Internet of Things 11 (2020) 100227

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Review article

Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology

Bhabendu Kumar Mohanta[a,*], Debasish Jena[a], Utkalika Satapathy[a], Srikanta Patnaik[b]

[a] Department of Computer Science & Engineering, IIIT Bhubaneswar, Odisha 751003, India
[b] Department of Computer Science and Engineering, SOA University, Bhubaneswar 751030, India

ARTICLE INFO

Article history:
Received 24 January 2020
Revised 8 May 2020
Accepted 12 May 2020
Available online 20 May 2020

Keywords:
IoT
Security
Machine learning
Artificial intelligence
Blockchain technology

ABSTRACT

Internet of Things (IoT) is one of the most rapidly used technologies in the last decade in various applications. The smart things are connected in wireless or wired for communication, processing, computing, and monitoring different real-time scenarios. The things are heterogeneous and have low memory, less processing power. The implementation of the IoT system comes with security and privacy challenges because traditional based existing security protocols do not suitable for IoT devices. In this survey, the authors initially described an overview of the IoT technology and the area of its application. The primary security issue CIA (confidentially, Integrity, Availability) and layer-wise issues are identified. Then the authors systematically study the three primary technology Machine learning(ML), Artificial intelligence (AI), and Blockchain for addressing the security issue in IoT. In the end, an analysis of this survey, security issues solved by the ML, AI, and Blockchain with research challenges are mention.

1. Introduction

Internet of Things (IoT) is a network of smart things that share information over the internet. The smart things are used to deploy in a different environment to capture the information, and some events are triggered. The applications of IoT is a smart city, smart home, Intelligent transportation system, agriculture, hospital, supply chain system, earthquake detection, a smart grid system. As per CISCO estimated, the IoT devices connected will be 50 billion at the end of 2020. The grown of IoT devices is rapidly changing as it crosses the total world population. The data generated by the IoT devices are enormous. In traditional IoT, architecture is three types physical, network, and application layer. In the physical layer, devices are embedded with some technology which way they sense the environment and also able to connect in wired or wireless to the other device. Like in the smart home system fridge can place an order automatically to the registered retailer whenever the fruits chamber empty it, and notification will be sent to the home users. The similarity in smart hospital patients can monitor in an emergency through sensors and corresponding computing devices. As the sensors are low-end devices, less computation power, and have heterogeneous properties. Implementation of IoT comes with lots of challenges. The standardization, interoperability, data storage, processing, trust management, identity, confidentiality, integrity, availability, security, and privacy

* Corresponding author.
E-mail addresses: C116004@iiit-bh.ac.in (B.K. Mohanta), debasish@iiit-bh.ac.in (D. Jena), A117010@iiit-bh.ac.in (U. Satapathy).

https://doi.org/10.1016/j.iot.2020.100227
2542-6605/

Table 1
Related surveys work on IoT security.

Reference paper	Year	Contribution
Jing et al. [3]	2014	The security issue of three layers of IoT and its corresponding solution are surveyed in this paper.
Ngu et al. [4]	2016	The IoT middleware based architecture is proposed and explained each layer details. The authors also described the adaptability and security issues in the IoT middleware system.
Mosenia et al. [5]	2016	The authors in this survey explained the reference model and security threads present on the edge side of the model. The paper also reviewed the countermeasure to address the possible solutions.
Lin et al. [6]	2017	The paper initially described the IoT and Cyber-Physical Systems (CPS) integration. The security and privacy issues survey in detail. The edge/fog computing integration with IoT is also explained in this survey paper.
Yang et al. [7]	2017	The paper has done a survey on security and privacy issue on IoT applications and systems. The authors reviewed the authentication protocol in the IoT system. The challenging security issue in four-layer architecture based IoT application are explained in details.
Alaba et al. [8]	2017	The authors in this survey investigated the state of art security issues in IoT applications. The threats and vulnerability of the system in terms of communications, architecture, and applications are extensively reviewed. the paper concludes with the solution approach for different security issues.
Grammatikis et al. [9]	2018	The paper provides a detailed study of IoT security layer-wise. The suitable countermeasure and potential threats model are discussed in detail.
Das et al. [10]	2018	The authors in this paper investigate the security and threat model in IoT applications. The paper mentioned some of the issues in IoT systems like authentication, trust management, and access control. Some solution approach was also addressed.
Di Martino et al. [11]	2018	This paper reviewed the different standardized architecture of IoT systems and the current solution approach in terms of Security and Interoperability are explained.
Hassija et al. [12]	2019	The authors of this paper reviewed the security and threat in IoT applications. The different solution approach using machine learning, fog computing, edge computing, and Blockchain was proposed.
Proposed paper	2020	The authors in this paper initially identified the necessary Infrastructure, Protocol, Application of the IoT system. Then security issue is identified in the IoT model. Some emerging technique which can be used to solve the security issues in IoT is identified. After a rigorous survey, the authors found that machine learning, Blockchain, and Artificial intelligence are the current solution approach to solve the Security issue in IoT.

are some of the open challenges in various IoT applications [1]. The IoT is one of the most emerging technologies in the last decade and its uses in numerous applications area. Security and privacy are still challenges in many applications area. Some research work addressing security and privacy issue in IoT is already done. But as the new technology comes, which can address so of the security issue in IoT. So in this work, authors have identified three leading technologies like ML, Blockchain, and AI, which address different security issues.

1.1. Objective and contribution

The main objective of this survey is to find out the security and privacy challenges that exist in IoT applications. The authors also identified some emerging technology that can address security issues present in the system. Here the main goal is to find the research challenges and corresponding solution approach in IoT security.

The following are the contribution of the paper:

- The paper explained the IoT architecture and its enabling technology with challenges.
- The security issues in the IoT system are identified as in-depth layer-wise.
- An extensive survey on similar technologies like machine learning, artificial intelligence, and Blockchain technology integration with IoT security are performed.
- The research challenges and corresponding solution approach with emerging technology (ML, AI, Blockchain) are also explained.

1.2. Paper organization

The rest of the paper organized as in Section 2 related work of security and privacy issues of IoT are identified, and comparison was also made. The IoT architecture details and associated technology are described in Section 3. The security issues are explained in Section 4. The different security issues address in IoT applications using Machine Learning, Artificial intelligence, and Blockchain technology are explained in detail in Sections 5–7 sequentially. An analysis of the entire survey and future challenges are summarized in Section 8. The paper concludes with a summary of the work done in Section 9.

2. Related work

The authors explain the underlying system architecture and security issues in paper[2]. Previously some works related to a security issue in IoT applications, infrastructure are already done. In Table 1, a summary of some of the survey works is mentioned. Although several works already exist in this regard from different perspectives, for implementation purposes, there is no such study done. So in this survey, authors have identified the recent emerging technology (ML, AI, Blockchain), which can be addressed security issues in IoT. Some of the work integration with recent technology and IoT has already

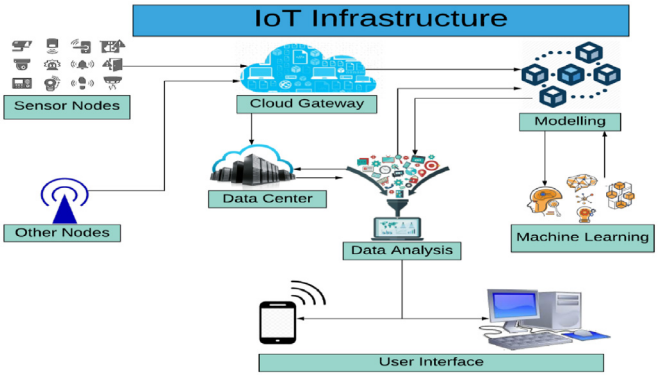

Fig. 1. Internet of things infrastructure.

been done. In this survey, the authors tried to give the details about the insight of that technology how it will solve security challenges in IoT. This will helps the reader to understand the IoT infrastructure creation and implementing it securely.

3. Internet of things (IoT) infrastructure,protocol, application

Internet of Things (IoT) has lots of potentials to apply in different real-time applications. It integrates sensors, smart devices, radiofrequency identification (RFID), and the Internet to build an intelligent system. As per Goldman Sachs estimated 28 billion smart things would be connected to a different network by 2020. The growth of IoT in the last decade in such a way that it incorporates everything from sensors to cloud computing intermediate with fog/edge computing. The IoT has different types of a network like a distributed, ubiquitous, grid, and vehicular. The applications of IoT made a huge impact in day to day life like sensors deploy in the patient body to monitoring in critical condition, monitoring gas leakage in smart kitchen, agriculture field, smart car parking, smart transportation, tracking goods details in supply chain system using sensors in the vehicle. The sensors are resource constraint devices connected through wired or wirelessly across heterogeneous networks. The IoT networks are possessed different security, privacy, and vulnerable to the attacker.

3.1. IoT infrastructure

IoT application consists of different smart things that collect, process, compute and communicate with other smart things. IoT has three layers physical, network, and application layer. Recently industries are developed many things which are embedded with intelligent things. As shown in Fig. 1 IoT infrastructure consists of not only sensors, but it also integrates with some emerging technology. The IoT application is based on either IoT-Cloud or IoT-Fog-Cloud. The security issue like data privacy [13], machine to machine communication [14], real-time monitoring [15] and IoT testbed [16] are need to be addressed for efficient IoT applications. The architecture of IoT may be centralized, distributed, decentralized structure. In IoT application processing and computing in real-time is one of the most challenging issues. Cloud computing provides more storage and assures security to the data. But recently, most of the real-time monitoring IoT application demand processing and computing in the edge of the network. So that quick action can be taken like monitoring the health condition of the serious patient, fire detection. When processing and computing are done on the edge of the network using fog devices, it becomes more vulnerable to the attacker as their devices are lightweight device traditional security is not applicable. During analytic data, a technique like a machine learning is recently used to make the IoT system more intelligent and independent to make a decision. The different smart devices are connected to make an application using some standard protocols. The security issue exists in IoT infrastructure, which needs to be addressed to build trust among end-users and make the system temper-proof. The data interoperability [17] in the IoT system works using an intelligent algorithm.

