Telecommunication Systems (2024) 85:503–538
https://doi.org/10.1007/s11235-023-01089-z

Secure and trustworthiness IoT systems: investigations and literature review

Wiem Bekri[1,3] · Rihab Jmal[1,2] · Lamia Chaari Fourati[1,2]

Accepted: 9 December 2023 / Published online: 23 January 2024
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2024

Abstract
Internet of Things (IoT) is creating a new automated environment where human interaction is limited, in which smart-physical objects obtain the power to produce, acquire, and exchange data seamlessly. Hence, diverse IoT systems concentrate on automating various tasks. These automated applications and systems are highly promising to increase user satisfaction while also increasing security-related challenges. Accordingly, Security and Trust are critical elements for users' well-being. In this paper, we investigate the security and trust properties along with the focus on various existing novel technologies (Software-defined networking, Blockchain, and Artificial Intelligence) and provide a survey on the current literature advances towards secure and trustworthy IoT. Furthermore, we present a detailed study on various security and trust issues in various IoT environments. Moreover, we discuss real-life IoT-security projects, specify research challenges, and indicate future research trends.

Keywords Internet of Things · Software defined networking · Blockchain · Artificial intelligence · Security · Trust

1 Introduction

The Internet of things (IoT) [1, 2] is a combination of several devices that can interact directly with one another without any external mediation. The ITU has defined the IoT as "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*" [26]. "Devices" or "things" refers to multiple physical sensing devices and technologies, such as sensors, infrared sensor, RFID (Radio Frequency Identification Devices), GPS (Global Position System), etc. Which monitors and gathers all kinds of information upon machines and individual social behavior. The IoT monitor, collect, and process data in real-time. The IoT exists in every life domain, E-health [3], IoV (Internet of Vehicles) [4], Smart-Grid [5], Smart-Home [6], Smart-City [7], Agriculture [8].

The IoT is expanding swiftly, consequent to the growth of transmission technologies, devices, and computational systems. Humans have become overly dependent on IoT technologies. Therefore, securing many interconnected devices in the IoT systems will be an area of concern. The productivity of different IoT components will no longer be efficient without security. Furthermore, the absence of security will give access to unauthorized users (i.e., humans and devices) to access and usurp the device functionalities and manipulate the user digital data. Finally, trust is a fundamental issue since the IoT environment is characterized by different devices which have to process and handle the data in compliance with user needs and rights. Face to these threats and issues, it is necessary for the IoT architectures to guaranty the end-to-end (E2E) security and trust.

Recently, several emerging advanced technologies has attracted extensive attentions for its ability to manage and secure the IoT domains. Software defined networking (SDN) [12, 13] is an advanced paradigm that manages in a secure and trustworthy way the IoT networks. This context was discussed by the authors in [14–16]. Securing the IoT network using SDN, is an opportunity to create smart response on a granular basis by singling out and blocking malicious transmissions and permit the other transmissions to their destinations. In addition, it has the power to redirect specific

✉ Rihab Jmal
rihab.jmal@isims.usf.tn

[1] SM@RTS Laboratory, Digital Research Center of Sfax (CRNS), Sfax, Tunisia

[2] ISIMS, University of Sfax, Sfax, Tunisia

[3] ENETCOM, University of Sfax, Sfax, Tunisia

network traffic to exceptional enforcement entities or security services (i.e., Firewalls, intrusion detection systems). Blockchain (BC) [17] is becoming one of the most promising paradigms for the next age of internet interaction systems. This technology can be used in various financial services such as digital assets, remittance, and online payment as in the Bitcoin case [18]. Blockchain and IoT are interesting partners as both represent distributed systems with no central point of control. Blockchain offers a solution for the IoT security and trust challenges. To highlight some of its benefits, BC can be used to track the sensor data measurements and prevent duplication with any another malicious data. Moreover, BC offers to exchange the sensors' data without using an outer party to establish trust. Furthermore, the deployment and operation costs of IoT can be reduced through blockchain since there is no intermediary. Artificial Intelligence (AI) [19] represents the computational devices that can replace human intelligence in the achievement of specific assignments. It has the ability to improve risk-management, by understanding and predicting a diversity of risks and automate fast response. Furthermore, IoT together with AI help to manage and improve security and access devices, such as opening electronic doors. AI can be used to learn regular path patterns of many operators to provide perception for future office layouts and possibly recognizing suspicious activities.

There have been several successful attempts to implant security/trust approaches in different IoT fields, such as Vehicular network (VANET) [22] in which vehicles and their transmitted data could be categorized and managed in a trustworthy way.

Furthermore, several other recent approaches were presented for wireless body area network (WBAN) [54, 55], Smart City [56, 57], and Industrial IoT [58]. Similarly, a number of surveys and studies exist that discuss various present IoT security/trust approaches in a variety of fields. To the best of our knowledge, this is the first survey to address IoT security and trust approaches in several domains, with a focus on blockchain, SDN, and AI-related mechanisms.

1.1 Major contribution

This study aims to analyze he most relevant available solutions related to security and trust in IoT field. We also focus on proposals regarding security/trust with Blockchain (BC), Software-defined networking (SDN), Artificial Intelligence (AI), as well as several technologies such as Network functions virtualization (NFV) [46], Mobile Edge Computing (MEC) [47], Cloud Computing [48, 49], Fog Computing [50, 51], Wireless Sensor Network (WSN) [52], which are considered as enabling technologies supporting the development of IoT. One of the goals of our study is to provide a brief investigation concerning the different threat sources in IoT. We also present a detailed review of some of the latest proposed countermeasure's mechanisms and projects concerning security/trust issues in IoT. An evaluation of the open issues, challenges, and future research directions to develop the future IoT security/trust applications further efficiently.

1.2 Paper organization

The remainder of this paper, is organized as follows. In Sect. 2, we analyze and describe various functions related to IoT security and IoT trust. Section 3 presents the methodology of the paper. We delineate and describe different IoT attacks along with a presentation of the IoT security and trust in Sect. 4. Also, different mechanisms examples related to Blockchain, SDN, and AI toward secure/Trustworthy IoT systems are displayed and discussed in Sect. 5. In Sect. 6, Different application domain approaches are discussed. In Sect. 7, real world projects are presented and discussed in detail. Open challenges are discussed in Sect. 8. Section 9, Presents recommendation and Future Directions. Finally, conclusions are drawn in Sect. 10. Figure 1 highlights the survey road map.

2 Related works

Recently, there has been a lot of effort in overcoming security and trust issues in IoT systems. Various surveys discuss IoT security and IoT trust from several perspectives in the published works. In this section we discuss different security/trust IoT surveys based on BC, SDN, AI and other technologies, and we summarize and highlight their differences in Table 1. Acronyms and key terms can be found in Table 2.

From IoT general prospect, researchers in [9] presented an analysis of the status and concerns of IoT security. They outlined the IoT concept. Furthermore, a comparative study of protocols, standards, and security models is provided. The paper highlights the necessity of standardization at the information transfer and monitoring level. Authors offered an insight through the most recent security research tendencies. Various surveys have mainly analyzed IoT systems and addressed important security challenges. Neshenko, N. et al. [60] focused on the IoT vulnerabilities by providing comprehensive classification surveys that discussed numerous aspects of the IoT. They also presented an IoT-vulnerabilities taxonomy in terms of attack vectors and several other unanalyzed dimensions. Furthermore, researchers proposed a data-driven approach that concludes compromised IoT devices, threats, and data sharing capabilities. Challenges and open issues are presented in the end. Security, privacy, and trust were the key elements that Sharma, V., et al. focused on in the mobile IoT environment [99]. They presented a comparison of the state-of-the-art solution along with an overview

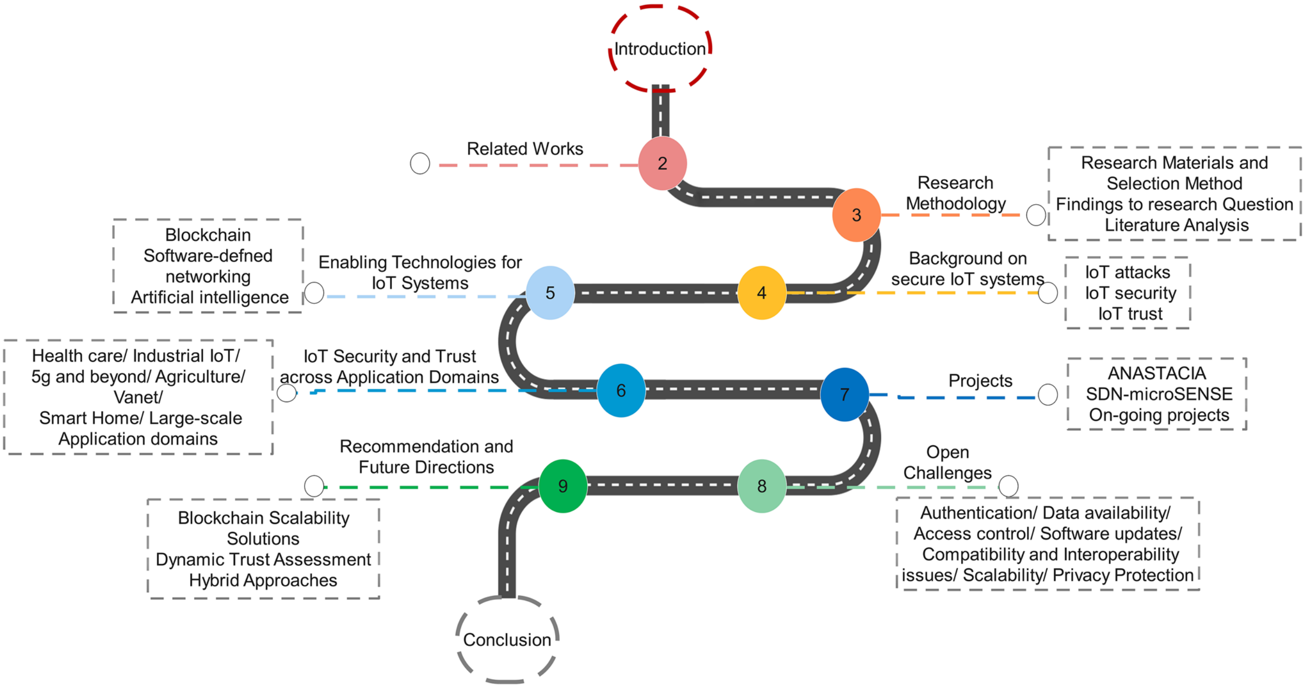

Introduction
Related Works
2
Research Methodology
3
Research Materials and Selection Method Findings to research Question Literature Analysis
Blockchain Software-defned networking Artificial intelligence
Enabling Technologies for IoT Systems
5
4
Background on secure IoT systems
IoT attacks IoT security IoT trust
Health care/ Industrial IoT/ 5g and beyond/ Agriculture/ Vanet/ Smart Home/ Large-scale Application domains
IoT Security and Trust across Application Domains
6
7
Projects
ANASTACIA SDN-microSENSE On-going projects
Recommendation and Future Directions
9
8
Open Challenges
Blockchain Scalability Solutions Dynamic Trust Assessment Hybrid Approaches
Authentication/ Data availability/ Access control/ Software updates/ Compatibility and Interoperability issues/ Scalability/ Privacy Protection
Conclusion

Fig. 1 Paper Roadmap

Table 1 Comparison on related works

	Paper, year	Attacks	Trust	Security	Architectures	BC	SDN	AI	Projects	Challenges
Short review	[25], 2019	X	✓	✓	✓(***)	✓(***)	X	X	X	X
	[61], 2020	✓(***)	X	✓	X	✓(**)	✓(**)	X	X	✓(**)
	[62], 2020	✓(**)	X	✓	X	✓(***)	✓(***)	X	X	✓(**)
	[104], 2021	X	X	✓	X	X	X	✓(**)	X	X
	[105], 2021	X	X	✓	X	X	✓(**)	✓(***)	X	X
	[111], 2019	X	X	✓	X	X	✓(**)	✓(**)	✓(*)	✓(**)
Long review	[9], 2021	✓(***)	X	✓	X	X	X	X	X	✓(**)
	[10], 2018	✓(***)	✓	✓	X	✓(***)	X	X	✓(*)	✓(***)
	[32], 2018	✓(***)	X	✓	✓(*)	X	✓(***)	X	X	✓(*)
	[60], 2019	✓(***)	X	✓	✓(**)	X	X	X	X	(***)
	[33], 2020	✓✓(***)	X	✓	X	(***)	X	(***)	X	(**)
	[63], 2020	✓(***)	X	✓	X	X	(***)	X	X	✓(***)
	[99], 2020	✓(*)	✓	✓	X	X	X	X	✓(*)	✓(***)
	[34], 2021	✓(**)	X	✓	X	✓(***)	X	X	X	✓(**)
	[98], 2021	✓(***)	✓	✓	✓(*)	✓(***)	X	X	X	✓(**)
	[100], 2021	X	X	✓	X	✓(***)	X	X	X	✓(**)
	[109], 2022	✓(***)	✓	✓	✓(**)	✓(**)	X	✓(**)	X	X
	[110], 2021	✓(***)	X	✓	X	X	X	✓(***)	X	✓(**)
Our paper		✓(**)	✓	✓	✓(***)	✓(***)	✓(***)	✓(***)	✓(***)	✓(**)

X, Not supported; *Briefly treated; **Moderated; ***Well treated; ****Deeply treated

Table 2 Acronyms and key terms

Acronyms	Full form	Acronyms	Full form
IoT	Internet of things	P2P	Peer-to-Peer
SDN	Software defined networking	CPAN	Personal Area Network Coordinator
AI	Artificial Intelligence	DoS	denial of service
NFV	Network Function Virtualization	DDoS	Distributed DoS
RFID	Radio Frequency Identification Devices	BOT	Botnet traffic
GPS	Global Position System	PSCAN	Portscan
IoV	Internet of Vehicles	LR	Linear Regression
E2E	End-to-End	LDA	Linear Discriminant Analysis
BC	Blockchain	KNN	k-Nearest Neighbor
VANET	Vehicular network	CART	Classification and Regression Tree
ME	Microenterprises	NB	Naive Bayes
WBAN	wireless body area network	SVC	Support Vector Classification
SMEs	Small-medium-sized enterprises	LSTM	Short-Term Memory
MEC	Mobile Edge Computing	CDR	Correct Decision Ratio
WSN	Wireless Sensor Network	IoHT	Internet of Health Things
ML	Machine Learning	BPS	Blood Pressure Sensor
DL	Deep Learning	HE Network	Health-Edge network
DNN	Deep Neural Network	PoW	Proof of Work
IIoT	Industrial Internet of Things	PoET	Proof of Elapsed Time
BLS	Boneh–Lynn–Shacham	PoS	Proof of Stake
RPI	Raspberry Pi	BS	Base station
TZ	Trust Zone	OSS	Operation Support System
AAA	Authorization, Authentication, and Accounting	VNF	Virtual network function
UDM	Unified Data Management	SNR	Signal-to-Noise Ratio
LSS	Local Subscriber Server	NS2	Network Simulator2
AMF	Core Access and Mobility Management Function	IoAT	Internet of Agriculture Things
CCCM	Central Cloud Connection Monitoring	QoS	Quality of Service
ES	Emergency services	RSU	Roadside units
ZM	Zone management	OBUs	on-board units
LAA	Local Access Assistant	PK	Public Key
SA	Security Auditing	AUs	Application Units
VM	Virtual Machine	CIDS	Collaborative Intrusion Detection System
GW	Gateway GW	CIA	Confidentiality, Integrity, and Availability
EC4	Edge-Cloud-to Central-Cloud Connection	6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
DApp	Decentralized Application	CI	Critical Infrastructures
SLA	Service Level Agreement	UI	User Interface
DSPS	DAYNAMIC Security and Privacy Seal	MMT	Montimage Monitoring Tool
BMS	Building management system	MAS	Mitigation Action Service
EU	European Union	S-RAF	Risk assessment framework
XL-EPDS	Cross-layer energy and detection system	SDN-SELF	Self-healing framework
BIAD	Blockchain-based Intrusion and Anomaly Detection	DSOs	Distribution System Operators
TSOs	Transmission System Operators	RQ	Research Question

of technologies, challenges, and methodologies for security, privacy, and trust. Moreover, researchers conducted a discussion on the security-aware protocols. Besides, presents a detailed study on trust management, privacy, and security approaches. The survey did not highlight or focus on specific technologies such as blockchain or SDN.

As for Blockchain-related papers, a survey on major security issues is given in [10]. Authors presented different IoT challenges such as data privacy, authentication, availability of service, etc. Furthermore, they categorized the main security issues, and analyzed and discussed proposed solutions some are related to blockchain and the absence of other technologies such as SDN, NFV, and AI. In [34] an overall literature study was conducted to discuss recent IoT security and privacy challenges, in which researchers categorized these challenges according to the IoT layer (perception, network, application). Besides, an entire study on Blockchain technology as a promising resolution for the IoT security problems was presented. An investigation was conducted on the challenges and effects that can occur due to the integration of blockchain in IoT systems. Furthermore, researchers proposed a framework of IoT security and privacy requirements through the blockchain mechanism. This work lacks an in-depth analysis of the studied approaches in the literature. In [25], Zhang, Y. et al. focused on a specific mechanism and presented a holistic investigation of it. They illustrated the blockchain-based security and trust mechanism along with an illustration of the proposed blockchain approach In the IoT smart-manufacturing environment. An overall detailed study is presented, but this study lacks in the number of studied approaches and comparison between them. In [98] Da Xu, L., et al. analyzed IoT-blockchain-based approaches, focusing on security characteristics, problems, and used technologies. Furthermore, they proposed a classification for different blockchain-based IoT security and attacks. Moreover, a study of various frameworks in different scenarios is presented. However, the presented architectures related to blockchain mechanism are limited, and "trust" was treated as subside challenge. For MEC-IoT systems, researchers analyzed and presented in [100] blockchain-based applications with a focus on the management of the security approaches. Furthermore, they proposed a study that underlines the feasibility of using blockchain in IoT security and a BC-based approaches taxonomy. However, the studied mechanisms needed additional detailing, such as highlighting architectures.

