Threats and Challenges for Security Measures on the Internet of Things

Submitted: 08 July 2021
Revised: 04 October 2021
Accepted: 28 October 2021

Article submitted to peer blind review

Mohammad Faiz*
https://orcid.org/0000-0002-7831-4267
A. K. Daniel**
https://orcid.org/0000-0001-6900-0867
DOI: https://doi.org/10.26512/lstr.v14i1.38843

Abstract

[Purpose] The Internet of Things (IoT) has grown rapidly in the past few years and billions of devices are connected to the IoT network for collecting and sharing data globally for various applications. Due to the billions of connected devices, there is a potential risk of data loss, identity theft, device manipulation, trust issues, falsification of data, network/server manipulation, and various impacts in the application of IoT platforms. The IoT-enabled devices are growing rapidly day by day leading to amplify the threats to the reliability of the network.

[Methodology/Approach/design] The research work aims to push the present state of the art by identifying privacy and security requirements that IoT is presently needed.

[Findings] Various existing solutions for security in IoT and their limitations are addressed. Security issues such as trust based privacy policies for context-awareness, efficient holistic frameworks, and lightweight strategy for system resource constraints are identified.

[Practical Implications] The technological age of IoT will be relying on a large number of devices is forecast to expand substantially. Although many of the technology-related privacy and security challenges exist, developers and researchers need to work in collaboration to resolve those threats, as they have accomplished with several other related technologies.

---

* Mohammad Faiz received M. Tech degree in Computer Science Engineering from M.M.M. University of Technology, Gorakhpur, India in 2016. Presently he is working as a research scholar in the Department of Computer Science & Engineering. His current research interests are Wireless Sensor Networks and Cloud computing. He has published various papers in International Journals and International conferences. E-mail: faiz.techno20@gmail.com.

** A. K. Daniel is presently working as a Professor in the Department of Computer Science and Engineering, M.M.M. University of Technology, Gorakhpur. He is a senior member of ACM, CSI, IEEE, and various reputed journals. He has published more than 100 papers in various national and international conferences and journals. His area of research includes artificial intelligence, wireless communication, and mobile ad-hoc network protocol. E-mail: danielak@rediffmail.com.

Keywords: Internet of Things. Security. Smart City. Privacy.

INTRODUCTION

IoT is one of the most important breakthroughs in today's era and a promising invention to change our lives. The idea of the Internet of things (IoT) was foremost conceived by Kevin Ashton of Auto ID-Center at MIT in 1999. According to Ashton, IoT is a system in which the Internet is connected to the physical world via ubiquitous sensors(Vermesan et al. 2011). The sensors are key components of IoT. The IoT allows us to connect people and things through the internet to achieve some common goals (Dohr et al. 2010). About 50 to 100 billion devices are projected to connect to the Internet by the year 2025. In 2010 the global sensor market stood at about $56.3 billion. This was about $62.8 billion in 2011. The global sensor market is projected to increase by 2016 to $91.50 billion, at a combined annual growth rate of 7.8% (Forecasting 2011).

Due to the huge number of internet-based devices the configuration, communication, and management of such devices is not feasible if there no automatic system available to manage them. The sensor networks consist of one or more sensing nodes that use wired or wireless means to communicate with each other. Each sensor node can locally or remotely sense, communicate, and process data. Sensor nodes in sensor networks can be homogenous or heterogeneous. These sensor nodes are built with the phenomenon that we would like to sense the environmental activities (Akyildiz et al. 2002).

Through the development of hardware and software innovations, a mixture of real-world entities' Wireless Sensor Networks (WSN) and smart objects has become a practical solution through the Internet capabilities. IoT engineers operate in tandem with WSN hardware, but the deployment and analysis procedures for sensor devices to act as smart objects are not insignificant. The expansion of applications for the IoT relates in particular to various usability characteristics of WSN (Narayan and Daniel 2020). The design and implementation of IoT systems need the basic issues such as hardware and software heterogeneity linked networking and compatibility problems, flexibility and scalability of the application, standardized communication and descriptions of the services, procedures for the automation, handling the Big Data (Corcho and Castro, 2010).

The IoTs can deploy billions of very low-cost, internet protocol (IP) enabled wireless sensor nodes(Narayan and Daniel 2021), allowing sensors to sense and track any object or individual in the real world. The integration of sensing

objects allows us to communicate easily with others in the world (Atzori, Iera, and Morabito 2010). An IP address is provided for any device that connects to the Internet. The existing Internet Protocol version-4 (IPv4) has an address space of 32 bits (i.e. approximately 4.3 billion distinctive IPs to represent devices connected to Internet, which is less than today's population of the world. IPv6 is the latest version active to solve the limitation of the 32-bit address space issue and plays a significant role in IoT implementation. IPv6 can handle more than 340 undecillion distinct IP addresses (128-bit). So even, the new IPv6 will recognize trillions of WSN nodes (Vasseur and Dunkels 2008). Internet technologies and WSN is realizing a new trend in the age of ubiquity.

A rapid growth in internet usage and improvements to various networking technologies allow the internetworking of daily objects (Surie, Laguionie, and Pederson 2008). IoT has always been about real objects communicate with each other, a machine-to-machine contact would be applied to things (Garrido et al. 2010). Main IoT driving technologies are linked to sensor technologies like WSN, miniaturization and nanotechnology, etc. The advent of small IP protocol architectures [HC-08], explicitly designed for the WSN, decreased the complexity of the gateway. This is a point of integration in the IoT, with IP-like protocol used in WSNs and on the internet.

As a result, at the level of can routers, gateways are much simpler tools that only have to convert between different physical media. The wider implementation of IPv6[RFC-2460], and its adaptive layers for WSN (Narayan and Daniel 2020). This pattern will continue in the future. The phase of convergence supports the core concept of the IoT, two-way communication is possible between two network devices. The tools may be overwhelming in nature, such as a High-speed server system tracking out a weather monitor, or a Smartphone user manipulating bulbs. This correspondence is made possible by the presence of a universal communication network, using structured protocols. This extensive-scale integration is expected to enhance many of the existing systems, such as logistics, transport, and different automated systems. However, it will also allow the implementation of novel applications such as a smart city(Narayan and Daniel 2021a). Even though there is no widely agreed concept or set of criteria for what makes a city smart. All urban planning projects are defined by the advancement of technology to efficiently utilize the resources of a city.

