International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Internet of Things Security and Privacy: A Systematic Investigation

S. Shiva Prakash[1], Dr. M. P.Vani[2*]

Submitted: 03/02/2024 **Revised**: 11/03/2024 **Accepted**: 17/03/2024

Abstract: The Internet of Things (IoT) paradigm shift is one of the most remarkable phenomena of recent times.Many security issues are triggered when disparate IoT devices are combined with the traditional Internet. This is because conventional internet connection methods were never intended to accommodate IoT. As a result, there are now countless ways in which IoT-enabled equipment could be compromised. This assessment of the literature centred on the primary concerns regarding the safety of IoT. The adaption of machine learning techniques in IoT, as well as its layered architecture, protocols for communication, and energy-efficient data routing strategies, were all subjects of our research. In addition to discussing the current attacks, hazards, and state-of-the-art remedies, we lay out a road map for meeting the security needs of the Internet of Things. We also compile a table of IoT security issues and a map of published remedies. We conclude that an attacker can compromise an IoT device, infrastructure, or network based on the results of this study. As a result of the information gathered in this poll, researchers are more motivated than ever to create a foolproof intrusion detection system for the Internet of Things (IoT).

Keywords: *IoT Security, IoT Protocols, Neural Networks, IOT Energy Management.*

1. Introduction

In current Due to the widespread use of IoT-based technologies, cybercriminals are drawn to them. Criminals target IoT devices to gain access to sensitive information such as bank records, personal health records, and credit card details. Despite the increasing number of Internet of Things deployments and solutions, security remains a top priority. The addition of new devices, new upgrades, and third-party protection of data causes problems for IoT's layered architecture. End-to-end data communication has pros and cons for each of the IoT protocols established by IEEE and ETSI. Many scientists as of late have been motivated to create healthcare monitoring systems based on the Internet of Things. However, the wireless communication route of medical devices or health data kept in internet databases are vulnerable to a wide variety of attacks.

The attackers are peddling sensitive medical data to the highest bidder, as stated in [2].Leakage of such sensitive information might create a serious privacy issues.[3] Leakage of IoT device information such like model, type, configuration, Operating systems and drivers may open a gate for integrity attack through easy access. It is proved that Eavesdropping of unencrypted wireless communication is trouble-free. [4] Smart factories, homes, towns, grids, and cars are just some of the areas that can benefit from automation and monitoring thanks to the Internet of Things. This implementation requires more investment for deployment. [5] But an attacker can use very cheap and limited resources as a powerful tool to launch powerful large-scale attacks against IOT deployments. Table-1 explains the possible attacks in their related IOT sectors.

Table-1 Possible attacks and vulnerabilities.

Attack type	**IoT Sector**	**Consequences**
Bruteforce	Sensor identification	Node compromise
DDOS	Protocol	illegitimate packets transmission
Reverse engineering	Protocol	Remote attacks
Eavesdropping	Between two devices	listening confidential conversations
Phishing	Smartphone	submitting confidential information to others
Replay	Between two devices	bypass the authentication
Poisoning	integrity of machine learning algorithm	adding malicious data points to the training set
battery draining	Protocol	energy depletion
integrity attack	Edge devices	Violation of legitimate data
Routing attack	Communication	Reliable routing
Malicious Injection	Communication	Overall control

[1] *Research Scholar- SCOPE, VIT University Vellore- 632014, Tamil Nadu, India, Email: shivaprakashsthaneekam@gmail.com*
[2] *Associate Professor-SITE, VIT University, Vellore- 632014, Tamil Nadu India*
** Corresponding Author Email: mpvani@vit.ac.in*

Node replication	Edge Nodes	Network Traffic
Unauthorized conversation	Communication	Violation of roles
Inessential logging	Edge computing	Finding browsing history
Side cannel attack	Computing Nodes	Channel compromise
DOS	Computing Nodes	Denial of Resources
Hardware Trojans	Computing nodes	Share the packets as public

Potential risks and likely attacks alongside the safety of such systems is developing severely, while, unhappily, the requirements for security are not yet recognised. Research into the safety of the Internet of Things (IoT) and its physical components & security techniques is a growing field of study in academia, industry, and government. All parts of the IoT's underlying architecture must incorporate the security mechanism. In this context, "components" refers to the base station, which acts as a central hub for data collection and processing, as well as wireless sensors that are constantly monitoring their surroundings and transmitting that information to the base station, and as physical objects which are under the control of the base station. Existing wireless communication protocols have a number of obstacles, including the need to deal with encryption methods, low compute power, low sensor energy, low memory, time stamp challenges, and difficulties in identifying individual sensors.

