constraints: Many nodes of IoT network have small energy, storage, and CPU. Due to this low resources, using high-level security mechanism in these IoT smart devices is very difficult.

Growth in minimal secure IoT nodes: Due to the resource constraints like memory and energy in IoT devices, they may not high-security protocols. This may lead to numerous weak nodes and gives a vulnerable opportunity for the attackers.

Scalability: Security mechanism in IoT network should be scalable as the count of interconnecting devices is increasing exponentially.

Compatibility: Providing security mechanisms for the functionality of various heterogeneous smart devices in IoT network is a serious issue as they need to be designed to work interoperably.

Ensuring Privacy: Majority of the RFID based devices in IoT network are lack of proper authentication procedure, intruders may track the identity of IoT objects and they can read/manipulate their data

Large volumes of Data: Even though some IoT based applications may use sensor-based data, other large-scale organization systems may need a large volume of data to be processed. This may require a central server.

## 7. OUR PROPOSAL

As discussed in the previous section, providing security for IoT creates many challenges for the security experts. To meet the major security requirements like Confidentiality, Integrity, Availability, and Authentication, we propose a novel Intrusion Detection System to thwart the attackers and to protect the IoT connected devices from a variety of attacks.

Authors designed and successfully evaluated the enhanced Snort IDS in conventional networks in [34] [35] [36] [37]. But conventional approaches are too costly, in terms of energy and bandwidth, to be implemented in IoT environments.

So, as an extension of the research contribution in [37], we propose an IDS scheme for IoT network as shown in Figure 5. For this, we consider the usage of Raspberry Pi device and enhanced Snort tool from [37].

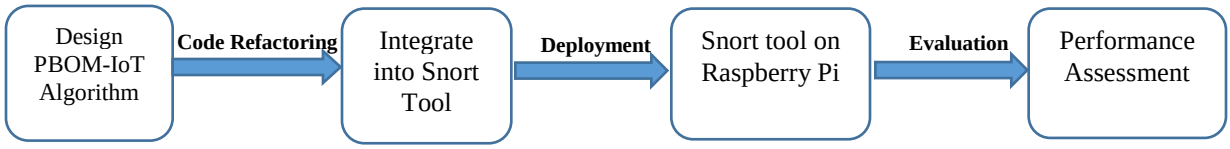


Figure 5. IDS architecture for IoT network

*7.1 Design PBOM-IoT Algorithm:*

Prospective Backward Oracle Matching (PBOM) algorithms were designed to improve the performance of search engines in IDS tool [35] [37]. These algorithms need more space as they use state flow information and can efficiently work on conventional systems. But for the resource-constrained IoT networks, these algorithms are not suitable.

To improve the performance of IDS search engine in IoT network, we design a new algorithm called PBOM-IoT. In this algorithm, we minimize the usage of states information and reduce the consumption of memory. This can increase the speed of the searching process and also reduces the data loss caused by high traffic.

*7.2 Integrate into Snort Tool:*

After designing the IoT applicable PBOM algorithm, we integrate the algorithm into Snort tool by using code refactoring. Code refactoring gives the flexibility to enhance the functionality of a software without a complete rewrite.

*7.3 Deploy on Raspberry Pi device:*

The Raspberry Pi [38] is an Advanced Reduced Instruction Set Computing Machine (ARM), which is smaller in size and low-cost. Even though it is less powerful than a desktop or laptop, it performs well for tiny Linux systems and one of the best selections for IoT related projects.

After code refactoring the Snort tool, we deploy the enhanced Snort tool on Raspberry Pi device to monitor the network activities in IoT network. We configure this device to act as the Wi-Fi hub for the IoT devices.

*7.4 Performance Assessment:*

We connect various devices to Raspberry Pi and build an IoT network. We assess the performance of this device hosting the enhanced Snort IDS, we attack the IoT network with several attacks like sinkhole attack, DoS attack, flooding, signal jamming, etc. During this process, the system gathers various performance parameters and we try to compare them against the existing approaches to prove the efficiency of the proposed approach.

