Cluster Computing (2021) 24:37–55
https://doi.org/10.1007/s10586-020-03137-8

A survey on boosting IoT security and privacy through blockchain

Exploration, requirements, and open issues

Omar Alfandi[1] · Salam Khanji[1] · Liza Ahmad[1] · Asad Khattak[1]

Received: 19 October 2019 / Revised: 23 May 2020 / Accepted: 2 June 2020 / Published online: 6 October 2020

Abstract
The constant development of interrelated computing devices and the emergence of new network technologies have caused a dramatic growth in the number of Internet of Things (IoT) devices. It has brought great convenience to people's lives where its applications have been leveraged to revolutionize everyday objects connected in different life aspects such as smart home, healthcare, transportation, environment, agriculture, and military. This interconnectivity of IoT objects takes place through networks on centralized cloud infrastructure that is not constrained to national or jurisdictional boundaries. It is crucial to maintain security, robustness, and trustless authentication to guarantee secure exchange of critical user data among IoT objects. Consequently, blockchain technology has recently emerged as a tenable solution to offer such prominent features. Blockchain's secure decentralization can overcome security, authentication, and maintenance limitations of current IoT ecosystem. In this paper we conduct a comprehensive literature review to address recent security and privacy challenges related to IoT where they are categorized according to IoT layered architecture: perception, network, and application layer. Further, we investigate blockchain technology as a key pillar to overcome many of IoT security and privacy problems. Additionally, we explore the blockchain technology and its added values when combined with other new technologies as machine learning especially in intrusion detection systems. Moreover, we highlight challenges and privacy issues resulted due to integration of blockchain in IoT applications. Finally, we propose a framework of IoT security and privacy requirements via blockchain technology. Our main contribution is to exhaust the literature to highlight the recent IoT security and privacy issues and how blockchain can be utilized to overcome these issues, nevertheless; we address challenges and open security issues that blockchain may impose on the current IoT systems. Research findings formulate a rigid foundation upon which an efficient and secure adoption of IoT and blockchain is highlighted accordingly.

Keywords IoT · Blockchain · Data privacy · Network security · Decentralized IoT

1 Introduction

Internet of Things (IoT) is an evolutionary technology that gained a profound utilization in various applications that aim to eliminate human intervention. It enables common operation picture (COP) through interconnections between human to machine or machine to machine [1] due to the massive advancements in wireless sensor network (WSN). According to Gartner report, by 2020 there will be approximately 20 billion IoT smart objects connected to the Internet that will exchange huge amount of information to bring more convenience to humans' lives [2, 3]. This number will most likely continue to increase. These smart objects range from simple wearable accessories as in Fitbit

✉ Salam Khanji
m80006416@zu.ac.ae

Omar Alfandi
omar.alfandi@zu.ac.ae

Liza Ahmad
liza.ahmad@zu.ac.ae

Asad Khattak
asad.khattak@zu.ac.ae

[1] Zayed University, Abu Dhabi, United Arab Emirates

Charge smart watch for analyzing fitness data to more sophisticated infrastructures as in self-driving vehicles (SDV) for automated vehicular system, smart city drones for surveillance systems, and microgrids for distributed energy resources systems [4, 5].

The microgrid system demonstrates a cyber-physical where it combines all distributed energy resources to provide power for a geographical area. However, current microgrid IoT systems rely on traditional SCADA systems, consequently, the integration between cyber and physical domains would significantly increase attack surface [6]. For instance, cyber-attacks might threaten SCADA systems that would disable the entire physical domain. Moreover, the drone market is evolving intensely towards automating critical operations as in firefighting and emergency responses. As the dependence of people and municipalities on such system increases, the necessity to maintain the security and reliability of these systems will increase as well.

From security and privacy perspectives, IoT can be considered a technology that is susceptible to the highest number of new attacks where hacked IoT devices might not only lead to data leakage but rather would profoundly impact the physical world. Stuxnet [7] and Mirai DDoS attack [8] are the most prominent IoT attacks where both demonstrated how the entire IoT infrastructure can be affected due to misconfigured IoT devices. There is a crucial need to preserve critical data collected and exchanged among distributed IoT devices through offering secure and trustworthy communication channels.

The advent of blockchain technology brings a fascinating approach to contain the distributed transactions in IoT ecosystem. The key compelling reason to propelling the integration of blockchain in IoT is to eliminate centralization so that to automate a secure exchange of real-time data among IoT devices. Blockchain deploys distributed, public ledgers to allow anonymous transactions where it shifts the current centralized business models into decentralization [9]. Additionally, blockchain empowers people to control their own personal data where they can share it only with intended parties and under consented circumstances [10]. Meanwhile, all transactions committed to blockchain's network can be traced where manipulation or data tampering require to commit a new block and hence, the public ledger can be a valuable source of reliable footprints and artifacts. However, blockchain as with any new technology has its own flaws especially when adopting it in IoT critical infrastructures. For instance, there are still many open issues in healthcare while preserving patients' data, and availability of IoT sensors in supply chain management.

Our contribution in this research paper can be summarized as follow:

- Present a rigid foundation where we exhaust the literature to identify the recent IoT security and privacy issues and how those issues affect the different layers in the architecture of and IoT system.
- Survey and present solutions on how blockchain is capable to overcome security and privacy issues in IoT systems.
- Investigate what challenges and open security issues blockchain would impose on blockchain-based IoT ecosystem.
- Present comprehensive recommendations and a way forward by proposing a blockchain-based IoT framework that shows how block-chain technology is integrated in each layer of the IoT system architecture layers to adopt a proper, efficient, and secure blockchain integration in IoT.

The rest of the paper is organized as follows. Section 2 delineates IoT architecture and categorizes the main security challenges faced at each layer. Section 3 describes the progression of blockchain technology and identifies its security and privacy features suitable for IoT systems where we exhaust the literature for recent blockchain-based approaches utilized to boost IoT security. Moreover, we identify potentials of integrating blockchain with other recent technologies such as machine learning to harness IoT paradigms. Section 4 highlights security and privacy challenges imposed by adopting blockchain in IoT systems. In Sect. 5 we propose our framework for proper and efficient blockchain and IoT integration and finally we conclude the paper in Sect. 6.

2 IoT security and privacy issues

2.1 IoT paradigm: architectural overview

IoT can be defined as the interconnected network of millions of heterogeneous devices with sensors, actuators, software, and network connectivity that capture and share data with various organizations such as: companies, governments, or even individuals. These devices are categorized by three characteristic features: limited computational capabilities, limited storage capabilities and limited processing capabilities.The huge growth in the use of IoT devices is mainly due to two factors which are: the decrease in the cost of processers and the wide availability of wireless connections.

While there is no proposed and agreed on IoT architecture, it is typically a multi layered model. Recently, researchers proposed four-layer or five-layer architecture for IoT system. Generally, the four layers are: the perception layer, the network layer, the processing layer, the

application layer. In [11], Those layers are described as follows:

Perception Layer is the layer where sensors are collecting a vast amount of data from the physical world. It may also contain actuators that can interfere in the physical reality and make changes without human interventions. Actuators can perform tasks like switching off the Air conditioning system. In addition to collecting data from things, it is responsible for successfully transmitting the data for further processing. Sensors would use either wired connection or a wireless connection to transmit the collected data.

