Journal Pre-proof

A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT

Jayasree Sengupta, Sushmita Ruj, Sipra Das Bit

PII: S1084-8045(19)30341-8

DOI: https://doi.org/10.1016/j.jnca.2019.102481

Reference: YJNCA 102481

To appear in: *Journal of Network and Computer Applications*

Received Date: 18 April 2019

Revised Date: 20 September 2019

Accepted Date: 30 October 2019

Please cite this article as: Sengupta, J., Ruj, S., Bit, S.D., A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT, *Journal of Network and Computer Applications* (2019), doi: https://doi.org/10.1016/j.jnca.2019.102481.

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2019 Published by Elsevier Ltd.

Journal Pre-proof

A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT

Jayasree Sengupta[a,*], Sushmita Ruj[b], Sipra Das Bit[a]

[a] *Indian Institute of Engineering Science and Technology, Howrah, India*
[b] *CSIRO Data61, Australia and Indian Statistical Institute, India*

Abstract

In recent years, the growing popularity of Internet of Things (IoT) is providing a promising opportunity not only for the development of various home automation systems but also for different industrial applications. By leveraging these benefits, automation is brought about in the industries giving rise to the Industrial Internet of Things (IIoT). IoT is prone to several cyberattacks and needs challenging approaches to achieve the desired security. Moreover, with the emergence of IIoT, the security vulnerabilities posed by it are even more devastating. Therefore, in order to provide a guideline to researchers, this survey primarily attempts to classify the attacks based on the objects of vulnerability. Subsequently, each of the individual attacks is mapped to one or more layers of the generalized IoT/IIoT architecture followed by a discussion on the countermeasures proposed in literature. Some relevant real-life attacks for each of these categories are also discussed. We further discuss the countermeasures proposed for the most relevant security threats in IIoT. A case study on two of the most important industrial IoT applications is also highlighted. Next, we explore the challenges brought by the centralized IoT/IIoT architecture and how blockchain can effectively be used towards addressing such challenges. In this context, we also discuss in detail one IoT specific Blockchain design known as Tangle, its merits and demerits. We further highlight the most relevant Blockchain-based solutions provided in recent times to counter the challenges posed by the traditional cloud-centered applications. The blockchain-related solutions provided in the context of two of the most relevant applications for each of IoT and IIoT is also discussed. Subsequently, we design a taxonomy of the security research areas in IoT/IIoT along with their corresponding solutions. Finally, several open research directions relevant to the focus of this survey are identified.

Keywords: IIoT, Security, Privacy, Blockchain, Smart Factory, Smart Grid, Supply Chain, E-Healthcare, VANET.

*Corresponding author
Email addresses: jayasree202@gmail.com (Jayasree Sengupta), sushmita.ruj@gmail.com (Sushmita Ruj), sdasbit@yahoo.co.in (Sipra Das Bit)

Journal Pre-proof

1. Introduction

With the advent of a large number of low-cost powerful devices like sensors, RFIDs, etc. coupled with a variety of communication mediums, Internet of Things (IoT) has gained tremendous popularity in the last decade. IoT is a group of interconnected static and/or mobile objects such as devices equipped with communication, sensors, and actuator modules connected through the Internet. IoT is diversifying its reach as the number of connected devices is spanning across cities to build smarter systems. Such systems are formed by integrating our daily objects with smart tiny devices to create a fully automated intelligent system capable of reducing human labor. For example, several household appliances, and other electronic devices can be connected together on the network, to bring humans a more intelligent life. According to a report published by Ericsson, the number of connected IoT devices in 2022 will be around 18 billion [1]. In addition to this, recently the application of IoT in the industries where the worlds of production and network connectivity are integrated with Cyber Physical Systems (CPS) is referred to as Industrial IoT (IIoT) [2]. IIoT aims to produce intelligent manufacturing goods and thereby establish smart factories with tight connections between customers and business partners. With the emergence of IIoT, Industry 4.0 forms a subset offering special emphasize to manufacturing industry scenarios where the focus is on digitizing and integrating all physical processes across the entire organization [3]. Industry 4.0 is an advancement over Industry 3.0 where the machines are equipped with sensors, wireless connectivity and connected with CPS in order to visualize the entire production flow to make intelligent decisions.

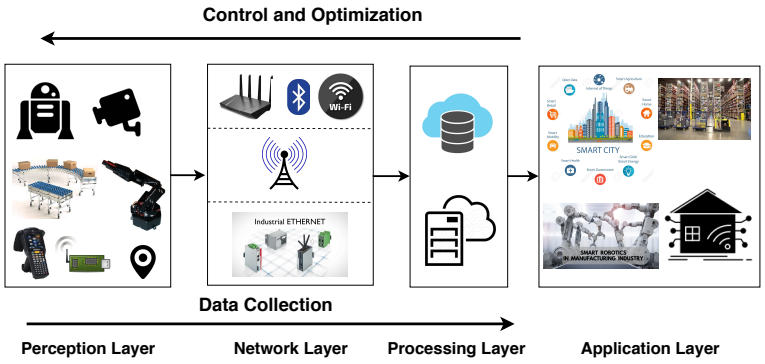

Figure 1: *Generalized IoT/IIoT System Architecture*

Figure 1 shows a general IoT/IIoT architecture which is composed of machines and equipments, networks, cloud and applications [4]. The system is a closed loop for producing specific and personalized products to cater the end users needs. It consists of four layers such as Perception, Network, Processing and Application Layer. The perception layer consists of devices like sensors of different types, RFID scanners, surveillance cameras, GPS modules etc. For an industrial setting, all these devices maybe accompanied by equipments like

Journal Pre-proof

Automated Guided vehicles (AGVs), conveyor systems, industrial robots etc. These devices are responsible for capturing sensory data, monitoring environmental conditions and production floors, transporting raw goods etc. [4]. The Network layer may consist of WiFi, Bluetooth, Zigbee, 3G etc. with protocols like IPv4, IPv6 and are responsible for transmitting information to the processing systems of the next layer. In an industrial setting, industrial Ethernet forms the basis of this layer and transmits data either to the cloud and/or other equipments [4]. The Processing layer consists of servers and databases and is responsible for executing several tasks such as decision making, computing optimization algorithms, storing massive amounts of data [4]. Finally, the Application layer is responsible for delivering application specific needs to cater the end users. Some of the important IoT based applications are Smart Home, Smart City, E-Healthcare, Vehicular Ad-Hoc Network (VANET) etc. while Smart Grid, Smart Factory, Smart Robotics, Supply Chain, Amazon's Reinventing Warehousing etc are considered as IIoT applications. Summarily, the centralized IoT/IIoT network architecture described above has the following drawbacks [5]:

- It creates a central point of failure which may cause the entire network to get paralyzed.
- Users have almost limited or no control over their data stored in centralized servers, and users' sensitive data maybe misused.
- Data stored in centralized servers can be tampered or deleted, therefore it lacks guaranteed traceability and accountability.
- A centralized server can significantly limit the growth of IoT due to inefficient handling of huge amount of end-to-end communications.

The tremendous growth of IoT also demands the enforcement of proper security and privacy policies to prevent any kind of system vulnerabilities/threats. Further, in IIoT as reliability, scalability and power consumption are a few of the additional important concerns. In this context, the traditional security solutions are not always appropriate. Therefore, this survey is primarily aimed to focus on the various security attacks categorized on the basis of objects of attack which are relevant to IoT. A few of these attacks are also equally important in an IIoT environment. This object based classification of attacks would help the researchers, practitioners and industry people to determine which attacks are relevant to their respective application domain. Further, they would easily be able to analysis the existing solutions and come up with new ones depending on the type of applications they are working on. Certain attacks relevant to IoT can have even more devastating effects in an IIoT environment. For example, if an adversary launches a replay attack on commands issued to an industrial robot carrying raw materials from the inventory to the production floor, it may lead to a shutdown of the assembly line at the production floor. Thus we also provide a detail overview of how the traditional security issues and the most relevant threats are dealt with respect to the industrial

Journal Pre-proof

IoT (IIoT) domain. To provide security and privacy benefits, the generalized IoT/IIoT architecture requires third-party entities, where the users share their sensitive data with such entities.

Blockchain provides a suitable alternative to the above challenges by proposing a secure and distributed environment for IoT. A blockchain is basically a chain of timestamped blocks which are linked by cryptographic hashes and acts like a distributed ledger whose data are shared among a network of peers [6]. Thus, in this survey we also highlight how the integration of blockchain technology has been able to provide solutions to a few of the major challenges faced by generalized IoT/IIoT architectures. This discussion is further enriched by providing application specific blockchain solutions for both IoT and IIoT. Our major contributions and the organization of the paper are provided in the following two subsections.

1.1. Major Contributions

Several surveys [7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25] have already been conducted on various aspects of IoT/IIoT security and its integration with blockchain, however to the best of our knowledge, no promising work on classification of security threats on the basis of objects of attack for IoT have so far been reported. Further, most of the reported works on IIoT have not highlighted the attacks, security vulnerabilities and their respective solutions. Also no significant work on efficient handling of security vulnerabilities of various IoT/IIoT applications by leveraging the benefits offered by Blockchain technology has been discussed. All of these facts motivate us to make the following contributions in our research paper:

- Firstly, we classify attacks on the basis of objects of vulnerability (i.e. devices, network, software or data) and provide some examples of relevant real life attacks for each of the said categories. We also map each of these attacks to one or more layers of the generalized IoT/IIoT architecture for which the attacks are relevant.
- We review each of these attacks individually and highlight the corresponding countermeasures proposed with respect to the IoT system.
- We further emphasis on the major security concerns prevalent in the industrial domain with the countermeasures proposed in literature. Additionally, we provide a case study on two of the most relevant applications of IIoT. The case study is characterized with a literature review on the most relevant security related research in the respective fields.
- Next we highlight the interesting features of blockchain and how integrating it with various IoT and IIoT applications can prove to be extremely beneficial. For this, we choose two applications from each of IoT/IIoT and review the relevant works that have proposed blockchain based solutions to handle challenges or offer additional benefits to such systems.

Journal Pre-proof

- We further contribute to this survey by providing a taxonomy of IoT/IIoT security research areas with their corresponding countermeasures proposed in literature.
- Finally, we discuss on some of the open research directions relevant to the areas highlighted in this survey.

1.2. Organization

The remainder of the paper is structured as follows. In Section 2, we discuss some of the prominent existing survey works on security/privacy concerns in IoT/IIoT and blockchain for IoT/IIoT as the background of the present work. In Section 3, we identify the security attacks in IoT in general followed by discussion on the countermeasures. Section 4 discusses on Industrial IoT and highlights the notable countermeasures proposed. It also provides a case study on two important applications of IIoT. Section 5 discusses how blockchain has left a noteworthy impact in the field of IoT in general and IIoT in particular by dealing effectively with some of the critical challenges faced by both IoT and IIoT. Section 6 provides a taxonomy of major IoT/IIoT security research areas including both blockchain and traditional based solutions. Finally, Section 7 highlights the open research areas and Section 8 concludes the work.

2. Related Work

In the recent years, few surveys have been conducted to emphasize the research advancements in various domains of IoT/IIoT security and privacy. In the following subsections we first categorize the existing survey works on the basis of IoT related objectives, followed by IIoT. Next, we review some of the important works relevant to the integration of blockchain in these two domains. Finally, we highlight how their broad objectives are different from our perspective.

2.1. Surveys on IoT

In the following two subsections we emphasize the research advancements in IoT security and privacy by categorizing the existing survey works [7, 8, 9, 10, 11, 12, 13, 14, 15, 16] on the basis of their broad objectives.

2.1.1. Security Issues

Huge advancements and commercialization in IoT has exposed several security vulnerabilities of the IoT systems. To explore this further and give a detail insight to the researchers, a few surveys have been reported which we review here.

In one such survey [7] authors have referred CISCO's seven layer model [26], where they have mainly concentrated on the edge-side layer of IoT. In another work [8], Yang et al. have highlighted the security problems and solution for a 4-layered IoT architecture. On the other hand, Frustaci et al. [9] have

Journal Pre-proof

demonstrated threats against the IoT system in three layers i.e. perception, transportation and application layers. Then they have highlighted the critical security vulnerabilities of the communication and networking protocols used in these layers. Correspondingly, in the survey [10], Alaba et al. have provided a taxonomy classifying security threats based on Application, Architecture, Communication and Data. They have also demonstrated security vulnerabilities in different application such as smart environment, healthcare etc. Contrary to that in [11], authors have discussed the security threats and solutions with respect to IoT deployment architecture. The survey [12], has highlighted security vulnerabilities and existing solutions in IoT majorly into categories like Lightweight Cryptographic Framework; Secure Routing and Forwarding; Robustness and Resilience Management & Denial of Service (DoS) and Inside Attack Detection. In comparison to that, Kouicem et al. [13] have initially highlighted the security requirements of six major IoT applications. Then they have explored IoT security solutions for three major categories of confidentiality, availability and privacy by discussing both classical approaches as well as new technologies (like blockchain). Finally, Sfar et al. [14] have presented an overview of IoT security using a cognitive and systematic approach.

2.1.2. Privacy Concerns

Presently, privacy is an important aspect as privacy threats are limiting the success of IoT. Therefore, surveys focused on critical aspects related to privacy are highlighted below.

Among the three works, already discussed under Section 2.1.1, one such work [12] has also highlighted privacy related vulnerabilities and its existing solutions. Contrary to that, the authors in [13] privacy solutions related to four domains : (a) Zero Knowledge Proof (b) K-Anonymity models (c) Data Tagging (d) Data Obfuscation. Additionally, in the work [14], authors have highlighted privacy preserving solutions for two major areas: (a) Data Privacy and (b) Access Privacy. Ziegeldorf et al. [15] have analyzed privacy threats in seven categories in the light of evolving IoT along with pointing out the major challenges. Finally, in the work [16] authors have reviewed principles of privacy laws and Privacy Enhancing Technologies (PETs) and studied privacy protection problem for 4-layered IoT architecture.

From the discussions in Section 2.1.1, we can conclude that in the domain of IoT security issues researchers have primarily focused on highlighting security vulnerabilities and their solutions across different layers of the IoT architecture and its communication protocols. They have also discussed about application specific security vulnerabilities and its respective solutions. Correspondingly, from Section 2.1.2, we can conclude that researchers have focused on privacy threats relating to IoT and its architecture along with privacy laws. However, none of these surveys focus on the different categories of security attacks that can be launched in an IoT system. This has motivated us to classify security attacks on IoT systems into four different categories on the basis of objects of attack (i.e. devices, networks, software or data). We further map each of these attacks to one or more layers of the IoT system architecture. This object based classification of attacks would help the researchers, practitioners and industry people to determine which attacks are

Journal Pre-proof

relevant to their respective application domain. Further, they would easily be able to analysis the existing solutions and come up with new ones depending on the type of applications they are working on. Although our work doesn't deal with privacy concerns in general, but a lot of the reviewed works have either dealt with data privacy or user privacy, which are discussed under Section 3.4.1 and 5 respectively. Therefore, we discuss Privacy related concerns as a broad research area under Section 6 along with their respective countermeasures.

2.2. Surevys on IIoT

Recently, with the growing popularity of applying IoT in industries, a number of surveys [17, 18, 19, 20] have highlighted the research advancements in the domain of Industrial IoT.