Still the IOT implementation suffer with crucial concerns that are a notable barrier for the adoption of the technology. The main barriers could be listed such on multiple sensor devices, indoor and outdoor environments, uneven data sensitivity ,Complex spatial and temporal data and multidimensional exploratory. Commercially there are variety semantics. Uncertainty is the major barrier when dealing with IOT data. There are many countermeasure mechanisms to provide security against such type of attacks. Most of these approaches, however, are narrowly focused on one or a few standards, technologies, or models of implementation. Some of the countermeasure mechanisms are as follows: Side channel signal analysis, Intrusion Detection systems, Securing firmware update, Blocking, personal firewall, information flooding and role based authorization. All safety and security approaches has advantages and disadvantages.

The aim of this survey leads towards security enhancement of IoT through providing a well standard security mechanism as well as easy adaptable. To develop an efficient IDS, here are numerous risks and obstacles that need to be considered. If this poll covers every facet of the IoT infrastructure, it could be a valuable resource for all IoT experts. Here is a quick rundown of the article's primary contributions:

1. Examining potential threats and vulnerabilities in the edge-layer of the Internet of Things
2. Studying several attacks and their countermeasures related to its layer.
3. Discussion of security solutions for addressing different security issues that exist in all layers.
4. Providing a road map for future research direction for IoT security problems.

This survey has a logical structure. In Part II, we present some of the work done before on the topic of IoT security. The Architectural Requirements & Protocol Strategies are described in Section III. The section IV reviews Cryptographic schemes and several IDS implementations. Section V studies the machine learning approaches associated with IOT security. The final section presents a tabulation regarding various recent security solutions with its advantages and disadvantages and provides a footstep for future research.

2. Open Challenges in Iot Security

This section concerns the existing challenges in the field of IOT deployment in general view. It also emphasize the importance of Security in health care systems. It provides an overview of the principles behind sensor networks and the Internet of Things, discussing its benefits, drawbacks, comparisons, and limitations. Particularly, it spotlights secure routing protocols and data transmission.

The abnormal condition of sensor leads to false judgment and trigger unwanted events. Smoke detectors are crucial to the operation of any fire evacuation system. If the node is compromised, an attacker can quickly send out an SOS signal. This make everything as public and create economical damage.

2.1. IoT Architecture

Over the IoT's layered architecture, data is transmitted and received. The main parts of an IoT architecture are the sensors, IOT gateways, objects, and cloud server. The typical layers of this architecture are as follows:

- Objects layer
- Object Abstraction layer
- Service Management layer
- Application layer
- Business layer

According to [6], the resource limitations of medical sensors make it impractical to use traditional cryptography in IoT-based health. In this study, a novel gateway-based architecture was presented to supply remote users with

authentication and permission.[7] proposed a novel SDN architecture to solve IoT security issues. It stated multiple SDN controllers especially Border Controllers which implied in equal interaction for inter communication. However, it necessitates alteration in complete network infrastructure to employ SDN protocol and SDN controller. Therefore it entails total reconfiguration of the network. This raise cost owing to reconfiguration. [8] Applied IOT SENTINEL to determine the types of devices that are connected to an IoT network. This mechanism support to enforce rules in the bidirectional communication of vulnerable devices. This effective mechanism minimizes the possibilities of attacks. [9] proposed a new IoT architecture named as representational state transfer (REST) architecture. This work introduced a new open protocol namely Open authorization (OAuth) to provide secure authorization. It operate by granting access tokens for service consumer which access the user's data stored by the service provider. The heterogeneity nature of IoT devices and small amount of sensor's memory are the major problems in designing efficient IoT architecture. Designing fully foolproof safety systems and pinpointing foolproof safety design solutions is a highly risky endeavour. When developing wireless sensors, it is crucial to select an appropriate communication protocol.