Network Layer is where data that was collected in the perception layer is reliably transmitted to the next layer which is the processing layer through different networks whether they are wired or wireless. In this layer, network access gateways work with different communication technologies to perform the data transmission.

Processing Layer which can also be called the middleware layer is where enhanced analytics, fast data processing, and massive data storage is performed with the help of cloud computing, edge computing, and data centers.

Application Layer is where data and information are combined and presented to the end users in a user-friendly format in the form of applications. These applications are designed for specific user needs or industry needs. they interact with users and present users with solutions to specific problems. These applications can also interact with other applications.

The real life applications of IoT are numerous and continually growing. The rapid development of technologies supporting IoT, has led to the increase of its usage in our daily lives across various fields where IoT devices are used to control our lives, analyze our lives, or optimize our lives. Any object in our lives can or will be transformed to a smart sensor. IoT devices are being used on an individual level to live healthier or reduce personal electricity costs or on a city level where IoT devices can be used to monitor traffic or recycling patterns among citizens. IoT has been heavily used in healthcare, industries, transportation, smart homes, smart grids and much more.

2.2 IoT-related security and privacy challenges

There are basic security requirements in any IoT system that were defined in [12]. Those requirements are Confidentiality, Integrity, Availability, Authentication. These security concepts can be defined as follows:

Confidentiality ensuring that only authorized parties can view and access private information. Also, ensuring the privacy of information.An example of confidentiality compromised is a data breach that reveals private information to the public.

Integrity ensuring that the information hasn't been modified or corrupted by unauthorized parties.One of the attacks that can compromise integrity is Man in the middle attack when the victim is redirected to access a malicious website instead of legitimate website.

Availability ensuring that authorized parties can access information immediately when needed.Attacks like DoS attacks affect availability and make data inaccessible to authorized users.

Authentication verifying the identity of the parties requesting access to the information.Several factors can compromise authentication, like the use of weak passwords or reusing passwords which makes it easier for attackers to perform password cracking attacks. That's why standards that support passwordless authentication are increasing in popularity such as FIDO protocol [13]. Those components are essential to achieve in any system. However, there are multiple challenges [12] that arise when applying those components in an IoT system. Firstly, Ensuring the security of the entities in the IoT system must be done without greatly affecting the functionality of these entities. Also, as it was mentioned before, entities in the IoT system has limited storage, processing, and computational capabilities. Those limited capabilities limit the security measures that can be taken on these entities. Finally, some IoT systems like smart cities and smart grids contain a huge number of entities which process a vast amount of sensitive and private data. Any security measures taken must be scalable to cover this large number of entities which are a target for a great number of attacks.

As the number and variety of the entities in the IoT increases, the potential of security threats increases as well. These threats affect each layer in the architecture of IoT, compromising the security requirements of the affected layer.

In the perception layer, some of the main threats that face the IoT systems and their underlaying infrastructure are in the physical environment. Entities in the IoT system can be damaged or lost by nature forces (example: Hurricane, flood, etc.) or by environmental factors (example: humidity, wild animals, etc.) [12]. They can also by threatened by human factor; humans can damage the IoT system or even steal or misuse entities.

Moreover, the perception layer heavily depends on technologies like RFID, Bluetooth, and Zigbee. The use of these technologies put the perception layer in risk of the many attacks, some examples from [14] are listed below:

Node Capture a node that has been compromised therefor leading to confidential data leakage.

Fake Node a fake node can be added to the IoT system by the attacker compromising the system and opening way to malicious code injection attacks.

Denial of Service Attack this attack would exhaust resources and cause the unavailability of the services.

In the next layer, the network layer, some of the attacks that can be faced are [12]:

Jamming Attack a jamming attack significantly delays the nodes from communicating by occupying the communication channel. An example of jamming attack is a constant jamming attack. In a constant jamming attack, the attacker will emit a radio signal nonstop which stops the legal nodes from utilizing the communication channel. Another example of a jamming attack is a reactive jamming attack. In a reactive jamming attack, the attack stays in inactive mode until it senses that there is activity on the communication channel and starts emitting the radio signal then which makes it harder to detect than a constant jamming attack.

Selective Forwarding Attack in this attack, the attacker nodes will destroy the routing paths of the network by declining to transmit pieces of packets, some packets, or all packets.

Sinkhole/Wormhole Attack in the sinkhole attack the malicious node responds to routing requests causing traffic to go through the attacker node. In a wormhole attack, a tunnel is created between two nodes ignoring intermediate nodes. These two attacks cause the violation of privacy, eavesdropping, and denial of service.

Sybil Attack the malicious node will copy the identity of other nodes, or fake multiple identities to take control of network areas or to degrade the functionality of the IoT system. A malicious node that is copying the identity of another node might cause denial of service.

Traffic Analysis Attack this attack captures and analyses the traffic packets compromising the confidentiality of the information.

Man in the Middle Attack in this attack, the malicious node will eavesdrop on traffic between two nodes and possibly alter it.

In the processing layer, the main security risks are [12]:

Unauthorized Access This threat is caused by unauthorized access by attackers which allows illegal access to confidential information.

Malicious Insiders these can cause a confidentiality and privacy violation by accessing information while it's being transmitted to its destination.

Insecure Software Service the processing layer provides software services that can be infected by malware. This will risk all the security components in an IoT system.

Unknown Risk Profile services in the processing layer are offered by third parties with unknown risk profile.

Finally, at the application later where the users' needs are met, the main risks are [12]:

Social Engineering Attack is psychologically manipulating users and tricking them into revealing confidential and private information or unknowingly perform malicious actions. For example: phishing attacks.

Software Attacks these are attacks targe ting the software like: buffer overflow and backdoors.

3 Blockchain-based IoT system: overview

Blockchain technology is a new model towards decentralized storage and data management where it deploys shared, secure, and distributed ledgers among all parties to store records without third-party authority [15]. Blockchain infrastructure allows nodes or participants to exchange data through decentralized peer-to-peer (P2P) while maintaining transactions transparency and data integrity accordingly. Blockchain has been foreseen a disruptive technology for many industrial key players where they are currently expanding their products portfolio on top of it to offer more efficient services. In this section we present an overview of integrating blockchain to current IoT paradigm to address the main improvements blockchain augment to boost IoT security and privacy.

3.1 Background

The popularity of Bitcoin [16] lead the researchers to investigate the concept of blockchain technology that manages it and to explore its ability to leverage other domains beyond cryptocurrencies. It is fundamentally a decentralized, distributed, and immutable ledger that records transactions across P2P network. Data is committed in blocks that are chained securely using elliptic curve cryptography (ECC) and SHA-256 hashing to maintain data integrity and authenticity [17]. Each block has a list of all transactions and the hash of previous and next block as well. Consequently, blockchain is immutable against manipulation as per it cannot alter any already committed block but rather changes require to commit a new block on the blockchain network. This immutability develops a trusted network of users where errors or flaws can be backtracked to guarantee the security of users' assets and data. Transactions are validated across the network through a consensus mechanism that controls committing data into new blocks and to be linked in the blockchain network.