In one such survey [17], authors have initially reviewed the relationship between IIoT and various concepts like Industry 4.0, Cyber Physical Systems (CPS) etc. Then they have developed an analysis framework to characterize IoT devices majorly into six categories, which has further helped to analyze security vulnerabilities. In another work [18], the authors have reviewed the Service Oriented Architecture (SOA) of IoT. Next it elaborates five industrial sectors in which IoT can be applied. Finally, they also demonstrate the standardization and open technical research challenges that arise by incorporating IoT in industries. The authors in [19] mainly discuss the predominant technologies that are required for setting up Industry 4.0. They explore each of these technologies in details and the corresponding works that have been done in each of these fields to promote the growth of Industry 4.0. Finally, the work [20] provides a comprehensive review on the key technologies required for Industry 4.0 similar to [19]. Additionally, they have done an extensive survey on the cyber physical systems and internet services required for the development of Smart Factory for Industry 4.0.

To the best of our knowledge gathered by summarizing the above discussions, it is clear that most of the reported works have not highlighted the attacks and security concerns prevalent especially in IIoT systems. Therefore, during surveying we emphasize on the major security concerns including certain basic security primitives like authentication, access control etc. and a few predominant attacks prevalent in the industrial domain along with their corresponding countermeasures proposed in literature. Such strong emphasis is made as developing proper authentication/authorization schemes are very crucial for IIoT systems because the presence of malicious users/users having improper access rights can severely affect these systems. Further, certain specific attacks may have devastating outcomes in IIoT specific scenarios.

2.3. Surveys on Integration of Blockchain in IoT/IIoT

As Blockchain technology is radically reshaping how different applications work and perform, a few surveys [21, 22, 23, 24, 25, 27, 28] have been conducted to highlight the possibilities of integrating blockchain into IoT/IIoT applications.

Journal Pre-proof

In one such work [21], the authors first discuss the most relevant Blockchain-based IoT (BIoT) applications. They also provide a detailed analysis on the important aspects pertaining to the development of BIoT applications along with the current challenges involved in doing so. In another work [22], the authors mainly highlight both the benefits as well as the challenges of integrating blockchain into IoT applications. Contrary to that, Reyna et al. [23] actually provide an extension of the aforementioned surveys by not only analyzing the improvements and the challenges brought about by Blockchain based IoT applications but also by studying the different existing blockchain-IoT platforms and evaluate their performances. On the other hand, Wang et al. [24] have highlighted the blockchain technologies which can be used to handle the potential challenges introduced by IoT. They also elaborate on the existing works that has proposed enhancements on the blockchain consensus protocols and data structures to suit the requirements of BIoT applications alongside handling their potential challenges. In another work, Wang et al. [25] have summarized the security requirements to develop blockchain based IoT as well as IIoT (specifically Industry 4.0) solutions. They have also explored how the integration of blockchain, using its intrinsic properties can help attain better security in both IoT and IIoT applications. Consequently, Makhdoom et al. [27] have mapped the security and performance benefits inferred by the blockchain technologies and some of the blockchain-based IoT applications against the IoT requirements. They have further discussed some of the practical issues that evolve due to the integration of blockchain into IoT. Finally, [28], Ferrag et al. have classified threats on blockchain protocols in IoT into five main categories: identity-based attacks, manipulation-based attacks, cryptanalytic attacks, reputation-based attacks, and service-based attacks. They have also provided a comparative analysis of the secure and privacy-preserving blockchain technologies with respect to their security goals achieved, limitations, communication overhead and computation complexity.

From the above discussions it can be clearly concluded that in this area, researchers have mainly focused on the following (a) identifying the major requirements for integrating blockchain into IoT/IIoT applications (b) leveraging the benefits offered by blockchain to handle the challenges of the existing applications (c) discussing about the existing blockchain-based IoT platforms and the several enhancements proposed in literature. This motivates us to explore how the integration of blockchain in IoT and IIoT can help handling the major security concerns existing in such systems. For this purpose, we choose two applications under each domain (i.e. IoT and IIoT) and highlight the existing works that propose blockchain based solutions for each of these applications.

Table 1: Comparison on Related Works

Survey	**Citation**	**Year**	**Objective**
A comprehensive study of security of Internet of Things	[7]	2017	Highlight security vulnerabilities, discuss attacks and possible countermeasures on the edge side layer

Journal Pre-proof

Survey	Citation	Year	Objective
A survey on Security and Privacy issues in Internet of Things	[8]	2017	Describe authentication and access control schemes; detail layerwise security problems and their solutions
Evaluating critical security issues of the IoT world: Present and future challenges	[9]	2017	Demonstrate layerwise threats; trust management issues; communication protocols; analyze critical security vulnerabilities on basis of BS metric
Internet of Things security: A survey	[10]	2017	Detail taxonomy of current security threats into four categories; Analyze possible attacks under these category; Discuss security vulnerabilities in terms of application deployments
IoT Security: Review, blockchain solutions, and open challenges	[11]	2018	Categorize communication and networking protocols, levels of security issues followed by their respective security solutions
Understanding security requirements and challenges in Internet of Things	[12]	2018	Classify security vulnerabilities highlight challenges, existing solutions and open research issues
Internet of things security: A top-down survey	[13]	2018	Classify security requirements of six major IoT applications; Enumerate both classical and new technology approaches for various IoT related security solutions
A roadmap for security challenges in the Internet of Things	[14]	2018	Case study on Smart Manufacturing; Discuss security issues related to privacy, trust, identification and access control
Privacy in the Internet of Things: Threats and Challenges	[15]	2015	Examine privacy threats in the light of evolving IoT; Identify major challenges
Privacy in Internet of Things: From principles to technologies	[16]	2018	Review IoT architecture, principles of privacy laws and PETs; Study privacy protection problem for each of these layers
The Industrial Internet of Things (IIoT): An analysis framework	[17]	2018	Group IoT devices into six categories to analyze their security vulnerabilities
Internet of Things in Industries: A Survey	[18]	2014	Elaborate five industrial sectors in which IoT is applied along with their relevant existing works

Journal Pre-proof

Survey	Citation	Year	Objective
Literature review of Industry 4.0 and related technologies	[19]	2018	Explore important technologies along with the corresponding works required for the growth of Industry 4.0
Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing Systems	[20]	2019	Provide a survey on the Smart Factory paradigm
A Review on the Use of Blockchain for the Internet of Things	[21]	2018	Highlight major BIoT applications; Discuss important aspects and challenges involved in the development of such applications
Blockchain with Internet of Things: Benefits, Challenges, and Future Directions	[22]	2018	Highlight benefits and challenges of integrating Blockchain into IoT applications
On blockchain and its integration with IoT. Challenges and opportunities	[23]	2018	Discuss and evaluate the performance of different existing BIoT platforms
Survey on blockchain for Internet of Things	[24]	2019	Elaborate existing works that enhance the blockchain data structures and consensus protocols to suit BIoT applications
Blockchain for the IoT and industrial IoT: A review	[25]	2019	Discuss security requirements to develop blockchain based IoT and IIoT applications
Blockchain's adoption in IoT: The challenges, and a way forward	[27]	2019	Map performance benefits of certain blockchain-based IoT solutions against its requirements; Discuss practical issues of integrating blockchain into IoT
Blockchain Technologies for the Internet of Things: Research Issues and Challenges	[28]	2019	Classify threats on blockchain IoT protocols into five categories ; Provide comparative analysis on secure blockchain techniques with respect to security goals

Journal Pre-proof

Journal Pre-proof

Survey	Citation	Year	Objective
Our work	-	-	Categorize major attacks on IoT system on the basis of objects of attack and map them to one or more layers of the architecture; Review the countermeasures; Discuss IIoT security related research trends; Case study on applications of IIoT highlighting security specific works; Elaborate blockchain based application specific solutions for IoT and IIoT; Design a taxonomy of security research areas with respect to IoT and IIoT; Discuss open research areas

Table 1 summarizes the objectives of each of these surveys including ours and mentions how our perspective is different.

3. Security Attacks in IoT

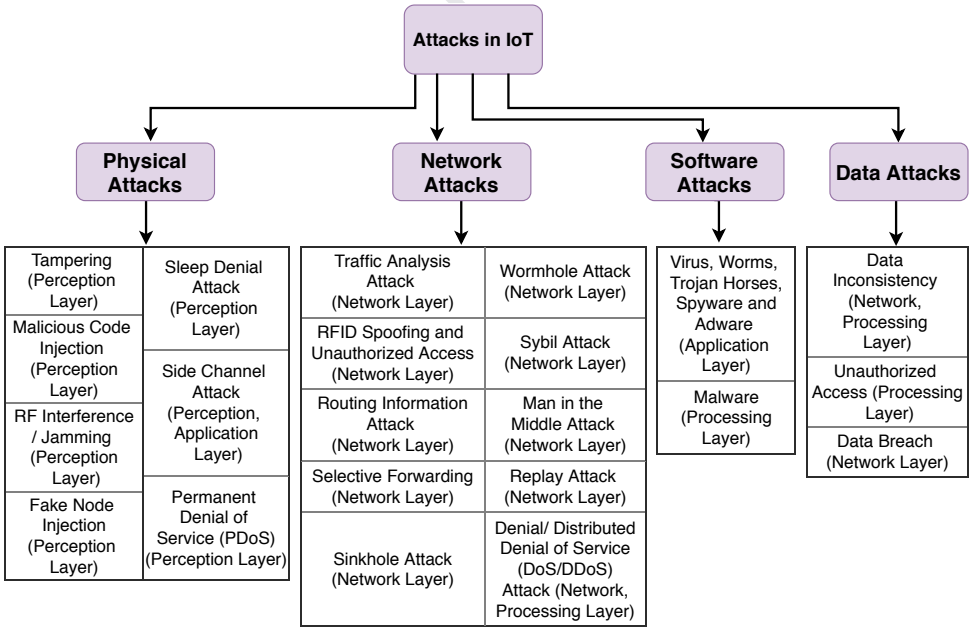

Figure 2: *Attacks in IoT*

The security attacks in IoT can be broadly classified into four domains : (a) Physical Attacks (b) Network Attacks (c) Software Attacks and (d) Data Attacks as depicted in Figure 2. In this section we give a detailed

Journal Pre-proof

overview of these attacks along with a literature review on the countermeasures adopted to deal each of these attacks.

3.1. Physical Attacks

Physical attacks can be launched if the attacker remains physically close to the network or devices of the system [29]. The common forms of physical attacks are listed below:

- **Tampering:** Refers to the act of physically modifying a device (e.g. RFID) or communication link [30].
- **Malicious Code Injection:** Here the attacker injects malicious code onto a physical device by compromising it which may help him/her launch other attacks too [29].
- **RF Interference/Jamming:** Attacker creates and sends noise signals over the Radio Frequency (RF)/WSN signals to launch DoS attacks on the RFID tags/sensor nodes thereby hindering communication [29].
- **Fake Node Injection:** Attacker drops a fake node between two legitimate nodes of the network to control data flow between them [29].
- **Sleep Denial Attack:** Attacker keeps the battery powered devices awake by feeding them with wrong inputs. This causes exhaustion in their batteries leading to shutdown [29].
- **Side Channel Attack:** In this attack, the attacker collects the encryption keys by applying timing, power, fault attack etc. on the devices of the system [30]. With the help of these keys it can encrypt/decrypt confidential data.
- **Permanent Denial of Service (PDoS):** Also known as phlashing, is a type of DoS attack, wherein an IoT device is completely damaged via hardware sabotage. The attack is launched by destroying firmware or uploading a corrupted BIOS using a malware [31].

The following subsections demonstrate the vulnerabilities of the physical devices along with the attacks launched against them. Further, the countermeasures adopted to deal with the said attacks are also discussed.

3.1.1. Vulnerabilities of Physical Devices

The works [32, 33, 34] that have highlighted the vulnerabilities against some well known physical devices (e.g. smart meters, IP cameras, Amazon Echo) are reviewed here.

In one such work [32], Ling et al. have performed a vulnerability analysis of Edimax IP cameras which identified that attacks like device scanning, brute force and device spoofing can take control of the cameras.

Journal Pre-proof

For example, using device spoofing attack, attackers can obtain a camera's password of any length and combination. Also by enumerating all possible MAC addresses the attacker can launch device scanning attack to find all online cameras. In this context, we highlight another work [33] where the authors have analyzed security vulnerabilities of both commercial (e.g. Haier SmartCare home automation system) and industrial (e.g. Itron Centron Smart Meter) IoT devices. Their experiments reveal that the home automation system is vulnerable to brute force attacks revealing the passwords. It also reveals that the smart meters can be hijacked to launch ransomware attacks against other systems. Another work [34], highlights that the security vulnerabilities of Virtual Personal Assistant (VPA) based IoT devices such as Amazon Echo and Google Home. These systems are vulnerable to attacks like voice squatting and voice masquerading. In voice squatting attack, the adversary uses a malicious skill with similarly pronounced name or paraphrased name to hijack the voice commands meant for a different skill whereas in voice masquerading the adversary uses a malicious skill to impersonate a legitimate one in order to steal user's data or eavesdrop on the conversations.

3.1.2. Countermeasures against Physical Attacks

Many works have so far been reported for mitigating the above attacks on devices. In this subsection, some of the important such works are reviewed.

In one such work, Aman et al. [35] have devised a mutual authentication protocol based on Physically Unclonable Function (PUF) for small sized IoT devices, which exploits the inbuilt variability of Integrated Circuit (IC). The authentication is carried out using a challenge-response mechanism whose output is primarily dependent on the physical micro structure of the device. Thus forging the PUF to clone the exact same structure is impossible which effectively eliminates attacks like tampering and malicious code injection.

The work [36] focuses on presenting a solution at the architectural level of a device to achieve energy efficiency combined with security capabilities. In this context, they have proposed a heterogeneous architecture to be implemented on a customizable and trustable end device mote (CUTE mote) to achieve benefits both in terms of energy and performance. The architecture is developed by combining reconfigurable computing unit (RCU) with an IEEE 802.15.4 radio transceiver and a hardcore micro-controller unit (MCU) which hosts Contiki-OS. Experimental results using context switching benchmark from the Thread-Metric benchmark suite have shown that the proposed architecture with Smart-Fusion2 SoC hardware platform is capable enough to prevent physical attacks like jamming.

Distributed IoT applications are an integral component of today's world. In such environment it is important to establish secure links between peer sensor nodes and end users. Therefore, Porambage et al. [37] have proposed a pervasive authentication protocol (PAuthKey) aimed for WSNs. The proposed protocol is based on obtaining implicit certificates from the Cluster Head (CH) and then establishing secure links between peer sensor nodes and end users and sensor nodes. The authentication scheme is based on the

Journal Pre-proof

Table 2: Physical Attacks, Effects and Countermeasures

Attack Name	**Effects**	**Countermeasures Proposed**	**Countermeasure References**
Tampering and Malicious Code Injection	Access to sensitive information and Gain access; DoS	PUF based Authentication	[35]
RF Interference/Jamming	DoS; Hinder/Jam Communication	CUTE Mote	[36]
Fake Node Injection	Control data flow; Man in the Middle	PAuthKey	[37]
Sleep Denial	Node shutdown	CUTE Mote; Support Vector Machine (SVM)	[36, 38]
Side Channel Attack	Collect Encryption Keys	Masking technique; Authentication using PUF	[35, 39]
Permanent Denial of Service (PDoS)	Resource Destruction	NOS Middleware	[41]

relative position of the sensor nodes and is responsible for guarantying end to end application layer security which successfully circumvents node compromise, masquerade and impersonation attacks. By preventing the said attacks, PAuthKey is able to restrict fake node injection.