3.2. Standard protocol

The basic IoT architecture is a four layer network. Each of these layer consists of some standard protocol as shown in Table 2.

3.2.1. MQTT

MQTT stands for transportation of MQ Telemetry. It is a straightforward and lightweight messaging protocol for publishing / subscribe, designed for restricted devices and low bandwidth, high latency, or unreliable networks. The design principles are to minimize the requirements for network bandwidth and device resources while also trying to ensure reliability and some degree of delivery assurance. These principles also result in making the protocol ideal for the emerging world of low end connected devices “machine-to-machine” (M2 M) or “Internet of Things.”

Table 2
Protocols & attacks on IoT layers.

Protocols & possible attacks in IoT layers		
Layer	Protocol name	Possible security attack
Application	MQTT, CoAP, REST, AMQP	Repudiation Attack, DDoS Attack, HTTP Flood Attack, SQL Injection Attack, Cross-Site Scripting, Parameter Tampering, Slowloris Attack
Transport	TCP, UDP, DCCP, SCTP, RSVP, QUIC	SYN Flood, Smruf Attack,Injection Attack, Mitnick Attack, Opt-ack Attack
Network	CLNS, DDP, EIGRP, ICMP, IGMP, IPsec, IPv4, IPv6, OSPF, RIM	IP Address Spoofing, DoS Attack, Black Hole Attack, Worm Hole Attack, Byzantine Attack, Resource Consumption Attack.
Pysical	DSL, ISDN, IDA, USB, Bluetooth, CAN, Ethernet	Access Control Attack, Physical damage 0r Destruction, Disconnection of Physical Links

3.2.2. CoAP

Constrained Application Protocol (CoAP), as defined in RFC 7252, is a specialized Internet Application Protocol for restricted devices. It allows those restricted devices called “nodes” to use similar protocols to communicate with the broader Internet. CoAP is designed to be used by devices on the same network.

3.2.3. REST

REST stands for State Transfer Member. REST is an architecture based on web standards and uses the HTTP protocol. It revolves around resources where each element is a resource, and a resource is accessed using standard HTTP methods through a specific interface. Roy Fielding introduced REST in 2000. A REST server offers access to resources in REST architecture, and REST user accesses and modifies resources. Here, URIs / global IDs classify each asset. REST uses a variety of representations to describe a resource such as text, JSON, XML.

3.2.4. AMQP

An open standard for transferring business messages between applications or organizations is the Advanced Message Queuing Protocol (AMQP). It connects systems, feeds business processes with the information they need, and transmits the instructions that achieve their goals reliably forward.

3.2.5. TCP

Transmission Control Protocol (TCP) is a connection-oriented communications protocol that provides the facility to exchange messages in a network between computer devices.

3.2.6. UDP

A Transport Layer protocol is the User Datagram Protocol (UDP). UDP is part of the Internet Protocol suite, known as UDP / IP. Like TCP, this protocol is unstable and unconnected. There is thus no need to create a link before transferring data.

3.2.7. DCCP

DCCP provides a way for congestion-control mechanisms to be accessed without having to implement them at the application layer. It allows flow-based semiconducting, as in the Transmission Control Protocol (TCP), but does not provide reliable delivery on-order. Sequenced transmission across multiple streams is not possible in DCCP, as in the Stream Control Transmission Protocol (SCTP). A DCCP link requires both the network acknowledgment and data traffic. Acknowledgments notify a sender that their packets have arrived and whether they have been labeled with an Explicit Notification of Congestion (ECN).

3.2.8. SCTP

The Stream Control Transmission Protocol (SCTP) is a computer networking communication protocol that operates at the transportation layer and serves a similar role to the popular TCP and UDP protocols. It is defined in RFC 4960 by IETF.SCTP incorporates some of the features of both UDP and TCP: it is message-oriented like UDP and ensures secure, in-sequence congestion-controlled transmission of messages like TCP. It differs from those protocols by providing multi-homing and redundant paths to increase resilience and reliability.

3.2.9. RSVP

The Resource Reservation Protocol (RSVP) is a transport layer [1] protocol designed to use the distributed infrastructure model to reserve resources across a network. RSVP works over an IPv4 or IPv6 and sets up resource reservations for multicast or unicast data flows, initiated by the recipient. It does not transmit data from applications but is similar to a control protocol, such as the Internet Control Message Protocol (ICMP) or the Internet Group Management Protocol (IGMP). RSVP is set out in RFC 2205.

3.2.10. QUIC

QUIC (pronounced' quick') is a general-purpose network layer protocol initially designed by Google's Jim Roskind, introduced and deployed in 2012, publicly announced in 2013 as an extended experiment and defined by the IETF. While still an Internet-Draft, more than half of all Chrome web browser connections to Google's servers use QUIC.[citation needed] Most other web browsers don't follow the protocol.

3.2.11. CLNS

Connectionless mode Network Service (CLNS) or simply Connectionless Network Service is an OSI Network Layer datagram service that does not require a circuit to be set up before data is transmitted, and routes messages to their destinations independently of any other messages. CLNS is not an Internet service but offers features similar to those offered by the Internet Protocol (IP) and User Datagram Protocol (UDP) in an OSI Network environment.

3.2.12. DDP

Distributed Data Protocol (or DDP) is a client-server protocol designed to query and update a server-side database and to synchronize such updates between clients. It uses a messaging pattern for publish-subscribe. The Meteor JavaScript application was developed for use.

3.2.13. ICMP

Connectionless-mode Network Service (CLNS) or simply Connectionless Network Service is an OSI Network Layer datagram service that does not allow a circuit to be set up before data is transmitted and routes messages to their destinations independently of any other messages. As such, it is a best-effort rather than a "reliable" delivery service. CLNS is not an Internet service but offers features similar to those offered by the Internet Protocol (IP) and User Datagram Protocol (UDP) in an OSI Network environment.

3.2.14. DSI

Digital Serial Interface (DSI) is a protocol for regulating lighting (initially electrical ballast) in buildings. It is based on Manchester-coded 8-bit protocol, 1200 baud data rate, 1 start bit, 8 data bits (dim value), 4 stop bits, and is the basis for the more advanced Digital Addressable Lighting Interface (DALI) protocol. The technology uses a single byte (0–255 or 0x00-0xFF) to communicate the lighting level. DSI was the first use of digital communication to control lighting and was the precursor to DALI.

3.2.15. ISDN

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. In the emergency mode of IoT devices, the ISDN facility can be useful.

3.3. Application

IoT applications are nowadays developed in many fields. The development of many open-source platforms like Azure IoT Suite, IBM Watson, Amazon Web Services (AWS), Oracle IoT, Kaa, Bevywise IoT platform used for industrial IoT, IoTIFY cloud-based platform used to build scalable IoT applications. Most of the opensource platform is enabled with AI and ML technology for intelligent processing and computing the information. The manufacture of smart devices that can read, process, and computing the things makes the IoT as one of the emerging fields. There are many application areas where IoT is used, as shown in Fig. 2. In these eight different application fields, IoT has already made an impact on enhancing and increasing the efficiency of the system.

3.3.1. Smart home

The IoT makes the traditional home system into an intelligent one. The refrigerator, smart television, security camera, gas sensors, temperature sensor, light system all can sense the home environment, communicate and connect to the internet through wired or wireless. Even the refrigerator can place an order to the registered retail shop and give notification to the user. Due to the development of smart things, the living standard becomes more comfortable. In paper [18], authors design a smart home system based on IoT technology. Using technology like IoT and Fog computing home converted into an intelligent home system where monitoring of the home can be done remotely as well as processing can be done instantly. The authentication of devices is essential to prevent unwanted access to the IoT network. The authors in Satapathy et al. [19] and Panda et al. [20] proposed different authentication schemes for a smart home network. Still, some security issues [21], are exist in IoT based smart home systems.

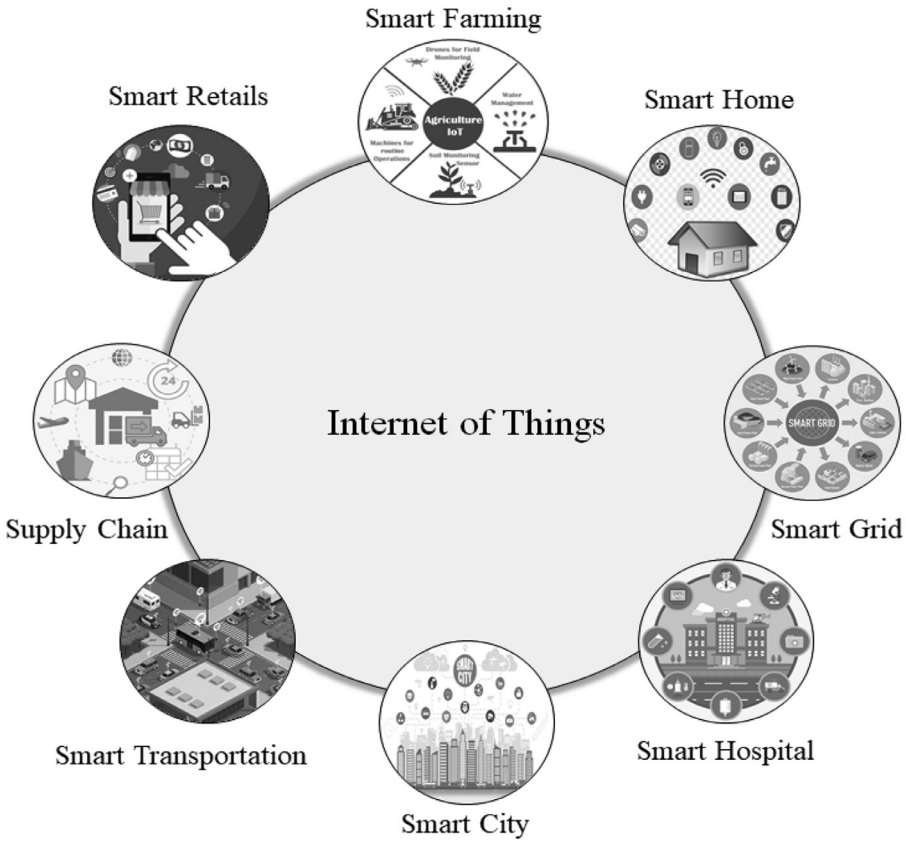

Fig. 2. Internet of things applications.