In particular, IoT plays a vital role, as demonstrated by the example of a city being smart is Singapore. Singapore is special in its being a town-state. It has recently announced as a nation an audacious Smart Singapore strategic plan aimed at transforming the city-state into a first smart country through a variety of smart initiatives that leverage intellectual ability, integration, innovation, and

entrepreneurship to become a major global superpower. The part of this planning includes the introduction of non-uniform (heterogeneous) networks which will facilitate mobile users to seamlessly move among wireless networks, and also the roll-out of sensor-containing smart integration gateway boxes, linked through fiber optic cables, to capture and distribute real-time data(Faiz and Shanker 2016) to citizens and government agencies (Garrido et al. 2010). If we don't robustly arrange and conFigure appropriate safety features, we will encounter an un-experienced security threat.

In IoT, configuration management, and security fixes, there are therefore some research efforts to tackle these challenges. In the IoT, computation, resources and bandwidth, the three key constraints are defined and used to establish the basis for the challenges posed. Further discussed the numerous potential futures for the IoT, and what challenges would involve in the successful operations of IoT. The approaches to the problems will vary from what resources are available and an in-depth overview of potential solutions will be discussed depending on available resources. The paper is divided into the following sections: section-2 role of IoT, section -3 motivation for security in IoT, section-4 layered architecture of IoT and security issues, section-5 IoT security vulnerabilities, section-6 types of attacks in IoT, section-7 open issues and future directions, and section-8 conclusion.

IoT ROLE

IoT can help to grow a vast range of industrial domains. The Internet of Things should not only be seen as an evolution of today's internet but as a collection of advance autonomous networks operating their services and infrastructures .While today's modern systems use easy to implement standards and function properly with most methods of communication, computation and storage, there is no such ideal solution that might work on every device within the IoT network, due to the varied restrictions among various devices, resulting in categorizing within the IoT. A huge number of IoT devices (about 25 billion) is used worldwide in 2020. Table 2 shows the various categories of industries where IoT is being used widely.

CATEGORY OF INDUSTRY	2014	2015	2020
Domestic consumer	2,244.5	2,874.9	13,172.5
Vertical business (IoT home-	836.5	1,009.4	3,164.4

security system etc.)			
Horizontal business (robotics etc.)	479.4	623.9	5,158.6
Automotive	189.6	372.3	3,511.1
Total(million)	3750.0	4,880.6	25,006.6

Table 1 – Various Domains Where IoT is Used Widely

Various sectors where IoT helps to grow are discussed as:

Healthcare

IoT can have an effect on health care, which can be helpful to improve living conditions. Sensors are mounted on the instruments that patients use to monitor their health. To increase service reliability, sensitivity, treatment, measurement, etc. (Ashton and others 2009) The data collected by such sensors can be available online to physicians, members of the household and all interested people. In (Korhonen, Parkka, and Van Gils 2003) said that functional deficiencies can be reimbursed through IoT surveillance systems, health monitoring inside home automation is necessary to promote independent living for elder people. A study reveals that wearable sensor technology-based innovations will transform healthcare by allowing for patients effective health monitoring and day-night health status monitoring of an ill person (Pantelopoulos and Bourbakis 2008). A continuous monitoring system of essential parameters allows patients with chronic illness to vacant their hospital bed and, above all, to stay in their own homes (Barnickel, Karahan, and Meyer 2010).

Smart House

IoT devices are installed in houses and workplaces inbuilt with smart sensors and actuators, IoT Technologies are being used to monitor energy usage, track and control infrastructure projects such as lights and HVAC equipment, and carry out workplace safety surveillance (Darianian and Michael 2008). IoT technology can also improve cities by ensuring more effective traffic management, monitoring parking space availability, measuring air quality and informing them when recycling bins are full (Schaffers et al. 2011).

Automated Vehicles

The IoT will impact transportation, and its inception into the market of self-driving cars is emerging. One such car was created by tech giants like Google and so has done by Tesla. The Vehicle Networks should be a global transportation system capable to make their own decisions on getting customers to their desired destinations (Gerla et al. 2014).

Big Data

Big Data is a collection of data that is in huge amount and growing exponentially such as stock market data. Big Data and IoT technologies are interconnected and approx. 90% of worldwide data has already been generated in just two years (Gudivada, Baeza-Yates, and Raghavan 2015). A rapid growth continuously increasing as we are moving towards high-speed networks, camcorders with gigapixel picture capabilities and high data consuming IoT devices. Such data that is collected through apps and websites continue to rise, business owners may attempt to use it to gain a competitive advantage in the current market. Privacy has now turned to be a strategic problem for businesses, and that businesses will target customers who are willing to share information to offer customer-driven personalized service.

DATA GENERATED		
Marker	**Statistics**	**Source**
Overall data generated	Humanity has produced 5 Exabyte (EB) of data from the beginning of human history until 2003	Intel corporation (2013)
Data structure type	Big data is unstructured in approx. 85 % of cases	Berry (2012)
Genome-based data per individual	4 Terabyte (TB)	Miller (2012)
Automobile generated data for each driving hour	25 Gigabyte (GB)	Taveira (2014)
Boeing jet engine generates data every 30 minutes of flight	10 Terabyte(TB)	Higginbotham (2010)
Data increase for electrical usage due to smart grid-enabled by iot:	Globally 680 million smart meters have been deployed by 2017. This will result in approx 280 petabytes (pb) data per year.	Bloomberg (2015)

Table 2 – Overview of Statistics Produced and Stored in the Digital Form about Global Data

.

MOTIVATION FOR SECURITY IN IOT

IoT security is a popular area of study that draws researchers from science, business, and government domains. Many other organizations are also involved in the development and deployment of IoT-based systems around the world (Khan et al. 2012). Threats to IoT systems are fast and easy to enforce. An attacker can breach a residential alarm device by infringing the Radio Frequency(RF) signal that is used to turn the alarm on and off (Ning, Liu, and Yang 2013). Security problems are discussed in (Cesare 2014), such as basic system security, network safety in the IoT. The internet will be connected with more than 200 million devices by the year 2020, with a large portion of such devices being phones, appliances, and a huge opportunity will also be there for the hackers to attempt "DoS" attacks, malicious emails from other hazardous Trojans or Worms.

A well-known organization's (Hewlett Packard) study report states that approx. 80 % of IoT-enabled devices infringed the privacy of user's data such as name, address, date of birth, contact number, etc. On commercial IoT deployments, more than 80 % of systems did not require passwords or having sufficient password length, and approx. 60 % had security flaws on their user application interfaces (Mulani and Pingle 2016). A wide range of protocols and algorithms are available in today's internet environment to solve the wireless network security issues, however, the latest methodologies comprise a restriction on their implementation in the Internet of Things (IoT) domain due to the hardware system and WSN constraints in IoT (Garrido et al. 2010)(Sirohi, Agarwal, and Maheshwari 2019).