The heterogeneous architecture of CUTE Mote [36] which has been explained earlier also makes it impossible to launch sleep denial attack. On the other hand, Hei et al. [38] have designed a novel Support Vector Machine (SVM) by utilizing patient's medical device access pattern. The classification algorithm of SVM detects resource depletion which is one of the primary reasons of sleep denial.

Side-channel (both timing and power analysis) attacks can be serious threats to IoT. The physical micro structure along with the inbuilt variablity of PUF-based authentication mechanism [35] described above makes forging impossible, thereby preventing side-channel attack. Another work [39] has proposed a masking technique to be used along with Lightweight Encryption Algorithm (LEA) as a countermeasure to side-channel attack. The masking technique makes it impossible for the attacker to analyze the secret key value, thereby preventing a type of side channel (i.e. differential side-channel) attack.

PDoS can have serious impacts on Industrial Control Systems (ICS) and can be used to disable critical equipment in an electrical substation, on a factory floor, or in a wastewater treatment plant [40]. In [41], Sicari et al. has developed a solution named REATO, to deal with different types of DoS attacks (including attacks on the data) in an IoT environment. They have considered a cross-domain and flexible middleware, named NetwOrked Smart object (NOS) and tailored REATO to it. The proposed solution is based on a HTTP connection request to NOS, and on validation, an encrypted information is sent back. Testbed implementation shows that this technique recognizes and counterfeits such DoS attacks efficiently.

Table 2 summarizes the physical attacks with its effects and the countermeasures proposed.

Journal Pre-proof

3.2. Network Attacks

Network attacks are performed by manipulating the IoT network systems to cause damage. It can easily be launched without being close to the network. The most common forms of network attacks are summarized below :

- **Traffic Analysis Attack:** Confidential information or other data flowing to and from the devices are sniffed by the attacker, even without going close to the network in order to gain network information [30].
- **RFID Spoofing:** The attacker first spoofs an RFID signal to get access of the information imprinted on the RFID tag [29]. By using the original tag ID, the attacker can then send its data, posing it as valid.
- **RFID Unauthorized Access:** An attacker is able to read, modify or delete data present on RFID nodes because of the lack of proper authentication mechanisms [30].
- **Routing Information Attacks:** These are direct attacks where the attacker spoofs or alters routing information and makes nuicance by activities like creating routing loops, sending error messages etc. [30].
- **Selective Forwarding:** In this attack, a malicious node may simply alter, drop or selectively forward some messages to other nodes in the network [42]. Therefore, the information that reaches the destination is incomplete.
- **Sinkhole Attack:** In this attack, an attacker compromises a node closer to the sink (known as sinkhole node) and makes it look attractive to other nodes in the network thereby luring network traffic towards it [29].
- **Wormhole Attack:** In a wormhole attack, an attacker maliciously prepares a low-latency link and then tunnels packets from one point to another through this link [42].
- **Sybil Attack:** Here, a single malicious node claims multiple identities (known as sybil nodes) and locates itself at different places in the network [30]. This leads to huge resource allocation unfairly.
- **Man in the Middle Attack (MiTM):** Here, an attacker manages to eavesdrop or monitor the communication between two IoT devices and access their private data [30].
- **Replay Attack:** An attacker may capture a signed packet and resend the packet multiple number of times to the destination [42]. This keeps the network busy leading to a DoS attack.

Journal Pre-proof

- **Denial/Distributed Denial of Service (DoS/DDoS) Attacks:** Unlike DoS attack, in DDoS multiple compromised nodes attack a specific target by flooding messages, or connection requests to slow down or even crash the system server/network resource [40].

The following subsections provide a discussion on the countermeasures proposed against the said attacks. It also highlights a couple of such network attacks which have been launched recently.

3.2.1. Countermeasures against Network Attacks

This subsection provides a review on the works that have so far been reported for mitigating the said attacks.

In one such work [43], Liu et al. have proposed a efficient and privacy preserving traffic obfuscation (EPIC) framework to protect smart homes against traffic analysis. They have designed a secure multihop routing protocol which guarantees strong differential privacy by assuring unlinkability of traffic flow to a specific smart home as well as between source and destination.

Guin et al. [44] have designed an on-board SRAM based Physically Unclonable Function (PUF) which produces a unique device footprint as the device ID. Then by using device ID matching technique probability of impersonation of an ID by an adversary is reduced, which further reduces the risk of spoofing as well as unauthorized access.

The work [45] has proposed a Secure Routing Protocol for Low power and Lossy Networks (SRPL). The protocol uses hash chain authentication technique along with the concept of rank threshold. SRPL requires authentication based on hash values to prevent malicious nodes from exploiting control messages thereby effectively dealing with routing attacks.

The hash chain authentication technique incorporating rank threshold [45] explained above can also effectively deal with selective forwarding and sinkhole attacks. Contrary to that, [46] has focused on dealing with forwarding misbehavior of nodes by proposing a monitor based approach, named as CMD which uses RPL as their routing protocol. Using the protocol, each node keeps a track of the packet loss rate of the preferred parent versus that of its one hop neighbors to detect forwarding misbehaviors. On the other hand, Cervantes et al. [47] have proposed an intrusion detection system called **I**nstrusion detection for Si**N**khole attacks over 6LoWPAN for Interne**T** of Th**I**ngs (INTI) which utilizes reputation, watchdog and trust strategies to detect potential attackers by analyzing the behavior of each node in the network. INTI reveals the identity of the node launching the attack as well as isolates the detected sinkhole node.

A work on wormhole attack [48], proposes three Intrusion Detection Systems (IDSs) for IoT. The first one is a K-means IDS (KM-IDS), an unsupervised clustering based IDS which detects wormhole attacks when a router tries to add a neighbor outside its cluster. The second one is Decision Tree based IDS (DT-IDS), a supervised centralized approach which detects wormhole attack when a router tries to add a neighbor

Journal Pre-proof

outside its safe distance (defined using training data). Lastly, the third approach is a hybrid IDS which combines the K-means to detect wormholes followed by DT-IDS which filters out the false positives.

The work [49] has aimed to detect and isolate the nodes launching sybil attacks. To achieve the said purpose, they have proposed a trust aware RPL routing protocol named SecTrust-RPL which uses a mechanism based on trust to fulfil the goal. The SecTrust framework is embedded in the ContikiRPL which serves as the trust engine for making routing decisions and malicious node detection. The decision is made purely on the basis on trust among the nodes, and the detected malicious nodes are quickly isolated from the network.

MiTM attacks can have serious impacts in an IoT system, for example in an industrial IoT setting an attacker can take control of a smart actuator [40]. It can then knock an industrial robot out of its designated lane and speed limit, thereby potentially damaging an assembly line [40]. Therefore, a couple of works address the issue of mitigating MiTM attacks. One such work [50] has proposed two protocols namely, secure MQTT and MQTT-SN. Both the schemes ensure secure device to device(D2D) communication where MQTT uses Key-Policy (KP) and MQTT-SN uses Cipherext-Policy (CP) Attribute Based Encryption (ABE) in implementing Elliptic Curve Cryptography (ECC) to prevent Man-in-the middle attack. Another work [51], also addresses the same attack by authenticating inter-device communication where each sensor is involved in the generation and distribution of session keys. However, in this scheme instead of central key generation, each node individually does the work. The specialty of this scheme is that it contains only one crypto-primitive module which significantly improves the performance for resource constrained IoT devices.

The work [52] has proposed a signcryption technique based on Identity Based Cryptography (IBC) that can efficiently satisfy confidentiality, integrity and authentication simultaneously. The proposed technique effectively combines encryption and signature schemes and also eliminates the need to access a trusted third party for fulfilling the authentication process which ensures resilience against replay attacks.

The work [53] has proposed a defensive framework against network DoS and Distributed DoS (DDoS) attacks, considering message flooding in general.They have used an EDoS server from a third party and the proposed algorithm for the server consists of two parts. The Analysis part analyzes the incoming traffic to decide on the suspicion level. The Monitoring part categorizes the suspicious traffic into DoS or DDoS. In another work [54], Yin et al. has proposed a framework based on SDx paradigm known as the Software Defined Internet of Things (SD-IoT). The proposed SD-IoT framework uses an algorithm to detect and mitigate DDoS attacks using the cosine similarity of vectors. The basic concept is, first a threshold value is obtained using the cosine similarity of the vectors of the packet-in message rate at the SD-IoT boundary. Whether a DDoS attack has occurred is determined using this threshold value and then the attacker is found out and blocked at the source.

Table 3 summarizes the network attacks with its effects and the countermeasures proposed.

Journal Pre-proof

Table 3: Network Attacks, Effects and Countermeasures

Attack Name	**Effects**	**Countermeasures Proposed**	**Countermeasure References**
Traffic Analysis Attack	Data Leakage (Network Information)	Privacy preserving traffic obfuscation framework	[43]
RFID Spoofing and Unauthorized Access	Data Manipulation and Modification (Read, Write, Delete)	SRAM based PUF	[44]
Routing Information Attacks	Routing Loops	Hash Chain Authentication;	[45]
Selective Forwarding	Message Destruction	Hash Chain Authentication; Monitor based approach	[45, 46]
Sinkhole Attack	Data alteration or leakage	Hash Chain Authentication; Intrusion Detection	[45, 47]
Wormhole Attack	Packet tunneling	Clustering based Intrusion Detection System	[48]
Sybil Attack	Unfair resource allocation; Redundancy	Trust aware Protocol	[49]
Man in the Middle Attack	Data Privacy violation	Secure MQTT; Inter-device Authentication	[50, 51]
Replay Attack	Network congestion ; DoS	Signcryption	[52]
DoS / DDoS Attack	Network Flooding; Network Crash	EDoS Server; SDN based IoT framework	[53, 54]

3.2.2. Examples of Network Attacks in Reality

Network attacks can cause serious consequences, at times leading to a complete shutdown. In this context, a few of the attacks which had the worst impact on mankind are discussed below:

- In October, 2016 a DNS service provider (named Dyn) was hit by a DDoS attack [55]. The attack lasted for a couple of hours, affecting services of Twitter, GitHub etc. Access to popular websites like PayPal, BBC etc. were also hampered.

- In 2015, a gang in Europe performed Man-in-the-Middle (MiTM) attacks to sniff out and intercept payment requests from email [56]. The investigations uncovered that the gang hauled around 6 million Euro. They had established illegitimate access to corporate email accounts by allegedly monitoring and sniffing around for payment requests.

3.3. Software Attacks

Software attacks are launched by an attacker taking advantage of the associated software or security vulnerabilities presented by an IoT system and can be listed below:

- **Virus, Worms, Trojan Horses, Spyware and Adware:** Through the use of these malicious

Journal Pre-proof

Table 4: Software Attacks, Effects and Countermeasures

Attack Name	**Effects**	**Countermeasures Proposed**	**Countermeasure References**
Virus, Worms, Trojan Horses, Spyware and Adware	Resource Destruction	Lightweight framework; High Level Synthesis (HLS)	[57, 58]
Malware	Infected Data	Malware Image Classification; Lightweight Neural Network Framework	[59, 60]

software, an adversary can infect the system to achieve tampering of data or stealing information, or even launch DoS [30].

- **Malware:** Data present in IoT devices maybe affected by malware, which may contaminate the cloud or data centres [42].

The following subsections discuss the countermeasures proposed to deal with the said attacks. It also highlights the most common software attacks launched in reality.

3.3.1. Countermeasures against Software Attacks

This subsection provides a review on the important works that have been reported so far for mitigating the said attacks.

Liu et al. [57] have developed a lightweight framework integrating three security aspects to defend hardware Trojans from being implanted on IoT devices. Firstly, vendor diversity is introduced to enable trusted communication among untrusted nodes. Secondly, message encryption is introduced to prevent unauthorized parties from accessing communications. Lastly, mutual auditing is enabled to allow authorized nodes to check encryption status and content of a message. In [58], Konigsmark et al. has also focused on preventing hardware Trojans by the use of High Level Synthesis (HLS). A security enhanced hardware design is produced by HLS to directly prevent the injection of hardware Trojans into the network.

The authors [59] have designed a Malware Image Classification System (MICS) for classifying malware and representing image globally and locally. MICS first converts the suspicious program into gray-scale image and then captures hybrid local and global malware features to perform malware family classification. The other solution [60], has first classified malware samples collected from two families. Then, they have proposed a lightweight conventional neural network framework which is feed with gray scale images converted from program binaries that detects malware with high accuracy.

Table 4 summarizes the software attacks with its effects and the countermeasures proposed.

3.3.2. Examples of Software Attacks in Reality

Experts have predicted that by 2025 there will be as many as 75 billion connected IoT devices [61]. In this context, a couple of most relevant attacks which are considered as the worst are discussed below:

Journal Pre-proof

- **The Mirai Botnet:** In October 2016, the largest DDoS attack was launched on DNS service provider (Dyn) by using an IoT botnet. The botnet was made possible by a malware named Mirai which led to shutdown of huge portions of the Internet including Twitter, Netflix etc [61].

- **The Jeep Hack:** In July 2015, a team of researchers was able to hijack the vehicle over Sprint cellular network by exploiting a firmware update vulnerability. They discovered that they could control the speed of the vehicle as well as veer it off from the road [61].

3.4. Data Attacks

The growth of IoT itself along with its advancement in the industrial sector is putting a strain on the computing resources necessary to maintain the level of connectivity and data collection that IoT devices require [62]. This is where cloud computing comes into picture by acting as the backbone of everything IoT has to offer. With cloud computing, setting up virtual servers, launching a database instance, and creating data pipelines to help for running IoT solutions becomes easier [62]. Moreover, data security is an important concern in such an environment where cloud can help improve security by providing proper authentication mechanisms, firmware and software update procedures, etc. Here, we discuss about the major data attacks that are prevalent in the IoT world today:

- **Data Inconsistency:** In IoT, attack on data integrity leading to inconsistency of data in transit or data stored in a central database is referred to as Data Inconsistency.

- **Unauthorized Access:** Access control implies giving access to authorized users and denying access to unauthorized users. With unauthorized access, malicious users can gain data ownership or access sensitive data.

- **Data Breach:** Data breach or memory leakage refers to the disclosure of personal, sensitive or confidential data in an unauthorized manner.

The following subsections discuss on the countermeasures proposed against the said attacks. Further, it also highlights some real life examples of a few of these attacks that had huge impacts on society.

3.4.1. Countermeasures against Data Attacks

Since protecting user data is of utmost priority, therefore research has been focused on dealing with the aforementioned attacks.

Integrity is protected cryptographically by either MAC or signatures. The challenge lies in creating MAC or signature for devices like mobile phones or sensors because it is computationally intensive and difficult to implement in IoT (due to limitations in devices). One such work [63] that has handled the challenge fairly efficiently has proposed a Chaos-based privacy preserving cryptographic scheme along with

Journal Pre-proof

Message Authentication Code (MAC) to secure data transmissions within a smart home. The proposed chaotic system uses logistic map to generate symmetric keys used for securing data transmissions thereby guarantying data integrity. In another work [64], the authors have proposed a three level split blockchain based architecture to ensure integrity of data stored in remote semi-trusted data storages. On the first level, they have introduced the Concept of Trust (PoT) for Trustful Space Time Protocol (TSTP). The upper levels are responsible for maintaining integrity verification and data availability in semi trusted storages.