3.3.2. Smart hospital

Since the development of IoT patient monitoring in real-time is possible with the use of sensors and fog/edge computing, the paper [22], authors have proposed an IoT-cloud based framework for data collection in the healthcare system. Similarly, in Moosavi et al. [23], authors performed the authentication and authorization of the smart devices in the healthcare system. In the healthcare system, privacy is one of the main issues, so proper security and privacy protocol need to be developed to secure the system.

3.3.3. Smart city

The ever-growing city has lots of problems like traffic management, waste management, waste management, and environmental management. The city needs a solution to monitor and control the problem exist. In papers [24,25], authors explained the challenges that exist in implementing smart cities and done a survey in detail about how IoT can solve an existing problem. Using IoT and associated technology, a smart city can be developed to enhance the living standard of the city, maintaining the security and privacy issue of the citizen.

3.3.4. Smart transportation

In recent times traffic is one of the major problems in a city. The intelligent transportation system is the need of the hour. The IoT enables vehicles can collect information from the roadside unit and process to get the details about journey path, time, and traffic details. Some of the research work [26,27] addressed the smart transportation issue using IoT. In paper [28], the authors proposed the IoT-ITS system for the transportation system. The authors in Dey et al. [29] proposed a “Magtrack” to detect condition of the road surface using in-build mobile sensors and machine learning concepts.

3.3.5. Smart grid

The smart grid is one of the application areas of IoT, where a grid system can be made automation using IoT. The electric power generation and distribution among consumers can be monitor in real-time. The cybersecurity solution approach [30] is explained in detail. The architecture of the IoT-Cloud based system proposed by the authors in paper [31]. The efficient, economical and distribution can be improved using the IoT technology in the smart grid system.

Table 3
The different security attacks in IoT.

Different attacks cases and relevant research papers	
Attacks type	Paper
IoT Jamming attacks	[43]
Attacks DoS attacks	[44]
Intrusion detection System	[45]
Malicious node	[46]
Power analysis attack	[47,48]
Internal attacks	[49]
Access control	[50]
Wormhole attack	[51]
Side channel security	[52]
Distributed Dos	[53]
Man in the Middle attack	[54]
Active attacks	[55]
Routing attacks	[56]
Sybil attacks	[57,58]
Deceptive attack	[59]
Spoofing	[60]
Buffer overflow attack	[61]
Impersonation attack	[62]

3.3.6. Supply chain system

The IoT smart devices, once used in a supply chain management system, can fundamentally change the traditional way to monitor the transport system. By using the IoT technique, the material is easily located, their current condition, packing details, and it is easy to track how goods are a move through the supply chain. It increases to maintain the demand-supply of good, easy to monitor the material movement, real-time tracking, efficient storage, energy efficient [32], and distribution. The authors in Li et al. [33], explained how tracking and tracing could be done in real-time using the IoT system. Similarly, in paper [34,35] authors, discussed the IoT based architecture and risk management in the supply chain system. In paper [34], authors have proposed artificial intelligent integration with IoT for the retail shop supply chain system.

3.3.7. Smart retails

The retail sector also using IoT services along with artificial intelligent[36] to enhance productivity, improve store operation, and to take the decision in real-time to manage the inventory system.

3.3.8. Agriculture

Agriculture is one of the promising application areas in IoT. In a smart agriculture system by deploying the sensors to monitor the soil quality, water management, crop growing condition, etc. which improve the farming efficiency by reducing time and cost. In real-time, a user can monitor all details from the remote locations. In paper [37,38] authors proposed smart irrigation using machine learning and IoT to enhance farming. similarly, in paper [39,40], smart water management and weather conditions in the agriculture system are explained in detail. Likewise, in paper [41,42], smart agriculture system integration with IoT technologies is explained in detail. As some of the work already done in the field of agriculture, still some security issues exist like mobility, infrastructure, and secure processing of the collected data.

4. Security attacks in internet of things

In Table 3 some common Internet of Things attacks in the different layer is shown along with the current research work done on the corresponding attacks types.

Jamming attack is a subset of DoS attacks where the attacker tries to affect the communication channel in paper [43] authors also explained the details about the jamming attacks.

Dos attack is one of the common attack used in IoT applications. Most of the IoT devices are a low-end device which is vulnerable to the attacker. The attacker gets under the data traffic stream through device connection or infrastructure. Denial of service (DoS) attacks, consists of a huge volume of network packets, targeting the node present in the application causes service interrupt in real-time [44].

Intrusion detection system(IDS) is the process in which network traffic is control by the attacker. There are some types of IDS attacks, like misuse detection, anomaly detection, Host-based IDS, and Network-based IDS. The authors in paper [45] described the IDS attacks in IoT network.

Malicious node attack is possible in a distributed IoT network due to the heterogeneous nature of the smart devices. The identify the genius node or fake node in the network is a challenging one. In paper [46] authors proposed a perception and K-mean to build the trust among the node and detect the malicious node.

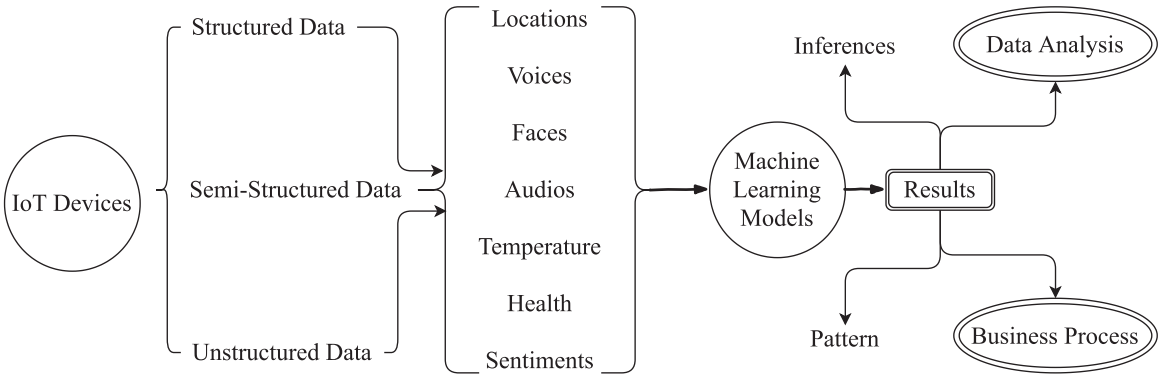

Fig. 3. The basic machine learning based model integration with IoT.

Power analysis attack and its corresponding solution approach are explained in papers [47,48]. This attack is mainly made to gain the computational power of the nodes so that the basic cryptographic algorithm is not possible to execute. In an IoT network, privacy also needs to be maintained to build trust among the node.

Internal attack in paper [49] and **Access control** attack in paper [50] are discussed in details. **Wormhole attack** is taken place at the 6LoWPAN layer, where the attacker makes a tunnel between two nodes that are connected [51].

The **Side channel security** attack in cloud-based IoT application along with the security challenges are explained in paper [52]. Similarly, **Distributed Dos** attack is the process where the server is unreachable so that smart nodes in the network can not get the services it desires to get [53].

Man-in-the-middle attack, where the attacker relays the message or change the message during the transmission in the insecure channel, explained in Li et al. [54] IoT-Fog network. **Active attacks** is explained in Zhang et al. [55] and its corresponding solution in the physical layer of the IoT network. There are different types of active attacks possible in IoT, where attackers make changes in the target node. The authors in Raoof et al. [56] explained the **Routing attacks** in routing protocol lossy network based on IoT application. The **Sybil attack** is one most common types of attack in IoT. The authors in Zhang et al. [57] and Mishra et al. [58] study the phases of Sybil attacks and their countermeasures in the internet of things. The **Deceptive attack** in La et al. [59] and **Spoofing attack** in Zhang et al. [60] authors have addressed the corresponding attacks and their security analysis in the internet of things applications. The **Buffer overflow attacks** is the process of writing the program in a block of memory where the memory space is insufficient. The A IoT network, when nodes execute the different programs in the deices for processing or computation purpose attackers, can capture that and perform memory overflow attack. The detecting buffer overflow attack and providing appropriate security design in explained in Xu et al. [61]. In a large IoT network where heterogeneous devices are connected and communicate with each other. The trust is one of the major issues in the network. The **Impersonation** [62] attacks where a fake node behaves like a genius node in the network and tries to gain the information from other nodes. This is one of the most challenging issues in IoT applications where smart devices are heterogeneous and low-end devices.

5. Security issue address using machine learning

The machine learning is a technique to perform computational intelligently. The model needs to design and test using different learning methods. Figs. 3 and 4 describe the basic principle of machine learning functionality and integration with IoT applications. As discussed in Section 3.3 application of the Internet of Things is many. Some of the application requirement is decision should be taken before the actual event occurs. For example, predicting the fire in a kitchen or any industrial area and alarm the sound to prevent the fire. This could be possible if machine learning technologies are used in IoT applications. Also, it needs to address the security issue present in the IoT system ta make the system tamper-proof. An efficient framework [63] is required to process and compute the huge data collection using a machine learning technique. In paper [64], authors review the security issue associated when applying machine learning in a smart grid application. In paper [65,66] authors address the intrusion detection in IoT application.

InTables 4–6 the details machine learning integration with IoT security issue related work are explained.