SDN-related surveys, in [32], the authors presented a detailed analysis of SDN-NFV-based security mechanisms. A structured study of IoT security threats was conducted, along with a background analysis. Furthermore, they presented a summarized description of the principal traditional security mechanisms by concentrating on authentication, encryption, access control, and detection solutions. Moreover, the authors provided an expanded analysis of security mechanisms provided by SDN and NFV. Iqbal, W. et al. in [63] provided as a first step a holistic overview of the IoT in terms of architecture, protocols, and security challenges. They also highlighted the Traditional network limitations, and to address those limitations, they provided a study of several security solutions. The main focus of the discussed security solutions was the SDN paradigm. The presented SDN-related IoT solution lacks specifications of the solutions architectures.

AI-based approaches for IoT were inspected by Gopalan, S. S., et al. in [104]. An IoT security mechanisms investigation in the healthcare environment presented and focused on AI-based methods. The authors highlighted and compared security issues, proposed models, experiment evaluations, and results for the selected studies. The overall observation presented needs more in-depth examination and lacks recent approaches. Zaman, S. et al. offer in [110] a detailed layer-by-layer analysis of IoT security vulnerabilities and AI-based security models to address them. Furthermore, a study is presented concerning the use of rule-based technics (such as Fuzzy Logic (FL) and Neuro-Fuzzy System (NFS)); ML algorithms (such as K-Nearest Neighbor (KNN)), and DL algorithms (such as Recurrent Neural Network (RNN)) for the countermeasure of the layer-wise threats. The countermeasure section was packed with approaches however these approaches need to be studied more in detail.

BC and SDN-related surveys, Zaman, S. et al. [61] analyzed the IoT's different features, challenges, and security specifications. They also proposed a brief analysis of several known threats to the IoT and presented the existing countermeasures based on SDN and BC emerging techniques for security and privacy. Case studies are also analyzed. In [62], Li, W. et al. discussed the existing problems and solutions for Blockchain-based SDN security approaches. Furthermore, they provided recent research studies along with a summarization of related BC-SDN frameworks. Besides, a discussion on relevant security challenges and solutions was conducted.

Blockchain and artificial Intelligence are the main focus in [33]. The authors presented mainly an overview of the IoT technology and the area of its applications. Furthermore, they defined Machine Learning (ML), Artificial intelligence (AI), and Blockchain technologies for addressing the privacy and security issues in IoT domains. The survey explained various IoT mechanisms, security issues related to the IoT, challenges, and corresponding solutions approaches with the integration of similar technologies like ML, AI, and Blockchain is also presented. In [109] authors examined recent security measures as well as current emerging technologies from the perspective of IoT security. Incorporating IoT with blockchain and AI-based authentication in cybersecurity, the authors provide a high-quality study on authentication and session keys. They also expose the flaws that remain in the current authentication IoT systems which are based on BC and AI technologies. This paper lacks the open challenges in the IoT security field.

Artificial Intelligence, Machine learning, and Software-defined networking technologies were the research focus of Ferreira, J. C., et al. in [105]. A systematic analysis was conducted related to diverse AI/ML algorithms to improve SDN functionalities. A systematic literature review is used to choose and analyze different overviews. However, this work lacks in-depth investigation and only a general classification is presented. In [111] a brief overview of the major applications of AI and ML in SDN and NFV-based networks is provided. According to their implementation history, authors categorized the most significant developments in the field into several groups and identified the associated AI methodologies used. Furthermore, they listed and discussed the major obstacles existing. Additionally, researchers highlighted the crucial function AI/ML can play concerning intelligent networks. The different studied approaches need in-depth study to clearly highlight the role of AI and SDN in the process.

Emerging technologies related to IoT, such as Blockchain, SDN, NFV, and AI, were explored by the authors presented in [103]. A comprehensive examination of security solutions for the IoT network based on SDN, Blockchain, and NFV is presented. Different challenges, threats, and attacks faced by IoT networks are explored in the review, along with detection methods. However, the focus of the discussed approaches did not include the trust issues as a challenge.

3 Research methodology

This section provides a methodology based on a systematic literature review conducted to analyze the current state of research in IoT security/trust and its relationship with different novel paradigms which are SDN, AI, and Blockchain.

3.1 Research materials and selection method

Identification of the main issues, new developments, and understanding gaps in IoT security and trust is the goal of this review. The assessment includes a thorough examination of articles released between 2016 and 2022 in recognized scholarly journals and databases. During the literature review, we came across parts of the research issue that were not fully covered in regular academic publications. To target these specific areas and provide a full study, we used a cautious and well-informed method to include respectable URLs connected to the research issue. The URLs were chosen from reliable sources, government studies and well-known organizations recognized for their knowledge in IoT security and trust. To verify the accuracy of the material contained in our study, we thoroughly evaluated the reliability and credibility of each web source. While academic publications served as the foundation of our study, the URLs we included gave us access to extra useful information and data that enhanced our analysis. Figure 2 depicts the selected papers after final filtering. Figure 3 depicts the scientific papers that were considered for inclusion in this survey. We have adhered to inclusion and exclusion criteria in order to avoid papers that do not address our research challenge. Each paper should only contain the dependent criteria, be written in English, be published in a journal, conference, proceedings, or book, be limited to the field of computer science, and include keywords. Based on the essential and alternative keywords which are: ("Internet of Things" OR "IoT") AND ("Security" OR "Trust") AND ("Software defined networking" OR "SDN") AND

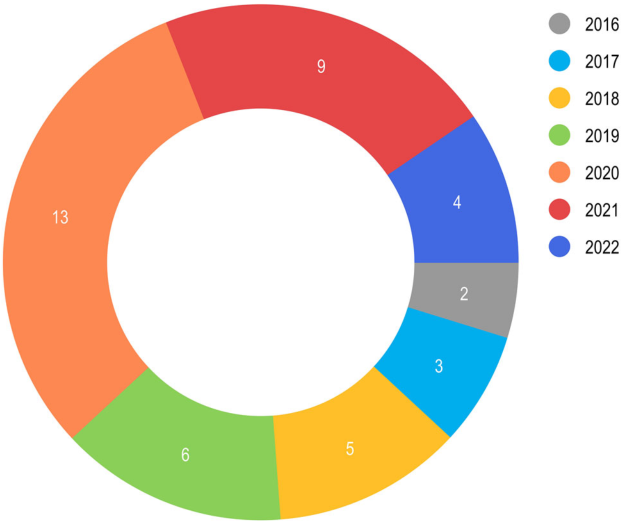


Fig. 2 Distribution of Selected Papers after applying the filtering stages Over the Years (2016–2022)

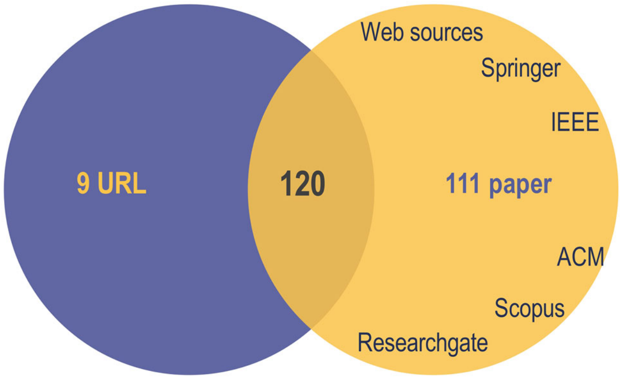


Fig. 3 Sources of Papers publisher in the Literature

("Blockchain") AND ("Artificial Intelligence" OR "AI") the following research questions are specified.

These research question (RQ) are defined in a simple and clear manner to be answered in our survey. The research questions addressed by this study are:

- (RQ1): What is the significance of SDN, Blockchain, and AI technologies as enabling factors in IoT systems?
- (RQ2): What are the defensive measurements that concerns with IoT security and IoT trust, also leverages from SDN, AI and blockchain in IoT different applications domain?
- (RQ3): What are the real-life projects of IoT security/trust?
- (RQ4): What are the open perspectives for building a secure and trustworthy IoT application?
- (QR5): What are the future Research directions and recommendations for securing IoT?

After answering the analytical questions, we gathered several publications that examine the security and trust concerns relating to IoT using defined keywords and similar alternatives.

3.2 Findings to research question

The 120 found studies that have been evaluated and analyzed are classified and studied. Prior to data analysis, the data collection was based on inclusion and exclusion standards. Regarding the studies that are consistent with the inclusion criteria and the filtering stages. Each listed RQ is answered with specific data that can be used. Below, the RQs are clarified.

(RQ1): What is the significance of SDN, Blockchain, and AI technologies as enabling factors in IoT systems?

The data of interest are papers that focuses on representing the fundamentals of each technology, their benefits and applicability with IoT.

(RQ2): What are the defensive measurements that concerns with IoT security and IoT trust, also leverages from SDN, AI and blockchain in IoT different applications domain?

The targeted data are the approaches that concerns with IoT security, and IoT trust as a primary focus, then the approach that leverages SDN, BC, and AI technologies and categorized by their application environment. The data collection includes experimental, theoretical, and practical solutions.

(RQ3): What are the real-life projects of IoT security/trust?

The targeted data are the studies about real-life existing, achieved, or on-going IoT security/trust solution, that uses one or more of the targeted enabling technologies discussed in RQ1.

(RQ4): What are the open perspectives for building a secure and trustworthy IoT application?

The data of interest includes methodologies recommended for protecting and creating trust in IoT applications. The data were gathered from recent studies examining potential opportunities and problems in the area of IoT security and trust.

(QR5): What are the future Research directions and recommendations for securing IoT?

3.3 Literature analysis

The data of interest are synthesized and summarized from the previous selected papers.

Numerous publications were chosen to answer the research questions and analyze the available literature. There are two phases to the search:

(Phase 1): We select the key words from bibliographic databases that are generally concerned with IoT trust/security challenges. These standards are based on the publications' titles, abstracts, keywords, similarity, and chosen publication years.

(Phase 2): To ensure the selected papers meet the inclusion criteria and are relevant to the field, a manual filtering process using hand-iterations is conducted.

These measures were taken to document the procedure for locating the selected studies. Search engines such as Springer Link, Scopus, Google Scholar, IEEE, and Science Direct have been utilized as search engines. As a result, after the initial count of surveys and conference papers produced by the primer search is, once the filtering stages have been applied, we are left with 42 papers and 9 URLs, total of 51 study.

4 Background on secure IoT systems

In this section, we define and present the different Attacks in IoT. Furthermore, we define the IoT security and trust terms by bringing to light the terms similarities and differences.

4.1 Attacks in IoT

The heterogeneity in the IoT infrastructure and interconnected resources leads to diversity in the attacks that threaten it. Hence, the security of the IoT network becomes more and more challenging against these threats. According to several studies [105, 106, 116], the classification of these threats/attacks can be divided into several categorizations based on different factors. Classifications could be based on the architectural layer of the IoT network, Vulnerabilities, Device property, location, Strategy, information damage level, Host, Access Level, Communication stack Protocol,

Table 3 IoT attacks classification

Attack name	OSI layer	Location	Access level
Node tampering	Physical	External, Internal	Active
Malicious Node injection	Physical	External, Internal	Active
Jamming	Physical	External	Active
Sinkhole	Network	External	Active
Sybil	Network	External, Internal	Active
Wormholes	Application	External, Internal	Active
Spoofing	Network	External, Internal	Active
Virus, Trojan-Horse, Spyware, and Aware	Network	External	Active
Side-channel	Physical, Application	Internal	Active, Passive
Denial of Service	Physical, Application, Network	External, Internal	Active
Man-In-The-Middle	Network	External, internal	Active

and Protocol. Thus, we discuss divers' classifications of different IoT attacks and summarized them in Table 3.

4.2 Attacks based on IoT network vulnerabilities

Based on the IoT vulnerabilities, attacks in IoT are divided into four categories, physical attack, network attack, software attack, and encryption attack. These categories are created based on their vulnerabilities, such as attacking by spoiling or manipulating a node (physical weakness), or by tampering with routing protocols inside the network (network weakness), or by the use of a malicious software (software weakness), or by destroying encryption procedure (encryption weakness). As shown in Fig. 4.

4.2.1 Physical attacks

These attacks target mainly physical devices that are likely to be manipulated as they have numerous peculiarities that can be of interest to others. Furthermore, the attack on the devices is done through some vulnerabilities in the device such as its memory, firmware, physical interface, unsecure default settings, outdated components.

4.2.2 Network attacks

As stated by its name, these attacks are localized in the IoT systems network. The attacks target the channels that link IoT elements.

4.2.3 Software attacks

This type of attack compromises the systems by using the vulnerabilities in the IoT devices' web applications and related software.

4.2.4 Encryption attacks

These attacks target the Data that circulates all the communication channels in the IoT system in an encrypted form.

4.3 Attacks based on device property

Based on the device properties, attacks in IoT are divided into low-power devices and high-power devices. Due to the power of the attacking devices, these types of attacks affect the IoT system differently.

4.3.1 Low-power devices attack

These attacks originated from low-power devices, in which the connection to the system is accomplished through radio links.

4.3.2 High-power devices attack

Unlike the previous attacks, the devices that initiate these types of attacks are full-fledged devices. Hence, the

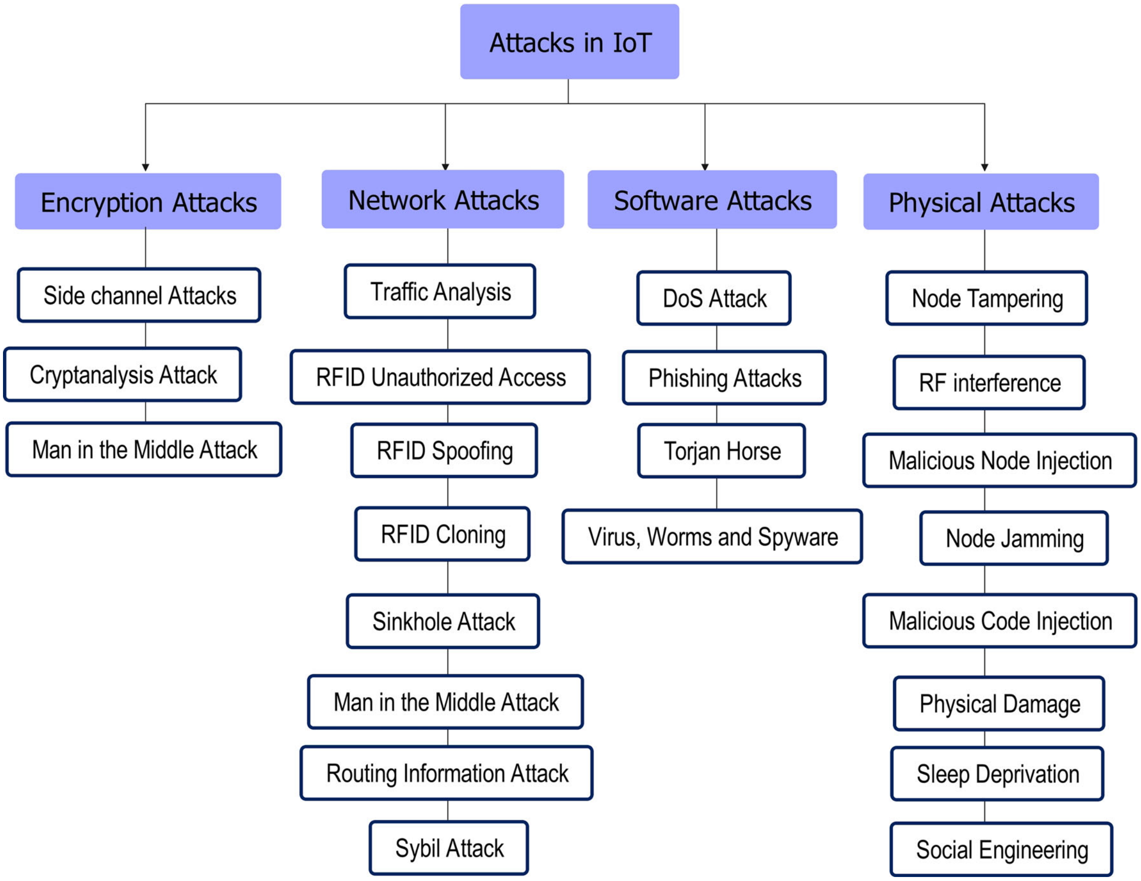


Fig. 4 Attacks in IoT based on IoT vulnerabilities

connection to the IoT system is done directly using a powerful device such as a laptop with a powerful CPU.