2.2. Choosing suitable Protocol

Recent research involves in designing optimal middleware architecture to provide the basic functionalities of IOT devices. Various components are integrated to provide Security, process execution, Data transfer and IOT device identification. This portion mainly deals the variety and veracity challenges of IoT data. i.e collection of IOT data, structuring and unifying IoT data streams. The problems and potential research avenues of the Internet of Things were thoroughly examined in [10]. In this paper, we outline some of the challenges associated with the Internet of Things (IoT), including its naming & identity management, connectivity and standardisation, information privacy, spectrum utilisation, and energy efficiency. It shows a guide map to achieve all possible applications through IOT. [11] surveyed several WSN based air pollution monitoring methods and this survey also stated different types of metal oxide gas sensitive sensors and their working principles. All the risks involved in creating a wireless sensor network for air pollution monitoring were detailed, and various existing methods, such as Static Sensors Network (SSN), Community Sensors Network (CSN), and Vehicle Sensor Network (VSN), were discussed. Finally, this survey left some challenges pertaining to observance with principles, availability of bandwidth, global execution, Hardware and Software Issues and architecture that need to be addressed.

Three different types of wireless sensors based on the Internet of Things were proposed in [12]. User Datagram Protocol (UDP) is used for wireless communication in the original sensor. A third sensor employs Bluetooth Smart technology, and a second uses Hypertext Transfer Protocol (HTTP). Energy usage, user friendliness, solution complexity, and availability of Internet access are all used to verify the performance of deployed sensors. [13]proposed indoor Air Quality monitoring architecture using IAQ sensors (SHT10, MQ7, T6615 CO_2, LDR5) and wireless Zigbee protocol for communication. The collected data were sent through wemos integrated Wi-Fi to MySQL database webservices. Generally, different sensors employ different protocols and every communication protocol has security weakness. [14] surveyed various IoT protocols and their weaknesses. The common weaknesses are listed below.

- Timestamps are not included in transferring packets .
- Setting default passwords for devices.
- Setting sensor identifier number as very small.
- Desynchronization issues.
- Routing change regarding topology changes.
- Mobility of sensors.
- Power efficiency.
- Reliability.
- Internet connectivity.

2.3. Cryptography based security mechanisms

The lack of support for cryptographic measures to ensure the safety and confidentiality of data provided by sensors is the main drawback of widely used non-standard communication protocols. An attacker's ability to launch a security attack can be severely hampered by using either conventional communication protocols, which provide robust encryption methods to assure confidentiality and integrity, or by adding encryption mechanisms to customised communication protocols. Attribute-based encryption's (ABE) applicability in Internet of Things systems was investigated in [15]. To demonstrate the viability of ABE in the IoT, it was implemented on Intel Jupiter Gen 2, Intel Edison, who was the Raspberry Pi 1 Model B, & Raspberry Pi Zero.. [16] applied a new 64-bit symmetric key block cipher technique with the use of 64-bit key. It enrooted that the key generation process should be not be complicated and not having complex mathematical operations. It applied various attacks with the cipher text and justified the trustworthy of the algorithm. [3] listed various considerations that have to be consider when applying encryption algorithm in IoT framework.

- Limited Energy Use and Storage
- Limited RAM and ROM
- It is challenging to implement on sensor nodes with limited resources.
- Extremely time-consuming and money-consuming to implement.
- Key generation and key exchange

Unfortunately, the high cost of cryptography renders it useless for protecting devices with little resources. Lightweight cryptography techniques that are optimised for such devices are needed. There is a requirement for adopting IDS to monitor any harmful conduct of the network to avoid early security threats to lessen its consequences. With IDS in place, you can rest assured that your network will continue to function normally even if an attacker manages to breach your cryptographic defences.