There are different blockchain platforms that can be categorized based on how nodes can join the network, what privileges each node is granted with, and what consortium is utilized to validate transactions across the network. The main three blockchain types are

3.1.1 Public blockchain

Public blockchain or permissionless blockchain is an open source platform that allows anyone to join the network anonymously and with no preconditions where each node has full privileges to validate, read, and write on the network as in Bitcoin [18]. Nodes or miners need to install the genesis block—the first block of the network -to be able to join the network and to have a replicate copy of the ledger. This redundancy ensures data integrity and eliminates data manipulation as well.

Miners validate transactions to be committed as a new block in the network through consensus mechanism that maintains consistency of blocks throughout the bloc-kchain network. For instance, proof-of-work (PoW) is the consensus mechanism used in Bitcoin and other public blockchain platform as Ethereum [19]. PoW works by broadcasting a mathematical puzzle that requires all nodes to solve and the node or miner that has the maximum computational power is the first one to solve the puzzle, commits a block, and rewarded with a Bitcoin added to his wallet accordingly [20].

In case adversaries try to control public blockchain they require to have 51% of the entire network's mining power. Additionally, transactions are secured using pairs of cryptographic keys; public and private keys where the hashed public key is used as the miner or node's address while the private key is used to sign transactions [21]. However, as per the high computational complexity involved in PoW, it would not be a suitable solution for some applications that require to operate on large volume of data as in the financial sector for instance.

Public blockchain has its own security risks and vulnerabilities especially its first use case—cryptocurrencies. For instance, in 2016 a hack into the Bitfinex exchange that caused a loss around $65 m [22]. This is probably due to the infancy blockchain code that is vulnerable to zero day attacks exploited by hackers. Another vulnerability is timejacking attack where adversary manipulates the network time counter through broadcasting inaccurate timestamp that might deceive connected nodes to accept alternate blocks [23].

3.1.2 Private blockchain

Permissioned or private blockchain is a decentralized network that allows exchanging data among designated nodes in specific organization. Any new node must be granted privileges to join and commit new blocks in the network previously. Hyperledger [24] is one of the famous private blockchain platform that utilizes PFBT [25] to validate transactions and to maintain its transparency. Private blockchain shifts towards centralization rather than decentralization in writing privileges where they are only granted for specific authorized nodes. Nevertheless, other properties private blockchain inherits as distributed ledger, consensus, and P2P communication network which would make it more convenient for critical financial fields to build their business model on top of it [26].

Private blockchain controls which nodes to operate in the network and how nodes are connected. Nodes are required to maintain certain number of connections to be considered active so that to receive information much faster [23]. However, the centralization characteristic in private blockchain hinders the ability to identify nodes that might deliberately restrict transmissions or transmit incorrect information. It is imperative for businesses to decide where to host their services taking into consideration the level of security risks they accept while maintaining their service proliferation and users' privacy and data security as well.

3.1.3 Consortium blockchain

Consortium blockchain is a semi or partially private blockchain where group of organizations or individuals are responsible for transactions validations and committing blocks. Each block is validated using a multi-signature scheme where all controlling nodes must approve and sign. They also delegate nodes to read or write on the network and they can revoke privileges at any time [27]. It provides the same benefits of private blockchain as in efficiency and transaction privacy, however; the power of controlling the network is not consolidated to single party. Consequently, consortium blockchain is more resilient against data tampering and transactions manipulation [28].

3.2 Blockchain security and privacy characteristics

Blockchain can leverage IoT applications to offer better services especially functionalities that require decentralized, secured, and trusted data sharing among all parties. Blockchain that utilizes smart contracts is expected immensely to revolutionize most of the IoT applications through securing IoT devices. Below we address major improvements imposed by integrating blockchain and IoT:

3.2.1 Decentralization

The decentralized nature of blockchain can overcome major centralized security issues in IoT applications as in single point of failure to guarantee the promptness of IoT services. Moreover, it offers a trusted governance, management, and tracking for the whole life cycle of IoT device such as factory, vendor, distributor, installer, owner,

and re-installer. Additionally, the decentralized and distributed ledger offers data redundancy in which all nodes are required to have a copy of the database and hence, data is immutable and reliable. Moreover, transactions can be validated in a trustless network where nodes are anonymous and their identities can be securely preserved.

3.2.2 Security and immutability

Blockchain utilizes 160-bit address space as hashed public key generated by ECDSA (Elliptic Curve Digital Signature Algorithm) to generate and allocate a huge number of addresses that can be considered secure and unique to assign IoT devices. Consequently, blockchain can be a scalable solution for IoT when compared to other addressing scheme as in IPv6 that offers 128-bit address space. With address uniqueness the blockchain offers, data transmitted across all IoT devices is cryptographically signed by true sender to ensure data security and authenticity. Moreover, transactions committed in the network cannot be altered and can be backtracked to guarantee data immutability and reliability.

Smart contract is one valuable feature that blockchain offers as in Ethereum to hard code rules that define privileges and access controls across nodes in the network. They can provide decentralized authentication logics that are less complex and hard coded into rules to effectively authorize IoT devices. It also maintains data security when configuring conditions and criteria under which certain nodes can access specific data. For instance, smart contracts can set rules on IoT software update or patch, change ownership, or establishment of a new keypair.

3.2.3 Identity

Ownership of IoT device might change during its life cycle which requires an efficient and secure identity management. Several attributes are related to IoT device as in manufacturer, GPS coordination, serial number, and type that all require secure and trustworthy management [29]. Blockchain can be foreseen as a promising solution to mitigate the above mentioned challenges in the whole life cycle of IoT devices. It can provide authorized and trustworthy identity management of connected IoT devices along with their complex attributes and relationships over a decentralized and distributed ledger. It can track the IoT device on every single point in its life cycle starting from manufacturer, supplier, and consumer.

3.3 Blockchain solutions for IoT security

3.3.1 Blockchain technology and its impacts on IoT

The evolution of Bitcoin blockchain platform has revolutionized the distributed ledger technology considering its substantial cryptographic security and immutability. Blockchain key benefits can overcome the challenge of secure data sharing between the heterogenous IoT devices to ensure the reliability of their data. There is a diverse number of blockchain platforms that can be an ideal solution for IoT systems that mostly operate on a centralized cloud network. It is imperative to address major differences between cloud and blockchain from security perspectives so that to highlight how IoT can leverage blockchain's key security features.

The most prominent difference between cloud and block-chain is the centralization or intermediary dependence. Cloud services are provided through a centralized control of a trusted party where it is prone to single point of failure that threatens data security, privacy, and availability. Moreover, cloud service provider must be trusted to avoid data manipulation where in some scenario cases cloud service provider can circumvent users' privacy and tamper their data without consent [30]. On the other hand, blockchain requires nodes to have a copy of the ledger that maintains the network states. Consequently, nodes that have tampered copy of the ledger will be rejected without disrupting the blockchain services as per there is no single point of failure. However, blockchain size increases intensely especially in IoT environments where data is collected from large number of sensors that creates a challenge for the constrained resources of IoT devices while storing and handling this huge volume of data. Consequently, this might affect the utilization of IoT devices as full nodes to validate transactions on blockchain network.

Moreover, cloud might be vulnerable to unconsented data sharing to unauthorized parties that evades users' privacy. Whereas, blockchain has the ability to empower its users to restrict access to their data through hard coding role-based access control in smart contracts. These smart contracts preserve users' data by encryption before committing a new block on the blockchain network. Additionally, encrypted data can only be decrypted by the user who owns the corresponding private key, hence, data can be stored and managed by all nodes without compromising its confidentiality [31].