WSNs play an important role in IoT, but due to its open wireless channel, providing authorized access to sensitive data becomes a challenge. Therefore, access control comes into picture and can be incorporated both by using cryptography or without it. However, attention has been paid on cryptographic techniques only. In one such work [65], Rahulamathavan et al. proposed a blockchain based architecture by incorporating Attribute based Encryption (ABE) with it. Apart from supporting integrity and non-repudiation, the proposed scheme also preserves the privacy of transaction data. The proposed privacy preserving blockchain based architecture imposes access control to address confidentiality of shared data in the blockchain and thus provide end to end privacy preserving IoT system. On the contrary, another work [66], has proposed a privacy preserving efficient medical data sharing scheme by utilizing ABE which hides all the attributes in the access control structure by utilizing the attribute bloom filter. The devices encrypt the data and send it to the server where only legitimate users satisfying the access control structure can decrypt the data.

Data Breach has posed serious threats to user's personal information in the recent years. Therefore, one such work [67] on preventing data breach has proposed a lightweight privacy preserving two-factor authentication scheme for securing the communication between IoT devices. In addition to a shared secret key they have also used PUF to achieve the two-factor authentication. Again in [68], authors have proposed a Dynamic Privacy Protection (DPP) model which focuses on resource constrained devices to produce optimal solutions for privacy protection levels by utilizing dynamic programming. They have used Content Oriented Data Pairs (CODP) and Optimal Data Alternatives (ODA) to minimize the potential of a privacy leakage. Finally, in the work [69] the authors have proposed an Improved Secure Directed Diffusion (ISDD) protocol for ensuring end to end data secrecy in IoT environments. The proposed protocol has generated shared keys by using bilinear pairing, which are then used to generate multiple encryption layers over the plaintext message. ISDD assures privacy of data at each hop because the message contains atleast one layer of encryption, therefore it is impossible for an attacker to devise the original data.

Table 5 summarizes the data attacks with its effects and the countermeasures proposed.

3.4.2. Examples of Data Attacks in Reality

Insider attacks have the ability to expose an organization to a wide range of cyber security hazards. In this context, we discuss some of the most prominent attacks that took place in history:

- In 2016, a UK based accounting and HR software provider, Sage was hit by an insider unauthorized

Journal Pre-proof

Table 5: Data Attacks, Effects and Countermeasures

Attacks	**Effects**	**Countermeasures Proposed**	**Countermeasure References**
Data Inconsistency	Data Inconsistency	Chaos based scheme; Blockchain architceture	[63, 64]
Unauthorized Access	Violation of Data Privacy	Blockchain-based ABE; Privacy Preserving ABE	[65, 66]
Data Breach	Data Leakage	Two Factor Authentication ; DPP; ISDD	[67, 68, 69]

access attack. An employee who worked for the company used unauthorized access to steal private customer information, including salary and bank account details [70].

- In March 2018, Cambridge Analytica had gained access to private information on more than 50 million Facebook users [71].

4. Industrial Internet of Things (IIoT)

With the emergence of fourth industrial revolution (namely, Industry 4.0), the use of certain IoT technologies and various smart objects in an industrial setting for the promotion of goals distinctive to the industry is referred to as Industrial IoT (IIoT) [17]. The IIoT system is capable of monitoring, collecting, analyzing and intelligently changing the behavior or environment without human intervention [17]. A mature system of software and hardware elements known as Supervisory Control and Data Acquisition (SCADA) is already in place in the industries for more than 20 years. SCADA systems consist of two elements: (a) the process/machinery that is to be monitored or controlled (b) a network of intelligent devices to control these process/machinery [17]. Yet, IIoT has come up as a technology that is built on top of SCADA due to the following four areas of improvement [72]:

- **Scalability:** IIoT has the ability to set up new plants whenever required by using resources collected from the cloud.
- **Data Analytics:** IIoT needs to allow long term data storage. Big data processing and machine learning techniques can then be applied to predict outcomes.
- **Standardization:** IIoT aims to standardize sensor networks, data gathering and aggregation to allow real-time communication within plants.
- **Interoperability:** : IIoT uses protocols such as MQTT that enables platforms which are communicable and programmable across devices regardless of vendors.

Journal Pre-proof

Integrating IoT technology into industries (IIoT) has brought benefits in productivity, efficiency etc. However, the connected, always-online nature of these systems means entire factories could be vulnerable to often devastating cyberattacks. Cyberattacks are primarily aimed at industrial control systems (ICS) [40] such as programmable logic controllers (PLC), distributed control systems (DCS), human machine interfaces (HMI) with supervisory control and data acquisition (SCADA) systems. IIoT is so vulnerable to cyberattacks primarily because of the following reasons:

- Decade-old devices and control systems never designed for exposure to the Internet and, therefore, not designed for security.
- A big increase in the number of sensors and devices being connected to each organization's IIoT, requires proper coordination among them. However, often the traditional algorithms are inefficient in handling such coordination.
- The number of potential attackers has also increased. Attackers now include sophisticated nation-states, cybercriminals with ransomware.

The concept of industrial IoT is slowly gaining popularity with its practical application in various domains. This has lead to the discovery of various security vulnerabilities and threats which specifically arise with the application of IIoT. However, since this research is almost in its nascent stage, to the best of our knowledge a very few works [73, 74, 75, 76, 77, 78, 79, 80, 81, 82] have been conducted to deal with security issues pertaining to industrial IoT. We primarily review these works in the following subsections from the perspective of providing authentication/authorization and defending/preventing attacks. Subsequently, we provide a case study on two of the most relevant applications of IIoT to highlight how the amalgamation of automation with the industrial processes has brought about a major shift in the industries.

4.1. Authentication and Authorization

Traditional or even IoT based authentication mechanisms cannot readily be applied to industrial environments since manufacturing machineries are limited in communication bandwidth and/or computation power. Thus, Trusted Execution Environment (TEE) and Intel Software Guard Extensions(SGX) are often implemented as modules in various IIoT environments to leverage the benefits offered by them and bring in extra security to the system. A secure area inside a main processor where data is loaded is known as TEE [83]. TEE effectively guarantees integrity and confidentiality of data loaded in it. TEE offers an execution space with high levels of security which is now-a-days effectively used by IIoT environments. Similarly, Intel SGX is a set of security-related instruction codes that are built into some modern Intel CPUs [84]. Intel SGX allows to define 'enclaves' (i.e. private areas within the memory), where content stored inside the enclave is protected. The encryption and decryption of data is performed by the CPU itself, hence such

Journal Pre-proof

data can neither be read nor modified by any other process. Therefore, a few works focus on proposing authentication and/or authorization mechanisms relevant to the industrial domain and these are discussed here.

In one such work [73], Esfahani et al. have proposed a Machine to Machine (M2M) lightweight authentication protocol which is simply based on hash and XOR operations. They have considered smart sensors equipped with Secure Element (SE) and routers equipped with Trusted Platform Module (TPM). The proposed authentication mechanism consists of two phases : (a) the registration phase in which each smart sensor registers itself to an Authentication Server (AS) and secure pre-shared keys generated by the AS are also shared with the routers (b) the authentication phase in which mutual authentication is achieved between the sensor and the router. In another work [74], the authors have proposed an anonymous lightweight user authentication mechanism based on chaotic map for IIoT environments. This method allows access to designated IoT devices only to the authorized users. The method has considered three factors for authentication namely personal biometric, password and smart cards where fuzzy extractor method has been applied by using smart card to validate user's biometric. The scheme also incorporates smart card revocation phase, password/biometric change phase as well as IoT device addition phase. Contrary to that, the work [75], in IIoT has proposed a privacy-preserving biometric based provable secure authentication protocol with ECC. In the said protocol, when a user, wishes to access a sensory data of a node, s/he has to authenticate her/himself to a gateway to agree on a session key for all future communications to be made secure. Similarly, the work [76] proposes a context sensitive seamless identity provisioning (CSIP) framework for IIoT to verify users. The CSIP proposes a mutual authentication scheme based on hash and mutual authentication value which operates in two parts. The client-based part gathers users data and sends it to the cloud. On the other hand, the cloud-based part receives it and applies deep analysis on it to gather further information.

With the advent of IIoT combined with the growing popularity of digitization, organizations are outsourcing their data to the cloud to reduce overhead of data management. This has brought about a pressing need of data authentication with low computation overhead. In this context, Karati et al. [77] have proposed a bilinear pairing based Certificateless Signature (CLS) scheme to provide data authenticity in IIoT systems. According to this algorithm, the signer performs two exponentiations and the verifier performs one pairing along with two exponentiation. However, the work [78] has improved upon [77] by proposing a Robust Certificateless Signature (RCLS) scheme based on elliptic curve cryptography. Apart from making the scheme robust, RCLS simultaneously provides resiliency against four types of signature forgery attacks which are not addressed in [77]. The proposed scheme has introduced the idea of partial private key generation into short signatures as well as key exchange to achieve robustness. Recently,Yang et al. [79] have claimed RCLS [78] to be insecure by showing that an attacker having the capabilities of replacing a public key can easily impersonate other legitimate users to upload false messages. They have shown that this can be achieved by

Journal Pre-proof

forging the target users' valid signatures and therefore data authenticity is not preserved as pointed out by [78].

In large scale IIoT environments, proper authorization and access control of IIoT objects are an important concern. The work [80] has proposed an authorization framework named *SecIIoT* on annotated metadata for securing IIoT objects. The authors propose an indexing framework for allowing IIoT object owners to define constraints such as location, time etc. on the IIoT services in a flexible and fine-grained manner. A prototype implementation shows that in-memory processing and high dimension filtering allows efficient large scale deployment suitable for IIot environments. Finally, Zhou et al. [81] have proposed a novel file centric multikey aggregate keyword searchable encryption (Fc-MKA-KSE) scheme for file centric data sharing in IIoT. They have proposed two security models, one which captures the trapdoor privacy, i.e., the indistinguishability against selective-file keyword guessing attack (IND-sF-KGA) and the other achieves indistinguishability against selective- file chosen keyword attack (IND-sF-CKA).

4.2. Attack Prevention/Defence

Research interests focused on dealing with attacks in industrial environment are mainly concentrated on preventing replay, MiTM and DDoS attacks. Therefore, in this section we highlight on how the said works prevent such attacks.

The mutual authentication scheme described in [73] is also resilient against replay attacks because the alias of a sensor (which is used in authentication) is calculated on the basis of hash of a random number, which is unknown to an adversary. Similarly, the authentication protocol described in [75] above, requires three random numbers in each session for the user, node and gateway. This ensures freshness of communication messages at each session thereby preventing replay attacks.

The mutual authentication scheme described in [73] is also resilient against MiTM attack. Even if an adversary is able to obtain a sensor's identity it will not be able to calculate the session key, because the secret key is unknown to the adversary which is securely stored in the AS. Moreover, the adversary would be unable to pose as a trustful router because of the unavailability of the pre-shared key with itself. Correspondingly, the user authentication scheme proposed in [74] above can also defend Man-in the Middle attacks. An adversary trying to intercept and modify the messages exchanged during the authentication process needs to posses several secret parameters including the secret ID's of user and its corresponding sensing device. These are completely secret and are unavailable to the adversary which makes it impossible for him to launch an MiTM attack.

DoS and DDoS can cause serious disruptions in manufacturing and utility services of industrial equipments [40]. The work [82] on DDoS mitigation in IIoT has proposed a Multi-Level DDoS Mitigation Framework (MLDMF). It defends DDoS attacks at three levels, i.e. fog, cloud and edge computing levels. The fog, cloud and edge computing levels use a cluster of SDN controllers and applications, SDN-based IIoT

Journal Pre-proof

gateways and big data along with intelligent computing respectively to analyze network traffic in order to detect and mitigate DDoS attacks.

From the discussions in Section 4.1 and 4.2, we get a clear idea that research on ensuring basic security or defending against dreadful attacks in IIoT is still in its infancy. Since, IIoT is a newly expanding domain there is a huge need of securing the overall system. In this context, in the following subsection we highlight how Blockchains have emerged to be an effective solution both in IoT and IIoT domains.

4.3. Case Study on Applications of IIoT

Application of IoT in various industries to bring about digitization is rapidly evolving and growing. IoT applications are being deployed and/or developed in various sectors including smart factory, smart healthcare, smart grid, smart transportation etc. In this context, we choose two of these sectors and perform a case study in the following subsections on the current research trends in these areas. We elaborate on the research works relating to security issues and privacy concerns in these areas.

4.3.1. Smart Factory

Smart Factory is a huge leap from traditional automation in industries to a fully automated, connected and flexible system. A smart factory integrates data from system-wide physical, operational, and human assets to drive manufacturing, maintenance, inventory tracking, digitization of operations and other types of activities across the entire manufacturing network [85]. Apart from the benefits that smart factories have brought about in the production, certain other security issues have also come to the forefront. Here, we highlight on some of the existing works to deal with the potential problems prevalent in smart factories.

Wan et al. [86] have introduced Blockchain technology into the existing IIoT architecture for constructing a more secure, reliable and distributed architecture suitable for industrial environments. The improved architecture has introduced the Bitcoin design to form a multi-center, easily expandable partially distributed architecture. They have also incorporated the Bell-La Padula (BLP) along with Biba Model to address three major security requirements such as confidentiality, integrity and availability (CIA) that further strengthens the security of the architecture.

The work [87] has introduced fog computing as an intermediate layer in the IIoT architecture to meet certain application specific requirements of smart digital manufacturing. However, introduction of fog layer has led to several other security issues to rise up. In this context, the authors have proposed an Attribute Credential based Public Key Cryptography (AC-PKC) scheme to meet authentication and privacy-preserving access control requirements of this new architecture. The algorithm proposes a two level verification scheme which requires a fog node to generate a signature for the command it issues for an actuator. The actuator on receiving this, has to perform the two level verification to authenticate that the command was indeed issued by a trusted fog node. Similarly, access control is imposed by introducing fuzzy authentication technique

Journal Pre-proof

which verifies whether data processing service is to be provided to the requester or not. Moreover, the shared data is also encrypted with a protected key to avoid data leakage.

4.3.2. Smart Grid

Smart Grid refers to an improved electricity supply chain that runs from a major power plant all the way to our homes [88]. The basic concept of Smart Grid is to add monitoring, analysis, control, and communication capabilities to the national electrical delivery system to maximize the throughput of the system while reducing the energy consumption [88]. Towards implementing the Smart Grid, the concept of IoT is introduced. Amid all the advantages that the traditional systems have gained, smart grid has also been exposed to several security vulnerabilities and threats. We highlight some of the ongoing research work to deal with these issues here.

Traditional TCP/IP based network communications are not suitable for secure communication in IIoT based Smart Grids. Therefore, the work [89] proposes a Software Defined Networking (SDN) enabled multi attribute secure communication model for IIoT based Smart Grid environment. The communication model is designed using a cuckoo-filter based forwarding scheme at SDN control plane. To secure the data generated at IIoT devices and stored at cloud servers, an Attribute Based Encryption (ABE) scheme is designed. Finally, to allow users to verify the integrity and authenticity of their data stored at cloud servers, a peer entity authentication scheme using Kerberos is also presented.

Electricity consumption data from a Smart Grid is largely used for big data analysis. This raises a need of data utility along with single user's privacy preservation. To achieve this objective Liu et al. [90] have proposed a practical privacy preserving data aggregation scheme without using a Trusted Third Party (TTP). In the proposed scheme the trusted users construct a virtual aggregation area to mask his own data.

5. Blockchain in IoT and IIoT

With the booming growth of IoT followed by IIoT, the number of connected IoT devices and the data generated by them has become a huge bottleneck in meeting Quality-of-Service (QoS) [28]. This is where Blockchain comes into the picture by supporting a decentralized way of storing data along with trustful and anonymous transactions. Blockchain technology can thereby be used for tracking and coordinating the billions of connected devices. It can also be used for enabling the processing of transactions to allow significant savings for IoT industry manufacturers. This decentralized approach would further eliminate single points of failure, creating a more resilient ecosystem for devices to run on [5]. The cryptographic algorithms used by blockchains, would also help to make consumer data more private [27].