4.4 Attacks based on access level

There are two types of attacks according to the IoT system access, which are passive attacks and active attacks. These attacks impact the availability of the system.

4.4.1 Passive attacks

These attacks are based on monitoring and spying with no distribution to the communication and no tampering action to the information. Furthermore, these attacks are made to acquire or make usage of the data from the system.

4.4.2 Active attacks

Active attacks are different from passive ones, are to interfere with the communication within the system and temper with it.

4.5 Attacks based on attacker location

This type of classification depends on the geographical location of the attacker, which gives us two types of attacks: internal and external.

4.5.1 External attacks

The attacker is located out of the IoT network range and remotely attacks it. In this case, the attackers are ignorant of the IoT network component they are trying to access.

4.5.2 Internal attacks

The attacker, in this case, is in range of the IoT network and inside of its security border. Furthermore, it knows all the components of the IoT network. The internal attacks can be classified into four types: compromised actors, unintentional actors, emotional attackers, and technology perception actors.

4.6 IoT different attacks

In this subsection we briefly define different IoT attacks:

- **Node tampering:** This attack compromises a node in the system by physically modifying it. Hence, acquire critical data.
- **Malicious node injection:** This attack is carried on by one or two nodes injected in the network that cooperate to alter the information and transmit it to other nodes in the network.
- **Jamming attack:** this attack interrupts and confuses IoT devices' wireless communication.
- **Sinkhole attack:** This attack compromises a node near the sink and conveys fraudulent routing data to other nearby nodes to attract traffic.
- **Sybil attack:** This attack is when a malicious node duplicate itself to multiple nodes using different identities in different locations.
- **Wormholes attack:** This attack is achieved by selectively sending data from a malicious node to another malicious node through a low-latency link.
- **Spoofing:** This attack obtains the transferred data from the RFID tag by spoofing the RFID signal. Then, send fraudulent data to the system.
- **Virus, worms, trojan-horse, spyware, and aware:** These attacks are malicious Softwares that exist on the Internet. These types of attacks happen with no human intervention and lead to system tampering.
- **Denial of service attack:** This attack disrupts the services in the system to block the users from the system. More in-depth, the DoS attack is performed by submerging the targeted devices with excessive flows in order to overload systems and limit their performance.
- **Side-channel attack:** This attack attempts to collect information or encryption keys through time attacks or power-monitoring attacks or Electromagnetic attacks, etc. Hence, the target information is encrypted or decrypted using the gained keys.
- **Man-in-the-middle attack:** This attack functions as a third invisible party in communication between Two users. The attacker has the ability to monitor and access the information exchanged.

4.7 IoT security

Security in IoT [107, 108] is every act or practice that maintains the safety of devices, machines, and the networks they're linked to from menaces and manipulations. While serving at the same time to resolve weak points which may present future threats. IoT is a heterogeneous network, in which there exist both wired and wireless communication. This diversity leads to new threats and vulnerabilities to appear. There are several major security requirements that require our consideration which are authentication, confidentiality, data privacy and integrity, Availability, and Energy efficiency. In this section, we investigate these requirements.

4.7.1 Authentication

Authentication is a technique that ensures the building of a dependable network by allowing only authorized parties to gain access to the data. The diversity in the IoT resources and devices made it hard to accomplish an authentication process in a simple manner. Authors in [23], and [79] tackled the authentication requirement.

4.7.2 Confidentiality

The confidentiality aspect is of the most fundamentals in IoT security. Shielding data facing different threats is a must in order to preserve the confidential trait. In [77] data confidentiality is preserved through different features that authors used to create the data acquisition framework., and in [78] IoT confidentiality was a major targeted subject.

4.7.3 Data privacy and integrity

The information circulating the network is different in terms of its importance and this information which could be of great importance is most vulnerable in the transmission operation. That leads to possible problems. Hence, the obligation of using encryption algorithms is a must to sustain data privacy and integrity [78, 80].

4.7.4 Availability

Availability [81, 82] in IoT is the accessibility to its services, information, wherever and whenever needed. Availability could be categorized into two categories which are physical resources availability and software availability.

4.7.5 Energy efficiency

Regular Devices along with Resource-constrained devices that usually operate on batteries are used everywhere in IoT networks. Almost the majority of these devices are recognized for their limited storage space and low computational abilities. Hence, it makes them weaker to threats consequent to their security design. Energy efficiency is a critical subject that is targeted by authors in [83] and [84].

4.8 IoT trust

The term "trust" has several meanings depending on the context. It has no global-specific scientific definition. Moreover, all the existing interpretations of IoT-trust agree on some common requirements which are goodness, strength, belief, and reliability. Trust in IoT is another interpretation for security in IoT. Hence, Security and Trust are very similar in which they have the same objectives and ways but are slightly different at the same time. Furthermore, the trust concept covers a larger range than security, therefore it is harder and more complex to set, ensure and sustain.

Researchers in [20, 21] concentrated on the trust level evaluation for IoT objects. A dynamic trust management protocol is proposed to handle misbehaving nodes whose function might develop or dynamically alternate. Almost all the smart gadgets are presumed to be human-carried or human-related devices, so they are usually opened to public spaces and wirelessly interact. Therefore, weak against attacks. Using three trust properties (cooperativeness, honesty, and community-interest) authors, used social network theory to define and quantify trust in terms of convergence time and accuracy to maximize application performance.

5 Enabling technologies for IoT systems

In this section, we briefly delineate the targeted technologies: blockchain, software-defined-networking and artificial intelligence.

5.1 Blockchain

The blockchain is an expanding, decentralized, distributed series of blocks, which packs an entire list of transaction records. It is a distributed open-source digital ledger. The blocks are connected via a hash value, each block refers to the directly previous block (also called the parent block) using its hash value. Any modification entered on the data in the block causes the changes of its hash value (creation of a new block), which simplifies the changed blocks detection. The hash identifies the block and all of its contents, and it's continuously unique. The first block of a blockchain (which has no parent block) is named the genesis block, see Fig. 5.

Blockchain data are managed autonomously on a peer-to-peer (P2P) basis. Once data are stored inside a blockchain, it becomes hard to change it. Each block contains data, the hash of the block, and the hash of the previous block. The data stored inside a block depends on the blockchain type. For example, the Bitcoin blockchain [59] stores the details about a transaction such as a sender, receiver, and the number of coins.

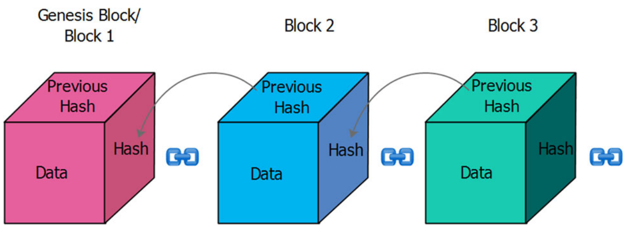


Fig. 5 Blockchain architecture

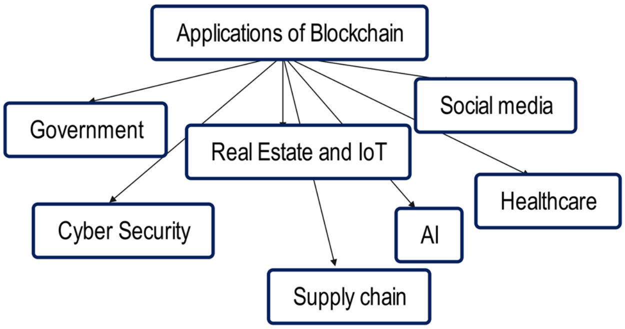


Fig. 6 Blockchain application domains

Proof-of-work is the original consensus algorithm that is used to verify the transaction and generate a new block in the blockchain. This mechanism slows down the creation of new blocks. The security of a blockchain originates from its productive use of hashing and proof-of-work. Moreover, being distributed is another way of security. Rather than adopting a central entity to control the chain, the peer-to-peer network is used and allows all to join.

The blockchain mechanism operates as follows:

- When a new member (node or miner) has joined the network, he receives the full copy of the blockchain.
- When a new block is created, it is sent to every node on the network.
- Next, each node examines the block to guarantee that it was not tampered with.
- Each node adds the block to its blockchain if it is safe.
- Furthermore, all the nodes create a consensus to agree on which blocks are valid and which are not.

The tampered blocks will get rejected later on.

Blockchain is constantly evolving and becoming more suitable to use in different applications domains as seen in Fig. 6.

The blockchain can be further secured by adapting a digital signature [115]. It is a digital form of a handwritten seal that is used to confirm the legitimacy and integrity of a document or a message. It starts with the owner creating a public and a private key, then creates a distinct digital signature for a message or transaction using their private key. Using the public key, users can check the integrity of the communication. Furthermore, in a blockchain network, digital signatures are stored in blocks along with transactions. Then, nodes check their digital signatures to make sure they are legitimate to validate them. Digital signatures and blockchain work together to make transactions secure, immutable, and attributable to the right parties. This promotes confidence and enables decentralized systems.

5.2 SDN

Software-Defined Network [71, 72] is a networking paradigm that enables the programmatic and dynamic control of a network. SDN provides: Computing and networking power, granular security, Low operating cost, Flexibility, holistic management, etc. Practically, SDN decouples the network and separates the intelligent part into a centralized layer. Using SDN, the network is separated into three layers:

- Application layer: Communication Interface.
- Control Layer: Centralized and could be distributed (contains several co-operating controllers) has a global view of the network and manage it.
- Data Layer: Composed of Virtual and physical switches and routers.

The Three above layers are interconnected with respectively Northbound API and Southbound API. There is several SDN controllers such as NOX [73], POX [74], Floodlight [75], ONOS [76], etc. Furthermore, we cannot talk about the SDN without mentioning the OpenFlow protocol as it is considered one of the important SDN standards. OpenFlow is a Southbound API.

Network control features, protection, energy efficiency, and routing optimization can all be provided using the SDN controller's centralized design and real-time monitoring. The scalable characteristics of SDN grant an efficient and easy way to address the network administration and programmability problems. SDN is a dynamic technology that could be and implemented and incorporate in different areas with other technologies, and also could be centralized or distributed. Distributed Ad-Hoc control Plane could be found in [112] and serves to control e the evolution of each SDN virtual switch on each Ad-Hoc device. Or centralized control plane in [113] which manage, monitor the network, and defend against attacks (DDoS) through the implementation of a detection algorithm.

5.3 AI

Artificial Intelligence [53, 64, 65] is the creation of Human-like thinking machines. AI is a combination of the learning process, deciding process to solve problems as the human brain operates. AI intends to promote machine functions that are related to mankind's knowledge. Some also consider it as a mixture of computer science, physiology science, and philosophy science. From a global perspective, the components of AI are Reasoning, Learning, Problem Solving, Perception, Linguistic Intelligence. AI is a global term that has six major subfields:

- Machine Learning [66]
- Deep learning [67]
- Neural Networks [68]
- Cognitive Computing [69]
- Natural Language Processing [70]
- Computer Vision

Artificial intelligence has a variety of uses. It may be used in several areas. In the healthcare sector, AI is being studied and employed for surgical operations in operating rooms, medicine administration, and various patient treatments, or monitoring patient's data and encrypt them [114]. Artificial intelligence can be found in important and critical domain such as the banking and finance sectors, in which it identifies and flag suspicious behavior (odd debit card use or significant account deposits). AI applications are also being utilized to facilitate and ease trade. This is accomplished by simplifying the estimation of securities' supply, demand, and pricing.

AI fall into two main types which are Weak and strong. Weak AI is represented by a system that is built to perform a single task (video games like the chess or personal assistants like Apple's Siri and Amazon's Alexa). Systems with strong artificial intelligence can do activities that are regarded to be human-like. These systems tend to be more complicated and difficult. They are trained to deal with circumstances when problem-solving may be necessary without human intervention. These sorts of technology are used in applications like self-driving automobiles and operating rooms in medical facilities.

6 IoT security and trust across application domains

In this section, we conduct an extensive study focusing on recent approaches and mechanisms that utilize novel technologies in various Internet of Things (IoT) application domains, mainly focusing on but not limited to Blockchain (BC), Software-Defined Networking (SDN), and Artificial Intelligence (AI). Our investigation covers a variety of industries, including e-health, vehicular ad-hoc networks (VANET), Industrial Internet of Things (IIoT), agriculture, Smart home, and others. We intend to offer a comprehensive viewpoint on the use of BC, SDN, and AI technologies in tackling security and trust concerns by looking at a wide range of IoT domains.

We evaluate the chosen methodologies throughout this study, highlighting their advantages, and disadvantages, stating their simulation setups if existed, and their application to the real world. To assist a thorough comparison, we present the results summary in two different tables: Table 4 focuses on security-related applications, while Table 5 delves into trust-related applications. With the help of these tables, readers will be able to quickly compare the properties of various techniques and determine how well they apply to various IoT domains.

6.1 Health technologies

In this section we inspect smart healthcare technologies related.

6.1.1 Trust-based decision making

Targeting one of the most vital domains, authors proposed in [42] an innovative Trust-Based Decision-Making protocol for Health IoT Systems. This protocol uses trustful information shared between IoT devices to build a collective knowledge base to rate the environment at a particular location and time. This base will grant the IoT devices to act instead of its owner for deciding on visiting this environment for medical causes. The protocol regards patient risk classification, reliability-trust, and loss of health probability as three design factors for decision making. Besides, the trust protocol possesses noise-sensing data resiliency by using the trust score computation method. The system design space of the IoT health system proposed by the researchers consists of several sensors and a PAN that has a gateway device. The previous elements create a health IoT member who could be categorized as measuring Environment factor or a Measuring Personal Health Statics. The health IoT cloud environment is responsible for the trust-based decision-making model. The cloud contains three major modules: health expert, communication, and Trust management. The three models respectively are responsible for sustaining the thresholds data, managing incoming queries/data, and managing and calculating trust/risk.

The protocol design is described in Pseudocode1. All entities in the system will execute the protocol for trust-based decision-making. The protocol assures the location Rating, Query processing by the Central Authority (CA) using several equations, Aggregated rating and aggregated trust for decision making, Trust Score Computation, etc. The protocol description shows which actions to be made by the CA and the members as an answer to the active environments and status change.

The simulation was done using NS3 simulator for performance evaluation. Performance metric is the correct decision ratio (CDR). Simulation parameters: M X M: 10 × 10 (1kmx1km), Nt: 100, Pm: [0.30%], Sn 1 m/s, H: [0.25, 1], S(ph): 0.2 m/s, T(period): 1 h, T: [20, 30] hrs, T(comp): [5, 10, 15], T(thresh): 0.3.

The simulation results illustrated the efficiency of the approach based on the obtained high CDR relevant to the ground truth case with CDR = 1 regardless of the developing malicious node number in a health IoT system.

6.1.2 DITrust chain

In [43], Abou-Nassar, E. et al. propose a Blockchain Decentralized Interoperable Trust framework (DIT) for IoT zones. The DIT is a privacy-aware management approach that offers secure storage for the patient-important data. Moreover, it improves encryption and the Internet of Health Things (IoHT) access managing system. Furthermore, enhance the safety and interoperability tools while avoiding widespread tracking and profiling. Besides, it guarantees using IoT-based multi-Cloud solutions the confidentiality and integrity of patients' data.

The general architecture of the proposed DIT Blockchain IoHT framework contains four levels or layers. Device Sense Layer: it is the first layer and contains different sensors, actuators, and devices and it is responsible for collecting and processing data. The network Layer is the second layer and consists of gateways, transportation layer, routing, and addressing. It's mainly responsible for securely transmitting the data. The Middleware layer: it is the third layer and consists of Data Analytics, Blockchain Decision unit, Database, Service and Application Support layer. Its main role is to hide different technologies for exempting the programmer from irrelevant issues. The Application layer is the last in the DIT architecture. This layer contains all the end-user system functionalities such as smart-transport, smart-health, smart-energy, etc. Each of these layers was associated with a specific security layer. First layer: sensor Data Integrity. Second layer: Authentication. Third layer: Privacy-preserving. Fourth layer: Trust-worthy.