However, blockchain technology has a prosper potential to address some of the current cloud services challenges. For instance, cloud exchange (CloudEX) has recently emerged to offer its customers with more convenient low

service prices and adaptable cloud services [31]. Nevertheless, CloudEX has number of security challenges that can be tackled when combined with blockchain technology. For example, CloudEX can attract hackers to tamper the reputation scores to illegally get revenue or they can simply sell users' private information in the market. Blockchain technology can be utilzed to maintain a pool of malicious IP addresses that are mapped to attackers, as a result,attackers will be blocked when detected.

Another security issue to data is to maintain its integrity where businesses need to upload their data into CloudEX before they publish the resources publicly. Consequently, users must have to trust central exchange not to tamper or steal their data. Blockchain technology can be deployed to address this problem through building a blockchain-based data access controls [32] to guarantee maintaining data access records permanently so that to ensure data integrity. Moreover, in [33] and [34] authors proposed a blockchain-based data sharing system to overcome access control challenges associated with sensitive data sharing in the cloud through leveraging blockchain's immutability and autonomity properties to verify users identities and cryptographic keys as well.

Since Bitcoin, many other blockchain platforms have been developed to offer different utility services other than cryptocurrencies such as Ethereum, IOTA [35], Hyperledger-Fabric [36]. When considering IoT ecosystem, it is imperative that the blockchain platform provides a hybrid network to validate participating nodes. For instance, in services offered for large smart cities, there are many stakeholders that are willing to contribute to the security of the public blockchain. On the other hand, smart home users need to validate their own transactions through a private network installed at their premises. Ethereum [19], is one platform that can provide this hybrid nature unlike Bitcoin and IOTA which offer public blockchain. On the other hand, IOTA and Hyperledger-Fabric offer fee-less transactions unlike Eth-ereum and they can solve blockchain's scalability issues when participating nodes are increasing.

Modern IoT systems require machine-to-machine (M2M) micropayment mechanisms while maintaining users' privacy and sensors' policies through smart contracts. IOTA has not implemented smart contracts unlike Ethereum and Hyperledger-Fabric. However, Hyperledger-Fabric is more suitable for IoT environment where it offers data confidentiality through creating private channels to restrict messaging between specific nodes and it also offers encrypting data values in chaincode [37]. Moreover, Hyperledger-Fabric offers transactions authorization and ID management that are essentials for IoT systems through a trusted certificate authority (CA). Additionally, Hyperledger-Fabric provides higher transactions throughput with over 3500 TPS (transaction per second) [36]. Consequently, Hyperledger-Fabric is better in performance than other blockchain platforms that is critical for IoT to guarantee its real-time and prompt responses.

3.4 Blockchain-based mechanisms for IoT security: literature review

In this section we provide a comprehensive overview for recent approaches that utilized blockchain to overcome IoT security and privacy issues from the literature. These approaches can be classified as follows:

3.4.1 IoT software update

In general, most of IoT devices are not perfect by design and have security weaknesses, hence; it is imperative to update these devices securely and patch their vulnerabilities while maintaining the privacy of involved users. Authors in [38] introduced a secure software update through BitTorrent as firmware sharing network on blockchain with a new block structure. Another layer of security added in [39] through integrating a special node in blockchain network to check the availability of software update and its validity so that only approved updates can be downloaded.

Incentive approach was utilized in [40] where a decentralized and incentivized delivery network used to update IoT devices while being rewarded by vendors. However, the previously mentioned mechanism was not considering users' privacy while updating IoT devices, unlike the approach utilized in [41] where a new blockchain based privacy-preserving software update was proposed to deliver secure software update while incentivizing node participants and protecting the privacy of involved users. They utilized proof-of-delivery consensus mechanism to validate software update using double authentication preventing signature (DAPS) [42] and outsourced attribute-based signature (OABS) [43] where they evaluated the time cost of OABS signature algorithm on both Dell laptop with 2.50 GHz CPU and Raspberry Pi 3B+ with 1.4 GHz CPU. It was found that when an IoT device has 20 attributes, the time cost was almost 0.077 s on the laptop and 1.61 s on the Raspberry Pi. Meanwhile, the total time cost in the protocol for an IoT device was 0.09 s and 1.72 s on the laptop and on the Raspberry Pi respectively.

3.4.2 Secure communication

Messaging protocol is an important factor for the development of IoT applications especially in industry where M2M communications require efficient and reliable channels to exchange data. Examples of emerging messaging protocols are MQTT, CoAP, and AMQP [44]. Blockchain

can be used as a reliable messaging protocol to offer secure communication between IoT devices. In [45] authors compared using MQTT and Ethereum blockchain in a simple use case scenario throu-gh simulating sniffing attacks on both protocols used. In their experiment, blockchain met the messaging requirements between IoT devices just as MQTT, meanwhile; blockchain was more resilient to sniffing attacks as per the avalanche effect of hashing function in block-chain network illustrated better performance. For instance, when deploying the ECDSA encryption algorithm with 4-bit change in input, 99% of output were changed which indicated a better security performance.

Complex encryption algorithms ensure data security and privacy, nevertheless; IoT limited computation resources constraints using standard cryptographic algorithms. In [46] authors introduced a light-weight cryptographic scheme for proof-of-authentication (PoAh) on blockchain where it replaced the existing consensus algorithms. PoAh allows the trusted nodes in the network to authenticate the blocks and add them into the distributed ledger through authenticating each block source and increment the trust value by one unit. Consequently, any miner that performs a false authentication will lose one unit from their trust value and will not be considered as a trust node. Their proposed approach can avoid inverse hash computations for secure and energy-efficient [47] communications in IoT system. Another similar approach proposed in [48] where a light-weight cryptographic key management scheme used in healthcare to overcome key management issues to secure patients' data. In their scheme, the healthcare blockchain network needs only to store clues for the encrypting keys generated inside the block itself. Consequently, the scheme demonstrated a significant performance improvement and it reduced storage cost as well. whereas in [49] a combination scheme of two protocol-based secure public service network (PSN) deployed; IEEE 802.15.6 to establish a secure communication channels between sensor nodes or mobile devices, and blockchain to share healthcare data across PSN. The proposed framework significantly reduced black hole and falsification attacks across connected node.

3.4.3 Scalability and optimization

Transactions throughput is a primary constraint for IoT applications to ensure the real-time responses. In [49] authors proposed a scheme to reduce the overhead of transaction's auditing through blockchain where a server creates off-chain logs of communication between parties. To audit blockchain transaction, nodes require to store block headers and Merkle tree of the block only.

Moreover, the CPU overhead is insignificant as per it requires to either perform a block signature or to verify a transaction every 10 min that adds virtually no overhead.However, one major drawback for the proposed approach is relying on a central server to manage logs and it is limited to applications that require its participants to store their logs on the blockchain and not other applications that need participants to verify the content of transactions.