6. Security issue address using artificial intelligence

The innovation of smart devices having sensing and acting capability makes the IoT system usability in widely. As the numbers of devices are connected to the network are huge, which generate a large volume of data. To process and perform computation is a challenging task in an IoT environment. So Artificial intelligence comes as a rescue along with some other emerging technology to address the security issue in IoT. As shown in Fig. 5, IoT and AI can combine to improve the analysis of the system, improve operational efficiency, and improve the accuracy rate. The authors in Ghosh et al. [82] explained that

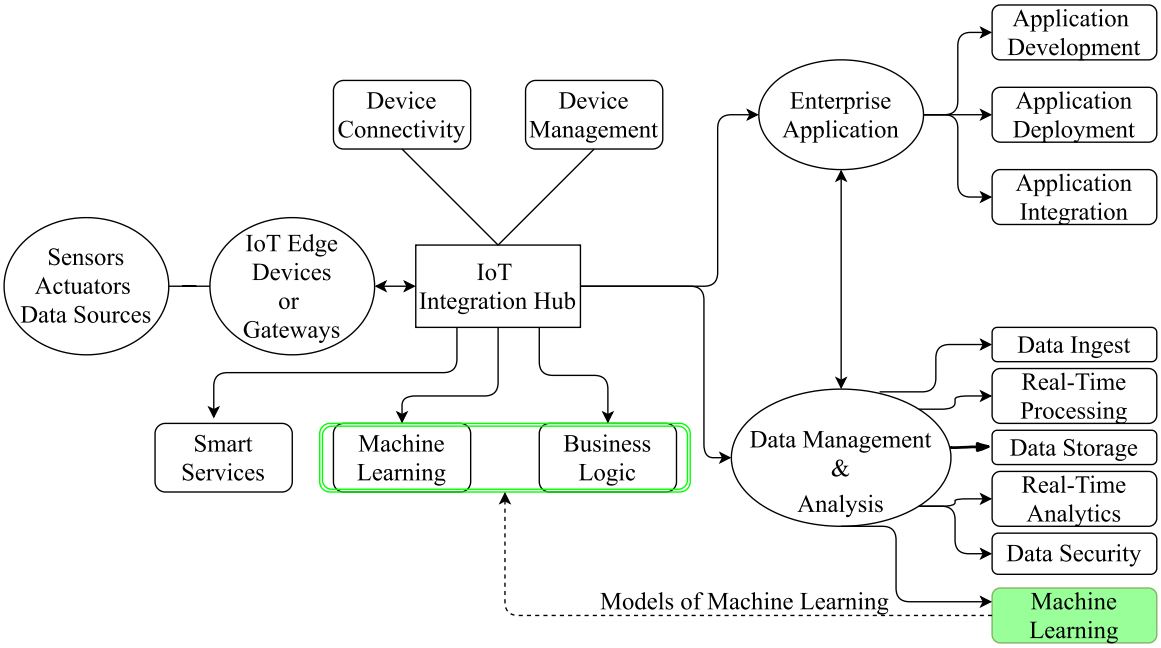

Fig. 4. In-depth model of machine learning in IoT application.

Table 4
Machine learning apply on different IoT security.

Reference	Years	Contribution
[63]	2018	The authors proposed a framework to monitor security in Mobile IoT using Big data processing and ML.
[64]	2019	Application of ML methods on big data generated in the smart grid to extract useful information and to detect and protect the data from cyber-security threats.
[65]	2019	Review on Network Intrusion Detection System (NIDS) in an IoT environment using ML algorithms.
[66]	2019	The authors proposed, a 3-layer Intrusion Detection System (IDS) using a supervised learning method of ML to distinguish between malicious or benign network activity and to detect network-based cyber-attacks such as DoS, MITM/Spoofing, Replay, and Reconnaissance and also to detect a multi-stage attack on IoT networks.
[67]	2017	Proposed a physical-layer authentication (PLA) scheme based on extreme learning machine (ELM)with a 2-dimensional measure space to ameliorate spoofing detection accuracy.
[68]	2017	Proposed an ML-based malicious app detection tool that uses naive Bayesian, J48 decision tree as a classifier model to detect malicious applications instantaneously in Android devices.
[69]	2018	Implemented an autonomous and adaptive detection mechanisms using ML and software-defined networking (SDN) for their IoT security framework to deal with the problem of erratic behavior and heterogeneity of IoT systems.
[70]	2018	Presented the different ML methods that can be applied to the data generated in the IoT system based environments like Smart cities to pull out the higher-level information if it.

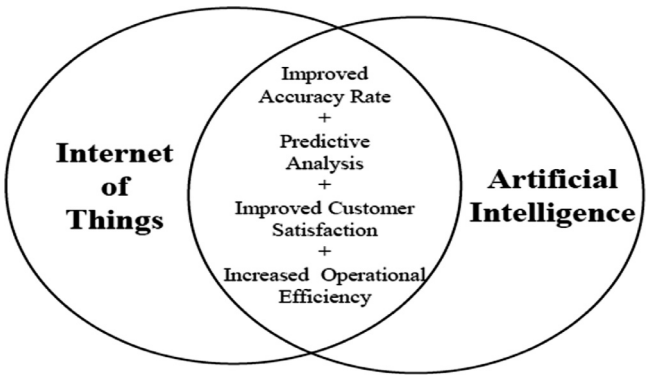

Fig. 5. The common functionality in IoT and artificial intelligence.

Table 5
Machine learning apply on different IoT security.

Reference	Years	Contribution
[71]	2018	The proposed a reliable, scalable, and robust Swarm Intelligence (SI)-based IoT system to overcome the problem of dynamic and heterogeneity behavior of IoT systems.
[72]	2018	The authors presented a Dense Random Neural Networks (RNN) based deep-learning technique by analyzing the traffic flow exchange in IoT gateways. To detect the network attacks online such as TCP SYN attack, which is a variety of denial-of-service (DoS) attacks.
[73]	2018	The authors proposed a robust real-time distributed fog-based attack detection framework for IoT, which relies on a fog computing paradigm and a newly proposed ELM-based Semi-supervised Fuzzy C-Means (ESFCM). Extreme Learning Machine (ELM) algorithm provides good generalization performance at a faster detection rate, and semi-supervised Fuzzy C-Means method handles the labeled data issue in IoT.
[74]	2018	The proposed a new darknet analysis method to find the traffic patterns of a specific scanning attack i.e., TCP SYN packets due to the majority of darknet packets using the association rule learning.
[75]	2018	The authors proposed a novel algorithm for quantifiable intelligent trust assessment model to overcome the issue of potential discrimination. The data analytics is done over delicate information such as locations, interests, and activities, using the SVM model of ML. This process generates exact and inherent trust values for probable actors. It helps in determining whether an incoming interaction is trustworthy or not, based on several trusts features corresponding to an IoT environment.

Table 6
Machine learning apply on different IoT security.

Reference	Years	Contribution
[76]	2018	The authors proposed a system for real-time monitoring of the health parameters to detect bombs nearby and to predict the warzone environment. Using various sensors to collect the data, network infrastructure like LoRaWAN and ZigBee to transmit those data to the cloud and K-Means Clustering machine learning algorithm to analyze the data.
[77]	2018	Proposed a Deep Learning (DL) based secure framework for Intrusion detection system using Restricted Boltzmann Machines (RBM) for SDN based IoT.
[78]	2019	The authors proposed a robust prediction model for real-life mobile phone data of individual users using a rule-based machine learning classification technique, i.e., decision tree on the noise-free quality dataset. Naive Bayes classifier and Laplace estimator are used to improving the prediction accuracy of the model by removing the noisy instances in the data.
[79]	2019	Proposed an ML-based anomaly detection system which can detect cyber-attacks like backdoor, command injection, and Structured Query Language (SQL) injection attacks in the Industrial Internet of Things (IIoT) devices.
[80]	2019	Authors compared the performances of various ML models such as Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), and Artificial Neural Network (ANN) for predicting attacks like DoS, Data Type Probing, Malicious Control, Malicious Operation, Scan, Spying and Wrong Setup, and anomalies on the IoT systems accurately.
[81]	2019	Presented the preliminary work of neural network (NN)-based specific emitter identification (SEI) on IoT devices using raw in-phase and quadrature (IQ) streams, with protocols to secure IoT networks by providing an extra layer of security and trust.

AI could help IoT huge volume, unstructured data, heterogeneous data to compute in real-time, which makes the system realistic. The authors propose the large margin cosine estimation (LMCE) technique in this paper [83] to detect the adversary in IoT enable environments. The malware detection work in the IoT system using

AI is addressed in paper [84]. Similarly, in paper [85], the authors proposed a model using Blockchain and AI in IoT architecture to make the system tamper-proof. In Fig. 6, integration of IoT and AI with some basic functionality are shown. The combination of AI and IoT some work is already done by the researcher addressing that AI can be a driving force to make the IoT system more improve in decision making and doing computation.The authors apply a master attack in IoT enables smart city application based on AI [86]. Similarly, in Zou et al. [87], the authors explained Edge and fog computing for IoT applications.