Table 4 Security applications

Author	Year	Objective	BC	SDN	AI	Other	Pros and Cons	Application domains
Hakiri et al. [45]	2021	Securing IoT transactions using a Blockchain-based SDN and NFV solution	✓	✓	x	NFV	+ Low latency + High throughput + Prevent distributed attacks + High rate for false data detection −Data ownership and privacy	5 g Networks
Khoa et al. [37]	2020	Creation of new a collaborative learning-based intrusion detection system in the IoT Industry 4.0 to enhance security	x	x	✓	–	+ Improve of intrusion detection accuracy + Reduce traffic overhead + Increase the learning speed + High performance results + Information privacy disclosure − Limited targeted scope	Industry 4.0
Sengupta et al. [41]	2020	Securing end devices that have low ability in processing and handling delay-sensitive data problems through developing fog-based solution by conveniently plugging several security features in it	x	x	x	Cloud Fog computing	+ High-security level + low computation overhead for the low-end devices + Low decision-making latency rate + Optimal use for resource-constrained battery life + High performance − Few security features	Industrial IoT
Han et al. [44]	2017	Enhance the 5G security functions authorization, authentication, and accounting (AAA) in the edge cloud by creating a novel solution called Trust Zone	x	✓	x	NFV	+ High 5 g access network security level + Flexible security management + Disaster resistance	5 g Networks
Haseeb et al. [39]	2020	Create an IoT secure energy efficient based WSN solution to Smart-agriculture for the monitoring and production of rural areas	x	x	x	WSN	+ Intelligent data routing decision + Low energy consumption rate + High data delivery + Stable network performance + Secure data transmission − Small and specific experimental field	Smart agriculture

Table 4 (continued)

Author	Year	Objective	BC	SDN	AI	Other	Pros and Cons	Application domains
Shu et al. [36]	2020	Ensure protection from intrusion attacks in VANET by creating a collaborative intrusion detection system CIDS using distributed SDN and deep learning	x	✓	✓	_	+ Low system overhead + Effective collaborative intrusion detection + High performance rate + Solve biased flow issues	VANET
Zarca et al. [27] (*)	2019	Captures the main security and privacy challenges related to cyber-physical systems and IoT-critical infrastructures	x	✓	x	NFV	+ Dynamical orchestration and deployment for user security policies and actions + Automatic system adaptation through online real-time monitoring and testing technics + Run time privacy risks evaluation + Mitigate sudden security threats + Reinforcing security and trust policies + Multiple use cases	Different application domains
Li et al. [85]	2020	Design and implement a healthcare SDN-based edge computing security framework	x	✓	x	Edge computing	+ Enhance network performance + Consider the multi-dimensional data + Overcome the real-time and high-bandwidth edge server problems + Improve average response time, control overhead, average delay, etc − Low privacy rate for data	Healthcare

Table 4 (continued)

Author	Year	Objective	BC	SDN	AI	Other	Pros and Cons	Application domains
Prabavathy et al. [86]	2021	Design and develop an SDN-fog computing-based cognitive security framework for large-scale IoT systems	x	✓	x	Fog computing	+ Low energy consumption in the fog environment compared to the cloud + Low delay for attack detection in the fog environment + Higher throughput results in the fog environment + Provide edge intelligence for attack detection + High data-driven security using cognitive analytics − Lack in the used security policies − Low orchestration between fog nodes	Different application domains
Dorri et al. [11]	2017	Create a novel approach for blockchain optimization in the smart-home context through eliminating the POW	✓	x	x	–	+ Improved security and privacy + conserve energy + Efficient BC optimization + Low and manageable overhead − Limited scope	Smart-Home
Amangele et al. [30]	2019	Design a new two-stage hierarchical machine learning architecture based on SDN for network traffic anomaly detection and mitigation	x	✓	✓	–	+ Reduce in the number of processed packets in the classifier associated with the SDN switches + Reduction on effort in the second stage classifier + Simple design − Not suitable for all classification algorithms	Different application domains
Hasan et al. [24]	2020	Discover and combat malicious nodes and attacks in IoT environments through proposing a new SDN-enabled DL-based architecture	x	✓	✓	–	+ High efficiency + High detection accuracy − The proposed framework could be enhanced to improve the security	Different application domains

(*) project

Table 5 Trust applications

Author	Year	Objective	BC	SDN	AI	Other	Pros and Cons	Application domains
Al-Hamadi et al. [42]	2017	Developing Trust-Based Decision-Making health protocol that gives the devices the power to act instead of its user for deciding in critical medical conditions problems	X	X	X	Cloud	+ Trustworthy decision-making + Noisy sensing data resilient + High performance + High rate in recognizing malicious nodes + Effective trust management protocol - Accuracy of trust decision-making - The cloud centralization	Healthcare
Abou-Nassar et al. [43]	2020	Creating a privacy-aware management approach that offers secure storage for the patient-important data	✓	X	X	Cloud Computing	+ High Scalability, interoperability, availability, and trustworthiness + High confidentiality and privacy + Data integrity + High-rate semantic interoperability + Secure and trustworthy communications - Low elasticity in the identification learning stage	Healthcare
Awan et al. [40]	2020	Creating a safe environment for data transmission on the Internet of Agriculture Things (IoAT)	x	x	x	Cloud Computing	+ Efficient malicious nodes identifying + Optimal use of energy resources + Improved QoS + Low latency rate + High scalability + High-rate in identifying malicious nodes + High robustness	Smart Agriculture
Xie et al. [35]	2019	Design a trustworthy solution for the security and privacy issues in the transportation system for SDN-enabled 5G-VANET environment	✓	✓	x	_	+ High accuracy in detecting malicious nodes + High privacy + Real-time monitoring – Latency in detecting malicious nodes	VANET

Table 5 (continued)

Author	Year	Objective	BC	SDN	AI	Other	Pros and Cons	Application domains
Mbarek et al. [101]	2021	Create a novel Trust-based RFID authentication for connected smart home devices	x	x	x	–	+ Better detection probability for replica nodes in cloning attacks + Lower jamming attacks authentication failure rate + Higher authentication efficiency + Improved home security + Higher Trust rate in the security process	Smart city

The authors also presented a DITrust Blockchain IoHT virtual model. The steps of the proposed framework are outlined as follows:

- Creating Trusted virtual Zones: This step requires having a public–private key pair. Any device that seeks to join a trusted group must be named after it first, then it needs to create a trusted zone to be validated by the blockchain.
- Executing the proposed Framework: This step requires the accomplishment of sub-steps which are: The initialization step (each member or device must detect its group). A unique zone is built by the blockchain and then establish as trusted primary zones. After the zone creation step, the Blockchain verifies the members, the transaction, the legitimacy of the ID plate. The next step is to label every connected member to a specific zone. The last step states that the association requests are restricted to the same trusted zone, but the aggregation requests are executed in a different trusted zone.
- Aggregating and Association relationships.

A case study has been conducted to prove the agility and the efficiency of the DITrust blockchain IoHT framework. A scenario between Patient, Blood Pressure Sensor (BPS), and Doctor is presented. The main goal is to demonstrate the association/aggregation requests. Ethereum is used as a public blockchain in this study. It is used for the authentication phase for all the members. Next, the nodes (ambulance, doctor, and BPS) can upload their semantic annotation sheet to the health-edge network (HE network). Moreover, HE stores the incoming files each in its specific zone. The files are JSON-LD syntax hence they are lightweight. For the doctor and BPs communication (aggregation requests) JSON algorithm is used to match the sheets files with secure communication. Finally, after finishing the matching process, the nodes continue their transaction and store in the Ripple-chain, to grant data access and modification possibility for the other transaction-related nodes.

The results of the case study showed that the proposed model exceeds other similar methods in terms of confidentiality and privacy, trustworthiness, data integrity, authentication, interoperability, efficiency, etc.

6.2 Industry, industrial IoT, and industry 4.0

"Industry," "Industrial IoT," and "Industry 4.0", these three terms are intertwined and focus on the adoption of modern technology and digital transformation in industrial sectors. In this section we study SDN, BC, and AI based IoT security/trust technologies in intelligent industrial domain. We highlight, summarize and present different technics used along with simulation setup and results.

6.2.1 Collaborative learning model

Khoa et al. propose in [37] a new collaborative learning-based intrusion detection system in the IoT Industry 4.0 environment. First of all, Smart filters were developed. These filters are implemented in the IoT gateway on every network or subnetwork, and they are responsible for collecting information, detecting, and preventing cyberattacks on its subnetwork. The filters are made based on a deep neural network (DNN) and are trained with collected subnetwork information. However, instead of exchanging real information between the different filters, researchers proposed a collaborative learning model in which filters exchange their trained detection

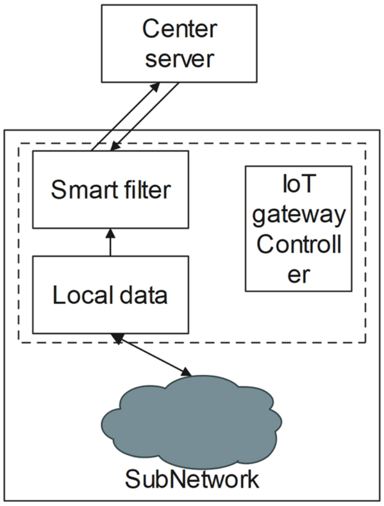


Fig. 7 Simplified architecture [37]

models. Hence the proposition of this paper aims to improve the precision in identifying attacks, besides, rise the learning pace, decrease the network transmission rate, and shield data privacy for the subnetworks.

The proposed architecture is as shown in Fig. 7 (simplified architecture) it contains multiple subnetworks, each of them is deployed to serve a specified goal in the industry 4.0 environment. They respectively all contain an IoT Gateway controller, which plays the role of a gate and manages all the incoming and outgoing transactions of the subnetwork. The implementation of the smart filter is made on the Gateway controller.

The filter uses as training information the data that was collected and gather in the local data storage of the subnetwork to train the deep neural network. The center server node is employed to exchange the trained model, in which it gathers the trained model from the filters and next assembles them employing the average gradient update algorithm, later the global model will be sent to every IoT gateways. As simulation parameters, researchers utilized KDD, NSLKDD, UNSW-NB15, and N-BaIoT data sets to assess the efficiency of their presented model.

6.2.2 A secure fog-based architecture for industrial internet of things and industry 4.0

In Industry 4.0 research field, Sengupta et al. addressed in [41] the low abilities of end devices in processing and handling delay-sensitive data problems, in addition to security concerning the nature of the cloud. They presented a secure Industrial Internet of Things (IIoT) fog-based architecture by conveniently plugging several security features within it and moving a few of the tasks intelligently to fog nodes. The mechanism presented decreases overhead on low-end tools and decision-making latency.

The proposed architecture consists of four layers:

- Perception layer: consists of several devices such as smart actuators (responsible for data collection), RFIDs (responsible for Offline/Online Encryption), Sensors, Smart Equipment (Responsible for command Execution), Smart Industrial Robot and surveillance Camera (Responsible for Aggregation Signature Generation). Using the Edge gateway, the gathered information is transferred to the next layer.
- Fog layer: This layer is the main contribution of authors in this work. It contains several fog nodes that are situated mostly near the network edge. This layer also could contain smart devices, virtual servers, or even Human smart mobile agents. The role of this layer is minimizing decision-making latency, transferring crucial tasks to the cloud, and saving the battery life of resource constrained IoT devices. The fog layer decreases the gap between IoT devices and the cloud by performing intensive time-sensitive tasks for security matters on their behalf. The performed tasks can be but are not limited to the following: Data storage, Key management, Re-encryption, Decision Making, Data analytics, Aggregate signature verification, Homorophic Encryption, Issuing commands, etc.
- Cloud layer: It contains several servers (Database server, Management server, Application server) together they perform storage and analysis of Big-data, decision making, and Issuing commands.
- Application layer: It consists of several users who are responsible for Equipment management production management and service management.

Performance evaluation was achieved using two ways of analysis, theoretical analysis in which authors measured the computation and communication overheads in terms of execution time and transmitting bytes number. Theoretical analysis parameters are: Type A pairings, Group element size 128 bytes, Cryptographic hash function SHA-256, Message digest size 32 bytes. Experimental analyses are accomplished through a simulation and a testbed implementation. For the simulation, the authors used two computers. First computer: 3.5 Gb Memory, Intel Core i5-7200U CPU @ 2.50 GHz * 4 Processor, 64-bit Ubunto 18.04.3 LTS OS, 100.3 GB Disk. Second computer: 7.7 GB Memory, Intel Core i7-6700 CPU @ 3.40 GHz *8 Processor, 64-bit Ubunto 18.04.3 LTS OS, 455.1 GB Disk. The first computer plays the role the industrial equipment (E), and the second computer plays the role of the fog node (F). Two separate Python codes were developed to control the computers.

Simulation metrics are Signature generation and verification time. Two experiments were conducted using this simulation environment and parameters. The simulation results confirm the results obtained through theoretical analysis which says that the overall execution time of aggregate Boneh–Lynn–Shacham (BLS) signature is lower than BLS.

Testbed setup: Raspberry Pi (RPI-3B) is used along with a laptop that acts as the fog node, and ThinkSpeak which is a cloud server running on a desktop. The data retrieving process is done through a remote terminal by a user. The Raspberry Pi (Sender): 1 GBB Memory, Cortex-A53, armv71 @1200 MHz * 4 Processor, 32-bit Raspbian OS, 16 GB Disk. Fog Node (Laptop)/ 3.5 GiB Memory, Intel Core i5-7200U CPU @2.50 GHz * 4 Processor, 64-bit Ubuntu 18.04.3 OS, 100.3 GB Disk. Data analyst (Laptop): 7.7 GiB Memory, Intel Core i7-6700 CPU @3.40 GHz *8 Processor, 64-bit Ubuntu 18.04.3 OS, 455.1 GB Disk.

The results obtained from the testbed confirm the results obtained from theoretical analysis. Through experimenting, researchers proved the efficiency of their proposition and its ability to secure, reduce the overhead on low-end devices, and reduce latency.

6.2.3 BCTrust

Authors in [28] proposed a robust, transparent, flexible and energy efficient blockchain-based authentication mechanism called BCTrust, which is designed especially for devices with computational, storage and energy consumption constraints. This work is established in a Wireless sensor network (WSN) environment. The WSN is composed of groups of devices interacting with each other. Each group is managed by a Personal Area Network Coordinator (CPAN). If a device migrates from a group to another, the authentication of the device in the new group is necessary. Basically, authors stated that the BCTrust is based on the principal of “The friend of my friend is my friend”. Which means that, if a device is authenticated in one group or cluster, it becomes trustful and accepted by all the other groups. The Ethereum Blockchain is used as a private blockchain where no proof-of-work is needed.

As shown in Fig. 8 there is three clusters: A, B, and C where a1 a device from cluster A, wants to migrate to cluster B.

1. The first secure association between a1 and A.
2. After the authentication of the device, A send a transaction to the Blockchain, in which A guarantees that a1 is trustful and that it shared symmetric keys for the secure data exchange with a1. This transaction is stored into a new block validated by the participating CPANs.
3. a1 migration from cluster A to B.
4. a1 send an association request to B.
5. B check if a1 is authenticated or not by sending a call to the blockchain.

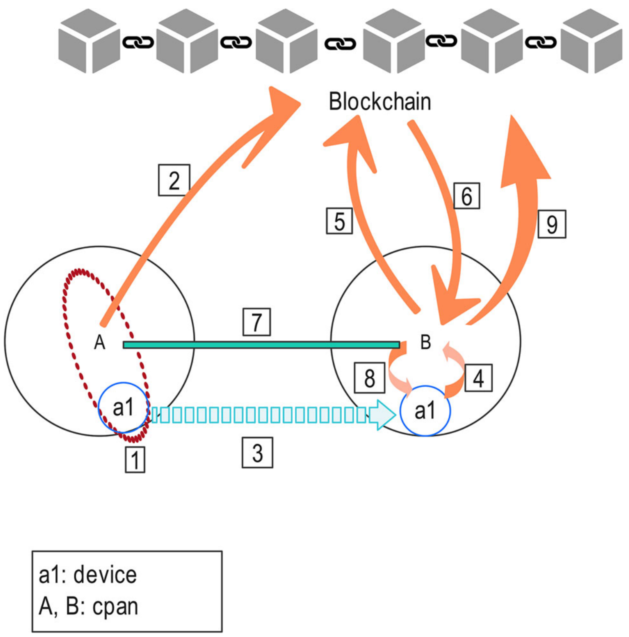


Fig. 8 Simplified architecture [28]

6. Blockchain confirms that a1 is authenticate by A.
7. B send a request to A to obtain a1 symmetric keys. (Through an asymmetric secure channel.
8. B associate with a1.
9. B send a transaction to the Blockchain. (Each time a transaction is sent, a new block is added).

For the migrating process, authors used three algorithms to explain it. Algorithm 1, Parameters and functions definition. Algorithm 2, Migration mechanism CPAN side. Algorithm 3, Migration mechanism device side.

To test and evaluate the mechanism, authors used a real implementation on a network composed of two CPANs A and B and one device that has the following characteristics: Dresden Elektronik deRFsam3 23M10-R3, have 48 kB of RAM, 256 kB of ROM and a Cortex-M3 Processor. The code was implemented using the C language.

To highlight the energy efficiency of the mechanism, researchers used the following equation to calculate the power consumption of the BCTrust mechanism and compare it with a classical association.

$$\begin{aligned} PC = {} & NT\,[Pte(Ton + Twu) + Po(Ton)] \\ & + NR[Pre(Ron + Rwu)] \\ & + Pidle \times Tidle \end{aligned}$$

where Pte is power consumed by transmitter. Pre is power consumed by receiver. Po is output power of transmitter. Ton is transmitter “on” time. Ron is receiver “on” time. Twu is start-up time for transmitter. Rwu is start-up time for receiver.

NT is the number of times transmitter is switched" on". NR is the number of times receiver is switched "on ". Pidle is the is power consumed during the idle mode. Tidle is the duration of the idle mode.

6.3 5 g and beyond

The studied papers in this section have been conducted in the fifth generation of wireless communication.

6.3.1 Security trust zone in 5G networks

In [44], Han, B. et al. proposed for 5G networks a novel architectural security solution called Trust Zone (TZ). TZ was designed as an enhancement for the 5G security functions authorization, authentication, and accounting (AAA) in the edge cloud. It can control the security administration and database access.

Furthermore, it offers a distinct and decentralized security policy, inducts an experience for disaster cognition, and increases the security functionalities for high emergency services available.