Optimized and flexible memory were introduced in [50] to mitigate the significant increase of blockchain size in IoT applications. The proposed scheme enables users to remove their transactions from the network while maintaining the blockchain consistency. They proposed three different modes for memory optimization; temporary: certain transactions between IoT nodes are valid for a specified period of time where after this time it

will be removed from the blockchain network, permanent: transactions are stored permanently on the network, and summarizable: certain marked transactions are selected to be summarized in a ledger in a single designated summary block after they have been created and verified. The proposed work illustrated a significant improvements in cost, memory, and processing time. For instance, while deploying the summarizable mode, it was evaluated to 0.0046$, 98.2 Mb, and 6.8 min respectively. However, transactions auditability and applicability are limited as proposed in [49].

3.4.4 Security and protection

Research is growing producing solutions that depends solely on blockchain technology like In [51] where the authors proposed a framework based on blockchain technology. The framework is a lightweight IoT information sharing security framework to solve the problem of IoT information sharing security. The proposed framework adopts a double-chain model that combines data block-chain and transaction blockchain. The data block-chain is responsible for distributed storage of data and integrity of data. It uses consensus algorithm to form data blocks that protect data and its integrity. The transaction blockchain handles data registration efficiency, resource, and data transaction by using a distributed accounting system. The framework was found to be extremely resistant to six attacks such as: DoS, DDoS, and device injection attack. Moreover, the framework was found to be highly resistant and moderate resistant to attacks as modify attack and consensus cycle attack respectively. Also In [52], the paper introduced the concept of a blockchain proxy. This proxy can be used by an IoT entity to offload communication while still maintaining full control of all transactions committed to a shared ledger. The blockchain proxy will only require a slim SDK in the device that will hold its own

private key which may allow the IoT device to save a good amount of CPU time and communication bandwidth. The proxy could save 38% of CPU time when compared to a regular SDK where it was estimated to be 80 ms. Moreover, it reduced both data sent and received by 21% (11 KB) and 81% (17 KB) respectively.

Some researchers introduced solutions that combine block-chain with other technologies like [53, 54] where the authors proposed a Decentralized Security Architecture based on Software Defined Networking (SDN) coupled with a blockchain technology for IoT networks in smart cities. They considered smart cities which rely on three main technologies which are: SDN, blockchain, and fog and mobile edge computing. In their model, blockchain serves as a decentralized attack detection to mitigate the single point of failure problem that is common in centralized architectures. The authors proposed architecture focuses on Ethereum blockchain technology and the Mininet emulator.They have evaluated their model through comparing it with other architecture such as centralized cloud model and fog-based distributed model. For instance, their decentralized model detected the TCP flooding attack at 6 s and could block the suspicious traffic at 12 s, consequently; the attack was mitigated with a recovery time of approximately 6 s. Meanwhile, the recovery time for the same TCP flooding attack scenario on both centralized and distributed architecture were 10 s and 7 s respectively. Moreover, [55] proposed firmware management architecture using blockchain and Interplanetary File System (IPFS). The proposed solution uses blockchain to improve data integrity and provide distributed database with guaranteed reliability to the firmware provider and the firmware requestor. This solution will prevent data manipulation when information is transmitted and enable firmware version management through continuous communication between IoT devices and blockchain networks.

3.4.5 Access control

Centralized access control systems maintain data security through granting and revoking privileges to users overlooking a disadvantage of a single point of failure. However, blockchain technology can overcome this limitation through providing a decentralized access control manager to grant or revoke permissions to users in a heterogeneous IoT architectures. In [56] authors proposed an access control method utilizing blockchain technology to offer access policies to users who wish to share resources. They have validated the system in a scenario where users request information about traffic signals and traffic flows so that to help them find free slots to park their vehicles. In their model, there are two types of policies; the general policy: where it is stored on public blockchain network and created once a resource is allocated to a user. Usually, the general policy is designated to basic actions as reading permission. Meanwhile, the second type of policies are the special policy: where it is stored on a private blockchain and created when a user requests an action on a specific resource. Each user has a pair of public and private keys where both are required to access data on the private blockchain, and hence, it adds an extra layer or security and data protection. A similar model was proposed in [57] where they offered to store all types of policies in a public blockchain which is less secure when compared to model proposed in [56]. Moreover, any modifications on policies in [57] requires manual intervention as per they have been published and created permanently on the blockchain and any new modification must be created and committed on the blockchain as a new block, unlike [56] where owners can update policies through a smart contract that requires only to store the URL of the policy on the blockchain.

Another approach utilized blockchain technology to offer FairAccess model to guarantee IoT security and privacy needs [58, 59]. Authors introduced a new type of transactions to grant, revoke, or delegate access where each node in the network can share data without intermediaries and smart contracts can guarantee a fine-granularity while implementing granular access control policies. For instance, a requester device A (with address rq) wants to execute an action on a specific object resource B (with address rs), A device must first send this request to Authorization Management Point (AMP wallet) that is designated to protect object resource B. Then AMP issues a new transaction (GetAccess transaction) and broadcasts it to the network so that other objects validate the request. A smart contract is triggered to validate the broadcasted transaction so that to either grant the access or revoke it. If access is granted, the smart contract will send device A (the requester) a grant token and a new transaction with allow access permission will be committed on the blockchain network. However, the model suggested in [58] has more number of transactions when compared to the model proposed in [56] that would reduce the traffic in the network and improve its efficiency. Meanwhile, in [60] authors offered a fair access control method as described in [58] but they also suggested to combine it with machine learning on a distributed block-chain network for heterogeneous IoT systems. Their model utilized the Reinforcement Learning (RL) algorithms to train smart devices to make better decisions through sending feedbacks after each successful or unsuccessful access transaction to both the requester object (device A) and the object resource (B). Hence, the smart contract will learn from its past experience to offer better business-related decisions, and the process of updating access control policies will be dynamic and decentralized accordingly.

3.4.6 Consensus algorithms

Consensus algorithms are crucial for ensuring integrity and security of blockchain network. They provide reliable means by which distributed nodes reach consensus on which blockchain network version is valid. The most common implementations of consensus algorithms are Pow and PoS. However, these algorithms are not suitable for efficient IoT systems where they require extensive computational power to validate blocks and consume significant bandwidth overhead. Consequently, researchers are introducing other scalable and IoT-centric consensus mechanisms. In [61], authors introduced AlgoRand algorithm that is based on Byzantine agreement where miners reach consensus in one round where next block is selected randomly by a miner and then it is propagated to the network. Each miner votes for one block and the block with more votes is chosen as the next block in the blockchain network. However, their approach might consume a significant network bandwidth as the number of IoT miners are huge.For instance, the latency for 500,000 users was 4X higher than 50,000 users owing to the bandwidth bottleneck.

A similar approach proposed in [62] where a reputation-based algorithm is utilized to reach consensus through considering the reputation of each node. More reputable nodes have a greater chance to commit a new block. To determine the reputation of each node, a group of nodes is created and a group leader is chosen randomly who is responsible for mining the next block. The process of forming group and voting for a group leader might also increase the packet overhead as in [61] especially in IoT systems. Their model could reach consensus in about 0.5–1.2 s when considering blocks of size 4MB.