Another major factor related to security is that traditional security protocols consume a huge quantity of computing and memory resources. The IoT devices generally have to operate in a harsh environment, unpredict and dangerous environmental conditions around them, where they are vulnerable to a variety of security breaches (Tawalbeh et al. 2020). The Sonic Wall estimates that IoT malware attacks in the IoT system in 2017 was 10.3 million, and in 2018 was 32 million so the growth is more than 200% in just one year. The initial two quarters of the year 2019 already outperformed 55% before the initial two quarters of 2018. If this frequency continues this will be another record-making year for attacks of IoT malware (Awad and Krishnan 2006). As per surveys, lack of security concerns, many of them are very susceptible and prone to exploit and even some can connect with multiple vulnerabilities over the Internet(Atzori, Iera, and Morabito 2010).

DATA IN DIGITAL FORMAT		
Yearly Statistics		**Source**
Rapidly every 18 months, the amount of data processed and stored in an electronic format almost becomes doubled.		Gantz (2011)
2013	5 GB per capita	Bahrami (2015)
	4.4 ZB (Zetta Byte) total	Gantz (2011)
	Datacenter traffic of approx 3.1 zettabytes (ZB)	Cisco (2014)
2014	2.5 billion GB daily; 1.70 megabytes (MB) per capita per minute	Gantz (2011)
2015	14.5 billion of indexed webpages	Woollaston (2013)
2016	1 Zetta Byte global IP data traffic annually	Cisco (2015)
2018	403 Zetta Byte IoE data traffic	Cisco (2014)
	14 GB per capita	Bahrami (2015)
2019	2 ZB annual Internet traffic globally	Cisco (2015)
2020	44 ZB approx. (44 trillion GB)	Gantz (2011)
	10% from IoT equipped Embedded Systems	
	27% via connected mobile devices	

Table 3 - Estimates on the Size of IoT and its Potential Value

LAYERED ARCHITECTURE OF IoT AND SECURITY ISSUES

The IoT network consists of five layers as shown in Fig. 1: perception, network, middleware, application, and business layers. These layers are discussed in details as follows.

Perception Layer

The layer equipped with various cognition systems is called the perception layer, this layer consists of the Wireless Sensor Network (WSN), Radio Frequency Identification (RFID to emit radio waves and receive signal), sensors of all sorts, GPS, Bluetooth and so on. The main objective of the layer of perception is to connect various devices within the IoT network. The perception layer's basic functions are the processing of data from different physical devices and the translation into digital signals. Then the layer of perception conveys data to the above layer i.e. network (Tandon 2020).

Network Layer

The network layer's key equipment is the mobile phone network, internet, and every other secure network type. This layer receives all perception layer information and transmits data to the middleware layer using communication protocols such as MQTT, DDS, IPv4 and IPv6 via transmission media such as 4G, 3G, GSM, ZigBee, Bluetooth, Wi-Fi and WiMAX. Data processing, management and maintenance are the responsibility of the network layer (Atzori, Iera, and Morabito 2010).

Middleware Layer

The middleware layer collects a large amount of information from the network layer and processes information using certain smart processing units, such as cloud computing, to provide explicit interaction with the database system to store the received information's in the cloud (Faiz and Daniel 2020). The middleware layer structure is based on Service Oriented Architecture (SOA) which consists of few processes grouped as applications, service composition, service management, object aggregation, trust, security and privacy management. The application method feature is to carry all machine functions to end-users. The composition of the service cycle gives functions to and manages every smart entity. The process of Object Abstraction is responsible for the access to harmony between various objects with a common language. The method of managing trust, privacy and protection is used to protect the exchanged data (Farooq et al. 2015).

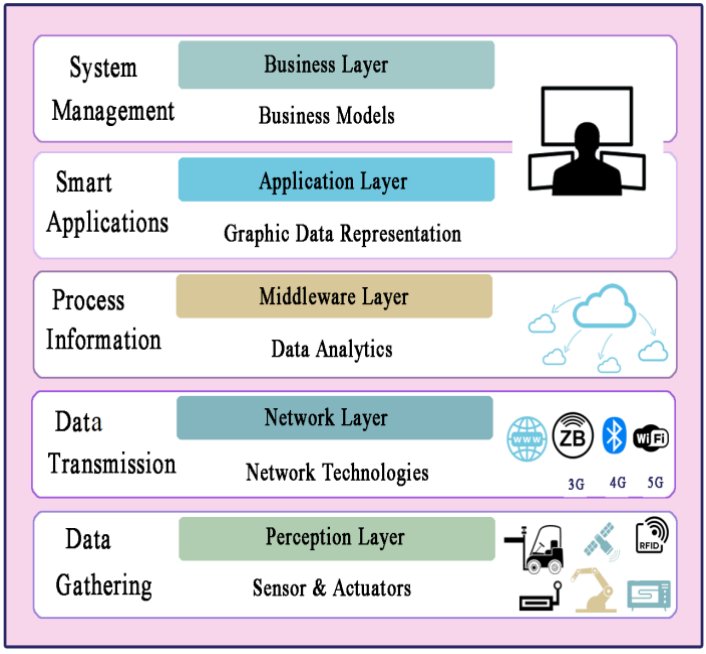

Figure 1 – IoT Layered Architecture

Application Layer

The application layer uses the information collected to accomplish a great deal of functionality. IoT implementations are based on consumer requirements such as business, education, the medical and communication sectors, and they are useful for IoT development (Farooq et al. 2015). The network layer uses different protocol numbers, such as the restricted application protocol (CoAP), the message queue telemetry transport (MQTT) protocol, the extensible message and presence protocol (XMPP) and the advanced message queuing protocol (AMQP).

Business Layer

The business layer is the last layer of architecture in the IoT layers. It is responsible for managing the IoT system's apps , services and business logics (Farooq et al. 2015). The previous business layer is often used to generate various models which are used for different advantages (Sethi and Sarangi 2017).

A comparative analysis of various solutions by different authors addressing the issues in different layers of IoT with limitations are shown in Table 4.