7. Security issue address using blockchain technology

Blockchain technology is a decentralized/distributed network where each is connected to others in some way. The message is broadcast in the Blockchain network. As shown in Fig. 7 distributed architecture based on blockchain techniques in IoT application. A block consists of lots of valid transaction and its associated attributes. The smart contract [88] are self executable program used to implement the business logic in the network. The Blockchain network uses different consensus algorithm [89] to meet the consensus among the nodes. The details Blockchain architecture and application areas are explained in paper [90] by the authors. The authors in paper [91,92] described the mechanism and related work on IoT security along with Blockchain as a solution approach.The authors have proposed a secure framework for the internet of

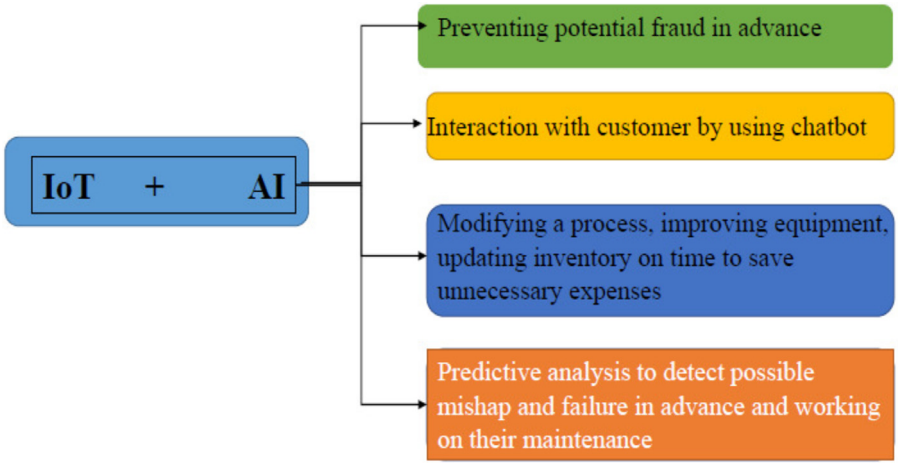

Fig. 6. Integration of IoT and AI and their basic properties.

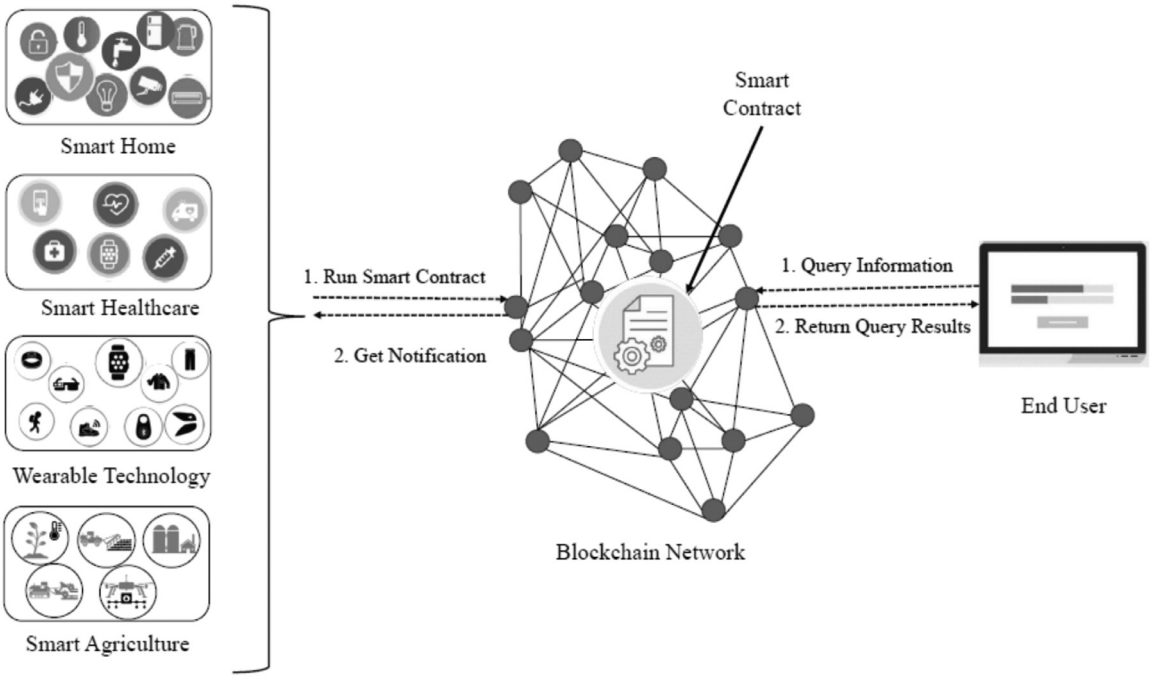

Fig. 7. Blockchain based different IoT applications.

things applications based on a distributed Blockchain system in Satapathy et al. [93]. The use of Blockchain technology in IoT is briefly given in paper [94] by the authors. The many IoT security challenges and corresponding Blockchain solutions, along with the implementation challenges, are review by the authors in paper [95]. InTables 7–10 details review regarding blockchain and IoT security issue are described.

8. Analysis of the survey and research challenges

The Internet of Things (IoT) in recent time attract lots of attention to the research community as well as an industry sector. The IoT devices are manufactures in large number which already cross the total world population. These smart devices are connected to different applications for capturing information from the environment. The IoT devices are resource constraint devices, so devices are vulnerable to the attacker. Security and privacy issues are important for IoT applications.

So this survey is carried out in-depth to identified security and privacy issues that exist in the IoT system up to March 2020. The solution approaches of these security and privacy issues solved by some emerging technologies are also discussed.

Table 7
Blockchain technology work on IoT security.

Reference	Years	Contribution
[96]	2017	The authors in this paper proposed a distributed Blockchain-based model. The proposed system one miner is used to control the communication within the smart home as well as an external source. The framework is secure against fundamental security goals.
[97]	2018	The authors evaluated the feasibility of using blockchain nodes on IoT devices.
[98]	2018	The authors proposed a distributed ledger-based blockchain (DL-BC) technology to address security and privacy issues in IoT, such as spoofing, false authentication.
[99]	2018	Proposed distributed intelligence that performs instance decision making and reduces unnecessary data transfer to the cloud, addressing various security challenges in the IoT paradigm.
[91]	2018	The authors proposed a blockchain-based compromised firmware detection and self-healing approach that can be deployed in an IoT environment for secure datasets sharing.
[100]	2018	The authors proposed a blockchain-based secure scheme to resolve the issue of time announcements in IoT.
[101]	2018	Proposed the Named Data Networking (NDN) of Things architecture and the blockchain solution to deal with the security attacks in this.
[102] [103]	2018	The authors proposed a blockchain-based high-level security management scheme for various IoT devices.
[104]	2020	The authors explored the major benefits and design challenges for integration of blockchain technologies for IoT applications.

Table 8
Blockchain technology work on IoT security.

Reference	Years	Contribution
[105]	2019	The authors proposed device classification methods by applying machine learning algorithms on the data stored in the blockchain network which in turn helps to enhance the security of IoT environment by detecting unauthorised devices.
[106]	2019	The authors proposed a trust management framework for providing secure and trustworthy access control and also detecting and removing malicious and compromised nodes in a decentralized IoT system.
[107]	2019	The authors proposed a Secure Private Blockchain-based framework (SPB) using which negotiations can be done among the energy prosumers over the energy price and trade energy in a distributed manner for a smart grid IoT application.
[108]	2018	The authors proposed a permissioned blockchain based framework to find provenance of supply chain products.
[109]	2019	The authors proposed a three-layered trust management framework - TrustChain, based on consortium blockchain for tracking the interactions among supply chain participants and based on these interactions it dynamically assign trust and reputation scores.
[110]	2018	The authors proposed a noble blockchain-based framework for providing a private and secure communication model for smart vehicles so that they can trust the data they receive are generated by a trusted node.

Table 9
Blockchain technology work on IoT security.

Reference	Years	Contribution
[111]	2018	Authors proposed a Permissioned blockchain architecture to handle the most expensive computation in pairing-based cryptographic protocols i.e., secure outsourcing of bilinear pairings (SOBP).
[112]	2019	The authors proposed a credit-based proof-of-work (PoW) mechanism in blockchain for IoT devices, which can guarantee system security and transaction efficiency.
[113]	2019	The authors surveyed some of the promising applications that are being implemented using blockchain and also outlined solutions to overcome numerous challenges.
[114]	2019	Proposed an anti-counterfeiting approach for IoT devices exploiting characteristics of memory chips to derive a cryptographic secret combined with a blockchain for trusted and reliable verification of device identities.
[115]	2019	Proposed a blockchain-based searchable encryption for electronic health records (EHRs) sharing scheme by using smart contracts to perform a reliable and confidential search.
[116]	2019	The authors proposed a blockchain-based privacy-preserving software update protocol to perform secure and reliable updates with an incentive mechanism without hampering the privacy of involved users.
[117]	2019	The authors proposed a blockchain-based energy trading scheme for secure energy trading in the Intelligent Transportation System (ITS) by utilizing energy coins.

Table 10
Related work blockchain and IoT security.

Focus area	Reference	Contribution
Privacy Perservation	[118,119] [120,121] [122]	In an IoT application, privacy is a significant concern for the end-users. The blockchain-based encryption techniques are proposed by different authors to solve the privacy preservation issue.
Authentication	[123,124] [125,126] [127] [128]	The device authentication is one of the important factors for secure communication in the IoT network. The different methods, like mutual authentication, PSO-AES, and distributed authentication, are used for IoT device authentication using blockchain techniques.
Access Control	[129,130]	The management of devices accessibility in the IoT system is essential as critical information is sense using different smart things. The attribute-based access control and blockchain-based permission delegation access control techniques are proposed by the researcher to manage the accessibility of the vital information securely.
Scalability	[131,132]	The work has already been done to address the scalable issue in IoT network using blockchain.
Information Share	[133,134] [135,136] [137,138] [139,140]	Information exchange in the IoT network is very important in real-time monitoring of the environment. The blockchain-based secure information share mechanism is integrated with the IoT system.
Trust Management	[141,142] [143,144] [145]	In many IoT applications, multiple nodes are required in the decision-making process for better and efficient decisions. Some work has already been done regarding trust management.

Initially, different research databases like ScienceDirect, IEEE Xplore, Inderscience, ACM Digital Library, DBLP, google scholar, Springer are used to search 500 articles. The word used to search the articles are “Internet of Things”, “IoT”, “security”, “privacy”, “machine learning”, “blockchain”, “artificial intelligence”.

The number of articles are reduces to number 250 after reading the abstract and title. Again duplicate or redundant articles are remove. In the final stage 145 numbers of article are consider after reading the full text.

8.1. Summary of the review

In this survey, authors have work on the Security issues that exist in the IoT system. The purpose of this survey is to identify the solution need to address the security issue. Security is one of the most challenging tasks and need to address in IoT applications to be successful.