Meanwhile, a lightweight scalable blockchain (LSB) is proposed in [63] by forming an overlay network where high resource devices in IoT systems can jointly manage the network. Distinct clusters are used to manage the blockchain network and to reduce overheads. They proposed Time-based Consensus Algorithm to reduce mining processing delay and to ensure that the blockchain throughput would not deviate from the increasing transaction load in the network. However, they evaluated end-to-end delay incurred by their model and other baseline methods, and found that it was around 17.62 ms for baseline and 48.74 ms for their model where the higher delay attributed to broadcasting transactions for other (overlay block manager) OBMs for verification.

3.5 Blockchain and machine learning: applications and future integration

Blockchain and Artificial Intelligence (AI) are both able to affect and enact upon data in several ways where the integration of machine learning techniques and AI into blockchain, or vice versa, would improve the underlying architecture of blockchain and boost AI's potential aswell. In this section we compare between both technologies from security applications perspective as Intrusion Detection Systems (IDS) and discuss potential integration of both technologies in the literature.

3.5.1 Machine learning-based and blockchain-based techniques in intrusion detection systems

Machine learning has been implemented in different areas to enhance the performance of existing systems such as in IDS. To counter the limitations faced by IDS nowadays like the high rate of false positives and low detection rate of serious attacks, authors in [64] have proposed an IDS model based on Extreme Learning Machine (ELM) that is enhanced by the use of Particle Swam Optimization Algorithm (PSO). PSO is a computational method that can be used for optimization. ELM is a feedforward neural network that can be used for multiple purposes such as: classification or regression. The layers in ELM consist of hidden nodes that do not need to be tuned. The authors optimized ELM using PSO to select the major parameters to enhance the performance of ELM and apply it in IDS model. The authors presented findings that show that the ELM improved model with PSO has more accuracy than the basic ELM.

Moreover, in [65, 66] authors present detailed work and suggestions for an IDS for connected devices in smart cities to counter the possible attacks that target those connected vehicles cloud environments. This paper details a vehicular node clustering mechanism that provides trusted and exclusive communication between service providers, cluster-heads and trusted third party entities. The IDS mechanism discussed in the paper is a hybrid solution that is titled D2H-IDS, it combines Deep Belief Network for data dimensionality reduction and ID3-based Decision trees for attacks classification. The IDS mechanism depends on three phases and is integrated in the cluster heads, trusted third parties and service providers. The papers evaluate the presented solution through performing 10 simulations that prove high accuracy rate up to 99.43% and high detection rate that reaches up to 99.92%. The simulations also show low false positive and false negative rates.

Additionally, authors in [67] used restricted Boltzmann machine (RBM) with support vector machine (SVM) and deep belief network (DBN) and applied those two hybrid algorithms on a provided data set. The purpose of their work is to study the characteristics and performance of applying deep learning in Intelligent IDS. The results are used to analyze different rates such as: the accuracy rate, the false positive rate, the false negative rate. The authors present their experiments results that confirm that the use of unsupervised learning algorithms such as RBM and DBN enhances the accuracy and rates in intelligent IDS. The experiment result show that RBM and DBN are suitable to use with large data sets such as the one resulting from Intelligent Intrusion Detection Systems. Another research that suggests enhancing the performance of IDS in wireless sensor networks (WSNs) with the use of machine learning and deep learning in [68]. The authors present a feasibility assessment of Restricted Boltzmann machine-based clustered IDS (RBC-IDS) which implements deep learning. The model presented shows a high detection ratio that reaches up to almost 99.12% and an accuracy rate of almost 99.91%.

Finally, NSL-KDD Data set was used in [69] and [70] to test presented models. In their proposed approach, authors in [69] apply machine learning in IDS and compare between Support Vector Machine (SVM) and Naïve Bayes to analyze their performance in solving classification problems. This is critical in enhancing the performance of IDS that require analyzing a massive amount of traffic data. The experiment results prove that SVM beats Naïve Bayes in accuracy and has a lower misclassification rate. While in [70]. The authors analyze various machine learning models and algorithms in addition to several feature selection methods to find the best model in detecting malicious network traffic. Experiment presented in [70] shows that Artificial Neural Network in addition to wrapper feature selection had the best performance and achieved a rate of 94.02% in detecting only known malicious network traffic.

In addition to machine learning and deep learning, block-chain has also been implemented to enhance the performance of IDS such as in [71] where authors presented a possible architecture for a signature based Collaborative Intrusion Detection Systems (CIDS) enhanced by the use Blockchain technology. The introduction of Blockchain in the signature based CIDS will help solve existing issues in CIDS such as: trust management and consensus building and enable signature sharing, creation between the hosts in CIDS.

Furthermore, [72] proposed a framework for blockchain networks to enable distributed community detection based on the Propose-Select-Adjust framework (PSA). The presented structural entropy-based PSA algorithm works in asynchronous runs and applies a local structural entropy which allows detection of communities by evaluating the information available in a sub network. Experiments conducted by the authors show the success of the algorithm in detecting community structures within dynamic Bitcoin trust networks. Lastly, various attacks are being targeted towards bitcoin exchange because of the decentralized nature of the transactions performed using bitcoin and the popularity of bitcoin exchange. These attacks are circumventing traditional IDS. In [73] author proposes a method that provides real-time protection for bitcoin-blockchain by using the replace by fee (RBF) transaction feature in bitcoin to eliminate malicious transactions and in this way complementing existing detection and mitigation methods.

3.5.2 Machine learning and blockchain integration

Machine learning requires to collect data in a central server so that to process them and cultivate better business decisions. However, applications may generate a large scale of data from various parties that can be geographically distributed. Deploying a central server to collect such substantial amounts of data would cause a significant traffic overhead and would circumvent data privacy and security accordingly.

In [74] authors introduced LearningChain—a decentralized privacy-preserving machine learning system on blockchain. They designed a decentralized Stochastic Gradient Descent (SGD) algorithm to work as a predictive model to formulate a differential privacy-based schemes to maintain user's data privacy and to proactively protect the system from Byzantine attakcs through *l*-nearest aggregation algorithm. Their model was built on top of Ethereum blockchain. The LearningChain consists of three processes: *blockchain initialization*: where both data holders and computing nodes establish connections and reach the consensus on the learning model; *local gradient computation*: data holders initiate the pseudo-identities, deploy a differential privacy scheme, and then broadcast messages to all the computing nodes in the network; and *global gradient aggregation*: computing nodes start to mine or commit new blocks through solving a mathematical puzzle. The node that wins will apply a Byzantine attack tolerant aggregation in the memory pool and update the model parameters. To evaluate the efficiency of their proposed model, they have used three different datasets; Syntheic, Wisconsin breast cancer dataset [75], and MNIST [76] dataset. Results were compared with a model trained in a centralized mode where it collects all data on one computing server and trains the learning model using multi-Krum [77] algorithms without any privacy or security controls. For instance, when only 10% of data holders were Byzantine attackers, both their model and the baseline model had similar performance (test error rate less than 0.2

%), while when Byzantine data holders increased to 40%, their model achieved a lower error rate (0.21%) and the baseline model achieved 0.29% error rate and hence, their proposed *l*-nearest aggregation scheme utilized in LearnChain is more efficient and effictive.