LAYER / METHOD / AUTHOR	ADDRESSING ISSUE	PROPOSED SOLUTION	LIMITATION
Perception layer(AAL) (Brush et al. 2011)	Secure a healthy lifestyle for senior persons	Be in Touch via Intelligent objects and systems like NFC and RFID	This approach does not tackle issues of security and privacy, although it does recognize privacy, Security, and confidentiality as always expected by intended users
Perception layer (cyber sensors) (Ning, Liu, and Yang 2013)	Limitation of dynamic time data/output from real objects	The sensors are capable to capture the data from real objects and the captured data can be made available to carry out actions or responses in dynamic time events	Few technologies for the sensors are yet to come
Perception layer (ASM) (Savola, Abie, and Sihvonen 2012)	Hazards to security are recognized as data integrity and it adapts changes in environmental and restricted changes found by security metrics.	The method has 4 basic steps: 1.Continuous tracking and monitoring 2. Predictive-analytic function. 3. Decision creation 4.Metrics-oriented adaptive security systems.	A major drawback is that sensors can be susceptible to obstruction from other electronic equipment. One major disadvantage is that they do not have security monitoring information.
Network layer (Security middleware) (J. Liu, Xiao, and Chen 2012)	Deliver security to smart home /systems and communicating devices	It uses secure storage, entity identification, audit, security, data encrypt/decrypt technique	Middleware's are future trends, it is still neither widely used nor integrated
Network layer (Authentication and Access control) (Kozlov, Veijalainen, and Ali 2012)	Fixes loopholes in device security and data integrity	To access a computer, a user requests authentication, devices request for approves/refuses a request from the "RA-Registration Authority"	Devices are still much susceptible to eavesdropping attacks and man-in-the-middle attacks.
Application layer (DSM) (Abie and Balasingham 2012)	Security metrics for e- healthcare information systems	To manage security policies and analysis, some essential elements are proposed	It does not answer the methods where to find collecting, measuring, or enforcing protection metrics to security concerns
Application layer (game theory) (Savola, Abie, and Sihvonen 2012)	Attacks in different dynamic systems	Systems attacking approach to build stronger security strategies	Prototyping has still not been released /completed. Therefore it is not clear how the program can handle different complex systems

Application layer (ASTM) (Weib, Weissmann, and Dressler 2005)	A device can respond to environmental changes	Adaptive learning methodology by adjusting the inner constraints and complex architectural changes	ASTM model needs to be tested against unknown threats and complex application domain scenarios.
Application layer (CCM) (You-guo and Ming-fu 2011)	A security metric system based on a risk estimation technique	Security is evaluated in terms of loss of incident assets under this model.	Data attainability and availability poses a major challenge in calculating all security measures

Table 4 – Various Existing Techniques for Security at Different Layers with Limitations

IoT SECURITY VULNERABILITIES

Open Web Application Security Project (OWASP) is a firm that emphasizes information system (IS) security concerns and seeks to raise security standards. Various standards to improve (IS) security is approved by Federal Trade Commission (FTC) an independent agency of the United States government whose aim is the enforcement of civil (non-criminal) antitrust law and to promote consumer protection (Enright 2016), Department of Defense & Information Systems, MITRE, and Payment Card Industry-Data Security Standard (PCI-DSS). They have developed the list of 'ten' major security vulnerabilities in IoT devices:

1. Insecure Network;
2. Privacy Breach;
3. Insecure Internet Interface,
4. Lack of Proper Authentication;
5. Lack of Proper Encryption in Data Transit;
6. Insecure Cloud Interface;
7. Insecure User Interface;
8. Weak Security Configuration;
9. Insecure Firmware; and
10. Weak Physical Protection of the Device (Zhao and Ge 2013).

Several of such security issues are discussed in detail further.

Attack Vectors

Security in IoT systems is one of the major challenges. The IoT system may consist of millions of devices that communicate together and all such communication must be protected against security flaws. Global connectivity ("connect with anyone") and global accessibility ("connect anywhere, anytime") are the main aspects of IoT, there could be a staggering number of networks open to malicious attackers (Leo et al. 2014). Through the design of IoT-enabled sensors, which express that the deployed sensors should have the potential to autonomously sense communicate and route the data; this in effect raises the vulnerability of security risks of the cyber-attack due to the global connectivity of sensors (Roman, Najera, and Lopez 2011).

Attacks Spread Quicker

There are high potential threats generated by different communicating devices every day, and in IoT devices, such risks can occur more frequently than the traditional internet devices have done up to now. Due to the interconnected property of IoT devices, any poorly protected device connected to the system potentially affects the system's reliability and security globally. The FTC (2015) article discussed how high-rate attacks on certain networks of IoT devices can be managed (Atzori, Iera, and Morabito 2010),(K. Rose, Eldridge, and Chapin 2015).

Data Integrity

It is a major issue with IoT. Data integrity includes authentication, reliable communication, and access control. It is important to answer some questions. (1) How do you rely on the data sent by our sensors and trust them? (2) How can we even know that the data is sent by a reliable sensor, not by a bot or any spyware, at all? Thus, protection should not be understood merely as an add-on feature to a system, but in fact, requires a holistic approach throughout all the layers. This means that not only must an IoT device be secure, but the system to which it connects must also be secured (Skarmeta and Moreno 2013).

Lack of Encryption

In the present era of the internet, wireless communication technology is made more reliable by encryption. Encryption is often seen as a key to maintaining the security of the information in IoT (Whitmore, Agarwal, and Da Xu 2015). However, algorithms ought to be developed more efficiently and less energy-consuming to make IoT devices encrypted, and effective key distribution strategies are required (Moore et al. 2006).

Eavesdropping

Eavesdropping is a major security issue in IoT. IoT systems can be more prone to eavesdrop attacks because communications are often wireless and which is mostly unreported thus they can be intruded on. It can be attacked physically which makes it more difficult to achieve high-level security (Moore et al. 2006). In IoT, safe security policies are required to protect from such issues.

DDoS Attack

In a DDoS (Distributed Denial of Service) attack, the targeted device is disrupted by sending a flood of internet traffic by the attacker. The device gets overwhelmed by the huge number of flooded data packets and unable to serve the requests of the legitimate users of the system.

Existing Solution for Various IoT Vulnerabilities

(Hu et al. 2014) proposed a concept of dynamically managing the threshold value of the network for packet transmission to avoid packet losses (one or more of data packets fails to reach its intended destination). The researchers have suggested a system to control the network with the help of a sensor node that monitors the network continuously. An algorithm is also proposed by authors that functions by dynamically managing the threshold value. Looking at the total packet loss situation, the threshold is adjusted in run time (dynamically).

(F. Liu, Cheng, and Chen 2007) proposed an analysis of neighborhood activities based on spatial correlation function with no malicious sensor information inside the concept. This reduces the unnecessary overhead of the network.