The TZ integrated with edge Cloud V-AAA server architecture is composed of: Unified Data Management (UDM), Local Subscriber Server (LSS), Core Access and Mobility Management Function (AMF), Operation Support System (OSS), Network Function virtualization (NFV), Virtual network function (VNF), V-AAA, SDN, IoT-GW, Central Cloud Connection Monitoring (CCCM), Emergency services (ES), Zone management (ZM), Local Access Assistant (LAA), and Security Auditing (SA). The 5G AAA architecture consists of four layers. Data-layer, which contains Common data layer functions and Dedicated data layer functions. Control Layer, which contains Common control layer functions, Dedicated control layer functions. Management and Orchestration layer, that contains Umbrella management (E2E service management and orchestration, OSS/NM, and NFV Orchestrator), VM, EM, cEM, etc. The previous two-layer are joined by a programmable Controller. Service layer, that contains BSS and Policies decision.

TZ is an edge cloud Virtualized-AAA server extended with a network monitoring function and emergency services. TZ is an assortment of network approaches covering a terrestrial space by a local cell.

The use case presents issues with communications that can appear in the local edge cloud, and the intra-edge-cloud availability is not affected following a shortage or missing edge-cloud-to central-cloud connection (EC4).

6.3.2 A blockchain-SDN architecture for secure and trustworthy 5G

A new blockchain-based architecture supported by Software Defined Network (SDN) and Network Function Virtualization (NFV) for securing IoT transactions is proposed in [45]. Using an SDN-aware Decentralized Application (DApp) allowed monitoring the mining nodes, detecting suspected IP addresses, and check anonymous packets. Hence, strengthen the security of the transaction. The architecture presents a selection method based on the Proof-of-Authority (PoA) consensus mechanism [45] who recognizes and reports suspicious IoT smart-gadgets.

Researchers also presented their intrusion detection system by Kubernetes testbed based on VNFs. Consequently, it drops malicious packets and allows DDoS detection and moderation on demand.

The blockchain-SDN enabled architecture presented of four layers:

- The blockchain networking layer: this layer permits the storage and sharing of information using the distributed file system. Blockchain validating nodes consists of transaction (Block) Generator, Identification (Keys, wallets, Transaction Hash), Authentication, Authorization, Accounting, Traceability, Trace management, Smart contract Deployment, Access control (White-lists, Black-lists, Gray-Lists). These nodes maintain a copy of all transactions and confirm the transaction based on consensus rules. Nodes communicate with each other through a distributed smart-service level agreement (SLA) which ensures the IoT transactions trust.
- The virtualized-controller network service abstraction layer: consists of SDN controllers, Virtualized Network appliances, VMs, SDN routers, etc. virtual appliances in this layer can perform communication with the main-blockchain network, agreement-driven decisions between each other, and communication with blockchain-SDN applications.
- The distributed SDN controllers' layer: responsible for diffusing security policies amongst blockchain nodes. This layer is a softwarized active, adaptable, and communication layer that interprets blockchain decisions to transmission rules to manage the SDN routers as stated by the application requirements. The decentralized controller monitors the IoT flows and reports suspecting IP addresses. Furthermore, malicious flows are managed by the VNFs intrusion detection located inside Kubernetes clusters.
- The Data plane abstraction layer: contains SDN virtual routers/switches, and an abstraction device layer. This layer is responsible for collecting IoT gateways sensing information that links remote sensors and actuators. This

layer ensures security by being straightly connected to the blockchain through the routers.

Researchers developed two algorithms for their approach. The first algorithm entitled 'Deploy the Smart Contract' illustrates the contract deployment to provide a trustworthy mechanism to secure the transactions. Second algorithm entitled 'Black-listing and White-Listing of IoT Nodes' illustrates the way the SDN controller plane use to recognize two types of devices and list them accordingly.

Transaction's latency and transaction throughput are the performance metrics determined by authors. A prototype including 20 nodes has been performed that plays the role of blockchain miners, while all nodes execute the leader-election consensus algorithm. A comparison is carried out against the Proof of Work (PoW) algorithm, Proof of Elapsed Time (PoET) algorithm, and Proof of Stake (PoS) algorithm. The approach proved improving performance and scalability, lower latency, and higher throughput when compared with PoW and PoS consensus algorithms.

6.4 Agriculture

In this section we tackle the studies and technologies that are dedicated, implemented in the agricultural sector.

6.4.1 An energy efficient and secure IoT-based WSN framework

Haseeb et al. proposed in [39] an energy-efficient and secure IoT-based Wireless sensor networks (WSNs) framework as a solution to Smart-agriculture for the monitoring and production of rural areas.

Different types of sensors are used (static or mobile) in order to create an easily controlled and configurated network infrastructure in the environmental field. Through this infrastructure, data is collected and transmitted towards the Base station (BS) with the help of gateways and cluster heads based on multi-criteria decision functions. Besides, the signal-to-noise ratio (SNR) is included in the resolution to measure the strength of wireless signals transmission links for enhancing the success rate of data transmissions. Security in the proposed framework is accomplished by the use of recurrence of the linear congruential generator. Also, security is provided for packets transportation from agricultural sensors towards BS while using the recurrence of the linear congruential generator based on secret keys.

The proposed Framework design of the Energy Efficient and Secure IoT Based WSN for Smart Agriculture consists of two main components. The first component is called the Energy and Link Efficient Routing. We find in the first component: Sensor nodes that gather information, Cluster heads each is responsible for a group of sensor nodes in a different area and aggregate information towards the BS. The process of selecting a suitable cluster head is performed using the Multicriteria decision function. Furthermore, the framework ensures the load balance and guarantees the reduction of network bottlenecks and network latency by using the single-hop transmission in another way. The second component is named Secure Data Encryption. The proposed security technique utilizes symmetric data encryption among agricultural sensors and grants strong data transportation.

BS generates a set of secret keys based on linear congruential– > Transmission of secret keys to sensor nodes– > XoR operation for data packets from sensor nodes to cluster heads– > Encrypted data transmission to BS using single-hop paradigm.

Moreover, the authors presented as a first step a discussion of the proposed design regarding energy and link efficiency routing, which includes two levels. Secure Data Transmission from Agriculture Sensors towards BS presented as a second step, in which authors presented three equations that respectively ensure the generating of secret keys (1), encryption of the data (2), and decryption of the Data (3).

$$\mathrm{Yn} + 1 = (\alpha \mathrm{Yn} + \beta) \bmod \mathrm{m} \tag{1}$$

$$\mathrm{Ej(mi)} = \mathrm{mi} \oplus \mathrm{Yi} \tag{2}$$

$$\mathrm{Dj(mi)} = \mathrm{Ej(mi)} \oplus \mathrm{Yi} \tag{3}$$

Yi stands for the generated secret random values.ni stands for sensor node.m stands for the modulus parameter.α stands for the multiplier parameter.β stands for the increment parameter.Y0 stands for the seed value. ⊕ stands for the XOR.Ej stands for the encrypted data.Yi stands for the key.

Researchers used in their experimental analysis Network Simulator2 (NS2), and as their simulation setup the following values: Simulation area: 200 m × 200 m, Deployment: Random, Sensor nodes: 100, Malicious nodes: 15, Packet size, k: 64 bits, Energy level: 2 j to 4 j, Payload size: 256 bytes, MAC layer: IEEE 802.11b, Control message: 25 bits, Transmission range: 20 m, Simulation rounds: 0 to 1000, Traffic flows: CBR.

Finally, to prove the efficiency of their proposed framework, the authors measured the network throughput, packets drop ratio, network latency, energy consumption, and routing overheads and compared it with other existing solutions. The simulation outcomes confirmed that the suggested framework remarkably improved the transmission performance, the packets drop ratio, the network latency, the energy consumption, and routing overheads.

6.4.2 AgriTrust

Creating a safe environment for data transmission on the Internet of Agriculture Things (IoAT) network is a critical challenge that Awan et al. addressed in [40]. They proposed a new privacy-aware trust management mechanism as an innovative solution that provides a lightweight approach to identify malicious nodes using the trust parameters. The presented approach introduces three distinguished trust management forms to assess the degree of trust between sensors to BS trust, cloud to BS trust, and BS to cloud. AgriTrust is a time-driven mechanism that measures trust for a particular period and operates communications based on the obtained trust degree that improves the scalability and lightens the computational burden in the network. Besides, it magnifies robustness and reduces non-repudiation. To estimate the aggregated trust degree the proposed approach employs the preceding and current trust degrees whereas computing direct trust values.

The proposed architecture is composed of: agriculture fields that contain soil sensors, diverse BS, Motor Pump, Power supply, Water supply, relay, and a cloud service provider. The sensors gather information regarding the soil and forward it to the BS. Sensors and BS communication are carried out using WIFI module ESP8266. The reception of gathered data by the BS initiates the computational process of the trust value then the obtained value is compared with the threshold value. The trust value is approved only if it reaches at least the merest trust requirement. If not, the BS drop the trust value and monitor that precise sensor for unusual actions. From another side, the BS/Cloud trust is also evaluated using the pre-defined parameters. The computed values are stored in their specified sections for later observation.

The Trust evaluation process for sensors was illustrated by authors in the first algorithm that contains Six different equations that are responsible for:

- Collecting the observation to determine if the trust value will be directly decided or should depend on the indirect/default trust degree (Eq. 1).
- Evaluating the direct degree of trust by assessing credibility (Eq. 2).
- Evaluating the robustness of a precise sensor based on the state of being tough facing possible attacks (Eq. 3).
- Evaluating the reliability (Eq. 4).
- Developing an absolute value of trust of the whole trust parameters evaluation (Eq. 5).
- Finding the whole trust using the former trust value that might give an aggregated trust (Eq. 6).

The Base Station to Cloud Trust Evaluation process was carried out through the second algorithm that contains three different equations that are responsible for:

- Evaluation of congenial trust, responsiveness trust based on previous observation, and evaluation of Quality of Service (QoS) based on transmit delay/overhead/throughput (Eq. 7a/7b/7c).
- Applying the summation by the BS to get the absolute value from the present values of trust (Eq. 8).
- Computing the aggregated trust by utilizing summation to the earlier trust value (Eq. 9a/9b).

The Cloud to Base Station Trust Evaluation process was carried out through the third algorithm that contains two different sets of equations that are responsible for:

- Evaluating the trust and applying the very same value for the predetermined period (Eq. 10a/10b/10c).
- Developing an absolute trust degree of the earlier value. Aggregate those values with the present trust estimation. Determining the last trust degree of a specific BS to compare it and the threshold value. Final decision making (Eq. 11a/11b/11c).

The simulations were performed in NS-3 open-source simulator. Simulation parameters were as follows: Nodes number varying under different situations. Trust degree between 0.0–1.0. The default trust degree of sensors is 0.5. The default trust degree of cloud and BS is 0.6. The monitoring time of sensors is 20 min (no trust). The monitoring time of BS is 30 min (no trust). The area minutes of one agriculture field are 245, 90, and 45 m2. The number of nodes is from 50 to 250. The transmission rate is eight megabits per second. The size of packets is from 10∼to 25 bytes. The minimum and maximum latency of the BS is 4000 and 5700. The minimum and maximum latency of the cloud is 2100 and 4260.

The authors stated in the result section that the simulation results proved the efficiency of their mechanism in knowing harmful nodes. Furthermore, they also stated that their mechanism proved its effectiveness in estimating the actual trust degree of nodes in a minimum period.

6.5 VANET

Studies in this section are related to VANET, which is a type of wireless network created specifically for inter-vehicle and inter-vehicle infrastructure communication.

6.5.1 Blockchain-based secure and trustworthy IoT in SDN-enabled 5G-VANET

The authors aimed in their work [35] to design a decentralized blockchain-based security framework and explicitly illustrates the SDN-enabled 5G-VANET model and the scheduling procedures of the framework. They also presented a study for the security and privacy issues in the transportation system for SDN-enabled 5G-VANET environment. A trust management blockchain system was designed as a first step in where they implemented vehicular IoT services including real-time cloud-assisted video report and trust management on vehicular messages. Vehicles accessing the 5G-VANET area require to be proved. Authentication is assigning valid public-key certificates and private keys to vehicles. After authentication, cars are allowed to continue to drive on their path and send real-time videos and road condition-related messages. To protect user confidentiality, the system keeps the vehicle authentication data apart from user identity information. A vehicle conveys the recorded videos every minute and diffuse traffic conditions messages. To forbid malicious information from accessing traffic, the vehicles close to the broadcasting vehicle will score its genuine. Roadside units (RSU) measure the trust value of the tag and packs it into blocks. Furthermore, proof-of-work and proof-of-stake are employed to handle regular selections.

The proposed architecture consists of numerous heterogeneous nodes including 5 g base station (gNBs), RSUs, and vehicles with on-board units (OBUs). RSUs are playing the role of 802.11p wireless access points to interact with OBUs. Video reports are gathered at the video cloud server. gNBs are deployed in the VANET to grant broadband wireless connection to the internet. RSUs and gNBs are managed by a centralized SDN controller which uses OpenFlow protocol. The vehicles, RSUs, and gNBs together create the data plane. They also form an overlay P2P network to maintain a blockchain. Hence each node is identified with a public key. The public key (PK) encrypts the communication and transaction done between different nodes in a way and in another way, it is used to verify the transaction signature by the nodes.

To demonstrate the efficiency of their approach authors used OMNeT + + 4.5, and crypto + + library 5.6.2. all experiments were executed on an Intel Core i7 and 16 GB RAM laptop with a display card GeForce 920 M. The dimension of the transportation zone is set to 1000 m × 1000 m. The RSUs (considered 802.11p Aps) were set to 10Mbps bandwidth, and for the gNBs, 1Gbps as a bandwidth. The number of RSUs is 30 and gNBs is 25. The number of the vehicle is set from 200 to 500. The speed of Vehicles is 110 km/h in random directions. V2N transmission range is 100 m, and for V2V transmission, the range is 50 m.

6.5.2 CIDS

Shu, Jiangang, et al. proposed in [36] proposed a collaborative intrusion detection system CIDS using distributed SDN and deep learning for VANET. Their proposition aims to protect from intrusion attacks in VANET. From one side, CIDS resolves the biased flow issue in individual detection and from another side, it bypasses the high system overheads in centralized detection. The proposed CIDS system model composed of a three-level structure which are:

First level: The Cloud server level.

Second level: Consists of multiple SDN controllers based on each base station. The controllers link the vehicles to the cloud server and manage the flows under the coverage of its base station.

Third level: Consists of multiple RSUs and vehicles which are equipped with OBUs and Application Units (AUs). they are all controlled by the SDN controller (vehicles are controlled by the SDN controllers through RSUs).

Furthermore, the authors specified the CIDS model in two phases to train an intrusion detection model to detect the data distribution of attacks from all the SDN controllers. In the cloud server, researchers trained a single discriminator but in SDN controller n pairs of generators were trained.

Phase 1) training of CIDS model across multiple distributed SDN controllers: The training phase is done on cloud and on SDN controllers in which the researchers proposed an algorithm for each of them.

Phase 2) CIDS detection of flows by each distributed SDN controller: After the training succeeds, the cloud server sends copies of the discriminator to all the distributed SDN controllers for intrusion detection. Moreover, in this phase, an equation is used to measure the abnormality of the coming flow and if the abnormality measured value is higher than the preset threshold, the flow is considered abnormal.

For the performance evaluation, Shu, Jiangang, et al. depended on efficiency and effectiveness. Python and Tensorflow 1.15 were used on a GPU-based computer with an Intel Core i5-8300H CPU and a GTX1050 GPU at 16 GB RAM.

In the emulation process, one cloud server and three distributed SDN controllers were emulated, and to guarantee the communication between them a socket is used.

KDD99 was chosen as the dataset for experimental evaluation. The whole dataset holds about 5 million records in which every record is represented by 41 features. Besides, four types of attacks are used: denial-of-service (DOS), user to Root (U2R), remote to local (R2L), and probing. Furthermore, a multi-layer perceptron (MLP) neural network is used to train all encoders, all generators, and the discriminator.

7 Smart home—smart city

This section presents smart home and smart city-based approaches.

7.1 Blockchain for IoT security and privacy

The work of [11] presents a new approach for blockchain optimization in the smart-home context. The authors proposed a new instantiation of blockchain by eliminating the concept of Proof of Work (POW) and the need for coins. The framework was designed based on hierarchical structure and distributed trust to maintain security and privacy.

The smart-home components presented in this paper are transactions, Local Blockchain BC, Home miner, and local storage.

Transactions are the communication done between the local devices or overlay nodes. These transactions are divided into five categories, and all use a shared key to secure the communication. The local private BC stores every transaction. The local BC stores and fix-in-place each device transaction together using two headers for each block in the BC. The headers (block and policy) are responsible for keeping the BC immutable, grant devices permission, and enforce the owner's control policy over his home. Home miner is a device that manages smart-home transactions. It can merge with the gateways or devices. The miner also performs a variety of tasks, from authentication and inspecting transactions to managing the local storage. Finally, Local storage is a storage device that can be inserted with the miner or an independent device.

The three main security requirements are Confidentiality, Integrity, and Availability (CIA). To test the performance of the proposed BC-based framework, the authors used two types of attacks (DDOS attack, Linking attack). The smart-home scenario simulation was achieved using the Cooja simulator. IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) is used as the underlying communication protocol. Three mote sensors play the role of IoT home devices, and another mote sensor plays the role of a home miner. Data is transmitted every 10 s. The simulation lasted for 3 min (multiple simulations have been achieved). Cloud storage is used and linked to the miner to store data and return the block number. The following metrics are evaluated: Packet overhead, Time overhead, and Energy consumption. The results show that the overheads acquired by the framework are low and manageable for resource constrained IoT devices. The presented overheads are measly relative to its security and privacy gains in terms of traffic, processing time, and energy consumption.