## 8. CONCLUSION

Being an emerging technology, IoT is attracting more researchers for contributing to make this technology as a part of daily life. On the other hand, many security issues in IoT need added research effort. In this paper, IoT related security concepts were discussed extensively. Security requirements of IoT and challenges to meet them were discussed. A simplified layer based IoT architecture was discussed and layerwise possible attacks were classified. For understanding the security concerns with better research directions, recent works in IoT were discussed and analyzed their methodologies, achievements, and challenges. To secure the IoT networks, this paper proposed an IDS architecture based on enhanced Snort tool deployed on Raspberry Pi device. As a future work, we implement the proposed PBOM-IoT algorithm, integrate it into enhanced Snort tool on Raspberry Pi device and compare its performance against the existing IDS techniques in IoT networks

## 9. ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for their valuable feedback. We would like to thank our Computer Science Department for providing necessary resources for our work. This paper reflects the views only of the authors, and others cannot be held responsible for any use which may be made of the information contained therein.

## 10. REFERENCES

[1] "The Internet of Things Vertical Solutions", Cisco.com, 2015. [Online]. Available: https://www.cisco.com/web/offer/emear/38586/images/Presentations/P11.pdf. [Accessed: 20- Jan- 2018].

[2] "Q3 2017 State of the Internet Security Report", Akamai.com, 2018. [Online]. Available: https://www.akamai.com/de/de/multimedia/documents/state-of-the-internet/q3-2017-state-of-the-internet-security-report.pdf. [Accessed: 20- Jan- 2018].
[3] S. Arseni, S. Halunga, O. Fratu, A. Vulpe and G. Suciu, "Analysis of the security solutions implemented in current Internet of Things platforms", 2015 Conference Grid, Cloud & High Performance Computing in Science (ROLCG), 2015.
[4] X. Huang, P. Craig, H. Lin and Z. Yan, "SecIoT: a security framework for the Internet of Things", Security and Communication Networks, vol. 9, no. 16, pp. 3083-3094, 2015.
[5] A. Mosenia and N. Jha, "A Comprehensive Study of Security of Internet-of-Things", IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602, 2017.
[6] S. Okul and M. Ali Aydin, "Security Attacks on IoT", 2017 International Conference on Computer Science and Engineering (UBMK), 2017.
[7] "Ransomware attacks will target more IoT devices in 2018", TechRepublic, 2018. [Online]. Available: https://www.techrepublic.com/article/ransomware-attacks-will-target-more-iot-devices-in-2018/. [Accessed: 20- Jan- 2018].
[8] S. Jaiswal and D. Gupta, "Security Requirements for Internet of Things (IoT)", Advances in Intelligent Systems and Computing, pp. 419-427, 2017.
[9] M. Daniel, "Hidden Dangers of Internet of Things", Women in Security, pp. 69-75, 2017.
[10] M. Haber and B. Hibbert, "Internet of Things (IoT)", Privileged Attack Vectors, pp. 139-142, 2017.
[11] M. Alioto and M. Shahghasemi, "The Internet of Things on Its Edge: Trends Toward Its Tipping Point", IEEE Consumer Electronics Magazine, vol. 7, no. 1, pp. 77-87, 2018.
[12] S. Jaiswal and D. Gupta, "Security Requirements for Internet of Things (IoT)", Advances in Intelligent Systems and Computing, pp. 419-427, 2017.
[13] A. Al-Gburi, A. Al-Hasnawi and L. Lilien, "Differentiating Security from Privacy in Internet of Things: A Survey of Selected Threats and Controls", Computer and Network Security Essentials, pp. 153-172, 2017.
[14] V. Adat and B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture", Telecommunication Systems, 2017.
[15] M. Sain, Y. Kang and H. Lee, "Survey on security in Internet of Things: State of the art and challenges", 2017 19th International Conference on Advanced Communication Technology (ICACT), 2017.