(Sarigiannidis, Karapistoli, and Economides 2015) proposed an algorithm to analyses neighborhood activities that are based on the spatial correlation principle no malicious sensor information is needed in the algorithm. A rule-based approach for anomaly detection was proposed by the authors. The proposed concept revolves around the identification of Sybil attacks in WSN monitoring where a reputation system is compromised by the creation of multiple identities.

(Juneja and Arora 2010) proposed a framework on existing infrastructure to avoid the extended version of existing infrastructure and avoid fraudulent messages being transmitted over the network. They propose the use of e-filters

to check false information at different nodes. These sensor nodes are labelled as "adjunct nodes" for tracking network status and carrying out appropriate actions where necessary.

(Kasinathan, Pastrone, et al. 2013) proposed architecture to detect DoS attacks in Low Powered Wireless Personal Area Networks (LoWPAN) based IoT devices. The costs of communication between the proposed architecture and the overhead components are not considered. It exposed to a single point of failure, being a centralized architecture. Variants of the broadcast protocol can be found, i.e. "TESLA" for the Internet of Things is DoS compliant. AI-driven approach to counteracting DDoS by implementing a machine learning-focused preventive design.

(Misra et al. 2011) proposed Service Oriented Architecture (SOA) in IoT to make software components reusable using the concept of interfaces , due to its broad potential to apply for a wide variety of applications such as to get rid of DDoS a cross-layer framework is used. Generally, IoT is a resource constraint and therefore interaction between layers involves a cost.

(Kasinathan, Costamagna, et al. 2013) proposed Intruder Detection System architecture (IDS) which is a software/or hardware component to make up the proposed framework to monitor the IoT systems and the attack detecting system. There is no consideration of the upward scale of the IPv6 over Low -Power Wireless Personal Area Network (6LoWPAN) assessment of the program structure In an IoT network, faulty nodes may be encountered through an attempt of a DoS attack initiated by multi-coordinate nodes. Addressing DDoS and intruder attacks numerous proposed mechanisms are focused on device control and intruder detection. The emergence of a security system over an IoT-based network is resource-intensive since it is based on AI-based algorithms. Therefore novel lightweight solutions are required to detect DoS attacks. In addition to innovative lightweight approaches, Software Defined Network-(SDN) is a new model that allows control of network location from a central premise called the controller. It is an advanced architecture which is dynamic, manageable, cost-effective, and adaptive, making it appropriate for today's applications with high-bandwidth, dynamic nature.

(Pongle and Chavan 2015) elaborates various possibilities to build algorithms to detect DDoS attacks and suspicious attacks such as insider attacks, by monitoring flaws in the controller. It would also remove the responsibility of beating IoT device DDoS attacks to resource enough systems to probably host SDN controllers to connect IoT devices to the gateway. A successful hybrid approach will be helpful to combine IoT gateways with increasing SDN applications and capable to detect effectively and mitigate DDoS in traditional IP networks (Hameed and Ali 2018).Various existing methodologies for

securing IoT in contrast with confidentiality, integrity, authenticity, and availability are shown in Table 5.

AUTHOR	YEAR	METHODOLOGY FOR ACHIEVING SECURITY	MAJOR SECURITY REQUIREMENTS FOCUSED			
			Confidentiality	Integrity	Authentication	Availability
(TAHIR ET AL. 2016)	2016	ICMetric coupled with CRRP	√	X	√	√
(C. LIU, ZHANG, AND ZHANG 2013)	2013	IoT dynamic security based on immune system principles	X	X	X	X
(ZHOU AND CHAO 2011)	2011	Key management, Watermarking	X	X	√	X
(G. S. ROSE 2016)	2016	Nano-electronic security Primitives	√	X	√	√
(DOS SANTOS ET AL. 2015)	2015	ECC cryptography	√	√	√	√
(ZEGZHDA AND STEPANOVA 2015)	2015	Graph topology	X	√	X	X
(RAZA ET AL. 2016)	2016	Shared keys	√	√	√	√

Table 5 – Various Proposed Solutions by Different Authors for Security in IoT

TYPES OF ATTACKS IN IoT

The IoT system could be affected by many types of attacks. The IoT attacks are broadly divided into four major categories: software attack, network attack, physical attack, and encryption attack. The physical attack in IoT occurs when the intruder is near the IoT system. When the attacker accesses the IoT network, network attacks happen and they exploit a certain computer to inflict harm. HW-attack are also called physical attacks these attacks interfere with hardware components and are more difficult to carry out since they require pricey materials. De-packaging of chips, micro-probing are some examples of it. The software attack (SW-attack involves injecting malicious code into the system via trojan horse scripts, worms, / viruses) happens when the IoT program has flaws that permit the hacker to gain access to the IoT devices and damage the system. Eventually, the attack on the encryption of the system occurs when the hacker breaches the IoT layer of encryption to cause an attack(Andrea, Chrysostomou, and Hadjichristofi 2015). Side-channel attack is based on data gained from a device implementation rather than flaws in the algorithm itself (e.g. software bugs). Timing data, power consumption, electromagnetic leakage, and even sound can all give additional sources of data that can be used. It is suggested that IoT must take additional steps to strengthen its protection, like authentication, safe booting of the system using digital certificates, data encryption, and use of the only secure application, so that only legitimate users may access and track IoT device data. Some researchers have identified other kinds of attacks besides these attacks (Babar et al. 2011), and shown in Figure 2.

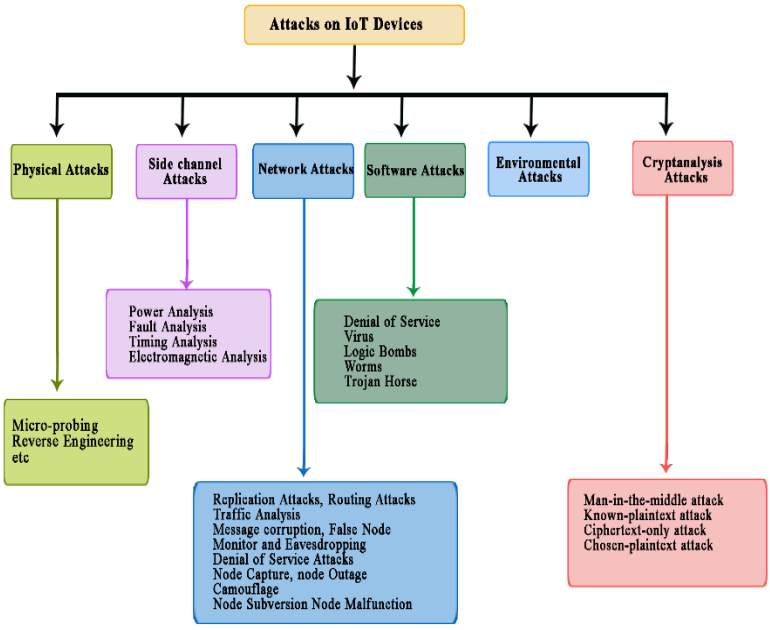

Figure 2 – Classification of Attacks in IoT

As shown in Figure 2, six major key categories of attacks occur in IoT and cause a flaw in the system. Different categories of such attacks are very harmful and among these attacks, the most dangerous type of attacks in IoT is “network attack” which could lead to several troubles for the IoT device and the sharing of information among IoT devices and servers. In Table 6, some existing solutions to these attacks and their role in optimizing the basic security features against most of the types of attacks are discussed.