7.2 TRAS

Mbarek, B., et al. proposed in [101] a Trust-based RFID authentication scheme (TRAS), a novel authentication approach for connected smart home devices through compiling trust parameters to authentication to improve trust between home device tags and Mobile RFID readers. The system's objective is to resolve RFID key updating algorithms weaknesses and strengthen them against jamming and cloning attacks. The authors' proposition proceeds as follows the tag determines several trust factors to be utilized by a reader to determine the trustworthiness of the tag. The key parameters specified by authors to determine trust for each home device tag (HDT) are Updated-key, Previous key-trust, and Historical Transactions Trust (HTT). The historical transaction trust is copied several times by HDT and then encrypted using previous encryption keys, and only one is encrypted using the updated key. Furthermore, the HTTs are gathered and sent in one message to the Mobile RFID (MRFID). After conducting the authentication process, the MRFID verifies the authenticity of the received HTT through the Updated key or previous keys. However, if the authentication process fails, it uses HTT and previous keys for authentication. The authors presented a "Trust-based historical transactions" Algorithm in which they described different MRFID authentication steps. Furthermore, to evaluate and prove the efficiency of their proposition, authors conducted different simulation scenarios using the NS3 simulator with the following simulation parameters: Simulation time 100 s, Run times 50times, Number of tags 800, Number of readers 1, Mobility of tags None. Authors achieved a comparison between TRAS and TAP protocol [102] in terms of authentication rate, authentication delay, and detection probability. In conclusion, the TRAS protocol resulted in a better detection probability for replica nodes in cloning attacks and for jamming attacks lower authentication failure rate.

7.3 Bubbles of Trust

The objective of the proposed approach in [29] is to create secure virtual zones in IoT environments. Each device should communicate just with devices of its section and considers other sections devices as harmful. These zones are called bubbles of trust. Therefore, a bubble of trust is a zone where all its members can trust each other. It is protected and inaccessible for non-member devices. A public blockchain is used to implement smart contracts.

An ecosystem lifecycle is presented, and it is mainly composed of six phases. Phase A, define the IoT nodes or devices which can belong to different areas (medical, industry, etc.).

Phase B, the initialization phase in which devices are chosen and grouped by the Master. The master, accord each object in the group with a ticket. Phase C, the creation of the bubble at the blockchain level. Phase D, the followers send transactions to the blockchain to be linked to their appropriate bubbles. At the blockchain level, the smart contract verifies the uniqueness of the Follower's identifier (objectID), then checks the validity of the Follower's ticket using the public key of the bubble's Master. If one of the conditions is not satisfied, the object cannot be associated to the bubble. Once the first transaction (association request) of a Follower is successful, the latter does no longer need to use its ticket to authenticate itself (sends it within the exchanged messages). Phase (E), highlights how the blockchain makes the access control upon the objects and transactions. Phase (F), describes a global view of the ecosystem. Different use cases were used in this work, Smart Home, Waste management, Smart factory, and Smartroad radar. All the mentioned scenarios use multiple sensitive messages and data are transmitted in the network, if a unauthorized user can access and forge, modify or in some cases replay these information, it will lead to dangerous outcomes.

Multiple algorithms are used in the previous phases. algorithm 1, Parameters and Function definition (phase A and B). Algorithm 2, The smart contract bubbles' association rules (phase D). Algorithm 3, The smart contract bubbles' communication rules (phase E).

C + + language is used to develop the end-nodes' applications, Researchers used 2 identical Hp laptops with x86_64 CPU architecture, 64 bits CPU operation mode, 2600 MHz CPU max speed, 8 GB RAM, and Ubuntu 14.04 along with 1 Raspberry Pi with armv6l CPU architecture, 32bits CPU operation mode, 700 MHz CPU max speed, 450 MB RAM, and Raspbian 4.9.41 Operation system. One laptop was designed as Master and the other as Followers. Ethereum is used as blockchain. for the interaction between end-nodes and the blockchain, a C + + interface that encode/decode data toward/from Ethereum was created.

8 Large-scale application domains

The large-scale application domain designates the area in which each technology, system, or solution described in this section is used.

8.1 SDN-fog computing-based cognitive security framework

Prabavathy, S. et al. proposed in [86] an SDN-fog computing-based cognitive security framework for large-scale IoT systems. The main feature of the proposed framework is its distribution. The distribution of the SDN controllers is carried out using the cloud service provider.

The proposed security framework architecture contains two levels, cloud level, and edge level. Furthermore, the main actors are the SDN controller, distributed database, fog node, and terminal nodes. The Edge layer includes a local docker registry, docker host, and docker client, which interact with the Cloud level using OpenFlow. The Cloud level contains a global docker registry, distributed DB, and the controller.

The distributed autonomous SDN controllers are managed by the service provider in which they are added or removed from the security mechanism based on traffic loads. Each controller has three core modules, cognitive security system, Network management, and Fog nodes orchestration. First, the cognitive security systems module interprets data and detects abnormalities through analyzing user and entity behavior, which will lead to the building of the security response system. Second, the Network Management module performs using the security policy driver and network policy driver. Finally, the fog nodes orchestration module, responsible for dividing the work among the fog nodes. Furthermore, the SDN controller develops and deploys cognitive security systems in the cloud. The distributed feature of IoT requires the migration of the cognitive systems to the fog nodes (edge nodes). Fog nodes might be low computing machines like access points, switches, or high computing machines such as servers. Thus, to adapt to these varieties, the security approach is lightweight.

To implement and test their proposition, the authors used Microsoft Azure cloud service and Python programming language. The Microsoft Azure cloud service has as computing resource 4xDual-Core AMD Opteron 2218 @ 2.6 GHz,8 core, 32 GB RAM,6*146 GB HDD. For the fog node researchers used a laptop with a DUAL-CORE N3050 processor, 2 GB RAM, 500 GB HDD configuration and connected it to WLAN. As for the cognitive security system, K-means clustering is used. Python programming language is used to simulate the SDN controller at the Microsoft Azure cloud. Two simulation scenarios are conducted using the Aegean Wi-Fi Intrusion Dataset Reduced dataset (AWID).

8.2 Hierarchical machine learning for IoT anomaly detection in SDN

In [30], researchers proposed a new two-stage hierarchical machine learning process integrated into an SDN architecture for network traffic anomaly detection and mitigation. The presented security architecture is composed of:

Two classifiers, Classifier1 (Central Classifier) and Classifier2 (Edge Classifier). Along with an SDN-Controller, and an SDN Switch as shown in Fig. 9.

Classifier 1 is the first instance of machine learning, which operates on summarized network flow traffic characteristics captured using methods such as IPFIX. It is implemented in

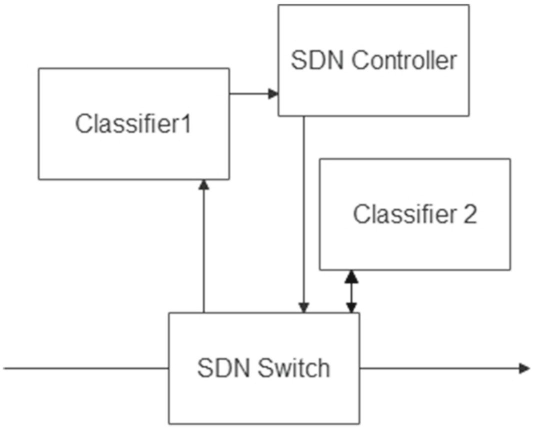


Fig. 9 Simplified architecture [30]

the SDN Controller and works on gross flow-level information. The central Classifier 1 identifies potentially harmful network traffic, which is, fed into a second machine learning stage. The edge Classifier 2 functions on a per-packet basis. The SDN controller grants a central computation resource that provides monitoring information. Besides, the SDN switch is efficiently capable of diverting (potential) malicious flow to Classifier 2. Hence, Classifier 1 recognizes which traffic is potentially harmful, and only packets of such flows are redirected to Classifier 2 using the SDN switch.

CICIDS2017 data set is used in model selection an evaluation in this work (specifically for security and intrusion detection testing) [31]. This dataset consists of seven categories attack as: denial of service (DoS), Distributed DoS (DDoS), botnet traffic (BOT), Patator, Infiltration, Portscan (PSCAN), and Web Attacks.

Authors used to assess the machine learning algorithms standard accuracy, precision, recall and F1 metrics. which respectively has as equations:

$$\text{Accuracy} = (\text{TP} + \text{TN})/(\text{TP} + \text{FP} + \text{FN} + \text{TN}) \tag{4}$$

$$\text{Recall} = \text{TP}/(\text{TP} + \text{FN}) \tag{5}$$

$$\text{Precision} = \text{TP}/(\text{TP} + \text{FP}) \tag{6}$$

$$\text{F1} = 2[(\text{Precision. Recall})/(\text{Precision} + \text{Recall})] \tag{7}$$

TP stands for true positive. FP stands for false positive. TN stands for true negative. FN stands for false negative.

Algorithm selection is based on several different metrics, including both machine learning quality metrics and prediction time. The performance was compared across six algorithms: Linear Regression (LR), Linear Discriminant Analysis (LDA), k-Nearest Neighbor (KNN), Classification and Regression Tree (CART), Naive Bayes (NB), and Support Vector Classification (SVC).

8.2.1 Orchestrating SDN control plane towards enhanced IoT security

In [24] authors proposed a new SDN-enabled Deep Learning-based architecture. The Deep Learning (DL) based architecture for combating malicious IoT nodes in addition to a control plane-based orchestration that leverages emerging Long Short-Term Memory (LSTM) classification models toward a quick and efficient discovery of advanced attacks in IoT environments.

The mechanism is highly scalable and decentralized that can sustain any commercial SDN controller. Researchers defined their work as an easily customized extended module that can integrate into any SDN controller. The envisioned architecture depends on two main aspects, LSTM classification models and orchestration through the SDN control plane.

The system model is composed of: Data Plane through which IoT devices connect, Control Plane in which security services and monitoring are orchestrated and managed and, Application Plane. Furthermore, the proposed architecture of the LSTM-enabled framework consists of Three integral components input, output, and forget, and one cell. The proposed LSTM model has the following parameters: from 4 to 5 layers, millions of neurons, Adam optimizer, 256 batch size, 10-epochs, Relu/ Softmax, and categorical cross-entropy for activation and loss function. The employed-LSTM models are used to predict and detect complicated attack vectors and harmful nodes in the IoT environment.

Researchers used a real-world dataset originated from N BaIoT 2018 dataset [38]. The dataset contains both standard and harmful data. Moreover, it is divided into a training set (80% fed into the learning algorithm for preparation) and a testing set (20% for system analysis).

For the experimental part, 3 cases were deployed and used to determine the performance value of the LSTM classifier in terms of its resistance to adversarial data infection. Besides, the suggested framework is strongly effective and dispenses encouraging outcomes in terms of detection accuracy (99.97%).

9 Projects

In this section we discuss real-life finished and on-going IoT security projects.

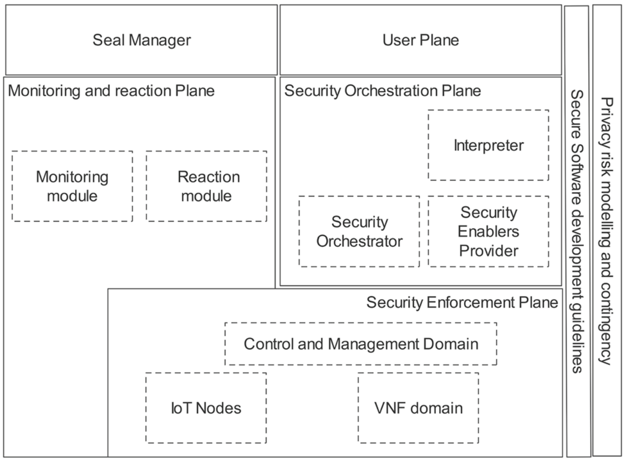

Seal Manager
User Plane
Monitoring and reaction Plane
Monitoring module
Reaction module
Security Orchestration Plane
Interpreter
Security Orchestrator
Security Enablers Provider
Security Enforcement Plane
Control and Management Domain
IoT Nodes
VNF domain
Secure Software development guidelines
Privacy risk modelling and contingency

Fig. 10 Simplified architecture [27]

9.1 ANASTACIA

ANASTACIA is an H2020-EU project that started in January 2017 and finished in December 2019. Researchers proposed in [27] a comprehensive architectural design that captures the main security and privacy challenges related to cyber-physical systems and IoT-CIs. The architecture is devised to empower IoT systems and networks to make autonomous security decisions through the usage of novel technologies such as software defined networking and network function virtualization. The architecture has been already implemented and evaluated in critical infrastructures (CI) deployed in smart buildings.

ANASTACIA is envisioned as a framework integrated on top of an IoT infrastructure where IoT devices, physical and virtual network elements interact in the data plane. It is composed of multiple planes as shown in Fig. 10 The first plane is the security enforcement plane. This plane connects the orchestration plane with the IoT platform. The control and management domain consists of IoT controllers, SDN controllers and NFV ETSI MANO-compliant modules. The first one (IoT controllers) responsible for enforcing security functions in heterogeneous IoT domain along with controlling different types IoT gadgets depending on various IoT protocols. The second one is responsible for the management of the flow rules, and the third one is responsible for orchestrating and managing the virtual network and its security.

The second plane is the security Orchestration Plane. This plane consists of Interpreter, Security policies repository, Security Enablers Provider, Security Enabler Repository, Security Orchestrator, and System Model repository. This plane organizes the enforcement plane resources. Moreover, it performs different activities like converting security properties to configuration rules and adjusting the security policies that are set by the policy interpreter with the provisioning of relevant security mechanisms. It has the entire sight of the underlying infrastructure to orchestrate resources and interfaces available at the security enforcement plane.

The monitoring and reaction Plane collects security-focused data about the system behavior through monitoring agent that exists in the security enforcement plane. Furthermore, it evaluates the achievement levels of security policies and produces filtering activities and data analysis for irregularities or anomalies detection. Besides, it mitigates the detected irregularities through reactions designed for them.

User plane contains the Policy editor user interface (UI), Alerting dashboard, and DSPS UI. This plane plays the role of communication channel between the Monitoring and reaction Plane (reaction module) and the ANASTACIA user plane. Besides, allows the users to model security policies with different levels of abstraction, along with warning them through alerts sent from the reaction module.

The last plane is the Seal Manager Domain. Composed of Security and Privacy Seal Manager Analysis, DAYNAMIC Security and Privacy Seal (DSPS) Agent, and DSPS Repository. It mainly monitors and provides a graphical representation of the system status to the end-user.

In order to prove the efficiency of their architecture, researchers used two different scenarios: 1) Mobile edge computing (MEC) scenario 2) Building management system (BMS). They respectively used sensors Attached to the IoT Network, Montimage Monitoring Tool (MMT) probe, and Operational Data Extracted from IoT devices as a main source for monitored information in the Two scenarios.

For the first scenario, researchers used The Cooja emulator to emulate IoT devices, an external server to play the role of the victim which will be attacked with ICMP ping packet (a ping flooding attack is considered), and the MMT monitoring tool for the attack detection along with a special sniffer that allows to extract packets from the IoT network, and a mitigation action service (MAS) machine to execute the mitigation service. They used the ONOS controller as their SDN controller. This scenario virtualized using VMs with the following features: two vCPUs @ 2.40 GHz, 2-GB RAM, and 20 GB of HDD.

The second scenario, the monitoring and reaction modules were deployed on the same basis as the first scenario. The policy interpreter, policy repository, security enabler provider, and security orchestrator have been virtualized and dockerized in an Intel Core i7-2600 CPU at 3.4 GHz, using three vCores, 3.5 GB of RAM, and 30 GB of HDD. The IoT controller has been virtualized and dockerized in an Intel Core Processor (Haswell) at 1.5 GHz using two vCores, 2 GB of RAM, and 15 GB of HDD. IoT devices: they are MSP430F5419A-EP at 25 MHz, 128-kB ROM, and 16-kB RAM, running a customized version of Contiki OS 2.7 and erbium CoAP server. The 6lowPAN bridge: it is an MSP430F5419A-EP at 25 MHz, 128-kB ROM, and 16-kB

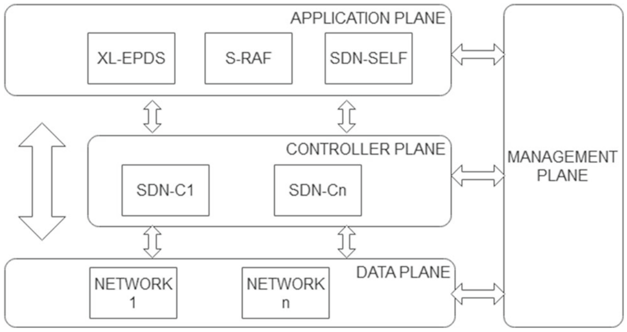


Fig. 11 Simplified architecture [88]

RAM, running a customized version of Contiki OS 2.7 to allow communication between 802.15.4 and 802.3.