8.1.1. Critical analysis of machine learning

The machine learning technique is consists of supervised and unsupervised. The IoT application generates a huge volume of information. Before data are computation is done, data are needed through the verification process to avoid any malicious data or redundancy data. This survey, authors identified 29 numbers of articles that address the security issue of IoT applications. Machine learning addresses the following security issues:

- Intrusion detection system.
- Malware detection.
- Anomaly detection.
- Unauthorized IoT devices identification.
- Distributed denial-of-service.
- Jamming attack, Spoofing attack.
- Authentication, Eavesdropping.
- False data injection, Impersonation.

8.1.2. Critical analysis of blockchain technology

In this survey, Section 7 the details blockchain technology and corresponding research works are mention in Tables 7–10. The 58 numbers of an article are listed. The authors found blockchain is the most promising technology recently researchers are working on to solve the security issue of IoT applications. The following security issues are address by the blockchain technology:

- Identity verification.
- Firmware detection and self healing.
- Privacy preservation and Address space.
- Data integrity and Secure communication.
- Authentication and authorization.
- Access control and Information Sharing.
- Secure storage and computation.
- Trust Management.

8.1.3. Critical analysis of artificial intelligence

As per the survey done in this paper, authors found 6 numbers of papers address the security issue of IoT. In an application like smart transportation and smart weather forecasting, the prediction is essential. The AI provides some of the security issues like malware detection, privacy preservation, and authorization.

8.2. Research challenges

Some of the research challenges are underlined below:

1. As the huge number of IoT devices are connected, system throughput and consensus algorithm problems still exist.
2. Scalability issue of IoT needs to be consider when addressing security protocols.
3. Secure computation and processing are other areas that need to address.
4. The security protocol should be design in terms of light-weight to meet the resource constraint devices.

9. Conclusion

In this paper, the authors firstly study in-depth the various security challenges exist in IoT application. Secondly, the authors have surveyed to address existing security challenges. From the survey, it was found that some research has already been done in various technology like Machine learning, Artificial intelligence, and Blockchain technology, which are capable of addressing the existing security issue. So in detail study has been made in three technology machine learning, artificial intelligence and Blockchain technology, and their integration with IoT. Security is an important issue that needs to address. In this survey, the authors outline the emerging technology like ML, AI, and Blockchain integrate with IoT to make the system more secure. Some of the research challenges mention in the end.

Declaration of Competing Interest

The authors do not have conflict of interest with any one.

References

[1] A. Čolaković, M. Hadžialić, Internet of things (IoT): a review of enabling technologies, challenges, and open research issues, Comput. Netw. 144 (2018) 17–39.
[2] D. Mocrii, Y. Chen, P. Musilek, IoT-based smart homes: a review of system architecture, software, communications, privacy and security, Internet Things 1 (2018) 81–98.
[3] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges, Wirel. Netw. 20 (8) (2014) 2481–2501.
[4] A.H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, Q.Z. Sheng, Iot middleware: a survey on issues and enabling technologies, IEEE Internet Things J. 4 (1) (2016) 1–20.
[5] A. Mosenia, N.K. Jha, A comprehensive study of security of internet-of-things, IEEE Trans. Emerg. Top. Comput. 5 (4) (2016) 586–602.
[6] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: architecture, enabling technologies, security and privacy, and applications, IEEE Internet Things J. 4 (5) (2017) 1125–1142.
[7] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in internet-of-things, IEEE Internet Things J. 4 (5) (2017) 1250–1258.
[8] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28.
[9] P.I.R. Grammatikis, P.G. Sarigiannidis, I.D. Moscholios, Securing the internet of things: challenges, threats and solutions, Internet Things 5 (2018) 41–70.
[10] A.K. Das, S. Zeadally, D. He, Taxonomy and analysis of security protocols for internet of things, Future Gener. Comput. Syst. 89 (2018) 110–125.
[11] B. Di Martino, M. Rak, M. Ficco, A. Esposito, S. Maisto, S. Nacchia, Internet of things reference architectures, security and interoperability: a survey, Internet Things 1 (2018) 99–112.
[12] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on IoT security: application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743.
[13] A. Al-Hasnawi, S.M. Carr, A. Gupta, Fog-based local and remote policy enforcement for preserving data privacy in the internet of things, Internet Things 7 (2019) 100069.
[14] K.-C. Chen, S.-Y. Lien, Machine-to-machine communications: technologies and challenges, Ad Hoc Netw. 18 (2014) 3–23.
[15] V. Casola, A. De Benedictis, A. Riccio, D. Rivera, W. Mallouli, E.M. de Oca, A security monitoring system for internet of things, Internet Things 7 (2019) 100080.
[16] S. Siboni, V. Sachidananda, Y. Meidan, M. Bohadana, Y. Mathov, S. Bhairav, A. Shabtai, Y. Elovici, Security testbed for internet-of-things devices, IEEE Trans. Reliab. 68 (1) (2018) 23–44.
[17] R. Nawaratne, D. Alahakoon, D. De Silva, P. Chhetri, N. Chilamkurti, Self-evolving intelligent algorithms for facilitating data interoperability in IoT environments, Future Gener. Comput. Syst. 86 (2018) 421–432.
[18] K. Bing, L. Fu, Y. Zhuo, L. Yanlei, Design of an internet of things-based smart home system, in: 2011 2nd International Conference on Intelligent Control and Information Processing, 2, IEEE, 2011, pp. 921–924.
[19] U. Satapathy, B.K. Mohanta, D. Jena, S. Sobhanayak, An ECC based lightweight authentication protocol for mobile phone in smart home, in: 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), IEEE, 2018, pp. 303–308.
[20] S.S. Panda, D. Jena, B.K. Mohanta, A remote device authentication scheme for secure communication in cloud based IoT, in: 2019 2nd International Conference on Innovations in Electronics, Signal Processing and Communication (IESC), IEEE, 2019, pp. 165–171.
[21] R.K. Kodali, V. Jain, S. Bose, L. Boppana, IoT based smart security and home automation system, in: 2016 International Conference on Computing, Communication and Automation (ICCCA), IEEE, 2016, pp. 1286–1289.
[22] K. Jaiswal, S. Sobhanayak, B.K. Mohanta, D. Jena, IoT-cloud based framework for patient's data collection in smart healthcare system using raspberry-pi, in: 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), IEEE, 2017, pp. 1–4.
[23] S.R. Moosavi, T.N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, H. Tenhunen, Sea: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways, Procedia Comput. Sci. 52 (2015) 452–459.
[24] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, S. Guizani, Internet-of-things-based smart cities: recent advances and challenges, IEEE Commun. Mag. 55 (9) (2017) 16–24.