All the solutions, listed in Table 5, could prevent software-related attacks. However, there is still no proper solution that could avoid the side-channel attack. Therefore, all of them have been configured to deal with basic security operations apart from the last for embedded security, which is a data-driven technique. From Table 5, it can be inferred that a security solution is required in IoT, as most of them concentrate on software attacks without being worried about the device's hardware elements.

COMPARISON PARAMETER OF EXISTING SOLUTIONS (Gordon and Loeb 2002);(Li et al. 2016); (Enright 2016);(Schatz and bashroush 2016);(Spanos and Angelis 2016);(Anderson and Agarwal 2010);(Mulani and Pingle 2016);(Hameed and Ahmed Khan 2018)	**COUNTERS AGAINST ATTACKS**			**SECURITY-BASED OPTIMIZATION FUNCTIONS**			
	HW-attack	**SW-attack**	**Side Channel Attack**	**Flexible**	**Energy Efficiency**	**Cost**	**Computational Time**
A data-driven approach for embedded security		√					
A compiler-hardware approach to software protection for embedded systems	√	√					
A security approach for off-chip memory in embedded microprocessor systems		√				√	
An FGPA (field programmable gate array-a semiconductor based integrated circuit) implementation of a flexible secure ECC (elliptic curve cryptography) processor		√		√			√
Embedded security: new trends in the personal recognition system	√	√				√	
Implementation of embedded security on dual-virtual CPU systems		√			√	√	
Hardware-software implementation of public-key cryptography for wireless sensor networks		√		√		√	

Table 6 – Comparison of Existing Solutions of Different Attacks

OPEN ISSUES AND FUTURE DIRECTIONS

There are various technology and platforms are used to increase the variety of IoT applications. So, there may be compatibility, portability, and scalability of the system for various application software and hardware. The technological age of IoT will be relying on a large number of devices is forecast to expand substantially. Although many of the technology-related privacy and security challenges exist, developers and researchers need to work in collaboration to resolve those threats, as they have accomplished with several other related technologies. It is required to discover various lightweight algorithms to prevent various types of attacks and to find a technique to prevent side-channel attacks in IoT that present a challenge that researchers need to solve. The security and privacy issues and their limitations should be tackled and build for the customer to easily retain the IoT devices and applications. Early efforts can be found in this direction. Many challenges and problems still need to be tackled such as establishing a robust unified IoT security management system, privacy policies for context-awareness, efficient holistic frameworks, lightweight strategy for system resource constraints and SDN needs to be extensively researched so that IoT network management systems can't be tailored. In the future, we would like to develop a desktop or mobile app to acquire higher awareness of security enhancement and control that would be implemented for various IoT systems for a robust and secure user experience.

Security Aspects	Major Challenges	Current Issues and Future Directions
Privacy	Profiling and tracking, Localization,Secure data transmission.	Enhanced privacy-preserving frameworks, privacy policies for context awareness, privacy-preservation based on game theory incentives, virtualization of network and Software Defined Networks (SDN)
Confidentiality	A system with Lightweight primitives (hash functions, low resource device etc.) to reduce encryption/decryption computation time, consume low number of resources.	Use of SDNs to provide lightweight security, Efficient holistic frameworks.

Secure Routing	Separation of malicious nodes, security protocol, self-stabilization, protection of location privacy, secure route adaption	Efficient and fine-grain control of SDN routing activities, Routing protocol architecture based on IoT Network efficiency.
Robust and Resilient management	Quick detection of threats and security attacks. Tolerance of attack. Rapid failure recovery.	SDN based centralized network management frameworks.
Detection of attack (insider and ddos)	Resource proficient DoS attack detection. An efficient resource mitigation system. Effective identification of intruder attacks.	Lightweight strategy for system resource constraints, centralized algorithms for SDN detection and prevention.

Table 7 – Comparative Assessment of Challenges and Current/ Future Problems in IoT for Different Security Requirements.

CONCLUSIONS

In IoT, privacy is extremely important since the features of this network differ from the traditional Internet network, such issues are identified and discussed in this paper. Privacy and security standards play the most vital role in the formulation of security solutions and IoT network management. The paper focused on the IoT layers and features to confront IoT security issues and described various types of threats, attacks, exposure, and vulnerabilities for each layer of IoT. The paper also presented comparisons between security measures for each IoT layer of security needed to evaluate the effect of the security mechanism on the utilization of power and time. Such comparisons had a major impact on the selection of appropriate security strategies that provide low energy and less time consumption. We have reviewed numerous algorithms such as ECC-cryptography, water-marking and their impacts to protect the IoT network from various attacks along with classifying and exploring the state-of-the-artwork in the IoT network to ensure security. Efforts in the provision of privacy, a lightweight security system, secure routing, robustness and resilience management, DoS, and the detection of intruder attacks are discussed in depth.

We have discussed the efforts and initiatives such as SDN in this direction along with future insight.

REFERENCES

Abie, Habtamu, and Ilangko Balasingham. 2012. "Risk-Based Adaptive Security for Smart IoT in EHealth." In **Proceedings of the 7th International Conference on Body Area Networks**, , 269–75.

Akyildiz, Ian F, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. 2002. "A Survey on Sensor Networks." **IEEE Communications magazine** 40(8): 102–14.

Anderson, Catherine L, and Ritu Agarwal. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions." **MIS quarterly**: 613–43.

Andrea, Ioannis, Chrysostomos Chrysostomou, and George Hadjichristofi. 2015. "Internet of Things: Security Vulnerabilities and Challenges." In *2015* **IEEE Symposium on Computers and Communication (ISCC)**, , 180–87.