[16] B. Payne and T. Abegaz, "Securing the Internet of Things: Best Practices for Deploying IoT Devices", Computer and Network Security Essentials, pp. 493-506, 2017.
[17] M. Dawson, "Cyber Security Policies for Hyperconnectivity and Internet of Things: A Process for Managing Connectivity", Advances in Intelligent Systems and Computing, pp. 911-914, 2017.
[18] M. Banerjee, J. Lee and K. Choo, "A blockchain future to Internet of Things security: A position paper", Digital Communications and Networks, 2017.
[19] M. Lopes De Faria, C. Cugnasca and J. Amazonas, "Insights Into IoT Data and an Innovative DWT-Based Technique to Denoise Sensor Signals", IEEE Sensors Journal, vol. 18, no. 1, pp. 237-247, 2018.
[20] M. Wolf and D. Serpanos, "Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems", Proceedings of the IEEE, vol. 106, no. 1, pp. 9-20, 2018.
[21] S. Hong, Y. Kim and G. Kim, "Developing Usable Interface for Internet of Things (IoT) Security Analysis Software", Human Aspects of Information Security, Privacy and Trust, pp. 322-328, 2017.
[22] S. Mohanty, M. Huebner, C. Xue, X. Li and H. Li, "Guest Editorial Circuit and System Design Automation for Internet of Things", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no. 1, pp. 3-6, 2018.
[23] Y. Fu, Z. Yan, J. Cao, O. Koné and X. Cao, "An Automata Based Intrusion Detection Method for Internet of Things", Mobile Information Systems, vol. 2017, pp. 1-13, 2017.
[24] L. Dahabiyeh, "The Security of Internet of Things: Current State and Future Directions", Information Systems, pp. 414-420, 2017.
[25] A. Malik and H. Om, "Cloud Computing and Internet of Things Integration: Architecture, Applications, Issues, and Challenges", Sustainable Cloud and Energy Services, pp. 1-24, 2017.
[26] S. Nandi, "Cloud-Based Cognitive Premise Security System Using IBM Watson and IBM Internet of Things (IoT)", Lecture Notes in Electrical Engineering, pp. 723-731, 2017.
[27] M. Oppitz and P. Tomsu, "Internet of Things", Inventing the Cloud Century, pp. 435-469, 2017.
[28] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad and L. Khoukhi, "IoT technologies for smart cities", IET Networks, vol. 7, no. 1, pp. 1-13, 2018.
[29] A. Shahid, B. Khalid, S. Shaukat, H. Ali and M. Qadri, "Internet of Things Shaping Smart Cities: A Survey", Studies in Big Data, pp. 335-358, 2017.
[30] H. Javdani and H. Kashanian, "Internet of things in medical applications with a service-oriented and security approach: a survey", Health and Technology, 2017.
[31] E. Turban, J. Outland, D. King, J. Lee, T. Liang and D. Turban, "Mobile Commerce and the Internet of Things", Springer Texts in Business and Economics, pp. 205-248, 2017.
[32] D. Serpanos and M. Wolf, "Industrial Internet of Things", Internet-of-Things (IoT) Systems, pp. 37-54, 2017.
[33] C. Xie and S. Deng, "Research and Application of Security and Privacy in Industrial Internet of Things Based on Fingerprint Encryption", Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 102-110, 2017.
[34] R. Gaddam and M. Nandhini, "An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment", 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), 2017.
[35] R. Gaddam and M. Nandhini, "Prospective Backward Oracle Matching Algorithm for Network Intrusion Detection System", 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017.
[36] R. Gaddam and M. Nandhini, "Analysis of Various Intrusion Detection Systems with a Model for Improving Snort Performance", Indian Journal of Science and Technology, vol. 10, no. 20, pp. 1-12, 2017.
[37] R. Gaddam and M. Nandhini, "Efficient Network Intrusion Detection System: An Architectural Approach Using Prospective Backward Oracle Matching Algorithms", Journal of King Saud University - Computer and Information Sciences. Unpublished.
[38] "Raspberry Pi", En.wikipedia.org, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Raspberry_Pi. [Accessed: 20- Jan- 2018].