2.4. Intrusion Detection System

To monitor network functions plus communication acquaintances, and to raise an alert abnormal circumstance as when a pre-defined rule is ignored, IDS is fundamentally necessary at the communication level as the next level of security. Sensed data is stored, organised, processed, and checked for vulnerabilities here. Intrusion detection systems (IDS) were used to conduct a comprehensive survey of all non-denial-of-service options in [17].A DOS assault is encountered, along with the necessary steps to secure the Internet of Things. Unauthorised access attacks can be thwarted with an access control system, while hostile insider attacks can be thwarted via event monitoring. The necessity of IDS at the application layer was determined by a study of availability & non-denial of service utilising IDS [18]. For harmful code injection assaults, an anti-virus technique is necessary, while spam filtering helps protect against phishing. Various researches discuss various attacks and dangers in various layer with the security procedures. Normal and malicious behaviours on an IoT network were the subject of [19]. The ANN method is checked using a simulated Internet of Things network. This study presents the usage of an ANN as an online IDS to collect and analyse data from different nodes in an IoT network in order to detect a DoS attack. In this study, we used a multilayer perceptron (MLP) network with three layers of feedforward neurons. This model proves the deployed ANN algorithm can identify DDoS/DoS assaults against benign IoT network traffic. In addition, it aids in enhancing network stability by alerting the response team to an assault at an early stage, thereby preventing substantial interruptions to the network. Computer security services for threats related to smart IoT devices in the home were presented in [20] as part of a framework for host-based Intrusion Detection & Mitigation dubbed IoT-IDM. IoT-IDM bridges (i) the development of software-defined networking (SDN), which allows for remote network visibility and flexibility in configuring, managing, and securing the network, and (ii) the advancement of methods based on machine learning in detecting network abnormal patterns. As part of this project, the popular SDN controller Floodlight now has a Java-based IoT-IDM module.In order to identify compromised hosts from which attacks are conducted, IoT-IDM use machine learning methods. Once an attack's origin has been determined, IoT-IDM can create preventative rules and push them to the routers and switches beneath the network. The general IDS security mechanism involves in any one of the following strategy.

- Digital Signature
- Access Control Table
- PKI
- Router Filtering
- Data Encryption
- Anti-virus
- Event Monitoring
- Spam Filtering

2.5. Machine Learning approaches

A machine learning technique that creates numerous iterations of a predictor then employs them to obtain a single aggregated prediction by averaging or utilising a plurality vote.

Fig 1.illustrates all the types of machine learning approaches

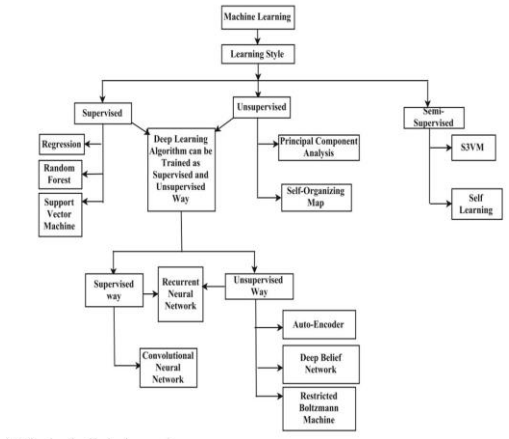
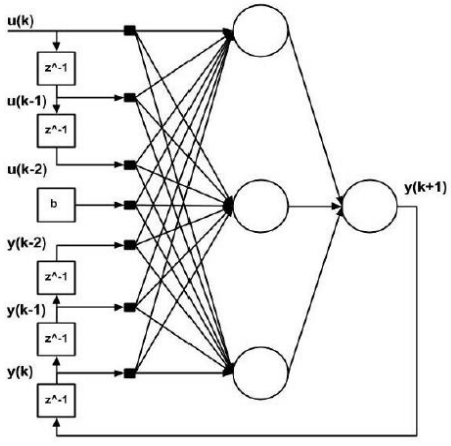