Ashton, Kevin, and others. 2009. "That 'Internet of Things' Thing." **RFID journal** 22(7): 97–114.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. 2010. "The Internet of Things: A Survey." **Computer networks** 54(15): 2787–2805.

Awad, Naveen Farag, and Mayuram S Krishnan. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization." **MIS quarterly**: 13–28.

Babar, Sachin et al. 2011. "Proposed Embedded Security Framework for Internet of Things (Iot)." In *2011* **2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace \& Electronic Systems Technology (Wireless VITAE)**, 1–5.

Barnickel, Johannes, Hakan Karahan, and Ulrike Meyer. 2010. "Security and Privacy for Mobile Electronic Health Monitoring and Recording Systems." In **2010 IEEE International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)**, 1–6.

Brush, A J Bernheim et al. 2011. "Home Automation in the Wild: Challenges and Opportunities." In **Proceedings of the SIGCHI Conference on Human Factors in Computing Systems**, 2115–24.

Bahrami, M., Khan, A., & Singhal, M. (2016, June). An energy efficient data

privacy scheme for IoT devices in mobile cloud computing. In ***2016 IEEE International Conference on Mobile Services (MS)*** (pp. 190-195).

Cesare, Silvio. 2014. "Breaking the Security of Physical Devices." **Presentation at Blackhat** 14.

Corcho, Oscar, and Raúl Garc\'\ia-Castro. 2010. "Five Challenges for the Semantic Sensor Web." **Semantic Web** 1(1, 2): 121–25.

Darianian, Mohsen, and Martin Peter Michael. 2008. "Smart Home Mobile RFID-Based Internet-of-Things Systems and Services." In **2008 International Conference on Advanced Computer Theory and Engineering**, 116–20.

Dohr, Angelika et al. 2010. "The Internet of Things for Ambient Assisted Living." In **2010 Seventh International Conference on Information Technology: New Generations,** 804–9.

Enright, Cathal. 2016. "An Exploratory Study of the Security and Privacy Issues Affecting the Adoption of the Internet of Things."

Faiz, Mohammad, and A K Daniel. 2020. "Fuzzy Cloud Ranking Model Based on QoS and Trust." In **2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)**, 1051–57.

Faiz, Mohammad, and Udai Shanker. 2016. "Data Synchronization in Distributed Client-Server Applications." In *2016 IEEE* **International Conference on Engineering and Technology (ICETECH)**, 611–16.

Farooq, M Umar et al. 2015. "A Review on Internet of Things (IoT)." **International journal of computer applications** 113(1): 1–7.

Forecasting, B R M. 2011. **Sensors: Technologies and Global Markets.**

Gantz, J., & Reinsel, D. (2011). Extracting value from chaos. **IDC iview**, 1142(2011), 1-12.

Garrido, Pilar Castro, Guillermo Matas Miraz, Irene Luque Ruiz, and Miguel Ángel Gómez-Nieto. 2010. "A Model for the Development of NFC Context-Awareness Applications on Internet of Things." In **2010 Second International Workshop on Near Field Communication**, 9–14.

Gerla, Mario, Eun-Kyu Lee, Giovanni Pau, and Uichin Lee. 2014. "Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds." In **2014 IEEE World Forum on Internet of Things (WF-IoT),** 241–46.

Gordon, Lawrence A, and Martin P Loeb. 2002. "The Economics of Information Security Investment." **ACM Transactions on Information and System Security (TISSEC)** 5(4): 438–57.

Gudivada, Venkat N, Ricardo Baeza-Yates, and Vijay V Raghavan. 2015. "Big Data: Promises and Problems." **Computer** 48(03): 20–23.

Hameed, Sufian, and Hassan Ahmed Khan. 2018. "SDN Based Collaborative Scheme for Mitigation of DDoS Attacks." **Future Internet** 10(3): 23.

Hameed, Sufian, and Usman Ali. 2018. "HADEC: Hadoop-Based Live DDoS Detection Framework." **EURASIP Journal on Information Security** 2018(1): 1–19.

Hu, Yu, Yuanming Wu, Hongshuai Wang, and others. 2014. "Detection of Insider Selective Forwarding Attack Based on Monitor Node and Trust Mechanism in WSN." **Wireless Sensor Network** 6(11): 237.

Juneja, Dimple, and Neha Arora. 2010. "An Ant Based Framework for Preventing DDoS Attack in Wireless Sensor Networks." **arXiv preprint arXiv:1007.0413.**

Kasinathan, Prabhakaran, Gianfranco Costamagna, et al. 2013. "An IDS Framework for Internet of Things Empowered by 6LoWPAN." In **Proceedings of the 2013 ACM SIGSAC Conference on Computer \& Communications Security**, 1337–40.

Kasinathan, Prabhakaran, Claudio Pastrone, Maurizio A Spirito, and Mark Vinkovits. 2013. "Denial-of-Service Detection in 6LoWPAN Based Internet of Things." In **2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)**, 600–607.

Khan, Rafiullah, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. 2012. "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges." In **2012 10th International Conference on Frontiers of Information Technology**, 257–60.

Korhonen, Ilkka, Juha Parkka, and Mark Van Gils. 2003. "Health Monitoring in the Home of the Future." **IEEE Engineering in medicine and biology magazine** 22(3): 66–73.

Kozlov, Denis, Jari Veijalainen, and Yasir Ali. 2012. "Security and Privacy Threats in IoT Architectures." In **BODYNETS**, , 256–62.

Leo, Marco, Federica Battisti, Marco Carli, and Alessandro Neri. 2014. "A Federated Architecture Approach for Internet of Things Security." In **2014 Euro Med Telco Conference (EMTC)**, 1–5.

Li, Tong et al. 2016. "Security Attack Analysis Using Attack Patterns." In **2016 IEEE Tenth International Conference on Research Challenges in Information Science (RCIS)**, 1–13.

Liu, Caiming, Yan Zhang, and Huaqiang Zhang. 2013. "A Novel Approach to IoT Security Based on Immunology." In **2013 Ninth International**

Conference on Computational Intelligence and Security, 771–75.

Liu, Fang, Xiuzhen Cheng, and Dechang Chen. 2007. "Insider Attacker Detection in Wireless Sensor Networks." In **IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications**, 1937–45.

Liu, Jing, Yang Xiao, and C L Philip Chen. 2012. "Authentication and Access Control in the Internet of Things." In **2012 32nd International Conference on Distributed Computing Systems Workshops**, 588–92.

Misra, Sudip et al. 2011. "A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things." In **2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing**, 114–22.