[25] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-Khah, P. Siano, IoT-based smart cities: a survey, in: 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), IEEE, 2016, pp. 1–6.
[26] A.J. Neto, Z. Zhao, J.J. Rodrigues, H.B. Camboim, T. Braun, Fog-based crime-assistance in smart IoT transportation system, IEEE Access 6 (2018) 11101–11111.
[27] L.F. Herrera-Quintero, J.C. Vega-Alfonso, K.B.A. Banse, E.C. Zambrano, Smart ITS sensor for the transportation planning based on IoT approaches using serverless and microservices architecture, IEEE Intell. Transp. Syst. Mag. 10 (2) (2018) 17–27.
[28] S. Muthuramalingam, A. Bharathi, N. Gayathri, R. Sathiyaraj, B. Balamurugan, et al., IoT based intelligent transportation system IoT-ITS for global perspective: a case study, in: Internet of Things and Big Data Analytics for Smart Generation, Springer, 2019, pp. 279–300.
[29] M.R. Dey, U. Satapathy, P. Bhanse, B.K. Mohanta, D. Jena, Magtrack: detecting road surface condition using smartphone sensors and machine learning, in: TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 2485–2489.
[30] X.C. Yin, Z.G. Liu, L. Nkenyereye, B. Ndibanje, Toward an applied cyber security solution in IoT-based smart grids: an intrusion detection system approach, Sensors 19 (22) (2019) 4952.
[31] A. Meloni, P.A. Pegoraro, L. Atzori, A. Benigni, S. Sulis, Cloud-based IoT solution for state estimation in smart grids: exploiting virtualization and edge-intelligence technologies, Comput. Netw. 130 (2018) 156–165.
[32] A.O. Akmandor, Y. Hongxu, N.K. Jha, Smart, secure, yet energy-efficient, internet-of-things sensors, IEEE Trans. Multi-Scale Comput. Syst. 4 (4) (2018) 914–930.
[33] Z. Li, G. Liu, L. Liu, X. Lai, G. Xu, IoT-based tracking and tracing platform for prepackaged food supply chain, Ind. Manag. Data Syst. 117 (9) (2017) 1906–1916.
[34] Y.P. Tsang, K.L. Choy, C.-H. Wu, G.T. Ho, C.H. Lam, P. Koo, An internet of things (IoT)-based risk monitoring system for managing cold supply chain risks, Ind. Manag. Data Syst. 118 (7) (2018) 1432–1462.
[35] C. Verdouw, R.M. Robbemond, T. Verwaart, J. Wolfert, A.J. Beulens, A reference architecture for IoT-based logistic information systems in agri-food supply chains, Enterp. Inf. Syst. 12 (7) (2018) 755–779.
[36] L. Liu, B. Zhou, Z. Zou, S.-C. Yeh, L. Zheng, A smart unstaffed retail shop based on artificial intelligence and IoT, in: 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, 2018, pp. 1–4.
[37] M. Mehra, S. Saxena, S. Sankaranarayanan, R.J. Tom, M. Veeramanikandan, IoT based hydroponics system using deep neural networks, Comput. Electron. Agric. 155 (2018) 473–486.
[38] A. Goap, D. Sharma, A. Shukla, C.R. Krishna, An IoT based smart irrigation management system using machine learning and open source technologies, Comput. Electron. Agric. 155 (2018) 41–49.
[39] C. Kamienski, J.-P. Soininen, M. Taumberger, R. Dantas, A. Toscano, T. Salmon Cinotti, R. Filev Maia, A. Torre Neto, Smart water management platform: IoT-based precision irrigation for agriculture, Sensors 19 (2) (2019) 276.
[40] B. Keswani, A.G. Mohapatra, A. Mohanty, A. Khanna, J.J. Rodrigues, D. Gupta, V.H.C. de Albuquerque, Adapting weather conditions based IoT enabled smart irrigation technique in precision agriculture mechanisms, Neural Comput. Appl. 31 (1) (2019) 277–292.
[41] N.K. Nawandar, V.R. Satpute, IoT based low cost and intelligent module for smart irrigation system, Comput. Electron. Agric. 162 (2019) 979–990.
[42] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, E.-H.M. Aggoune, Internet-of-things (IoT)-based smart agriculture: toward making the fields talk, IEEE Access 7 (2019) 129551–129583.
[43] M. López, A. Peinado, A. Ortiz, An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks, Comput. Netw. 165 (2019) 106945.
[44] Z.A. Baig, S. Sanguanpong, S.N. Firdous, T.G. Nguyen, C. So-In, et al., Averaged dependence estimators for dos attack detection in IoT networks, Future Gener. Comput. Syst. 102 (2020) 198–209.
[45] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, A. Razaque, Deep recurrent neural network for IoT intrusion detection system, Simul. Modell. Pract. Theory 101 (2019) 102031.
[46] L. Liu, Z. Ma, W. Meng, Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks, Future Gener. Comput. Syst. 101 (2019) 865–879.
[47] J. Moon, I.Y. Jung, J.H. Park, IoT application protection against power analysis attack, Comput. Electr. Eng. 67 (2018) 566–578.
[48] Y. Niu, J. Zhang, A. Wang, C. Chen, An efficient collision power attack on AES encryption in edge computing, IEEE Access 7 (2019) 18734–18748.
[49] N. Tariq, M. Asim, Z. Maamar, M.Z. Farooqi, N. Faci, T. Baker, A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT, J Parallel Distrib. Comput. 134 (2019) 198–206.
[50] H. Yan, Y. Wang, C. Jia, J. Li, Y. Xiang, W. Pedrycz, IoT-FBAC: function-based access control scheme using identity-based encryption in IoT, Future Gener. Comput. Syst. 95 (2019) 344–353.
[51] S. Deshmukh-Bhosale, S.S. Sonavane, A real-time intrusion detection system for wormhole attack in the RPL based internet of things, Procedia Manuf. 32 (2019) 840–847.
[52] H. Yi, Z. Nie, Side-channel security analysis of UOV signature for cloud-based internet of things, Future Gener. Comput. Syst. 86 (2018) 704–708.
[53] 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.
[54] C. Li, Z. Qin, E. Novak, Q. Li, Securing SDN infrastructure of IoT–fog networks from MitM attacks, IEEE Internet Things J. 4 (5) (2017) 1156–1164.
[55] N. Zhang, R. Wu, S. Yuan, C. Yuan, D. Chen, RAV: relay aided vectorized secure transmission in physical layer security for internet of things under active attacks, IEEE Internet Things J. 6 (5) (2019) 8496–8506.
[56] A. Raoof, A. Matrawy, C.-H. Lung, Routing attacks and mitigation methods for RPL-based internet of things, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1582–1606.
[57] K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the internet of things, IEEE Internet Things J. 1 (5) (2014) 372–383.
[58] A.K. Mishra, A.K. Tripathy, D. Puthal, L.T. Yang, Analytical model for Sybil attack phases in internet of things, IEEE Internet Things J. 6 (1) (2018) 379–387.
[59] Q.D. La, T.Q. Quek, J. Lee, S. Jin, H. Zhu, Deceptive attack and defense game in honeypot-enabled networks for the internet of things, IEEE Internet Things J. 3 (6) (2016) 1025–1035.
[60] P. Zhang, S.G. Nagarajan, I. Nevat, Secure location of things (SLOT): mitigating localization spoofing attacks in the internet of things, IEEE Internet Things J. 4 (6) (2017) 2199–2206.
[61] B. Xu, W. Wang, Q. Hao, Z. Zhang, P. Du, T. Xia, H. Li, X. Wang, A security design for the detecting of buffer overflow attacks in IoT device, IEEE Access 6 (2018) 72862–72869.
[62] S. Tu, M. Waqas, S.U. Rehman, M. Aamir, O.U. Rehman, Z. Jianbiao, C.-C. Chang, Security in fog computing: a novel technique to tackle an impersonation attack, IEEE Access 6 (2018) 74993–75001.
[63] I. Kotenko, I. Saenko, A. Branitskiy, Framework for mobile internet of things security monitoring based on big data processing and machine learning, IEEE Access 6 (2018) 72714–72723.
[64] E. Hossain, I. Khan, F. Un-Noor, S.S. Sikander, M.S.H. Sunny, Application of big data and machine learning in smart grid, and associated security concerns: a review, IEEE Access 7 (2019) 13960–13988.
[65] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, P. Faruki, Network intrusion detection for IoT security based on learning techniques, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2671–2701.
[66] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, P. Burnap, A supervised intrusion detection system for smart home IoT devices, IEEE Internet Things J. 6 (5) (2019) 9042–9053.
[67] N. Wang, T. Jiang, S. Lv, L. Xiao, Physical-layer authentication based on extreme learning machine, IEEE Commun. Lett. 21 (7) (2017) 1557–1560.

[68] L. Wei, W. Luo, J. Weng, Y. Zhong, X. Zhang, Z. Yan, Machine learning-based malicious application detection of android, IEEE Access 5 (2017) 25591–25601.
[69] F. Restuccia, S. D'Oro, T. Melodia, Securing the internet of things in the age of machine learning and software-defined networking, IEEE Internet Things J. 5 (6) (2018) 4829–4842.
[70] M.S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, A.P. Sheth, Machine learning for internet of things data analysis: a survey, Digit. Commun. Netw. 4 (3) (2018) 161–175.
[71] O. Zedadra, A. Guerrieri, N. Jouandeau, G. Spezzano, H. Seridi, G. Fortino, Swarm intelligence-based algorithms within IoT-based systems: a review, J. Parallel Distrib. Comput. 122 (2018) 173–187.
[72] O. Brun, Y. Yin, E. Gelenbe, Deep learning with dense random neural network for detecting attacks against IoT-connected home environments, Procedia Comput. Sci. 134 (2018) 458–463.
[73] S. Rathore, J.H. Park, Semi-supervised learning based distributed attack detection framework for IoT, Appl. Soft Comput. 72 (2018) 79–89.
[74] N. Hashimoto, S. Ozawa, T. Ban, J. Nakazato, J. Shimamura, A darknet traffic analysis for IoT malwares using association rule learning, Procedia Comput. Sci. 144 (2018) 118–123.
[75] U. Jayasinghe, G.M. Lee, T.-W. Um, Q. Shi, Machine learning based trust computational model for IoT services, IEEE Trans. Sustain. Comput. 4 (1) (2018) 39–52.
[76] A. Gondalia, D. Dixit, S. Parashar, V. Raghava, A. Sengupta, V.R. Sarobin, IoT-based healthcare monitoring system for war soldiers using machine learning, Procedia Comput. Sci. 133 (2018) 1005–1013.
[77] A. Dawoud, S. Shahristani, C. Raun, Deep learning and software-defined networks: towards secure IoT architecture, Internet Things 3 (2018) 82–89.
[78] I.H. Sarker, A machine learning based robust prediction model for real-life mobile phone data, Internet Things 5 (2019) 180–193.
[79] M. Zolanvari, M.A. Teixeira, L. Gupta, K.M. Khan, R. Jain, Machine learning based network vulnerability analysis of industrial internet of things, IEEE Internet Things J. 6 (4) (2019) 6822–6834.
[80] M. Hasan, M.M. Islam, M.I.I. Zarif, M. Hashem, Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches, Internet Things 7 (2019) 100059.
[81] J.M. McGinthy, L.J. Wong, A.J. Michaels, Groundwork for neural network-based specific emitter identification authentication for IoT, IEEE Internet Things J. 6 (4) (2019) 6429–6440.
[82] A. Ghosh, D. Chakraborty, A. Law, Artificial intelligence in internet of things, CAAI Trans. Intell. Technol. 3 (4) (2018) 208–218.
[83] S. Wang, Z. Qiao, Robust pervasive detection for adversarial samples of artificial intelligence in IoT environments, IEEE Access 7 (2019) 88693–88704.
[84] M. Zolotukhin, T. Hämäläinen, On artificial intelligent malware tolerant networking for IoT, in: 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), IEEE, 2018, pp. 1–6.
[85] S.K. Singh, S. Rathore, J.H. Park, BlockIoTIntelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence, Future Gener. Comput. Syst. (2019), doi:10.1016/j.future.2019.09.002.
[86] G. Falco, A. Viswanathan, C. Caldera, H. Shrobe, A master attack methodology for an ai-based automated attack planner for smart cities, IEEE Access 6 (2018) 48360–48373.
[87] Z. Zou, Y. Jin, P. Nevalainen, Y. Huan, J. Heikkonen, T. Westerlund, Edge and fog computing enabled ai for IoT-an overview, in: 2019 IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS), IEEE, 2019, pp. 51–56.
[88] B.K. Mohanta, S.S. Panda, D. Jena, An overview of smart contract and use cases in blockchain technology, in: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2018, pp. 1–4.
[89] S.S. Panda, B.K. Mohanta, U. Satapathy, D. Jena, D. Gountia, T.K. Patra, Study of blockchain based decentralized consensus algorithms, in: TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 908–913.
[90] B.K. Mohanta, D. Jena, S.S. Panda, S. Sobhanayak, Blockchain technology: a survey on applications and security privacy challenges, Internet Things (2019) 100107.
[91] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future for internet of things security: a position paper, Digital Commun. Netw. 4 (3) (2018) 149–160.
[92] D. Minoli, B. Occhiogrosso, Blockchain mechanisms for IoT security, Internet Things 1 (2018) 1–13.
[93] U. Satapathy, B.K. Mohanta, S.S. Panda, S. Sobhanayak, D. Jena, A secure framework for communication in internet of things application using hyperledger based blockchain, in: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2019, pp. 1–7.
[94] 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.
[95] M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.
[96] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: the case study of a smart home, in: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, 2017, pp. 618–623.
[97] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190.
[98] N.M. Kumar, P.K. Mallick, Blockchain technology for security issues and challenges in IoT, Procedia Comput. Sci. 132 (2018) 1815–1823.
[99] K.M. Sadique, R. Rahmani, P. Johannesson, Towards security on internet of things: applications and challenges in technology, Procedia Comput. Sci. 141 (2018) 199–206.
[100] K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, Y. Yang, Blockchain-based secure time protection scheme in IoT, IEEE Internet Things J. 6 (3) (2018) 4671–4679.
[101] K. Zhu, Z. Chen, W. Yan, L. Zhang, Security attacks in named data networking of things and a blockchain solution, IEEE Internet Things J. 6 (3) (2018) 4733–4741.
[102] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, M. Pustišek, Towards decentralized IoT security enhancement: blockchain approach, Comput. Electr. Eng. 72 (2018) 266–273.
[103] B.K. Mohanta, U. Satapathy, S.S. Panda, D. Jena, A novel approach to solve security and privacy issues for IoT applications using blockchain, in: 2019 International Conference on Information Technology (ICIT), IEEE, 2019, pp. 394–399.
[104] V. Dedeoglu, R. Jurdak, A. Dorri, R. Lunardi, R. Michelin, A. Zorzo, S. Kanhere, Blockchain technologies for IoT, in: Advanced Applications of Blockchain Technology, Springer, 2020, pp. 55–89.
[105] A. Dorri, C. Roulin, R. Jurdak, S.S. Kanhere, On the activity privacy of blockchain for IoT, in: 2019 IEEE 44th Conference on Local Computer Networks (LCN), IEEE, 2019, pp. 258–261.
[106] G.D. Putra, V. Dedeoglu, S.S. Kanhere, R. Jurdak, Trust management in decentralized IoT access control system, arXiv preprint arXiv:1912.10247(2019).
[107] A. Dorri, F. Luo, S.S. Kanhere, R. Jurdak, Z.Y. Dong, Spb: a secure private blockchain-based solution for distributed energy trading, IEEE Commun. Mag. 57 (7) (2019) 120–126.
[108] S. Malik, S.S. Kanhere, R. Jurdak, Productchain: scalable blockchain framework to support provenance in supply chains, in: 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), IEEE, 2018, pp. 1–10.
[109] S. Malik, V. Dedeoglu, S.S. Kanhere, R. Jurdak, Trustchain: trust management in blockchain and IoT supported supply chains, in: 2019 IEEE International Conference on Blockchain (Blockchain), IEEE, 2019, pp. 184–193.
[110] R.A. Michelin, A. Dorri, M. Steger, R.C. Lunardi, S.S. Kanhere, R. Jurdak, A.F. Zorzo, Speedychain: a framework for decoupling data from blockchain for smart cities, in: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, 2018, pp. 145–154.
[111] C. Lin, D. He, X. Huang, X. Xie, K.-K.R. Choo, Blockchain-based system for secure outsourcing of bilinear pairings, Inf Sci 527 (2018) 590–601.