A blockchain is a distributed immutable verifiable ledger. A typical design of a blockchain consists of a series of transactions which are put into one block. These blocks are then linked in such a way, that if a transaction is altered in one block it has to be updated in all the subsequent blocks [27]. Since the ledger

Journal Pre-proof

is maintained with many peers, it is difficult to alter a transaction [28]. All the blockchain peers need to agree or validate each transaction to get added to a block [23]. Once validated the block gets updated in the Blockchain. This agreement is achieved with the help of consensus algorithms like Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof-of-Stake (DPoS), Proof-of-Authority (PoA) etc. Blockchain technology is radically reshaping not only the modern IoT world but also the industries. Researchers of late have focused on integrating blockchain into the IoT ecosystem to include distributed architecture and security features into IoT. But before we discuss on how blockchain is bringing about a major paradigm shift in IoT, we explain the major features of Blockchain as follows [5]:

- The **decentralization** offered by Blockchain technology enables two nodes to engage in transactions without using a trusted third party. This eliminates the bottleneck of a single point of failure thereby enhancing fault tolerance.
- All new entries made in the Blockchain are agreed upon by nodes using decentralized consensus algorithm. The design is such that to modify an entry in a block, all subsequent blocks in all the peers have to be altered. This ensures *immutability* of blockchains.
- The **auditability** property of blockchains ensures transparency by allowing peers to look up and verify any transaction.
- The blockchain peers hold copies of identical replicas of ledger records. Blockchains therefore ensure **fault tolerance**. This property helps maintain data integrity and resiliency in the network.

The benefits of decentralizing IoT are numerous and notably superior to current centralized systems and are discussed below:

- **Improved Trust and Security:** The distributed and immutable nature of blockchain would eliminate single point of entry/vulnerability for attackers/hackers. All transactions are cryptographically signed using unforgeable signatures making them non-repudiable and resistant to attacks.
- **More Robust:** Decentralization will make IoT more accessible and damage costs from hacks can be more easily prevented or avoided all together. Intermediaries that operate for centralized IoT systems will be eliminated through decentralizing IoT, thereby reducing the associated costs.
- **Autonomy:** Blockchains enable smart devices to act independently according to the pre-determined logic (using *Smart Contracts*). This would completely remove intermediary players and central authority.
- **More trustworthy:** The use of efficient Smart Contracts for communication amongst IoT devices along with the decentralization offered by blockchain makes the entire system more trustworthy.

Journal Pre-proof

- **Data provenance:** Since all transactions are recorded on the ledger and signed by the devices/entities generating data, data provenance can be achieved.
- **Fairness:** By using native cryptocurrency in blockchain, parties can be incentivised. This makes the IoT system fair.

Despite the advantages (discussed above) that the integration of blockchain into the IoT platform will bring, the traditional blockchains (like Ethereum and Bitcoin) suffer from the follow drawbacks too [91]:

- **Scalability:** As the number of IoT devices increase, the amount of data generated will be huge, thereby leading to the requirement of more storage space to keep the transactions updated in the ledger. This will further lead to high transaction and storage costs.
- **Communication Overhead and Synchronization:** Since each new transaction that is added to the blockchain, needs to be broadcast to all the peers, it involves a lot of communication overhead. Further, all of the blockchain peers need to synchronize and maintain the same copy of the blockchain, which further adds to the overhead.
- **Efficiency:** In order to get a transaction approved, it needs to be verified by all other peers. Thus, the verification algorithm is run multiple times at each of the peers which drastically reduces the operational efficiency.
- **Energy Wastage:** A majority of the popular blockchain technologies use Proof of Work (PoW) to achieve consensus and are thereby inefficient. They need to perform a lot of computations, thereby leading to energy wastage.

Due to the aforementioned disadvantages of the traditional blockchain technology, a challenging direction of work is to design scalable, computable and energy efficient, secure blockhains for IoT and IIoT applications. A major step in this direction has been taken by the IOTA foundation [91], founded in 2014. IOTA was specifically designed for the IoT and it differs from the existing blockchains as it doesn't use any traditional Blockchain at all. The main structure of IOTA is the Tangle, which is a Directed Acyclic Graph (DAG) [91]. The transactions (referred to as *sites* in Tangle) are stored in a graph like format, where the nodes are entities that issue and validate transactions [91]. Whenever a new transaction arrives it is represented by directed edges and must be approved by two previous transactions. In order for a node to validate a transaction, it has to give Proof of Work, which on being successfully executed registers the transaction. This functionality of Tangle allows us to eliminate the need for miners in the network as the node itself acts as a miner now which further reduces the transaction costs to zero [91]. In order to issue a transaction, users must work to approve other transactions. If a node finds that a transaction is in conflict with the

Journal Pre-proof

Tangle history, the node will not approve the conflicting transaction thereby ensuring network security [91]. Despite all these, IOTA's Tangle has several advantages as described below [91]:

- **Scalability:** IOTA addresses this issue specifically by not using a blockchain-based decentralized network, instead opting for their Tangle platform. With IOTA, as the transaction rate increases, scalability also increases i.e. the more subscribers and transactions the system has, the faster it gets. More importantly, the latency, that is, the time between placing a transaction and validating it, also approaches to zero as soon as a certain size is reached.

- **Centralization of Control:** For a transaction to take place in the Tangle, the previous two transactions have to be validated by it. This makes the network faster with increasing use. Thus, IOTA allows each user who has initiated a transaction to act as a miner.

- **Quantum Computing:** IOTA uses 'exclusively quantum resistant cryptographic algorithms' which makes it future oriented and immune to brute force attacks. Moreover, Tangle holds the power to decrease the impact of quantum consensus attack by almost a million times.

- **Micro Payments:** In traditional blockchain platforms, the concept of mining involves transaction fees (i.e. financial rewards set by the sender of the transaction). As a rsult, even the smallest payment amounts result into high transaction fees. However, in IOTA's Tangle each site does its own PoW to get added to the network, so the concept of transaction fees is completed eliminated.

However, Tangle also has the following disadvantages for which Ethereum or Bitcoin is preferred over Tangle for commercial use in IoT [91]:

- Smart Contracts do not exist for IOTA/Tangle and is a major drawback while trying to build a decentralized application.

- It is mathematically more easy for a malicious node to attack Tangle. Only 34% of the total hashing power is required to attack a Tangle.

- IOTA has a concept of a single node (known as the coordinator) signing new 'milestone' every few seconds. This can be seen as a blockchain system with a single block issuer which raises problems related to a centralized architecture.

Apart from IOTA's Tangle there are a few other Blockchain designs specifically for IoT which are being explored lately and is slowly gaining popularity. These are as follows:

- **Hdac:** The Hyundai Digital Asset Company (Hdac) is developed to apply blockchain technology to smart homes, smart factories and smart buildings for M2M transactions [92]. Hdac incorporates a

Journal Pre-proof

double-chain system (public and private) to increase transaction rate in order to effectively communicate, authenticate IoT devices.

- **VeChain:** VeChain is a global enterprise-level public blockchain platform which can be used to hold automobile passports by creating digital records of cars — including registration, insurance, repair history and even driver behavior throughout its life cycle [93]. VeChain makes use of IoT technology for luxury goods by embedding smart chips within the luxury products so that brands can monitor their sales in real-time, thereby preventing illegal overstock trading and allowing consumers to verify the authenticity of the product.

- **Waltonchain:** Waltonchain is created using a combination of blockchain technologies with RFID for effective IoT integration [94]. They primarily focus is on tracking processes and products in the supply chain, like food and drug traceability by implanting RFID tags and reader-writer control chips into products. Information regarding the status of products is then downloaded for analysis onto a secure blockchain.

- **Streamr:** Streamr is an open-source blockchain infrastructure to power the world's data economy and to give people back control of their own information [95]. Their technology can be implanted into everyday objects such as cars to record data including traffic and local fuel prices. The user can then choose to sell this data to fellow car users or highway agencies, or buy information from other users that will help them make real-time decisions in a connected smart city.

However, due to the aforementioned disadvantages of Tangle, for practical implementation of IoT/IIoT applications Smart Contract based Blockchain platforms like Ethereum is preferred over Tangle. A Smart Contract is a self-enforcing piece of computer program that can be used to formalize simple agreements between two parties and control the transfer of digital currencies or assets between them under certain conditions [28]. A Smart Contract not only defines the rules and penalties related to an agreement in the same way that a traditional contract does, but it can also automatically enforce those obligations [27]. Smart Contracts in blockchain are managed by a P2P network of computers which allow devices to function securely and autonomously by creating agreements that are only executed upon completion of specific requirements [91]. It not only allows for greater automation, scalability and cheaper transfers (no third-party needed to oversee transactions) but these Smart Contracts can also prevent overrides by individuals that want to use the data for their own benefit [91].

In consideration to the above discussion, the works performed by the aforementioned surveys (Section 2.3), and with our view of this existing survey work we categorize proposed blockchain based solutions majorly into two categories. In the following two subsections, we discuss on how blockchain based solutions have helped IoT as well as industrial IoT domains.

Journal Pre-proof

5.1. Blockchain Solutions for IoT

Leveraging the benefits of integrating Blockchain in IoT, researchers have studied on how to handle important issues such as IoT device level security, managing huge volumes of data, preserving user privacy, ensuring trust, confidentiality, integrity etc. Therefore, in this section we discuss a few of the notable works [96, 97, 98, 99, 100, 101, 102, 103, 104] which have addressed the aforementioned issues and proposed blockchain-based solutions to handle them.

In one such work [96], the authors have proposed a Blockchain Connected Gateway for Bluetooth Low Energy (BLE) enabled IoT devices to maintain secure and adaptive user privacy preference. Individual user privacy is maintained because the gateway prevents users' sensitive data from being accessed without his/her consent. Moreover, for authentication and secure privacy preservation, a digital signature scheme based on bilinear pairing is also proposed. The blockchain network is adopted as the underlying architecture to resolve privacy disputes between IoT application providers and its users by encrypting users' preference and storing it in the network. In another work [97], the authors have proposed a Blockchain of Things (BoT) model to overcome problems related to hacking of IoT devices. Their proposed model solves the security vulnerabilities in the sensor multi-platform by using a color spectrum chain blockchain technique. The said technique uses multiple-agreement algorithm to performance of Thin Plate Spline (TPS) in order to measure various security strengths. Additionally, the work [98] has proposed and implemented an automatic door locking system based on mobile fingerprint verification using blockchain technology. A user authenticates himself through a mobile devices via fingerprint recognition and the underlying blockchain secures the system by preventing forging, tampering or leaking of a user's fingerprint information by malicious individuals. However, the work [99] points out that it would be very difficult for the resource-limited mobile devices to perform proof of work to reach consensus because of substantial resource requirement. Therefore, they propose a prototype for edge computing where the mobile devices would use the resources of the edge devices to perform complex proof of work operations.

To protect and store the huge volumes of data generated by IoT devices, the work [100] has proposed a distributed blockchain-based data storage scheme using certificateless cryptography. This secure proposed system uses edge devices which collect data from the IoT devices, register the data against that specific IoT device in the blockchain and finally forward the data to a Distributed Hash Table (DHT). When a requester queries for a specific data, a transaction is issued to the blockchain, which then authenticates the requester by using certificateless cryptography. On successful authentication, the DHT forwards the requested data. Thus, the blockchain acts as a trusted third party by managing data storage, allowing data protection and also performing user authentication. Similarly, the work [101] has proposed a blockchain based distributed cloud architecture by incorporating Software Defined Networking (SDN) enabled controller fog nodes at the edge of the network. This flexible architecture is capable of gathering, classifying and analyzing data streams at the edge of the network. The proposed architecture is sufficient enough to efficiently manage the

Journal Pre-proof

huge volumes of raw data produced by the IoT devices at the edge of the network. This model also brings in an efficient way to offload data to the cloud and thereby reduces end-to-end delay and also traffic load in the core network.

Traditional cloud based systems require third party service providers to build trust between data owners and users. To tackle this issue of trust and also scalability, Manzoor et al. [102] have proposed a blockchain-based proxy re-encryption scheme [105] by integrating runtime dynamic Smart Contracts. Involvement of the Smart Contract eliminates the need of a trusted third party. It also efficiently allows data visibility between a owner and the user registered to the Smart Contract by utilizing proxy re-encryption. Thus the proposed system allows secure sharing and storing of the IoT sensor data. This is achieved by encrypting the data before uploading to the cloud and re-encrypting it before sharing to a user thus acquiring complete confidentiality.

Dorri et al. [103] have proposed a Lightweight Scalable Blockchain (LSB) based scheme to achieve decentralization as well as end to end privacy and security. LSB is explored in a smart home setting which forms the first tier, and an overlay network forming the second tier. The overlay network is organized as clusters to ensure scalability and the public Blockchain is managed by the Cluster Heads (CHs). Symmetric encryption is used to manage transactions in both the tiers along with a Distributed Throughput Management (DTM) scheme. DTM dynamically adjusts certain system parameters to ensure security as well as throughput of the system.

Shen et al. [104] have proposed a blockchain-based privacy preserving Support Vector Machine (SVM) training scheme, named secureSVM to tackle challenges related to data integrity and privacy. Blockchain technology is used to build a reliable and secure data sharing platform where data providers encrypt their data locally using Pailier encryption before recording on a distributed ledger. Homomorphic cryptosystem [106] is used to build secure building blocks such as secure comparison and secure polynomial multiplication. Finally, a secure SVM training algorithm is designed which eliminates the need of a trusted third party and requires only two interactions in a single iteration. Through security analysis, the authors have shown that their algorithm ensures confidentiality of both the SVM model parameters and sensitive data.

Apart from the wide range of possibilities (discussed above) that Blockchain technology has brought in, it also empowers several traditional IoT applications to enhance their security and to bring about transparency within the IoT ecosystem. Therefore, in the following subsections we discuss how two of the most relevant IoT applications have used blockchain to add decentralization, scalability and other benefits to their system.

5.1.1. E-Healthcare

E-Healthcare maybe defined as an emerging field of medical informatics that uses modern information and communication technologies to prioritize the delivery of clinical information, care and services in order to cater the needs of citizens, patients, healthcare professionals, healthcare providers, as well as policy makers

Journal Pre-proof

[107]. Blockchain technology is being leveraged to remodel the entire healthcare setup alongside exchange of useful healthcare data, thereby enabling key stakeholders such as doctors, clinical researchers, patients, pharmacists, and other healthcare providers to gain simplified, faster, secure and reliable access to electronic medical information [108]. Therefore, in this section we discuss a few of the most relevant research works [107, 109, 110] that have used blockchain to achieve some potential benefits.

Data leakage in any IoT based application (especially Electronic Health Records (EHRs) in Healthcare) could result in privacy violation of the users. Thus, to eliminate such problems and to also allow flexible sharing of sensitive data, the work [107] has proposed a blockchain-based searchable encryption scheme for EHRs. According to this scheme, the real EHRs are stored in the public cloud servers whereas an index for each EHR is calculated using a complex logic expression. This index is then stored in the blockchain, which allows the data owners to have full control over their data. Further, this scheme also allows efficient sharing of EHRs across varied range of users, where users obtain authorization rights by authenticating themselves to the data owners. Similarly, the work [109] has proposed a privacy-friendly EHR storage platform in cloud, using blockchain known as MediBchain. As per MediBchain sensitive parts from a patients data are extracted and stored in the blockchain to attain security, integrity and accountability. Whereas the remaining part of the EHR is stored in encrypted format using ECC in the cloud.