Moore, David et al. 2006. "Inferring Internet Denial-of-Service Activity." **ACM Transactions on Computer Systems (TOCS)** 24(2): 115–39.

Mulani, Tanjim T, and Subash V Pingle. 2016. "Internet of Things." **International Research Journal of Multidisciplinary Studies** 2(3).

Narayan, Vipul, and A K Daniel. 2020. "Design Consideration and Issues in Wireless Sensor Network Deployment."

Narayan, Vipul, and A K Daniel. 2020. "Multi-Tier Cluster Based Smart Farming Using Wireless Sensor Network." In **2020 5th International Conference on Computing, Communication and Security (ICCCS)**, 1–5.

Narayan, Vipul, and A K Daniel. 2021. "A Novel Approach for Cluster Head Selection Using Trust Function in WSN." **Scalable Computing: Practice and Experience** 22(1): 1–13.

Narayan, Vipul, and A K Daniel. 2021. "RBCHS: Region-Based Cluster Head Selection Protocol in Wireless Sensor Network." In **Proceedings of Integrated Intelligence Enable Networks and Computing**, Springer, 863–69.

Ning, Huansheng, Hong Liu, and Laurence T Yang. 2013. "Cyberentity Security in the Internet of Things." **Computer** 46(4): 46–53.

Pantelopoulos, Alexandros, and Nikolaos Bourbakis. 2008. "A Survey on Wearable Biosensor Systems for Health Monitoring." In **2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society**, 4887–90.

Pongle, Pavan, and Gurunath Chavan. 2015. "A Survey: Attacks on RPL and 6LoWPAN in IoT." In *2***015 International Conference on Pervasive Computing (ICPC)**, 1–6.

Raza, Shahid, Ludwig Seitz, Denis Sitenkov, and Göran Selander. 2016. "S3K: Scalable Security with Symmetric Keys—DTLS Key Establishment for the Internet of Things." **IEEE Transactions on Automation Science and Engineering** 13(3): 1270–80.

Roman, Rodrigo, Pablo Najera, and Javier Lopez. 2011. "Securing the Internet of Things." **Computer** 44(9): 51–58.

Rose, Garrett S. 2016. "Security Meets Nanoelectronics for Internet of Things Applications." In **2016 International Great Lakes Symposium on VLSI (GLSVLSI)**, 181–83.

Rose, Karen, Scott Eldridge, and Lyman Chapin. 2015. "The Internet of Things: An Overview." **The internet society (ISOC)** 80: 1–50.

Dos Santos, Giederson Lessa et al. 2015. "A DTLS-Based Security Architecture for the Internet of Things." In **2015 IEEE Symposium on Computers and Communication (ISCC)**, 809–15.

Sarigiannidis, Panagiotis, Eirini Karapistoli, and Anastasios A Economides. 2015. "Detecting Sybil Attacks in Wireless Sensor Networks Using UWB Ranging-Based Information." **Expert Systems with Applications** 42(21): 7560–72.

Savola, Reijo M, Habtamu Abie, and Markus Sihvonen. 2012. "Towards Metrics-Driven Adaptive Security Management in e-Health IoT Applications." In *BODYNETS*, , 276–81.

Schaffers, Hans et al. 2011. "Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation." In **The Future Internet Assembly**, 431–46.

Schatz, Daniel, and Rabih Bashroush. 2016. "The Impact of Repeated Data Breach Events on Organisations' Market Value." **Information & Computer Security.**

Sethi, Pallavi, and Smruti R Sarangi. 2017. "Internet of Things: Architectures, Protocols, and Applications." **Journal of Electrical and Computer Engineering** 2017.

Sirohi, Preeti, Amit Agarwal, and Piyush Maheshwari. 2019. "A Comparative Study of Cloud Computing Service Selection." **International Journal of Engineering and Advanced Technology** 8(5): 259–66.

Skarmeta, Antonio, and M Victoria Moreno. 2013. "Internet of Things." In **Workshop on Secure Data Management**, 48–53.

Spanos, Georgios, and Lefteris Angelis. 2016. "The Impact of Information Security Events to the Stock Market: A Systematic Literature Review." **Computers & Security** 58: 216–29.

Surie, Dipak, Olivier Laguionie, and Thomas Pederson. 2008. "Wireless Sensor

Networking of Everyday Objects in a Smart Home Environment." In **2008 International Conference on Intelligent Sensors, Sensor Networks and Information Processing**, 189–94.

Tahir, Ruhma, Hasan Tahir, Klaus McDonald-Maier, and Anil Fernando. 2016. "A Novel ICMetric Based Framework for Securing the Internet of Things." In **2016 IEEE International Conference on Consumer Electronics (ICCE)**, 469–70.

Tandon, Aditya. 2022. "Survey of Security Issues in Cyber-Physical Systems." In **Machine Learning, Advances in Computing, Renewable Energy and Communication**, Springer, 347–57.

Tawalbeh, Lo'ai et al. 2020. "IoT Privacy and Security: Challenges and Solutions." **Applied Sciences** 10(12): 4102.

Vasseur, Jean-Philippe, and Adam Dunkels. 2008. "Ip for Smart Objects." **White Paper** 1: 1–7.

Vermesan, Ovidiu et al. 2011. "Internet of Things Strategic Research Roadmap." **Internet of things-global technological and societal trends** 1(2011): 9–52.

Weiß, Steffen, Oliver Weissmann, and Falko Dressler. 2005. "A Comprehensive and Comparative Metric for Information Security." In **Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM2005)**, 1–10.

Whitmore, Andrew, Anurag Agarwal, and Li Da Xu. 2015. "The Internet of Things—A Survey of Topics and Trends." **Information systems frontiers** 17(2): 261–74.

You-guo, Li, and Jiang Ming-fu. 2011. "The Reinforcement of Communication Security of the Internet of Things in the Field of Intelligent Home through the Use of Middleware." In **2011 Fourth International Symposium on Knowledge Acquisition and Modeling**, 254–57.

Zegzhda, Dmitry, and Tatiana Stepanova. 2015. "Achieving Internet of Things Security via Providing Topological Sustainability." In **2015 Science and Information Conference (SAI)**, 269–76.

Zhao, Kai, and Lina Ge. 2013. "A Survey on the Internet of Things Security." In **2013 Ninth International Conference on Computational Intelligence and Security**, 663–67.

Zhou, Liang, and Han-Chieh Chao. 2011. "Multimedia Traffic Security Architecture for the Internet of Things." **IEEE Network** 25(3): 35–40.