[112] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, P. Zeng, Towards secure industrial IoT: blockchain system with credit-based consensus mechanism, IEEE Trans. Ind. Inf. 15 (6) (2019) 3680–3689.
[113] A.R. Rao, D. Clarke, Perspectives on emerging directions in using IoT devices in blockchain applications, Internet Things (2019) 100079.
[114] M.Á. Prada-Delgado, I. Baturone, G. Dittmann, J. Jelitto, A. Kind, PUF-derived IoT identities in a zero-knowledge protocol for blockchain, Internet Things 9 (2019) 100057.
[115] L. Chen, W.-K. Lee, C.-C. Chang, K.-K.R. Choo, N. Zhang, Blockchain based searchable encryption for electronic health record sharing, Future Gener. Comput. Syst. 95 (2019) 420–429.
[116] Y. Zhao, Y. Liu, A. Tian, Y. Yu, X. Du, Blockchain based privacy-preserving software updates with proof-of-delivery for internet of things, J. Parallel Distrib. Comput. 132 (2019) 141–149.
[117] R. Chaudhary, A. Jindal, G.S. Aujla, S. Aggarwal, N. Kumar, K.-K.R. Choo, Best: blockchain-based secure energy trading in SDN-enabled intelligent transportation system, Comput. Secur. 85 (2019) 288–299.
[118] M.U. Hassan, M.H. Rehmani, J. Chen, Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions, Future Gener. Comput. Syst. 97 (2019) 512–529.
[119] G. Sagirlar, B. Carminati, E. Ferrari, Decentralizing privacy enforcement for internet of things smart objects, Comput. Netw. 143 (2018) 112–125.
[120] 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 Things J. 6 (5) (2019) 7702–7712.
[121] P. Lv, L. Wang, H. Zhu, W. Deng, L. Gu, An IOT-oriented privacy-preserving publish/subscribe model over blockchains, IEEE Access 7 (2019) 41309–41314.
[122] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: a blockchain-based privacy preserving scheme for large-scale health data, IEEE Internet Things J. 6 (5) (2019) 8770–8781.
[123] M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of trust: a decentralized blockchain-based authentication system for IoT, Comput. Secur. 78 (2018) 126–142.
[124] 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, J. Netw. Comput. Appl. 116 (2018) 42–52.
[125] A. Mohsin, A. Zaidan, B. Zaidan, O. Albahri, A. Albahri, M. Alsalem, K. Mohammed, Based blockchain-PSO-AES techniques in finger vein biometrics: a novel verification secure framework for patient authentication, Comput. Stand. Interfaces 66 (2019) 103343.
[126] M. Conti, M. Hassan, C. Lal, BlockAuth: blockchain based distributed producer authentication in ICN, Comput. Netw. 164 (2019) 106888.
[127] Z. Liu, H. Seo, IoT-NUMS: evaluating NUMS elliptic curve cryptography for IoT platforms, IEEE Trans. Inf. Forensics Secur. 14 (3) (2018) 720–729.
[128] B.K. Mohanta, A. Sahoo, S. Patel, S.S. Panda, D. Jena, D. Gountia, Decauth: decentralized authentication scheme for IoT device using Ethereum blockchain, in: TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 558–563.
[129] S. Ding, J. Cao, C. Li, K. Fan, H. Li, A novel attribute-based access control scheme using blockchain for IoT, IEEE Access 7 (2019) 38431–38441.
[130] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, Q.E. Ali, Blockchain based permission delegation and access control in internet of things (BACI), Comput. Secur. 86 (2019) 318–334.
[131] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, LSB: a lightweight scalable blockchain for IoT security and anonymity, J. Parallel Distrib. Comput. 134 (2019) 180–197.
[132] S. Biswas, K. Sharif, F. Li, B. Nour, Y. Wang, A scalable blockchain framework for secure transactions in IoT, IEEE Internet Things J. 6 (3) (2018) 4650–4659.
[133] H. Si, C. Sun, Y. Li, H. Qiao, L. Shi, IoT information sharing security mechanism based on blockchain technology, Future Gener. Comput. Syst. 101 (2019) 1028–1040.
[134] Z. Li, L. Liu, A.V. Barenji, W. Wang, Cloud-based manufacturing blockchain: secure knowledge sharing for injection mould redesign, Procedia CIRP 72 (2018) 961–966.
[135] P. Danzi, A.E. Kalør, Č. Stefanović, P. Popovski, Delay and communication tradeoffs for blockchain systems with lightweight IoT clients, IEEE Internet Things J. 6 (2) (2019) 2354–2365.
[136] D.G. Roy, P. Das, D. De, R. Buyya, QoS-aware secure transaction framework for internet of things using blockchain mechanism, J. Netw. Comput. Appl. 144 (2019) 59–78.
[137] J. Yang, Z. Lu, J. Wu, Smart-toy-edge-computing-oriented data exchange based on blockchain, J. Syst. Archit. 87 (2018) 36–48.
[138] L. Zhou, L. Wang, Y. Sun, P. Lv, BeeKeeper: blockchain-based IoT system with secure storage and homomorphic computation, IEEE Access 6 (2018) 43472–43488.
[139] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, Y. Zhao, EdgeChain: an edge-IoT framework and prototype based on blockchain and smart contracts, IEEE Internet Things J. 6 (3) (2018) 4719–4732.
[140] R. Li, T. Song, B. Mei, H. Li, X. Cheng, L. Sun, BlockChain for large-scale internet of things data storage and protection, IEEE Trans. Serv. Comput. 12 (5) (2018) 4719–4732.
[141] R. Casado-Vara, P. Chamoso, F. De la Prieta, J. Prieto, J.M. Corchado, Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management, Inf. Fusion 49 (2019) 227–239.
[142] S. Huh, S. Cho, S. Kim, Managing IoT devices using blockchain platform, in: 2017 19th International Conference on Advanced Communication Technology (ICACT), IEEE, 2017, pp. 464–467.
[143] A. Maw, S. Adepu, A. Mathur, ICS-BlockOpS: blockchain for operational data security in industrial control system, Pervasive Mob. Comput. 59 (2019) 101048.
[144] L. Xie, Y. Ding, H. Yang, X. Wang, Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs, IEEE Access 7 (2019) 56656–56666.
[145] B.K. Mohanta, S.S. Panda, U. Satapathy, D. Jena, D. Gountia, Trustworthy management in decentralized IoT application using Blockchain, in: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2019, pp. 1–5.