Machine learning algorithms can boost blockchain security when deployed in a decentralized, peer-to-peer network architectures as illustrated in [74], moreover, machine learning can also overcome some of the blockchain's limitations as the double spending or majority attacks that took place in the Bitcoin. In [78] authors proposed utilizing Algorithmic Game Theory combined with supervised machine learning algorithms to reduce collusions in the blockchain to overcome the majority attack where attacker miners control 51% of the network's computational power through submitting multiple transactions to overwhelm the network and causes the network to stop mining new blocks. Meanwhile, attackers privately mine a blockchain fork and later

releases the fork to regain tokens/coins. In order to overcome this attack, they proposed to design an intelligent agent in the application layer of the blockchain network that checks every transaction sent to the network for verification. This agent utilizes the supervised machine learning algorithms that take input from a function of Algorithmic Game Theory to classify whether this transaction is fair or not and if it will cause an attack to take place or not. Consequently, it prevents the transaction confirmation that would stop mining a new block to generate a token/coin as a reward consequently.

On the other hand, blockchain can be utilized to enhance machine learning process through creating an open source of machine learning models that can be utilized in several experiments and framweworks. For instance, in [79] authors introduced WekaCoin - a block-chain-based token that mimics Bitcoin but it uses the proof-of-learning consensus mechanism instead of PoW utilized in Bitcoin. The proposed model has WekaCoin nodes that communicate in a peer-to-peer network where two types of nodes have been introduced; trainers that submit machine learning models for tasks committed previously by other nodes in the network known as suppliers. The validation process of such models is conducted by random nodes in the network so that to rank the models and to reward trainer nodes with WekCoin accordingly. Proof-of-learning consensus can help in storing machine learning models and experiments in a distributed ledger that can be used as an open repository for other future experiments on machine learning.

Both blockchain technology and machine learning can be combined not only to enhance each other's security features, but they can also harness the security of IoT architectures. With the significant amount of data generated by IoT devices in real-time applications, deep learning can be a key pillar to support efficient data analysis that can avoid single point of failure and data leakage of IoT devices when combined with blockchain technology. In [80] authors introduced BlockDeepNet—a blockchain-based secure deep learning technique to overcome IoT privacy leakage problem where deep learning works as an efficient data analysis agent and blockchain ensures the confidentiality and integrity of the collected data. They suggested a reconfigured IoT network where a designated device and edge layer are proposed. Each IoT device is configured with blockchain application and deep learning model while the edge server is configured with collaborative deep learning and blockchain mining tasks. IoT devices communicate with the edge server through private blockchain to conduct a collaborative and secure deep learning tasks. They evaluated their model through conducting an experiment where two architectures have been developed; one with BlockDeepNet layer and one without this layer. They used the PASCAL VOC dataset [81] to perform an object detection task for 10 Raspberry Pis. Though their model could overcome single point of failure, privacy leak, and insufficient trainind data problems; nevertheless, it demonstrated an additional computation overhead due to blocks mining and collaborative deep learning where it added additional 40% of CPU utilization and 68% memory utilization when compared to the architecture without the BlockDeepNet layer.

4 Blockchain-based IoT paradigm: security and privacy issues

The heterogenous interconnected IoT devices through blockchain networks might be susceptible to security and privacy issues that must be addressed as per they can hinder the quality of services provided by the IoT systems. Some of the most important security and privacy issues are discussed below:

4.1 Lack of IoT-centric consensus mechanisms

All consensus protocols currently deployed in different blockchain platforms share a common issue in which the consensus process is probabilistic and not final. The lack of consensus finality while permanently committing new blocks might result in delayed transactions confirmation and hence, it is not suitable for the instantaneous IoT systems [82]. Several aspects are required to be improved in blockchain consensus protocols to be integrated in IoT applications such as increasing the fault tolerance, resistance to denial of service attack, and low communication complexity.

4.2 Transaction validation controls

Usually, transaction validation rules include correct transaction format, signature, and other parameters depending on blockchain platform. For instance, in Bitcoin, transaction validation rules also include that the same transaction has been spent before, and in Ethereum, other rules are included such as nonce and checking the balance of sender's account. However, in IoT systems there are plenty of heterogeneous IoT devices that are feeding different format of sensory data to blockchain network. Consequently, other validation rules must be created to meet the heterogeneity of sensed data [83].

4.3 IoT device integration

One aspect of integrating IoT device to blockchain network is the integrity of data sent from an IoT device. The blockchain network is only useful to maintain an immutable distributed ledger, however, data sensed from IoT devices can be compromised through a malicious code execution or corrupted by human errors. Moreover, IoT device requires a third part library web3.js as an interface to communicate sensor data to the blockchain network that might be vulnerable to several attacks as in SQL and XSS attacks. Consequently, it is important to check the authentication of data and to provide a proof that it has not been changed when collected from the source IoT device.

4.4 Software update

Considering a ransomware attack hitting an IoT system, this will encrypt all data including the operating system firmware files. To mitigate such a problem, we need to initiate a firmware update during runtime to ensure that all IoT devices are updated and immune to these attacks. However, due to the decentralization in blockchain it is difficult to synchronize firmware software update procedure during runtime. Consequently, most IoT devices operate without software update and might be more vulnerable to several attacks accordingly.

4.5 Data scalability and management

One key issue of blockchain is the orchestration of distributed ledgers or databases that are growing rapidly due to the massive volume of data collected from a wide range of interconnected IoT devices. Without proper security controls the heterogeneity of IoT devices might cause compatibility issues that would result in severe security issues accordingly. For instance, a poorly designed security software might provide a backdoor for malware injection attack [84].

4.6 Network performance

IoT systems require to offer real-time services and deliver prompt responses to guarantee the proliferation of its applications. It is imperative to consider blockchain network speed in terms of throughput that defines number of transactions that can be validated in a second and the size of each committed block in blockchain network. However, modern IoT systems require to use micropayments for monetary transactions as in Bitcoin or Ether where they utilize the PoW consensus mechanism that consumes lots of time and power to validate transactions [85].

4.7 Interoperability

With the diverse IoT devices interconnected on blockchain network, interoperability is one major problem that is due to lack of standardization or compatibility between heterogenous IoT device. In this modern ecosystem, there is a crucial need to manage information, machine and user data, financial data, and analytical data shared across incompatible IoT devices [86].

4.8 User experience

Most applications built on top of blockchain requires the end user to manage their own transactions through e-payment methods instead of delegating the process to a middle man. It requires end users to check their wallet balances to validate transactions that might make user experience more difficult and they will not appreciate the advantages of using blockchain [87]. Another prominent issue is the computational power users must acquire to be able to mine or commit new blocks. Moreover, blockchain network might be cumbersome to log transactions due to the complexity of decentralization.

5 Secure and efficient blockchain-based IoT paradigm

IoT devices increase the convenience in people's lives, but in the same time their applications raise many security and trust challenges. The heterogenous IoT devices require a mechanism to maintain security for both smart IoT devices and participants' personal data.In this section we provide a comparitive analysis of the general security requirements that are crucial in IoT devices and whether blockchain's features provided in the literature can be utilized to meet these requirements or not. The objective is to evaluate the

efficiency of integrating blockchain technology into IoT system to boost its security and privacy. Then, we propose a framework towards more efficient and secure blockchain and IoT integration in each layer of the IoT system architecture layers.