9.2 SDN-microSENSE

SDN-microgrid reSilient Electrical eNergy System [87, 88] is a European Union H2020 project; that aims to provide a safe, privacy-enabled solution for decentralized Electrical Power and Energy Systems (EPES) that shields data from breaches. This project has a total of nine objectives, and down below are some of these objectives:

- Design a novel resilient, multi-layered, and SDN-enabled microgrid architecture.
- Create a framework for management and risk assessment.
- Provide a secure and flexible energy trading platform.
- Provide an EPES privacy-preserving framework.
- Creation of five large-scale pilots across Europe.

The proposed architecture in [88] (shown in Fig. 11 simplified architecture) gets hold of the Software-Defined Networking (SDN) technology advantages in order to identify, mitigate or avert possible cyberattacks and anomalies. In the SDN-microSENSE architecture planes, three major sub frameworks are deployed: Risk assessment framework (S-RAF), cross-layer energy and detection system (XL-EPDS), and self-healing framework (SDN-SELF). The S-RAF framework is distributed between the data plane and application plane and serves to collaboratively assess the risks, manage vulnerabilities and honeypot, etc. The XL-EPDS is located in the application plane and provides detection based on the specification/signature, based on ML/DL, based on visual, etc. SDN-SELF exists in the data plane, control plane, and application plane and serves to mitigate cyberattacks based on SDN, energy management, and islanding mechanisms. The common dashboard is located in the management plane and provides a common web-based dashboard.

The control plane in the project is a multi-modular application that installs numerous modules to enhance the Ryu functions and is based on the Ryu SDN controller. This enhancement serves to maintain track of source MAC addresses and Ethernet frame entry ports. As a result, the SDN Controllers may identify situations of broadcast storms and implement appropriate OpenFlow rules to avoid them.

Also, Blockchain technology was used in the project as an efficient security measure. The Blockchain-based Energy Trading System, built on top of SDN-SELF, intends to protect the information across the EPES/islanded SG's parts. The e-auction module and the Blockchain-based Intrusion and Anomaly Detection (BIAD) module are the key elements that define the system. The e-auction module creates safe and reliable communication between the participating parties in energy transactions. Also, secure communication for the Energy Service Company Organizations that handle the financial transactions. Furthermore, for the communication among the members, Hyperledger Fabric is used for the blockchain network fabric.

Traditional power sources, Distribution System Operators (DSOs), Transmission System Operators (TSOs), and prosumers are all part of the SDN-microSENSE project, which aims to solve security and privacy concerns across the entire energy value chain. Six use cases were conducted to demonstrate the whole potential of the proposed architecture:

- 1st Use Case: Investigation of Versatile Cyberattack Scenarios and Methodologies Against EPES.
- 2nd Use Case: Massive False Data Injection Cyberattack Against State Operation and Automatic Generation Control.
- 3rd Use Case: Large-scale Islanding Scenario Using Real-life Infrastructure.
- 4thUse Case: EPES Cyber-defence against Coordinated Attacks.
- 5th Use Case: Distribution Grid Restoration in Real-world PV Microgrids.
- 6th Use Case: Realising Private and Efficient Energy Trading among PV Prosumers.

9.3 On-going projects

The INSPIRE-5Gplus [89] project, supported by the European Union H2020, will provide new solutions to leverage the most of AI, ML, and Blockchain. The project's ultimate goal is to provide unique attributes that will enable intelligent and trustworthy multi-tenancy throughout the multi-tenant's structure. It will also help infrastructure owners and renters gain better management over their systems and decrease risks and intrusions.

CONCORDIA [90] is European Union H2020 project that aims to solve the existing fragmentation and strengthen the EU's digital authority. The goal of the project is to unite all of Europe's cybersecurity abilities into a network of proficiency to enable the creation of a safe, trustworthy, resilient, and competitive environment. CONCORDIA aims to create a strong collaboration network among all stakeholders, knowing that each has its own KPIs and supporting the creation of IT products and solutions across the whole supply chain.

The TERMINET [91] project supported by the European Union H2020 aims to create a new generation of a reference architecture for IoT and focus on technologies like SDN, multiple-access edge computing, and virtualization. Furthermore, incorporates new smart IoT gadgets for low-latency and market-oriented use cases. The goal of TERMINET is to deliver (precise and effective) choices to the area of focus in order to best satisfy the end-user, with a focus on combining faster hardware and advanced software to assist local AI model training through federated learning. Via a dynamic SDN-enabled middleware layer comes the simplification of connecting a big number of heterogeneous devices. Researchers also intend to design, develop, and implement unique smart devices to enable novel market-oriented use cases such as smart-eyewear, haptic gadgets, energy harvesting modules, autonomous drones, etc.

The SERUMS (Securing Medical Data in Smart Patient-Centric Healthcare Systems) [92] project funded by EU H2020 serves to develop innovative patient-centric solutions that will improve self-care, treatment quality, and patient trust in the confidentiality and privacy of their medical data. SERUMS aims first of all to create innovative patient-centered healthcare practices that incorporate personal medical care with centralized hospitals, specialized consultants, etc. It also aims to build trust in the system's operation, enabling the safe and secure transmission of personal private health information amongst the concerned parties. Furthermore, ensuring that the patient retains complete control over their data. Besides, SERUMS also aims to show the efficacy and generalization of its' outcomes by looking at a variety of different use cases.

The BAnDIT (advanced Blockchain Attacks and Defense Techniques) project [93] funded by European Union Marie Skłodowska-Curie Programme is a new Training Network that aims to create a developed platform to test an actual growing threat to Blockchain technology. Moreover, it evaluates the weak spots of blockchain systems and fosters collaboration between industry and academia in a powerful emerging technology with a great impact on society. BAnDIT is divided into four individual research projects (IRPs), one for each Early-Stage Researcher (ESR), and four major research topics.

C4IIoT (Cyber security 4.0-Industrial Internet of Things) [94] project funded by European Union H2020 serves to develop and demonstrate an innovative IIoT cybersecurity architecture for anticipating, detecting, mitigating malicious and abnormal activity. This project offers a holistic and disruptive security solution for reducing potential vulnerabilities in IIoT systems. It uses the emergence of security software and hardware protection mechanisms, state-of-the-art machine and deep learning and privacy-aware analytics, new encoded network flow analysis, and blockchain technologies to offer a feasible scheme for facilitating security and accountability. The C4IIoT framework will be presented and validated by real-life scenarios.

5GZORRO (Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks) [95] project was funded by EU H2020 and envisions the development of 5G to attain fully production-level support of various Application areas that coexist on a shared network infrastructure through automatic E2E network slicing, etc. Furthermore, 5GZORRO provides cognitive network orchestration and management with a low human intervention using distributed AI (Zero-Touch Automation). Distributed Ledger Technologies is used to incorporate effective and flexible distributed security and trust throughout the involved parties in a 5G E2E service chain. These technologies are used to create an updated 5G Service Layer for Smart Contracts that permits SLA monitoring, spectrum allocation, etc.

PUZZLE [96] project funded by EU and part of the Horizon 2020 program. It addresses small-medium-sized enterprises (SMEs) and microenterprises (ME). Furthermore, allow them to track, anticipate, analyze, and manage cyber threats. The project monitors the relationships between every small and microenterprise's cyber assets. It also uses the available network, compute, and storing infrastructures to evaluate individual and propagated threats, and proposes and implements mitigation measures. The project aims to provide solutions that can be quickly accepted by end-users and readily installed by external cybersecurity providers. Blockchain-oriented technologies are used to efficiently process data flows and establish secure and trustworthy SMEs and ME collaboration.

The ECHO (European network of Cybersecurity centres and competence Hub for innovation and Operations) [97] project funded under the Horizontal H2020 program intends to provide an organized and coordinated strategy to enhance the European Union's proactive cyber defense, enabling it to act in advance and fight against cyber assault. ECHO is establishing a network for better managing and optimizing the EU's Cybersecurity and Competence Centres.

10 Open challenges

After investigating different security and trust studies and approaches, models comprising SDN, BC, and AI technologies proved to deliver better security compared to models that do not incorporate them in terms of IoT systems protection. Despite the benefits of SDN, BC, and AI, new challenges always arise [10, 117]. Hence, we present in this section some of the most significant open challenges and future research direction in terms of IoT security and IoT trust.

10.1 Authentication

This term will always be a challenge considering the massive number of devices joining the global network each day and the different methods they use to guarantee the authentication process. Authentication is now a multi-way process in which user, machine, and services authentication are obliged. Moreover, many users do not prefer multi-factor authentication as they consider it expensive (for enterprises that use centralized systems like Active Directory Domain Services) and time-consuming, while others don't.

10.2 Data availability

The enormous amount of data generated quickly by everything connected to the internet causes information overload. Hence, it complicates the data collection and analysis process by designated organizations while they need to be keeping up in real-time developments to respond timely.

10.3 Access control

Different IoT-connected device types need distinct security measures before granting access (each device type has its specific vulnerabilities). Moreover, access control can be tricky in which some devices may need only a little access to the platform while others need read-only access for precise parts of the system.

10.4 Software updates

Not all the systems and devices perform their updates in time, many devices and even companies still use old models that do not support many new features. Therefore, it will lead to a slower response to threats and create new vulnerabilities due to outdated securing and testing methods.

10.5 Compatibility and interoperability issues

New systems are constantly emerging in the IoT industry, but these systems are not always compatible to work efficiently with each other. It takes time and effort to create trustworthy versions that are fully interoperable with other systems in the network, but until then, these systems are vulnerable. Attackers could use these vulnerabilities (like an application can access only one part of a system) as a back-door to perform their attacks.

10.6 Scalability

Scalability presents a major problem when using IoT security/trust solutions in the context of SDN, AI, and blockchain. It is necessary to create scalable systems and protocols that are capable of processing the rising number of transactions and data while maintaining security and performance.

10.7 Privacy protection

Maintaining the privacy of IoT data continues to be a major challenge. Although constancy and transparency are benefits of blockchain, data confidentiality is a challenge. In order to maintain private data while keeping the necessary trust and security, future studies should investigate privacy-preserving methods that can be combined with SDN, AI, and blockchain.

11 Recommendation and future directions

To tackle these challenges and further the study of IoT security/trust in relation to SDN, AI, and blockchain, Numerous suggestions and future initiatives are proposed.

11.1 Blockchain scalability solutions

For blockchain technology to be successfully integrated into IoT security/trust platforms, the scalability issue must be solved. To increase blockchain scalability without jeopardizing security or decentralization, more research should look into novel consensus methods or sharding strategies solutions. It would be beneficial to prototype these solutions and assess their effectiveness in actual IoT implementations.

11.2 Dynamic trust assessment

The development of dynamic trust evaluation tools that can adjust to shifting network conditions and growing threats should be the main goal of future research. Using machine learning and anomaly detection algorithms, among other AI approaches, can improve one's capacity to quickly identify and address new security concerns. The reliability of IoT devices and network components should be regularly assessed using these approaches.

11.3 Hybrid approaches

In the future, studies should consider hybrid strategies that combine the characteristics of SDN, AI, and blockchain to get around the drawbacks and optimize the advantages of individual technologies. The identification and mitigation of IoT security risks, for instance, may be improved by combining AI-driven threat intelligence with SDN-based traffic analysis and blockchain-based auditing. Investigating such synergistic pairings may result in IoT security trust solutions that are completer and more efficient.

12 Conclusion

Security and trust are similar terms yet different at the same time. These terms are crucial for all IoT environments in order to maintain the integrity, privacy, and safety of data that flows through the internet. Hence, securing IoT systems is a delicate subject that will always be a must to maintain order. There are several technologies to enforce IoT systems security, such as Blockchain, SDN, and AI. We present a brief interpretation for security and trust in IoT along with the blockchain, SDN, and AI technologies. Furthermore, we conduct a detailed study and comparison of the latest security and trust studies and approaches related to BC, SDN, and AI in different applications domains like healthcare, IIoT, Smart home, etc. Moreover, we present existing real-world IoT security and trust projects. Finally, we present challenges open issues then highlight future and promising research directions.

Our study offers a complete assessment and analysis of the recent methods for IoT security trust, focusing on the potential for synergy between SDN, AI, and blockchain. It gives an extensive comprehension of the subject while consolidating prior knowledge. This survey demonstrates novel strategies that improve IoT security and trust through the integration of SDN, AI, and blockchain technology. By examining these methods, researchers may learn about prospective solutions and innovative approaches to reduce security concerns. To conclude, we focus on the value of combining SDN, AI, and blockchain to address IoT security trust issues, explain the advantages of the most recent techniques, and offer a roadmap for further research projects in this field of study.

Author contributions Wiem BEKRI wrote the main manuscript text. Rihab JMAL and Lamia CHAARI FOURATI proposed the structure of the paper, and designed the tables. All authors reviewed the manuscript.

Funding No funding.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787–2805.
2. Bekri, W., Jmal, R., & Fourati, L. C. Internet of Things Management Based on Software Defined Networking: A Survey.
3. Scarpato, N., Pieroni, A., Di Nunzio, L., & Fallucchi, F. (2017). E-health-IoT universe: A review. *Management, 21*(44), 46.
4. Gerla, M., Lee, E. K., Pau, G., & Lee, U. (2014). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In: *2014 IEEE world forum on internet of things (WF-IoT)* (pp. 241–246). IEEE.
5. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. *IEEE transactions on Industrial informatics, 7*(4), 529–539.
6. Risteska Stojkoska, B. L., & Trivodaliev, K. V. (2016). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*. https://doi.org/10.1016/j.jclepro.2016.10.006
7. Su, K., Li, J., & Fu, H. (2011). Smart city and the applications. In: *2011 international conference on electronics, communications and control (ICECC)* (pp. 1028–1031). IEEE.
8. Zhao, J. C., Zhang, J. F., Feng, Y., & Guo, J. X. (2010). The study and application of the IOT technology in agriculture. In: *2010 3rd International Conference on Computer Science and Information Technology* (Vol. 2, pp. 462–465). IEEE.
9. Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. *SN Applied Sciences, 3*(1), 1–14.
10. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411.
11. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). 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)* (pp. 618–623). IEEE.
12. Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE, 103*(1), 14–76.
13. Farhady, H., Lee, H., & Nakao, A. (2015). Software-defined networking: A survey. *Computer Networks, 81*, 79–95.
14. Kalkan, K., & Zeadally, S. (2017). Securing internet of things with software defined networking. IEEE Communications Magazine, 56(9), 186–192.
15. Mohammed, A. H., KHALEEFAH, R. M., & Abdulateef, I. A. (2020, June). A Review Software Defined Networking for Internet of Things. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1–8). IEEE.
16. Yan, Z., Zhang, P., & Vasilakos, A. V. (2016). A security and trust frameyanwork for virtualized networks and software-defined networking. *Security and communication networks, 9*(16), 3059–3069.
17. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business and Information Systems Engineering, 59*(3), 183–187.
18. Karame, G. O., & Androulaki, E. (2016). Bitcoin and blockchain security. Artech House.
19. Mitchell, R. S., Michalski, J. G., & Carbonell, T. M. (2013). *An artificial intelligence approach*. Springer.
20. Bao, F., & Chen, I. R. (2012). Dynamic trust management for internet of things applications. In *Proceedings of the 2012 international workshop on Self-aware internet of things* (pp. 1–6).
21. Bao, F., & Chen, R. (2012). Trust management for the internet of things and its application to service composition. In: *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)* (pp. 1–6). IEEE.