Fig 1. Machine learning approaches

In [21], the authors created a technique called weighed feature selection for collecting and choosing deep features, which they then integrated with the data obtained by a stacked AE (SAE) algorithm in order to detect attacks

based on impersonation in a Wi-Fi context. A neural network was trained to distinguish between two classes (i.e., impersonation and normal) using the combined features.The high detection accuracy demonstrated by this hybrid of unsupervised DL (i.e. SAE) and supervised DL (i.e. ANN) algorithms demonstrates the promising future of deep algorithms in protecting Wi-Fi networks against impersonation attempts. Intrusion detection using methods based on machine learning and data mining was the main topic of [22]. They analysed cyberspace misuse and anomaly detections, built an Android malware detection tool to protect Internet of Things devices, and used a linear support vector machine (SVM) to analyse the results. They evaluated SVM's detection abilities with those of naive Bayes (NB), RF, and DT, among other ML methods. SVM fared better than the other ML algorithms, as evidenced by the comparative findings. These findings validated the usefulness of SVM in the detection of malware. The goal of a malicious input attack is to install malicious code on the compromised Internet of Things device. A code an injection will be executed by this programme. Because of the inherent vast and well-connected surface area of IoT systems, the injected spyware is highly dynamic, and new forms of assaults are regularly created to significantly compromise IoT components. In contrast, data tampering refers to the deliberate alteration of data through unauthorised means (such as deletion, alteration, manipulation, or editing). Information is frequently sent, received, and stored. Both scenarios pose risks of data capture and tampering, which could compromise vital IoT system operations like adjusting billing prices in a smart grid that relies on IoT.

Fig 2. Nonlinear autoregressive neural network



By analysing and categorising network traffic data, nonlinear autoregressive neural networks[24] took on the problem of identifying IoT devices within a network. Although MAC addresses may be used to pinpoint a device's maker, no universal system exists for doing so. However, the ratio of incoming to outgoing bytes and the mean duration to live are just two of the high-level network statistics that have been utilised to spot fraudulent activity in network interactions. Using analysis of traffic, machine learning, & HTTP packet properties, this work proves that it can accurately identify among IoT and non-IoT devices. It suggested a multi-step procedure in which a group of classifiers based on machine learning is applied to a continuous flow of sessions coming from a single device.

3. Summary

We surveyed various security issues and solutions associated with IoT architecture, communication protocols, Threats and attacks, intrusion detection system and machine learning methods. When it comes to the practical side of things, security is paramount. Different intrusion detection systems (IDS) look for the best possible safety measures. The utilisation of IoT becomes developing research fields in monitoring & mistake detection which are extremely vital for the adaption of newest technologies. There will need to be a lot more study in the future to solve the IoT security problems. All IoT layers, from elements to networks to services to applications, will need to be protected by the new IDS. In Table II, we provide an in-depth analysis of the various methods now in use to secure the Internet of Things.

Table 2: Comprehensive Review of Security Services and Mechanisms in IoT

Technique	Author& Ref No.	Year	Description	Advantages	Disadvantages
Security challenges in Architecture level					
DistBlockNet	Sharma, et al. [25]	2017	Combined SDN and blockchains technology	Automatic adaptation of security	1.Scalability issues 2.Processing power and time

					3.Storage hurdle
lightweight Blockchain architecture	Dorri, et al. [26]	2017	faith in a decentralised network to speed up the block validation process.	1. Increased fraud detection. 2. Instant Transactions. 3.Financial Efficiency 4.Credential Security	Extremely Volatile.
Gateway based architecture	Haddadi, et al. [27]	2018	system wherein an ISP and a home gateway work together to prevent hacking attempts.	1.Connect different protocols 2.Gateway authentication .	1. Troubleshooting is difficult. 2. Very low fault tolerance. 3. Instant transfer is refused.
control system gateways	Condry and Nelson [28]	2016	In order to authenticate users and grant them permissions, gateway devices utilise their computational, cryptographic, signal/image processing, and communicative prowess.	1.more secure 2.scalable 3.resilient with real-time performance . 4.Quicker Response Time 5.Better interoperability	1.Decreased data exposure.
Embeded system security	Yoon, et al. [29]	2018	embedded Wi-Fi module server function provide cances for the expansion small-scale IoT.	Dedicated tasks hIgh Specifications and low cost	Limited energy constraint.
Security challenges in protocol level					
IEEE 802.15.4	Granjal, et al. [14]	2015	confidentiality, integrity, authentication and nonrepudiation of the information flows.	Analyzed all standard protocols.	
ERGID routing protocol	Qiu, et al. [30]	2016	Emergency Response IoT based on Global Information Decision (ERGID) to improve the performances of reliable data transmission and efficient emergency response in IoT	To achieve load balancing in the network, the probabilistic approach known as remaining energy probability selection (REPC) is proposed.	Very expensive
IETF constrained application protocol (CoAP)	Sheng, et al. [31]	2018	synchronous request/response protocol	1.interoperable with HTTP. 2.Runs over the UDP. 3.Supports well with resource-constrained devices	1.Unreliable data transmission.
Security mechanisms based on cryptographic systems					
physical unclonable functions	Aman, et al. [32]	2016	Secrets are hidden in the complex micro-structure of an IC instead of volatile memory.	1Restrict Side Channel Attacks. 2. Works well against Man-in-the-	Susceptable to model attacks.