To promote secure handling and management of Protected Health Information (PHI) generated by medical sensors, the work [110] has proposed the use of blockchain based Smart Contracts. They have deployed their protocol on an Ethereum based private blockchain where medical sensors communicate with a smart device to trigger Smart Contracts in order to write records of the events onto the blockchain. The Smart Contract further supports medical interventions and real-time patient monitoring by sending notifications to the proper participants as and when required.

5.1.2. Vehicular Ad-Hoc Network (VANET)

A Vehicular Ad-Hoc Network or VANET is a wireless communication system composed of vehicles equipped with radio interfaces capable of exchanging data among themselves as well as with road-side base stations with the aim of providing efficient and safe transportation [111]. Recently, blockchain is being typically introduced into the VANET network to not only manage the event messages and trustworthiness of nodes but also for secure, accurate delivery of data. Therefore, in this section we discuss a few of the recent research works [111, 112, 113, 114] that have integrated blockchain into vehicular networks to achieve potential benefits.

In VANET, secure sharing of data among the vehicles is critical to ensure transportation efficiency as well as driver/passenger security. In this regard, the work [111] has initially designed a secure reputation-based voting scheme for miner selection which uses candidates past transactions and other vehicles opinion to choose a suitable miner. Miners are categorized as active and standby. Whenever a new block is generated,

Journal Pre-proof

it is audited by the standby miners to prevent collusion amongst active miners. Efficient Smart Contracts are also designed to incentivize the standby miners for their participation. Contrarily, the work [112] has proposed the design of a new blockchain, where message trustworthiness and node trustworthiness are stored as transactions in the block. They have also proposed maintaining a separate blockchain based on geographical location for each country to improve scalability. Further, they have proposed the use of edge servers to offload high computational tasks in order to reduce latency in block generation.

Since VANETs operate in non-trusted environments therefore it becomes extremely difficult for the vehicles to ensure the credibility of the received event messages. Yang et al. [113] have proposed a decentralized trust management system applicable for VANETs where vehicles can validate received messages using Bayesian Inference Model. A rating is generated by the vehicles based on this validation which can further be used by the roadside units (RSUs) to calculate the trust values which is put into each block. They have also implemented a joint Proof of Stake (PoS) and Proof of Work (PoW) to achieve consensus. However, the work [114] has contradicted by saying that the RSUs cannot be fully trusted and may thereby lead to serious security/privacy challenges. To handle this, they claim to use consortium blockchain [115] along with Smart Contracts to achieve secure data sharing via authorization. Additionally, they have also proposed a reputation based scheme to achieve high quality data sharing.

5.2. Blockchain Solutions for IIoT

Integrating Blockchain technologies into industrial IoT systems has proved to be quite beneficial. It has immensely helped to further strengthen the industrial systems by offering benefits like secure data sharing, privacy preserving data aggregation, data confidentiality etc. Therefore, here we first discuss a few of the notable works [116, 117, 118, 119] that have handle these challenges efficiently.

Untrusted or malicious service providers and dishonest clients may maliciously deny service provisions for their own benefits. To prevent such malicious repudiation activities, the work [116] has proposed a blockchain based non-repudiation network computing service scheme, especially for industrial IoT environments. According to this scheme, blockchain is used as a service publication proxy as well as an evidence recorder where the required service program is divided into two non-executable parts. To enforce non-repudiation, each of these parts is delivered separately via on-chain and off-chain channels along with mandatory evidence submissions.

Additionally, Lin et al. [117] have proposed a blockchain-based system named BSeIn for Industry 4.0, to enforce secure mutual authentication remotely with fine-grained access control. The proposed scheme integrates attribute signatures along with blockchain to authenticate end user terminals anonymously. For the purpose of gateway authentication, Message Authentication Code (MAC) is utilized. Further, BSeIn utilizes multi-receivers encryption [120] technique to provide confidentiality to authorized participants. Finally, Smart Contracts are utilized to process requests in order to ensure scalability.

Journal Pre-proof

Two of the major challenges (apart from the ones discussed above) of industrial IoT lies in primarily achieving high quality data collection with limited sensing range of energy constrained Mobile Terminals (MTs). The other challenge lies in ensuring secure sharing and exchange of data among MTs. To address this concern, the work [118] has proposed an Ethereum blockchain-enabled mechanism to achieve the said objective along with Deep Reinforcement Learning (DRL) to create a reliable IIoT environment. The distributed DRL based approach helps the MTs to move to a suitable location based on geographic fairness in order to maximize data collection. After data collection, an MT can encrypt the data with its private key and send it to the blockchain as a signature for storage. Since Ethereum is a tamper-proof ledger, it ensures reliability and data security. Now, to simultaneously guarantee transaction efficiency and system security, Huang et al. [119] have proposed a credit-based proof-of-work (PoW) mechanism for IIoT devices. The proposed mechanism is based on directed acyclic graph (DAG)-structured blockchains which is further used to develop a data authority management method. This method regulates access to sensor data thereby protecting sensitive data confidentiality as well as data privacy.

Apart from the wide range of possibilities (discussed above) that Blockchain technology has brought in, it also empowers several IIoT applications to enhance their security,transparency and add additional features within their pre-existing systems. Therefore, in the following subsections we discuss how two of the most relevant IIoT applications have used blockchain to add decentralization, scalability and other benefits to their system.

5.2.1. Supply Chain

The network of all individuals, organizations, resources, activities and technology involved in the creation and sale of a product, from the delivery of source materials to its eventual delivery to the end user is referred to as Supply Chain [121]. As an immutable and better-automated alternative to centralised databases, Blockchain can eliminate certain challenges of supply chain management such as complicated record keeping and tracking of products [122]. Blockchain introduces transparency and traceability within the Supply Chain logistics. It further secures and optimizes trading relationships and business transactions within the organization [122]. Firstly, in a blockchain-based supply chain management, record keeping and provenance tracking becomes easy as the product information can be accessed with the help of RFID tags and embedded sensors [122]. Secondly, blockchain can applied to speed up administrative processes in supply chains by eliminating the middlemen and intermediaries, with reduced expenditure. This is because the risks of frauds, product duplicacy is completely eliminated while still guaranteeing the security of transactions [122]. Further, payments can be processed by customers and suppliers within the supply chain by using cryptocurrencies rather than relying on Electronic Data Interchange (EDI). Moreover, efficiency will be improved and the risk of losing products will be reduced with accurate record keeping [122]. Lastly, the immutable nature of blockchain in the supply chain helps to establish trust by prevent tampering.

Journal Pre-proof

In this context, Azzi et al. [121] has described how a reliable, transparent, authentic and secure system can be created by integrating blockchain into the supply chain architecture. They have also studied the benefits of introducing the blockchain to the supply chain and the challenges encountered in a blockchain-based supply chain management ecosystem. Therefore, in this section we discuss a couple of research works [123, 124] that has revolutionized the supply chain by introducing blockchain technology.

The work [123] has proposed a blockchain based food supply chain which uses a proof-of-object (PoO) based authentication protocol. An RFID is attached to the food product which tracks its location throughout its lifetime within the supply chain. All the real-time tracking and monitoring results generated are stored in the blockchain thus assuring better quality of the food.

The work [124] has proposed connecting a blockchain like Ethereum with each enterprises' (involved in the supply chain) information system. This would allow the companies to share their information with other peers with different visibility levels while simultaneously verifying the authenticity and integrity of the data. They have used a simulation model to recreate such a supply chain and integrate it with blockchain in order to establish their architecture.

5.2.2. Smart Grid

The network of transmission lines, transformers, substations and other necessary infrastructures that deliver electricity from the power plant to our home/business is referred to as the "electric grid" or "the grid". The integration of digital technology with the electric grid where equipments would work together with the computers to bring about automation for better handling of customer needs is referred to as the Smart Grid [88]. Smart Grid is an application of industrial IoT that has been vastly studied by researchers from industries as well as academia. With the popularity of blockchain technology, smart grids maybe hugely benefited with improved security standards of inter connectivity, permission control and data exchanges [125]. In this regard, the work [126] provides a extensive survey on blockchain solutions for the smart grid sector. They explore the relevance of applying blockchain to smart grids and also discuss the limitations and challenges of such applications. Finally, they have also provided a classification of different fields within the energy sector where blockchain can be applied along with the consensus strategy and implementation platforms that has been used in literature. Thus, in this section we highlight the works [127, 128, 129, 130, 131, 132] that have used blockchain to achieve the aforementioned benefits in Smart Grid.

In one such work [127], the authors have first examined the necessity of smart grid and then the requirement of security in smart grid. Next, it has suggested using Rainbowchain, which is a type of blockchain technology that uses seven authentication techniques to achieve superior performance and better energy exchange compared to the other traditional blockchain designs. The real-time data collected by Smart Meters (SMs) in Smart Grids may disclose personal information of users. Therefore, the work [128] has proposed a privacy preserving efficient data aggregation scheme which divides users into different groups. The members'

Journal Pre-proof

data of each group is recorded in a private blockchain. The inner privacy within a group is preserved by using pseudonyms, where each user may create and associate his/her data to multiple pseudonyms. Further, a bloom filter is used to realize fast authentication while protecting users' privacy. It is also used to judge the validity of pseudonyms using asymmetric encryption to provide zero knowledge proof. Similarly, peer-to-peer energy trading is an important activity in IIoT, especially in microgrids and vehicle-to-grid networks. However, untrusted and nontransparent energy markets introduce security and privacy concerns in such settings. To address these challenges Li et al. [129] have proposed a secure energy trading system (named energy blockchain) using the consortium blockchain technology. They have also designed a credit based payment scheme to reduce transaction delays and support fast payment along with frequent energy trading. Finally, they have also used Stackelberg game to propose an optimal pricing strategy for credit loans in order to maximize utility of credit banks. All transactions taking place in the energy grid are digitally signed and are also publicly authenticated and audited by other entities. This ensures transaction authentication as well as data unforgeability.

The Service Providers (SPs) are often prone to becoming a single point of failure while offering service to their respective Smart Meters (SMs). To address this issue, the work [130] has proposed an efficient and secure decentralized keyless signature scheme based on consortium blockchain. The proposed consensus mechanism turns the blockchain into an automated access control manager where SPs can track each other via the blockchain, without the requirement of a trusted third party (TTP). Correspondingly, the work [131] has proposed a localized point to point (P2P) Electricity Trading system with Consortium Blockchain (PETCON) to improve transaction section without depending on a TTP. The amount of traded electricity and the electricity pricing are solved using an iterative double auction mechanism. Energy transactions are uploaded to the Local Aggregators (LAGs) after encryption which then audit the transactions and record them in a distributed ledger. Finally, the work [132] has presented a new consensus algorithm known as Hyper Delegation Proof of Randomness (HDPoR) to introduce parallel computing capabilities in blockchain. The design attempts to deliver an efficient, secure peer-to-peer (P2P) transaction service model for energy exchange in smart grid.

6. Taxonomy of Security Research in IoT/IIoT

This section provides a taxonomy of security research in general for the domain of IoT and IIoT. Here, we segregate the works discussed in the above sections into seven broad categories on the basis of typical security research areas. With regard to research in the domain of security for IoT/IIoT, the predominant categories are as follows : (a) Designing Authentication Protocols (b) Developing Authorization schemes (c) Preventing Attacks (d) Privacy Preservation (e) Secure Data Management (f) Ensuring Basic Security (g) Ensuring Trust.

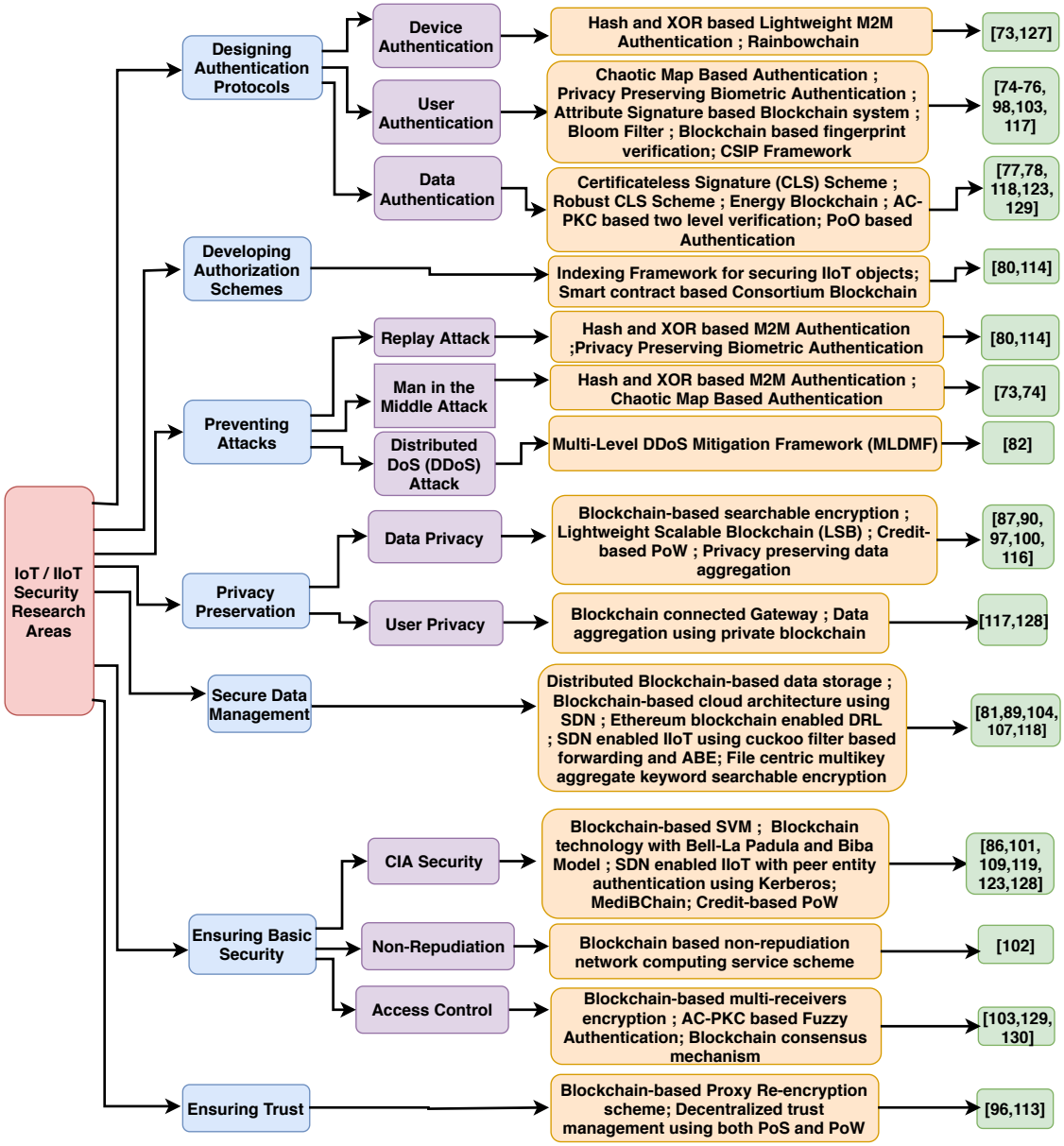

Figure 3: *Taxonomy of IoT/IIoT Security Research*

Journal Pre-proof

Authentication protocols are designed to authenticate users, devices or data in transit. Simple crytographic operations are coupled together to achieve device authentication. Biometric or chaotic map based solutions, even blockchain based fingerprint verification methods are primarily used to achieve user authentication. Also, data authentication can be achieved by designing proper signature schemes depending on the suitability of different applications. On the other hand, specialized Smart Contracts are deployed in the blockchain framework to develop proper authorization schemes. Apart from that, indexing framework for smart objects is another traditional approach of achieving authorization, especially for IIoT systems.