22. Abassi, R., Douss, A. B. C., & Sauveron, D. (2020). TSME: A trust-based security scheme for message exchange in vehicular Ad hoc networks. *Human-centric Computing and Information Sciences, 10*(1), 1–19.
23. Zhao, Y. L. (2013). Research on data security technology in internet of things. In: *Applied Mechanics and Materials* (Vol. 433, pp. 1752–1755). Trans Tech Publications Ltd.
24. Hasan, T., Adnan, A., Giannetsos, T., & Malik, J. (2020). Orchestrating SDN Control Plane towards Enhanced IoT Security. In: *2020 6TH IEEE CONFERENCE ON NETWORK SOFTWARIZATION (NETSOFT)* (pp. 457–464). IEEE.
25. Zhang, Y., Xu, X., Liu, A., Lu, Q., Xu, L., & Tao, F. (2019). Blockchain-based trust mechanism for IoT-based smart manufacturing system. *IEEE Transactions on Computational Social Systems, 6*(6), 1386–1394.
26. Zennaro, M. (2017). Introduction to the Internet of Things. Telecommunication and ICT4D Lab, The Abdus Salam International Centre for Theoretical Physics Trieste, Italy, pp. 1–48.
27. Zarca, A. M., Bernabe, J. B., Trapero, R., Rivera, D., Villalobos, J., Skarmeta, A., & Gouvas, P. (2019). Security management architecture for NFV/SDN-aware IoT systems. *IEEE Internet of Things Journal*, *6*(5), 8005–8020.
28. Hammi, M. T., Bellot, P., & Serhrouchni, A. (2018, April). BCTrust: A decentralized authentication blockchain-based mechanism. In: *2018 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1–6). IEEE.
29. Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers and Security, 78*, 126–142.
30. Amangele, P., Reed, M. J., Al-Naday, M., Thomos, N., & Nowak, M. (2019). Hierarchical Machine Learning for IoT Anomaly Detection in SDN. In: *2019 International Conference on Information Technologies (InfoTech)* (pp. 1–4). IEEE.
31. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *ICISSP* (pp. 108–116).
32. Farris, I., Taleb, T., Khettab, Y., & Song, J. (2018). A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Communications Surveys and Tutorials, 21*(1), 812–837.
33. Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, p. 100227.
34. Alfandi, O., Khanji, S., Ahmad, L., & Khattak, A. (2020). A survey on boosting IoT security and privacy through blockchain. *Cluster Computing*, pp. 1–19.
35. Xie, L., Ding, Y., Yang, H., & Wang, X. (2019). Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. *IEEE Access, 7*, 56656–56666.
36. Shu, J., Zhou, L., Zhang, W., Du, X., & Guizani, M. (2020). Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach. *IEEE Transactions on Intelligent Transportation Systems*.
37. Khoa, T. V., Saputra, Y. M., Hoang, D. T., Trung, N. L., Nguyen, D., Ha, N. V., & Dutkiewicz, E. (2020, May). Collaborative learning model for cyberattack detection systems in iot industry 4.0. In 2*020 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1–6). IEEE.
38. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—Network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing, 17*(3), 12–22.
39. Haseeb, K., Ud Din, I., Almogren, A., & Islam, N. (2020). An energy efficient and secure IoT-based WSN framework: An application to smart agriculture. *Sensors, 20*(7), 2081.
40. Awan, K. A., Ud Din, I., Almogren, A., & Almajed, H. (2020). AgriTrust—a trust management approach for smart agriculture in cloud-based internet of agriculture things. *Sensors, 20*(21), 6174.
41. Sengupta, J., Ruj, S., & Bit, S. D. (2020). A secure fog-based architecture for industrial Internet of Things and industry 4.0. *IEEE Transactions on Industrial Informatics*, *17*(4), 2316–2324.
42. Al-Hamadi, H., & Chen, R. (2017). Trust-based decision making for health IoT systems. *IEEE Internet of Things Journal, 4*(5), 1408–1419.
43. Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O. Y., Bashir, A. K., & Abd El-Latif, A. A. (2020). DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE Access, 8*, 111223–111238.
44. Han, B., Wong, S., Mannweiler, C., Dohler, M., & Schotten, H. D. (2017, May). Security trust zone in 5G networks. In *2017 24th International Conference on Telecommunications (ICT)* (pp. 1–5). IEEE.
45. Hakiri, A., & Dezfouli, B. (2021, April). Towards a blockchain-sdn architecture for secure and trustworthy 5G massive IoT networks. In: *Proceedings of the 2021 ACM International Workshop on Software Defined Networks and Network Function Virtualization Security* (pp. 11–18).
46. Herrera, J. D. J. G., & Vega, J. F. B. (2016). Network functions virtualization: A survey. *IEEE Latin America Transactions, 14*(2), 983–997.
47. Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2017). Mobile edge computing: A survey. *IEEE Internet of Things Journal, 5*(1), 450–465.
48. Hayes, B. (2008). Cloud computing.
49. Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., & Fu, C. (2010). Cloud computing: A perspective study. *New generation computing, 28*(2), 137–146.
50. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In: *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13–16).
51. Vaquero, L. M., & Rodero-Merino, L. (2014). Finding your way in the fog: Towards a comprehensive definition of fog computing. *ACM SIGCOMM Computer Communication Review, 44*(5), 27–32.
52. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422.
53. Minh, D., Wang, H. X., Li, Y. F., & Nguyen, T. N. (2022). Explainable artificial intelligence: a comprehensive review. *Artificial Intelligence Review*, pp. 1–66.
54. Jovanov, E., Milenkovic, A., Otto, C., & De Groen, P. C. (2005). A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of NeuroEngineering and Rehabilitation, 2*(1), 1–10.
55. Kumar, M., & Chand, S. (2020). A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network. *IEEE Systems Journal, 15*(2), 2779–2786.
56. Fang, W., Cui, N., Chen, W., Zhang, W., & Chen, Y. (2020). A trust-based security system for data collection in smart city. *IEEE Transactions on Industrial Informatics, 17*(6), 4131–4140.
57. Singh, S. K., Jeong, Y. S., & Park, J. H. (2020). A deep learning-based IoT-oriented infrastructure for secure smart city. *Sustainable Cities and Society, 60*, 102252.
58. Cao, B., Wang, X., Zhang, W., Song, H., & Lv, Z. (2020). A many-objective optimization model of industrial internet of things based on private blockchain. *IEEE Network, 34*(5), 78–83.
59. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation, 2*(6–10), 71.

60. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys and Tutorials, 21*(3), 2702–2733.
61. Zaman, S., Kaiser, M. S., Khan, R. T., & Mahmud, M. (2020, December). Towards SDN and Blockchain based IoT Countermeasures: A Survey. In: *2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)* (pp. 1–6). IEEE
62. Li, W., Meng, W., Liu, Z., & Au, M. H. (2020). Towards blockchain-based software-defined networking: Security challenges and solutions. *IEICE Transactions on Information and Systems, 103*(2), 196–203.
63. Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal, 7*(10), 10250–10276.
64. Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. *Journal of Industrial Information Integration, 23*, 100224.
65. Thiebes, S., Lins, S., & Sunyaev, A. (2021). Trustworthy artificial intelligence. *Electronic Markets, 31*, 447–464.
66. Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets, 31*(3), 685–695.
67. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT press.
68. Borisov, V., Leemann, T., Seßler, K., Haug, J., Pawelczyk, M., & Kasneci, G. (2022). Deep neural networks and tabular data: A survey. IEEE Transactions on Neural Networks and Learning Systems.
69. Behera, R. K., Bala, P. K., & Dhir, A. (2019). The emerging role of cognitive computing in healthcare: A systematic literature review. *International journal of medical informatics, 129*, 154–166.
70. Qiu, X., Sun, T., Xu, Y., Shao, Y., Dai, N., & Huang, X. (2020). Pre-trained models for natural language processing: A survey. *Science China Technological Sciences, 63*(10), 1872–1897.
71. Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R. U., & Dou, W. (2020). Complementing IoT services through software defined networking and edge computing: A comprehensive survey. *IEEE Communications Surveys and Tutorials, 22*(3), 1761–1804.
72. Bekri, W., Jmal, R., & Chaari Fourati, L. (2020). Internet of things management based on software defined networking: A survey. *International Journal of Wireless Information Networks, 27*, 385–410.
73. Sheikh, M. N. A., Halder, M., Kabir, S. S., Miah, M. W., & Khatun, S. (2019). SDN-Based approach to evaluate the best controller: Internal controller NOX and external controllers POX, ONOS, RYU. *Global Journal of Computer Science and Technology, 19*(1), 21–32.
74. Mishra, A., Gupta, N., & Gupta, B. B. (2021). Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. *Telecommunication systems, 77*, 47–62.
75. Bholebawa, I. Z., & Dalal, U. D. (2018). Performance analysis of SDN/ OpenFlow controllers: POX versus foodlight. *Wireless Personal Communications, 98*(2), 1679–1699.
76. Eljack, A. H., Hassan, A. H. M., & Elamin, H. H. (2019, September). Performance Analysis of ONOS and Floodlight SDN Controllers based on TCP and UDP Traffic. In: *2019 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)* (pp. 1–6). IEEE.
77. Zhang, Y., He, Q., Chen, G., Zhang, X., & Xiang, Y. (2019). A low-overhead, confidentiality-assured, and authenticated data acquisition framework for IoT. *IEEE Transactions on Industrial Informatics, 16*(12), 7566–7578.
78. Valea, E., Da Silva, M., Flottes, M. L., Di Natale, G., Dupuis, S., & Rouzeyre, B. (2019, April). Providing confidentiality and integrity in ultra low power iot devices. In: *2019 14th International Conference on Design and Technology of Integrated Systems In Nanoscale Era (DTIS)* (pp. 1–6). IEEE.
79. Fadi, A. T., & Deebak, B. D. (2020). Seamless authentication: For IoT-big data technologies in smart industrial application systems. *IEEE Transactions on Industrial Informatics, 17*(4), 2919–2927.
80. Zhao, Q., Chen, S., Liu, Z., Baker, T., & Zhang, Y. (2020). Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Information Processing and Management, 57*(6), 102355.
81. López-Peña, M. A., Díaz, J., Pérez, J. E., & Humanes, H. (2020). DevOps for IoT systems: Fast and continuous monitoring feedback of system availability. *IEEE Internet of Things Journal, 7*(10), 10695–10707.
82. Amini, M. R., & Baidas, M. W. (2020). Availability-Reliability-Stability trade-offs in ultra-reliable energy-harvesting cognitive radio IoT networks. *IEEE Access, 8*, 82890–82916.
83. Song, K., Zhang, J., Ji, Z., Jiang, J., & Li, C. (2020). Energy-efficiency for IoT system with cache-enabled fixed-wing UAV relay. *IEEE Access, 8*, 117503–117512.
84. Metallidou, C. K., Psannis, K. E., & Egyptiadou, E. A. (2020). Energy efficiency in smart buildings: IoT approaches. *IEEE Access, 8*, 63679–63699.
85. Li, J., Cai, J., Khan, F., Rehman, A. U., Balasubramaniam, V., Sun, J., & Venu, P. (2020). A secured framework for sdn-based edge computing in IOT-enabled healthcare system. *IEEE Access, 8*, 135479–135490.
86. Prabavathy, S., & Supriya, V. (2021, August). SDN based Cognitive Security System for Large-Scale Internet of Things using Fog Computing. In: *2021 International Conference on Emerging Techniques in Computational Intelligence (ICETCI)* (pp. 129–134). IEEE.
87. Accessed 7 january 2022, <https://www.sdnmicrosense.eu/>
88. Grammatikis, P. R., Sarigiannidis, P., Dalamagkas, C., Spyridis, Y., Lagkas, T., Efstathopoulos, G., & Arce, A. (2021). SDN-Based Resilient Smart Grid: The SDN-microSENSE Architecture. *Digital*, *1*(4), 173–187.
89. Ortiz, J., Sanchez-Iborra, R., Bernabe, J. B., Skarmeta, A., Benzaid, C., Taleb, T., & Lopez, D. (2020). INSPIRE-5Gplus: intelligent security and pervasive trust for 5G and beyond networks. In: *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1–10).
90. Accessed 14 january 2022, <https://www.concordia-h2020.eu/> .
91. Accessed 14 january 2022, <https://terminet-h2020.eu/>.
92. Accessed 14 january 2022, <https://www.serums-h2020.org/>.
93. Accessed 15 january 2022, <https://www.upf.edu/web/bandit>
94. Accessed 16 january 2022, <https://www.c4iiot.eu/>
95. Accessed 16 january 2022, <https://www.5gzorro.eu/>
96. Accessed 20 january 2022, <https://puzzle-h2020.com/>
97. Accessed 23 january 2022, <https://echonetwork.eu/>
98. Da Xu, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: a survey. *IEEE Internet of Things Journal*.
99. Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, M. H., & Lim, J. (2020). Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey. *IEEE Access, 8*, 167123–167163.
100. Liao, Z., Pang, X., Zhang, J., Xiong, B., & Wang, J. (2021). Blockchain on Security and Forensics management in edge computing for IoT: a comprehensive survey. *IEEE Transactions on Network and Service Management*.
101. Mbarek, B., Ge, M., & Pitner, T. (2021). Trust-based authentication for smart home systems. *Wireless Personal Communications, 117*(3), 2157–2172.

102. Naija, Y., Beroulle, V., & Machhout, M. (2018). Security enhancements of a mutual authentication protocol used in a HF full-fledged RFID tag. *Journal of Electronic Testing, 34*(3), 291–304.

103. Babiker Mohamed, M., Matthew Alofe, O., Ajmal Azad, M., Singh Lallie, H., Fatema, K., & Sharif, T. (10). A comprehensive survey on secure software-defined network for the Internet of Things. *Transactions on Emerging Telecommunications Technologies*, e4391.

104. Gopalan, S. S., Raza, A., & Almobaideen, W. (2021, March). IoT Security in Healthcare using AI: A Survey. In: *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)* (pp. 1–6). IEEE.

105. Ferreira, J. C., Teixeira, D., & Macedo, J. (2021). Systematic literature review of AI/ML in software-defined networks using the snowballing approach.

106. Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016). Internet of Things (IoT): Taxonomy of security attacks. In: *2016 3rd international conference on electronic design (ICED)* (pp. 321–326). IEEE.

107. Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014, November). IoT security: ongoing challenges and research opportunities. In: *2014 IEEE 7th international conference on service-oriented computing and applications* (pp. 230–234). IEEE.

108. Zhang, J., Chen, H., Gong, L., Cao, J., & Gu, Z. (2019). The current research of IoT security. In: *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)* (pp. 346–353). IEEE.

109. Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex and Intelligent Systems*, pp. 1–33.

110. Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: A comprehensive survey. *Ieee Access, 9*, 94668–94690.

111. Gebremariam, A. A., Usman, M., & Qaraqe, M. (2019, March). Applications of artificial intelligence and machine learning in the area of SDN and NFV: A survey. In: *2019 16th International Multi-Conference on Systems, Signals and Devices (SSD)* (pp. 545–549). IEEE.

112. Flauzac, O., González, C., Hachani, A., & Nolot, F. (2015, March). SDN based architecture for IoT and improvement of the security. In: *2015 IEEE 29th international conference on advanced information networking and applications workshops* (pp. 688–693). IEEE.

113. Sambandam, N., Hussein, M., Siddiqi, N., & Lung, C. H. (2018). Network security for iot using sdn: Timely ddos detection. In: *2018 IEEE Conference on Dependable and Secure Computing (DSC)* (pp. 1–2). IEEE.

114. Ghazal, T. M. (2021). Internet of things with artificial intelligence for health care security. *Arabian Journal for Science and Engineering*, pp. 1–12.

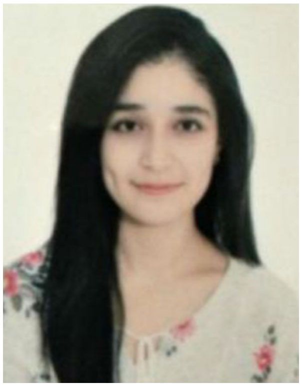
115. Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: A state of the art review. *EURASIP Journal on Wireless Communications and Networking, 2020*(1), 1–15.

116. Bekri, W., Layeb, T., Rihab, J. M. A. L., & Fourati, L. C. (2022, May). Intelligent IoT Systems: Security issues, attacks, and countermeasures. In: *2022 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 231–236). IEEE.

117. Rahouti, M., Xiong, K., Xin, Y., Jagatheesaperumal, S. K., Ayyash, M., & Shaheed, M. (2022). SDN security review: Threat taxonomy, implications, and open challenges. *IEEE Access, 10*, 45820–45854.

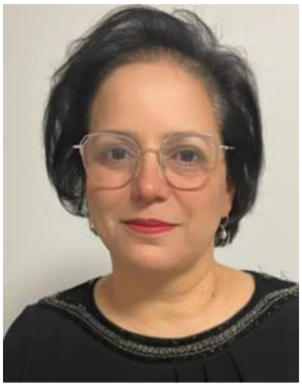
Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



Wiem Bekri is a Ph.D. student in National School of Electronics and Telecommunications of Sfax (ENET'COM), and SM@RTS Laboratory. She received her master degree from the Higher Institute of Informatics and Multimedia, University of Sfax in 2020. In 2015 she obtained her Informatics science bachelor degree from the Higher Institute of Informatics of Mahdia, University of Monastir, Tunisia. She is currently working on the IoT domains management and security issues.

Rihab Jmal is an assistant professor of computer science at University of Sfax, and a researcher at SMA@RTS Laboratory belonging to the Digital Research Center of Sfax (CRNS), Tunisia. She worked as Project Advisor from September 2019 to February 2021 at Sfax Technopark, her main mission was to collaborate with international partners in setting up projects proposal and participate to international funding programs (H2020). She received the Ph.D. degree in Computer Systems Engineering from University of Sfax in 2018. During her Ph.D. studies, she carried out two internships: the first was at INRIA Sophia Antipolis and the second was at IMT Atlantique Rennes, France. Her research interests include new technologies related to telecommunications networks. Especially, she focuses on Next Generation Networks, Software Defined Networking, Information Centric Networks, Internet of Things and Network slicing. She is the author and co-author of several international articles and has been a reviewer for various international conferences and journals.



Lamia Chaari Fourati is a professor at Computer Science and Multimedia Higher Institute and researcher at SMA@RTS Laboratory of the Digital Research Center of Sfax. She focused her research activities on conception and validation of new protocols and mechanisms for emerging networks technologies. Her research activities are very important and up-to-date which are related to digital telecommunication networks, in particular wireless access networks, sensor networks, vehicular networks, Internet of Things, 5G, software defined network, information centric network and wireless body area network, unmanned aerial vehicle. In these areas, she is interested in problems such as QoS provisioning (congestion control, admission control, resources allocations), cyber security and ambient intelligence. Furthermore, she focused her research on applications that impact positively our society such as healthcare domain, through the conception of innovative protocols and mechanisms for health monitoring, remote systems, the environmental control as well as energy saving approaches. Her scientific publications have met the interest of the scientific community and her work has been published in a very good journal and conferences. She has more than 50 papers published in journals and more than 70 papers published in conferences. She is the laureate for the Kwame Nkrumah Regional Awards for women 2016 (North Africa Region).