				middle Attacks.	
fuzzy identity-based encryption	Mao, et al. [33]	2016	Identity ID's private key can decrypt ciphertext encrypted with Identity ID's public key if only if the two identifiers are statistically close.	The key and ciphertext sizes don't have to grow for tighter security to be achieved.	rely on randomoracle models
probabilistic and lightweight algorithm	Muhammad, et al. [34]	2018	Using random bits placed in otherwise unadorned images, a probabilistic cypher can be created.	An attacker is unable to deduce any relevant information regarding a keyframe from the encrypted version of that frame.	More computation complex.
white-box cryptography	Bertino [35]	2016	This method makes it more difficult for attackers to obtain encryption secrets by hiding them in massive look-up tables.	Efficient Key management	very expensive
Blockchain based re-encryption	Manzoor, et al. [36]	2018	After encrypting data from IoT devices, the system stores it on a decentralised cloud..	1.very efficient proxy reencryption scheme 2.smart contract. 3. table mechanism counter the eavesdropping attacks.	1.limites storage 2.limited energy.
Intrusion detection systems in IOT					
intelligent gateway	Al-Fuqaha, et al. [37]	2015	It optimize the performance by controlling the underlying wire protocol based on the specific application.	1.interoperability. 2.Reduce the market fragmentation between IoT protocols.	1.protocol translation issues.
Attack analysis	Buja, et al. [38]	2018	protection of the Simeck32/64 blocks cypher from cube attacks using a side-channel attack model predicated on the assumption of Hamming weight leakage.	Defences, Methods, and Commands for Blocking, Isolation, Killing, and Sleeping	protection against tampering and self-destruction, concealment methods, and measures to prevent the spread of sensitive data.
Attacks and countermeasures	Abdul-Ghani, et al. [39]	2018	Study of all attacks in every layer of architecture.	1.Reliabilty enhancement 2.Access point 3.Error checking. 4Routing methods.	Very weak in determining extent of damages.
Machine learning methods					
Machine	Mishra, et al. [40]	2018	various machine learning	1. detect	1.Detect known

learning based IoT			algorithms are applied to detect various kinds of attacks.	novel attacks. 2. study the patterns of traffic movement. 3. capture the complex properties of the attack.	attacks. 2.false positives for unspecified protocols
Artificial neural network IDS	Hodo, et al. [19]	2016	To combat DDoS/DoS attacks, a multi-level perceptron (a supervised ANN) is trained on packet data collected from the internet and then evaluated.	1.Works based on attack signatures. 2.It uses Port scan technique. 3.Very flexible. 4.Noisy data is not a matter.	Recognize only known suspicious events
Network traffic analysis	Shenfield, et al. [41]	2018	Deep packet inspection	distinguish benign and malicious network traffic	Difficult to define rules.
Deep Neural Network	Kang and Kang [42]	2016	neural network start with a blank slate by pre-training a DBN without any external supervision.	1.Accuracy improved. 2. Very effective in controller area network	Complex process