Attacks can create havoc to an IoT system, especially the damage caused to industrial IoT systems can be even more devastating. Therefore, apart from the broad classification of IoT attacks discussed in Section 3, attacks (like Replay attack, MiTM attack and DDoS attacks) that are specifically relevant to IIoT and require special emphasis are discussed here. Preventive methods against these attacks are also IIoT specific and are provided using simple cryptographic techniques or other multi-level mitigation frameworks.

Maintaining data and user privacy are the two most important requirements in an IoT/IIoT system. Various types of blockchain based solutions have been proposed in this regard. Different data aggregation techniques using blockchains have also been recently suggested by the research community to help in preserving privacy. Apart from preserving data privacy, secured data management is also another important concern where researchers have focused their attention. A large number of blockchain specific solutions incorporating SDN or ABE have also been explored in this domain. As a traditional way of securing data management, multi key aggregate keyword searchable encryption has been proposed.

Ensuring basic security includes CIA security, non-repudiation and access control. Solutions using SVM, credit based consensus mechanisms and various encryption techniques coupled with the blockchain platform have been proposed. Also, to ensure trust a combination of consensus algorithms and re-encryption techniques coupled with blockchain have been proposed.

Figure 3 shows the entire taxonomy of security research advancements undergone in the IoT and IIoT sector. From this figure followed by the discussions we get a clear idea about which areas researchers have paid attention and what kind of solutions have been proposed. This helps us to investigate further and highlight in the next section the open research areas that need to be paid attention to both IoT and IIoT.

7. Open Research

This section provides the list of open research areas that still remain less investigated based on the major divisions made above:

Attack specific Security Vulnerabilities in IoT:

- Developing lightweight cryptographic protocols to protect IoT devices against vulnerable attacks.
- Developing preventive techniques against Traffic Analysis attacks.

Journal Pre-proof

- Securing RPL to handle the problem of routing loops or preventing alteration of routing information.
- Developing preventive measures to combat sinkhole and wormhole attacks in an IoT system.
- Proposing techniques or solutions to prevent or solve network DDoS attacks.
- Lightweight Anti-Malware solutions need to be devised to protect the IoT devices from Malware.
- Developing lightweight schemes to simultaneously provide data security while maintaining accessibility to only authorized users.
- Need for developing lightweight cryptographic algorithms and efficient key management schemes for protecting data confidentiality and integrity.
- Maintaining data transparency and allowing users to set their own privacy preferences is another open research area.
- Developing application specific data protection techniques is of dire need. For example, Healthcare system require proper access control mechanisms in order to provide protection to sensitive health records however, in case of VANET maintaining data integrity and confidentiality is of topmost priority.

Security Issues in IIoT:

- Designing a secure Fog-based IIoT architecture to reduce feedback latency and computation overhead on resource constrained devices.
- Securing all cloud based interactions in an industrial environment. This includes data transferred and stored in the cloud.
- Securing all device to device communications in IIoT from attacks like tampering.
- Designing security algorithms in a way to eliminate trust on third party cloud service providers entirely.
- Developing application specific attack prevention schemes for IIoT environments like Smart Factories, Smart Grids etc.
- Developing a common and standardized security policy for all IoT devices from different vendors in an industrial setting.

Security Loopholes in Blockchain based IoT/IIoT:

- Designing adaptable and dynamic blockchain-based security framework for both high end servers and low powered IoT devices.
- Need for developing energy efficient blockchain consensus algorithms because of energy constraint IoT devices, typically industrial machinery.

Journal Pre-proof

8. Conclusion

With the emergence of IoT, several security vulnerabilities ranging from attacks on devices to attacks on data in transit has drawn attention of the research community. Further, the extensive application of IoT in industries has made IIoT as a separate research domain. The tight coupling of the physical world with the virtual world through the use of intelligent systems has further aggravated the vulnerabilities in Industrial IoT based systems. Therefore, in this work during surveying IoT specific security problems and their solutions are discussed with special emphasis to IIoT. We claim that, to the best of our knowledge, we are the first to report on the object based categorization of attacks in IoT. This classification would immensely help the researchers, practitioners and industry people to determine which attacks are relevant to their respective domain of interest. Further, with the emergence of Blockchain technology, its integration into both IoT and IIoT has proved to be beneficial over the traditional centralised systems. Also, through a comprehensive taxonomy, researchers would get a better understanding of the major security research problems and their solutions in the field of IoT and IIoT.

Finally, there is an urgent need of proactively addressing newly emerged threats, given the wide applicability of IoT/IIoT and also developing robust security solutions using latest technologies like Blockchain. Thus, this survey provides interesting open research areas on security issues in IoT/IIoT both for traditional and blockchain based solutions which still remain less investigated.

References

[1] Ericsson, The connected future, https://www.ericsson.com/en/mobility-report/internet-of-things-forecast.

[2] L. D. Xu, E. L. Xu, L. Li, Industry 4.0: state of the art and future trends, International Journal of Production Research 56 (8) (2018) 2941–2962. arXiv:https://doi.org/10.1080/00207543.2018.1444806, doi:10.1080/00207543.2018.1444806.
URL https://doi.org/10.1080/00207543.2018.1444806

[3] PwC, Industry 4.0: Building the digital enterprise, https://www.pwc.com/gx/en/industries/industrial-manufacturing/publications/assets/pwc-building-digital-enterprise.pdf (2017).

[4] J. Wan, S. Tang, Z. Shu, D. Li, S. Wang, M. Imran, A. V. Vasilakos, Software-defined industrial internet of things in the context of industry 4.0, IEEE Sensors Journal 16 (20) (2016) 7373–7380.

[5] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M. H. Rehmani, Applications of blockchains in the internet of things: A comprehensive survey, IEEE Communications Surveys Tutorials.

[6] T. M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.

[7] A. Mosenia, N. K. Jha, A comprehensive study of security of internet-of-things, IEEE Transactions on Emerging Topics in Computing 5 (4) (2017) 586–602.

[8] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in internet-of-things, IEEE Internet of Things Journal 4 (5) (2017) 1250–1258.

[9] M. FRUSTACI, P. PACE, G. ALOI, G. FORTINO, Evaluating critical security issues of the iot world: Present and future challenges, IEEE Internet of Things Journal.

Journal Pre-proof

[10] F. A. Alaba, M. Othman, I. A. T. Hashem, F. Alotaibi, Internet of things security: A survey, Journal of Network and Computer Applications 88 (2017) 10 – 28.
URL http://www.sciencedirect.com/science/article/pii/S1084804517301455

[11] M. A. Khan, K. Salah, Iot security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems 82 (2018) 395 – 411.
URL http://www.sciencedirect.com/science/article/pii/S0167739X17315765

[12] F. I. Khan, S. Hameed, Understanding security requirements and challenges in internet of things (iots): A review, ournal of Computer Networks and Communications.
URL https://doi.org/10.1155/2019/9629381

[13] D. E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of things security: A top-down survey, Computer Networks 141 (2018) 199 – 221.
URL http://www.sciencedirect.com/science/article/pii/S1389128618301208

[14] A. R. Sfar, E. Natalizio, Y. Challal, Z. Chtourou, A roadmap for security challenges in the internet of things, Digital Communications and Networks 4 (2) (2018) 118 – 137.
URL http://www.sciencedirect.com/science/article/pii/S2352864817300214

[15] J. H. Ziegeldorf, O. G. Morchon, K. Wehrle, Privacy in the internet of things: Threats and challenges, CoRR abs/1505.07683.
URL http://arxiv.org/abs/1505.07683

[16] C. Li, B. Palanisamy, Privacy in internet of things: From principles to technologies, IEEE Internet of Things Journal 6 (1) (2019) 488–505.

[17] H. Boyes, B. Hallaq, J. Cunningham, T. Watson, The industrial internet of things (iiot): An analysis framework, Computers in Industry 101 (2018) 1 – 12.

[18] L. D. Xu, W. He, S. Li, Internet of things in industries: A survey, IEEE Transactions on Industrial Informatics 10 (4) (2014) 2233–2243.

[19] E. Oztemel, S. Gursev, Literature review of industry 4.0 and related technologies, Journal of Intelligent Manufacturing.
URL https://doi.org/10.1007/s10845-018-1433-8

[20] V. Alcácer, V. Cruz-Machado, Scanning the industry 4.0: A literature review on technologies for manufacturing systems, Engineering Science and Technology, an International Journal 22 (3) (2019) 899 – 919.
URL http://www.sciencedirect.com/science/article/pii/S2215098618317750

[21] T. M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.

[22] M. O. A. G. B. W. Hany F. Atlam, Ahmed Alenezi, Blockchain with internet of things: Benefits, challenges, and future directions, International Journal of Intelligent Systems and Applications(IJISA) 10 (6) (2018) 40–48.

[23] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with iot. challenges and opportunities, Future Generation Computer Systems 88 (2018) 173 – 190.
URL http://www.sciencedirect.com/science/article/pii/S0167739X17329205

[24] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things, Computer Communications 136 (2019) 10 – 29.
URL http://www.sciencedirect.com/science/article/pii/S0140366418306881

[25] Q. Wang, X. Zhu, Y. Ni, L. Gu, H. Zhu, Blockchain for the iot and industrial iot: A review, Internet of Things.
URL http://www.sciencedirect.com/science/article/pii/S254266051930085X

[26] CISCO, The internet of things reference model, http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf (2014).

Journal Pre-proof

[27] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in iot: The challenges, and a way forward, Journal of Network and Computer Applications 125 (2019) 251 – 279.
URL http://www.sciencedirect.com/science/article/pii/S1084804518303473

[28] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: Research issues and challenges, IEEE Internet of Things Journal.

[29] M. M. Ahemd, M. A. Shah, A. Wahid, Iot security: A layered approach for attacks and defenses, in: 2017 International Conference on Communication Technologies (ComTech), 2017, pp. 104–110.

[30] I. Andrea, C. Chrysostomou, G. Hadjichristofi, Internet of things: Security vulnerabilities and challenges, in: 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 180–187.

[31] D. Foundry, What is a permanent dos (pdos) attack?, https://www.datafoundry.com/blog/what-is-permanent-dos-pdos-attack/t (2017).

[32] Z. Ling, K. Liu, Y. Xu, Y. Jin, X. Fu, An end-to-end view of iot security and privacy, in: IEEE Global Communications Conference, 2017, pp. 1–7.

[33] J. Wurm, K. Hoang, O. Arias, A. Sadeghi, Y. Jin, Security analysis on consumer and industrial iot devices, in: 21st Asia and South Pacific Design Automation Conference (ASP-DAC), 2016, pp. 519–524.

[34] X. F. X. W. Y. T. F. Q. Nan Zhang, Xianghang Mi, Understanding and mitigating the security risks of voice-controlled third-party skills on amazon alexa and google home (2018).
URL https://arxiv.org/abs/1805.01525

[35] M. N. Aman, K. C. Chua, B. Sikdar, A light-weight mutual authentication protocol for iot systems, in: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1–6.

[36] T. Gomes, F. Salgado, A. Tavares, J. Cabral, Cute mote, a customizable and trustable end-device for the internet of things, IEEE Sensors Journal 17 (20) (2017) 6816–6824.

[37] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, M. Ylianttila, Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications, International Journal of Distributed Sensor Networks 10 (7) (2014) 357430.
URL https://doi.org/10.1155/2014/357430

[38] X. Hei, X. Du, J. Wu, F. Hu, Defending resource depletion attacks on implantable medical devices, in: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1–5.

[39] J. Choi, Y. Kim, An improved lea block encryption algorithm to prevent side-channel attack in the iot system, in: 2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2016, pp. 1–4.

[40] Rambus, Industrial iot: Threats and countermeasures, https://www.rambus.com/iot/industrial-iot/.

[41] S. Sicari, A. Rizzardi, D. Miorandi, A. Coen-Porisini, Reato: Reacting to denial of service attacks in the internet of things, Computer Networks 137 (2018) 37 – 48.
URL http://www.sciencedirect.com/science/article/pii/S1389128618301348

[42] P. Varga, S. Plosz, G. Soos, C. Hegedus, Security threats and issues in automation iot, in: 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), 2017, pp. 1–6.

[43] J. Liu, C. Zhang, Y. Fang, Epic: A differential privacy framework to defend smart homes against internet traffic analysis, IEEE Internet of Things Journal 5 (2) (2018) 1206–1217.

[44] U. Guin, A. Singh, M. Alam, J. Cañedo, A. Skjellum, A secure low-cost edge device authentication scheme for the internet of things, in: 31st International Conference on VLSI Design and 17th International Conference on Embedded Systems (VLSID), 2018, pp. 85–90.

[45] G. Glissa, A. Rachedi, A. Meddeb, A secure routing protocol based on rpl for internet of things, in: IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–7.

Journal Pre-proof

[46] C. Pu, S. Hajjar, Mitigating forwarding misbehaviors in rpl-based low power and lossy networks, in: 2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC), 2018, pp. 1–6.

[47] C. Cervantes, D. Poplade, M. Nogueira, A. Santos, Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things, in: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2015, pp. 606–611.

[48] P. Shukla, Ml-ids: A machine learning approach to detect wormhole attacks in internet of things, in: Intelligent Systems Conference (IntelliSys), 2017, pp. 234–240.

[49] D. Airehrour, J. A. Gutierrez, S. K. Ray, Sectrust-rpl: A secure trust-aware rpl routing protocol for internet of things, Future Generation Computer Systems.

[50] M. Singh, M. A. Rajan, V. L. Shivraj, P. Balamuralidhar, Secure mqtt for internet of things (iot), in: 5th International Conference on Communication Systems and Network Technologies, 2015, pp. 746–751.

[51] N. Park, N. Kang, Mutual authentication scheme in secure internet of things technology for comfortable lifestyle, Sensors 16 (1).

[52] Y. Ashibani, Q. H. Mahmoud, An efficient and secure scheme for smart home communication using identity-based signcryption, in: 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), 2017, pp. 1–7.

[53] V. Adat, B. B. Gupta, A ddos attack mitigation framework for internet of things, in: 2017 International Conference on Communication and Signal Processing (ICCSP), 2017, pp. 2036–2041.

[54] D. Yin, L. Zhang, K. Yang, A ddos attack detection and mitigation with software-defined internet of things framework, IEEE Access 6 (2018) 24694–24705.

[55] C. Analysis, Cert analysis on iot botnet and ddos attacks, `https://dzone.com/articles/cert-analysis-on-iot-botnet-and-ddos-attacks`.

[56] SOPHOS, 49 busted in europe for man-in-the-middle bank attacks, `https://nakedsecurity.sophos.com/2015/06/11/49-busted-in-europe-for-man-in-the-middle-bank-attacks/` (2015).

[57] C. Liu, P. Cronin, C. Yang, A mutual auditing framework to protect iot against hardware trojans, in: 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), 2016, pp. 69–74.

[58] S. T. C. Konigsmark, D. Chen, M. D. F. Wong, Information dispersion for trojan defense through high-level synthesis, in: 2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2016, pp. 1–6.

[59] H. Naeem, B. Guo, M. R. Naeem, A light-weight malware static visual analysis for iot infrastructure, in: International Conference on Artificial Intelligence and Big Data (ICAIBD), 2018, pp. 240–244.

[60] J. Su, V. D. Vasconcellos, S. Prasad, S. Daniele, Y. Feng, K. Sakurai, Lightweight classification of iot malware based on image recognition, in: IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Vol. 02, 2018, pp. 664–669.

[61] I. F. All, The 5 worst examples of iot hacking and vulnerabilities in recorded history, `https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/` (2017).

[62] M. Chan, Why cloud computing is the foundation of the internet of things, `https://www.thorntech.com/2017/02/cloud-computing-foundation-internet-things/` (2017).

[63] T. Song, R. Li, B. Mei, J. Yu, X. Xing, X. Cheng, A privacy preserving communication protocol for iot applications in smart homes, IEEE Internet of Things Journal 4 (6) (2017) 1844–1852.

[64] C. Machado, A. A. M. Fröhlich, Iot data integrity verification for cyber-physical systems using blockchain, in: 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC), 2018, pp. 83–90.

[65] Y. Rahulamathavan, R. C. . Phan, M. Rajarajan, S. Misra, A. Kondoz, Privacy-preserving blockchain based iot ecosystem using attribute-based encryption, in: IEEE International Conference on Advanced Networks and Telecommunications

Journal Pre-proof

Systems (ANTS), 2017, pp. 1–6.

[66] D. Zheng, A. Wu, Y. Zhang, Q. Zhao, Efficient and privacy-preserving medical data sharing in internet of things with limited computing power, IEEE Access 6 (2018) 28019–28027.

[67] P. Gope, B. Sikdar, Lightweight and privacy-preserving two-factor authentication scheme for iot devices, IEEE Internet of Things Journal.

[68] K. Gai, K. R. Choo, M. Qiu, L. Zhu, Privacy-preserving content-oriented wireless communication in internet-of-things, IEEE Internet of Things Journal 5 (4) (2018) 3059–3067.

[69] J. Sengupta, S. Ruj, S. D. Bit, End to end secure anonymous communication for secure directed diffusion in iot, in: Proceedings of the 20th International Conference on Distributed Computing and Networking, ICDCN '19, 2019, pp. 445–450.
URL http://doi.acm.org/10.1145/3288599.3295577

[70] ObserveIT, 5 examples of insider threat-caused breaches that illustrate the scope of the problem, https://www.observeit.com/blog/5-examples-of-insider-threat-caused-breaches/ (2018).

[71] K. Granville, Facebook and cambridge analytica: What you need to know as fallout widens, https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (2018).

[72] K. Mandittereza, 4 key differences between scada and industrial iot, https://www.linkedin.com/pulse/4-key-differences-between-scada-industrial-iot-kudzai-manditereza/ (2017).

[73] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, J. Bastos, A lightweight authentication mechanism for m2m communications in industrial iot environment, IEEE Internet of Things Journal 6 (1) (2019) 288–296.

[74] J. Srinivas, A. K. Das, M. Wazid, N. Kumar, Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things, IEEE Transactions on Dependable and Secure Computing.

[75] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, S. Kumari, A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3599–3609.

[76] F. Al-Turjman, S. Alturjman, Context-sensitive access in industrial internet of things (iiot) healthcare applications, IEEE Transactions on Industrial Informatics 14 (6) (2018) 2736–2744.

[77] A. Karati, S. H. Islam, M. Karuppiah, Provably secure and lightweight certificateless signature scheme for iiot environments, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3701–3711.

[78] Y. Zhang, R. Deng, D. Zheng, J. Li, P. Wu, J. Cao, Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial iot, IEEE Transactions on Industrial Informatics.

[79] W. Yang, S. Wang, X. Huang, Y. Mu, On the security of an efficient and robust certificateless signature scheme for iiot environments, IEEE Access 7 (2019) 91074–91079.

[80] G. Chen, W. S. Ng, An efficient authorization framework for securing industrial internet of things, in: TENCON 2017 - 2017 IEEE Region 10 Conference, 2017, pp. 1219–1224.

[81] R. Zhou, X. Zhang, X. Du, X. Wang, G. Yang, M. Guizani, File-centric multi-key aggregate keyword searchable encryption for industrial internet of things, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3648–3658.

[82] Q. Yan, W. Huang, X. Luo, Q. Gong, F. R. Yu, A multi-level ddos mitigation framework for the industrial internet of things, IEEE Communications Magazine 56 (2) (2018) 30–36.

[83] J. Guilbon, Introduction to trusted execution environment: Arm's trustzone, https://blog.quarkslab.com/introduction-to-trusted-execution-environment-arms-trustzone.html (2018).

[84] Intel, Intel software guard extensions, https://software.intel.com/en-us/sgx.

[85] Deloitte, The smart factory, https://www2.deloitte.com/us/en/insights/focus/industry-4-0/

Journal Pre-proof

smart-factory-connected-manufacturing.html.

[86] J. Wan, J. Li, M. Imran, D. Li, F. e-Amin, A blockchain-based solution for enhancing security and privacy in smart factory, IEEE Transactions on Industrial Informatics.

[87] X. Yao, H. Kong, H. Liu, T. Qiu, H. Ning, An attribute credential based public key scheme for fog computing in digital manufacturing, IEEE Transactions on Industrial Informatics.

[88] P. Mazza, Why the smart grid is important?, https://grist.org/article/adventures-in-the-smart-grid-no-1/ (2007).

[89] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, J. J. P. C. Rodrigues, Sdn-enabled multi-attribute-based secure communication for smart grid in iiot environment, IEEE Transactions on Industrial Informatics 14 (6) (2018) 2629–2640.

[90] Y. Liu, W. Guo, C. Fan, L. Chang, C. Cheng, A practical privacy-preserving data aggregation (3pda) scheme for smart grid, IEEE Transactions on Industrial Informatics 15 (3) (2019) 1767–1774.

[91] S. Popov, Tangle white paper, https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf (2018).

[92] Hdac, Hdac white paper, https://github.com/Hdactech/hdac/wiki/Hdac-Technical-Whitepaper (2018).

[93] V. Team, Vechain white paper, https://cdn.vechain.com/vechain_ico_ideas_of_development_en.pdf (2018).

[94] Waltonchain, Waltonchain white paper v2.0, https://www.waltonchain.org/en/Waltonchain_White_Paper_2.0_EN.pdf.

[95] Sreamr, Streamr white paper v2.0, https://s3.amazonaws.com/streamr-public/streamr-datacoin-whitepaper-2017-07-25-v1_0.pdf (2017).

[96] S. Cha, J. Chen, C. Su, K. Yeh, A blockchain connected gateway for ble-based devices in the internet of things, IEEE Access 6 (2018) 24639–24649.

[97] U.-M. H. J.-H. Kim, S.-K.; Kim, A study on improvement of blockchain application to overcome vulnerability of iot multiplatform security, Energies 12 (402).

[98] J.-H. Huh, K. Seo, Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing, The Journal of Supercomputing 75 (6) (2019) 3123–3139.
URL https://doi.org/10.1007/s11227-018-2496-1

[99] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, Z. Han, When mobile blockchain meets edge computing, IEEE Communications Magazine 56 (8) (2018) 33–39.

[100] R. Li, T. Song, B. Mei, H. Li, X. Cheng, L. Sun, Blockchain for large-scale internet of things data storage and protection, IEEE Transactions on Services Computing.

[101] P. K. Sharma, M. Chen, J. H. Park, A software defined fog node based distributed blockchain cloud architecture for iot, IEEE Access 6 (2018) 115–124.

[102] A. Manzoor, M. Liyanage, A. Braeken, S. S. Kanhere, M. Ylianttila, Blockchain based proxy re-encryption scheme for secure iot data sharing, CoRR abs/1811.02276.
URL http://arxiv.org/abs/1811.02276

[103] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, LSB: A lightweight scalable blockchain for iot security and privacy, CoRR abs/1712.02969.
URL http://arxiv.org/abs/1712.02969

[104] M. Shen, X. Tang, L. Zhu, X. Du, M. Guizani, Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities, IEEE Internet of Things Journal.

[105] Y. Lu, J. Li, A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds, Future Generation Computer Systems 62 (2016) 140 – 147.
URL http://www.sciencedirect.com/science/article/pii/S0167739X1500360X

[106] S. J. De, S. Ruj, Efficient decentralized attribute based access control for mobile clouds, IEEE Transactions on Cloud

Journal Pre-proof

Computing.

[107] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, N. Zhang, Blockchain based searchable encryption for electronic health record sharing, Future Generation Computer Systems 95 (2019) 420 – 429.
URL http://www.sciencedirect.com/science/article/pii/S0167739X18314134

[108] Forbes, Blockchain in healthcare: How it could make digital healthcare safer and more innovative, https://www.forbes.com/sites/forbestechcouncil/2019/06/18/blockchain-in-healthcare-how-it-could-make-digital-healthcare-safer-and-more-innovative/#149394c63e5a (2019).

[109] A. A. Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, M. S. Rahman, Privacy-friendly platform for healthcare data in cloud based on blockchain environment, Future Generation Computer Systems 95 (2019) 511 – 521.
URL http://www.sciencedirect.com/science/article/pii/S0167739X18314201

[110] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, Journal of Medical Systems 42 (7) (2018) 1–7.
URL https://doi.org/10.1007/s10916-018-0982-x

[111] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, J. Zhao, Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory, IEEE Transactions on Vehicular Technology 68 (3) (2019) 2906–2920.

[112] R. Shrestha, R. Bajracharya, A. P. Shrestha, S. Y. Nam, A new type of blockchain for secure message exchange in vanet, Digital Communications and Networks.
URL http://www.sciencedirect.com/science/article/pii/S2352864818303092

[113] Z. Yang, K. Yang, L. Lei, K. Zheng, V. C. M. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Internet of Things Journal 6 (2) (2019) 1495–1505.

[114] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, Y. Zhang, Blockchain for secure and efficient data sharing in vehicular edge computing and networks, IEEE Internet of Things Journal 6 (3) (2019) 4660–4670.

[115] X. Huang, Y. Zhang, D. Li, L. Han, An optimal scheduling algorithm for hybrid ev charging scenario using consortium blockchains, Future Generation Computer Systems 91 (2019) 555 – 562.
URL http://www.sciencedirect.com/science/article/pii/S0167739X18313578

[116] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, Y. Zhang, A blockchain-based non-repudiation network computing service scheme for industrial iot, IEEE Transactions on Industrial Informatics.

[117] C. Lin, D. He, X. Huang, K.-K. R. Choo, A. V. Vasilakos, Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, Journal of Network and Computer Applications 116 (2018) 42 – 52.
URL http://www.sciencedirect.com/science/article/pii/S1084804518301619

[118] C. H. Liu, Q. Lin, S. Wen, Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning, IEEE Transactions on Industrial Informatics.

[119] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, P. Zeng, Towards secure industrial iot: Blockchain system with credit-based consensus mechanism, IEEE Transactions on Industrial Informatics.

[120] S. H. Islam, M. K. Khan, A. M. Al-Khouri, Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing, Security and Communication Networks 8 (13) (2015) 2214–2231.
URL https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1165

[121] R. Azzi, R. K. Chamoun, M. Sokhn, The power of a blockchain-based supply chain, Computers & Industrial Engineering 135 (2019) 582 – 592.
URL http://www.sciencedirect.com/science/article/pii/S0360835219303729

[122] IBM, Ibm blockchain for supply chain, https://www.ibm.com/blockchain/industries/supply-chain.

Journal Pre-proof

[123] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, P. Chahal, Blockchain inspired rfid-based information architecture for food supply chain, IEEE Internet of Things Journal 6 (3) (2019) 5803–5813.

[124] F. Longo, L. Nicoletti, A. Padovano, G. d'Atri, M. Forte, Blockchain-enabled supply chain: An experimental study, Computers & Industrial Engineering 136 (2019) 57 – 69.
URL http://www.sciencedirect.com/science/article/pii/S0360835219304139

[125] Forbes, How blockchain can help increase the security of smart grids, https://www.forbes.com/sites/andrewarnold/2018/04/16/how-blockchain-can-help-increase-the-security-of-smart-grids/#1b59ad95b489.

[126] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renewable and Sustainable Energy Reviews 100 (2019) 143 – 174.
URL http://www.sciencedirect.com/science/article/pii/S1364032118307184

[127] J.-H. Kim, S.-K.; Huh, A study on the improvement of smart grid security performance and blockchain smart grid perspective, Energies 11 (1973).

[128] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, Y. Ma, Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities, IEEE Communications Magazine 56 (7) (2018) 82–88.

[129] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium blockchain for secure energy trading in industrial internet of things, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3690–3700.

[130] H. Zhang, J. Wang, Y. Ding, Blockchain-based decentralized and secure keyless signature scheme for smart grid, Energy 180 (2019) 955 – 967.
URL http://www.sciencedirect.com/science/article/pii/S0360544219310096

[131] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain, Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains, IEEE Transactions on Industrial Informatics 13 (6) (2017) 3154–3164.

[132] S.-K. Huh, J.-H.; Kim, The blockchain consensus algorithm for viable management of new and renewable energies, Sustainability 11 (3184).

Journal Pre-proof

Journal Pre-proof

Jayasree Sengupta is currently pursuing PhD in the Department of Computer Science and Technology at Indian Institute of Engineering Science and Technology, Shibpur, Howrah. Previously, she has received her Mtech degree in Distributed and Mobile Computing from Jadavpur University, Kolkata. She has published research articles in international conference proceedings. Her research interests include Network security, Cryptography, IoT and Industrial IoT, Blockchain.

Sushmita Ruj received her B.E. degree in Computer Science from Bengal Engineering and Science University, Shibpur, India and Masters and PhD in Computer Science from Indian Statistical Institute. She was a Erasmus Mundus Post-Doctoral Fellow at Lund University, Sweden and Post-Doctoral Fellow at University of Ottawa, Canada.
She is currently a Senior Research Scientist at CSIRO Data61, Australia. She is also an Associate Professor at Indian Statistical Institute, Kolkata. Her research interests are in Blockchains, Applied Cryptography, and Data Privacy. She serves as a reviewer of Mathematical Reviews, Associate editor of Elsevier Journal, Information Security and Applications and is involved with a number of conferences as Program Co-Chairs or committee members. She is a recipient of Samsung GRO award, NetApp Faculty Fellowship, Cisco Academic Grant and IBM OCSP grant. She is a senior member of the ACM and IEEE.

Sipra Das Bit is a Professor of the Department of Computer Science and Technology, Indian Institute of Engineering Science and Technology, Shibpur, India. A recipient of the Career Award for Young Teachers from the All India Council of Technical Education (AICTE), she has more than 30 years of teaching and research experience. Professor Das Bit has published many research papers in reputed journals and refereed International conference proceedings. She also has three books to her credit. Her current research interests include Internet of things, wireless sensor network, delay tolerant network, and mobile computing. She is a senior member of IEEE.

Journal Pre-proof

Journal Pre-proof

Conflict of Interest and Authorship Conformation Form

Please check the following as appropriate:

- All authors have participated in (a) conception and design, or analysis and interpretation of the data; (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version.
- This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.
- The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript
- The following authors have affiliations with organizations with direct or indirect financial interest in the subject matter discussed in the manuscript:

Author's name	Affiliation
Jayasree Sengupta	IIEST, Shibpur
Sushmita Ruj	CSIRO, Australis & ISI, Kolkata
Sipra Das Bit	IIEST, Shibpur

Journal Pre-proof