4. Conclusion

In this paper, we took a look at the security measures built into the Internet of Things (IoT) and the many dangers, assaults, and difficulties that come with them. The first efforts in this area examined the importance of security administration and different types of threats. Due to the complexities of IoT-based security, the techniques have been broken down into distinct classes so far. Various types of methods to IoT design are compared and contrasted in tables to further illustrate their benefits and drawbacks. The survey found that there is no reliable machine learning IDS approach due to security risks. This study analysed past security challenges and provided recommendations for implementing IoT protocols. The protocols, technology, and deployment strategies were the primary areas of interest. The report found that the requirement for thorough security policies is further bolstered by the persistence of typical issues that can arise in a bad protocol implementation system. Our long-term goal is to build an IDS using the principles of machine learning so that its components can communicate with one another in a streamlined, standardised fashion.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. J. I. c. s. Ayyash, and tutorials, "Internet of things: A survey on enabling technologies, protocols, and applications," vol. 17, no. 4, pp. 2347-2376, 2015.

[2] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017, pp. 32-37: IEEE.

[3] Y. Yang, L. Wu, G. Yin, L. Li, and H. J. I. I. o. T. J. Zhao, "A survey on security and privacy issues in Internet-of-Things," vol. 4, no. 5, pp. 1250-1258, 2017.

[4] M. Amadeo, C. Campolo, A. Iera, and A. Molinaro, "Information Centric Networking in IoT scenarios: The case of a smart home," in 2015 IEEE international conference on communications (ICC), 2015, pp. 648-653: IEEE.

[5] M. Mohsin, Z. Anwar, G. Husari, E. Al-Shaer, and M. A. Rahman, "IoTSAT: A formal framework for security analysis of the internet of things (IoT)," in 2016 IEEE Conference on Communications and Network Security (CNS), 2016, pp. 180-188: IEEE.

[6] S. R. Moosavi et al., "SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," vol. 52, pp. 452-459, 2015.

[7] F. Olivier, G. Carlos, and N. J. P. C. S. Florent, "New security architecture for IoT network," vol. 52, pp. 1028-1033, 2015.

[8] M. Miettinen et al., "IoT Sentinel Demo: Automated device-type identification for security enforcement in IoT," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017, pp.

2511-2514: IEEE.

[9] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. J. I. s. j. Ferrari, "Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios," vol. 15, no. 2, pp. 1224-1234, 2015.

[10] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in 2012 10th international conference on frontiers of information technology, 2012, pp. 257-260: IEEE.

[11] M. Pavani, P. T. J. I. J. o. C. N. Rao, and I. Security, "Urban air pollution monitoring using wireless sensor networks: a comprehensive review," vol. 9, no. 3, pp. 439-449, 2017.

[12] G. Mois, S. Folea, T. J. I. T. o. I. Sanislav, and Measurement, "Analysis of three IoT-based wireless sensors for environmental monitoring," vol. 66, no. 8, pp. 2056-2064, 2017.

[13] G. Marques, R. J. I. j. o. e. r. Pitarma, and p. health, "An indoor monitoring system for ambient assisted living based on internet of things architecture," vol. 13, no. 11, p. 1152, 2016.

[14] J. Granjal, E. Monteiro, J. S. J. I. C. S. Silva, and Tutorials, "Security for the internet of things: a survey of existing protocols and open research issues," vol. 17, no. 3, pp. 1294-1312, 2015.

[15] M. Ambrosin et al., "On the feasibility of attribute-based encryption on internet of things devices," vol. 36, no. 6, pp. 25-35, 2016.

[16] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. J. a. p. a. Shah, "SIT: a lightweight encryption algorithm for secure internet of things," 2017.

[17] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," in 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud), 2016, pp. 84-90: IEEE.

[18] N. Vipin and M. A. Nizar, "Efficient on-line SPAM filtering for encrypted messages," in 2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), 2015, pp. 1-5: IEEE.

[19] E. Hodo et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," in 2016 International Symposium on Networks, Computers and Communications (ISNCC), 2016, pp. 1-6: IEEE.

[20] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," in 2016 11th International conference on availability, reliability and security (ARES), 2016, pp. 147-156: IEEE.