Table 1 summarizes the view of the general requirements where the mark (✓) indicates that the referenced approach provides the requirements and the mark (X) indicates the opposite. The idea is to present a comparitive analysis to evaluate blockchain efficiency

to boost the security and privacy of IoT systems where we highlight the main security requirements that are crucial to maintain in IoT systems and focus on some of the blockchain approaches provided in the literature to show whether security and privacy requirements are met in the referenced approach or not.

Real-time database synchronization is essential in IoT systems while being updated. Consequently, it is imperative to maintain the database consistency throughout the life cycle of data, and to guanrantee its integrity, confidentiality, and availability. As depicted in Table 1, most of the proposed approaches in the literature met integrity and confidentiality requirements while some other approaches failed to meet availability of required information or devices to the authorized users. Consequently, it is important to enforce secure deployment of both logical and physical infrastructure through security algorithms running on clouds or fog networks rather than depending on deploying them on a blockchain network. Additional requirement is to authenticate credentials of users to provide access to a file through comparing it within credentials provided in the database. Some approaches suggested to define new protocols and standards such as anonymous authentication [89], password-based [91], certificate-based [93], and identity-based cryptography and signature schemes [94].

Moreover, database immutability, users anonymity, and transaction nonrepudiation are all enforced in most of the referenced approaches as per the blockchain technology utilized leveraged its security features to meet these requirements. For instance, in [90] authors suggested to utilize Proof-of-Identity (POI) and Proof-of-Posession (POP) to secure user's identity where POP was integrated in the transaction's certificates through an efficient symmentric cryptographic algorithms in order to hide devices from being accessed by unauthorized users. Moreover, a non-transferrable proof-of-ownership was also enforced in their transactiob certificates. Meanwhile, in [89] authors proposed to use proof-of-concept where its role is to describe specific processes with a group of objectives mapped to certin participants' roles. Consequently, this would signify the autonomous verification of users with integration of a cloud-based environment where the cloud service provider can act as a miner and can earn gas. However, in [88] authors used proof-of work (POW) where new blocks are added by users and they were rewarded by coins in the Bitcoin blockchain. Further, they also suggested using a local immutable ledger and an overlay blockchain to avoid mining process as well. In [94], authors propose Secure Fog-based Platform (SeFoP) which is a novel platform. One of its components is a security toolbox that preserves the integrity, security and privacy of SCADA based IoT critical infrastructure at the fog layer. It provides an identity-based cryptography and identity-based signature schemes approach to the cloud services. The security toolbox in the SeFoP is hosted between the IoT nodes and the fog layer. It handles all requested coming from the IoT devices and authenticates those requests, encrypts them, and assigns cryptographic keys (eliminating the need for trusted external parties). Additionally, it encrypts and decrypts any services offered by the fog layer.

Cryptography and hashing are usually adopted in general blockchain approaches, nevertheless; some researches suggested to adopt additional data and communication security where hashing and pairs of public and private keys are no longer sufficient to maintain applications security. For instance, in [88] a lightweight blockchain was suggested to provide essential security and privacy

Table 1 Comparitive analysis between IoT security requirements and blockchain utilization in the literature

Security requirements	Approach [88]	[89]	[90]	[91]	[92]	[93]
Integrity	✓	✓	✓	✓	✓	✓
Confidentiality	✓	X	✓	✓	✓	✓
Availability	✓	X	X	✓	X	✓
Authentication	✓	✓	✓	✓	X	✓
Anonymity	✓	✓	✓	✓	X	✓
Immutability	✓	✓	✓	✓	✓	✓
Access control	X	X	✓	✓	✓	X
Privacy	✓	✓	✓	X	✓	✓
Nonrepudiation	✓	✓	✓	✓	✓	✓

requirements. They utilized a simple generic Bitcoin blockchain, a local immutable ledger, and an overlay netowrk where a symmetric encryption was utilized to reduce process overhead. Meanwhile, in [91] authors used 4 protocols in their Data Integirty as a Service (DIaaS) framwork integrated with the cryptographic process. Protocol 1 was designed to verify the data integrity where data owner application (DOA) aims to verify the data stored in the cloud storage that supports the cryptographic functionalities, while protocol 2 was designed to verfiy data integrity where DOA aims to verfity data stored in the cloud storage but does not support cryptographic functionalities. However, protocol 3 and 4 were designed to enable the integrity of data in scenario where data customer application (DCA) aims to verify the data integiryt that is owned by DOA and stored in the cloud storage servic that either support cryptographic functionalities or do not support.

Another approach referenced to ensure security and privacy is by making the transactions more robust against the trustless parties through encrypting the blockchain document with SHA256 [93] under the platform Pyethereum and employed in the network through implementing serpent programming in smart contracts. Meanwhile in [90] a parallel hashing was used in a permissioned blockchain to improve the robustness of user's identity against frauds. The hash based message authentication code (HMAC) ciphertexts were utilized to reduce the exploitable bias and were stored off-chain and can be referenced by their hashes on the blockchain network after a request by authorized users only. Finally, in [89] authors introduced a layered security framework where proper identity management and public key infrastructure were used to secure session establishment through utilizing a certificate X.509.

With reference to IoT architecture mentioned in Sect. 2 and the discussion mentioned in this section, we propose a framework towards more efficient and secure blockchain and IoT integration through utilizing conventional IoT-centric security controls combined with blockchain technology (Fig. 1). It is imperative to consider blockchain technology to overcome some of the current IoT systems security problems while considering other conventonal centric security countermeasures to boost IoT security and privacy.

5.1 Perception layer

The most related challenges to perception layer are devices with low storage capacity, DoS, and object theft. Blockchain technology can tackle these issues through a distributed ledger to maintain a unique ID for each IoT device. A new device can only join the network if it is granted with permission from network minor who is required to solve a puzzle so that to validate the new device (proof-of-identity-PoI). Consequently, data generated from the connected IoT devices is encrypted, a designated public and private key is assigned, and then pushed to the blockchain network.

5.2 Network layer

Once the IoT device is connected to the network it can start transmitting its encrypted data through committing blocks. Two key pillars must be maintained; an efficient network connection so that to avoid any block loss, and a stable and reliable connection as well. The distributed ledger can address these two requirements through maintaining the ledger on each participant system and each object has its own privileges assigned when joining the network.

5.3 Processing layer

A combination of private and public blockchain network is suggested to manage the storage of IoT systems instead of storing data on a centralized cloud infrastructure. Public blockchain is utilized to record transactions using timestamp and hence, this would ensure data immutability, non-repudiation, data integrity and authenticity. On the other hand, private or permissioned blockchain can be used to securely store sensitive personal information and hence, empowers users to control access to their data through validation. Additionally, blockchain can serve as a secure communication layer when a request is made to share user's private information with a trusted third party for analytics. In this case, user can grant permission to access his data saved on the permissioned blockchain and once the request is validated, encrypted data can be shared securely.

5.4 Application layer

This layer is responsible for data retrieval and visualization where data is assumed to be authentic upon retrieval from the storage or processing layer. Data retrieval requests are made by end users to get responses to their various types of queries. As discussed above, the node must be verified and its read and write permissions are granted before becoming part of the blockchain network. Next, data stored on the blockchain network can be accessed securely for analytics and real-time responses. Meanwhile, no servers are required to visualize big data-bases for analytics as per the blockchain network is utilized and all authentic IoT devices joined the network can easily feed data for visualization.

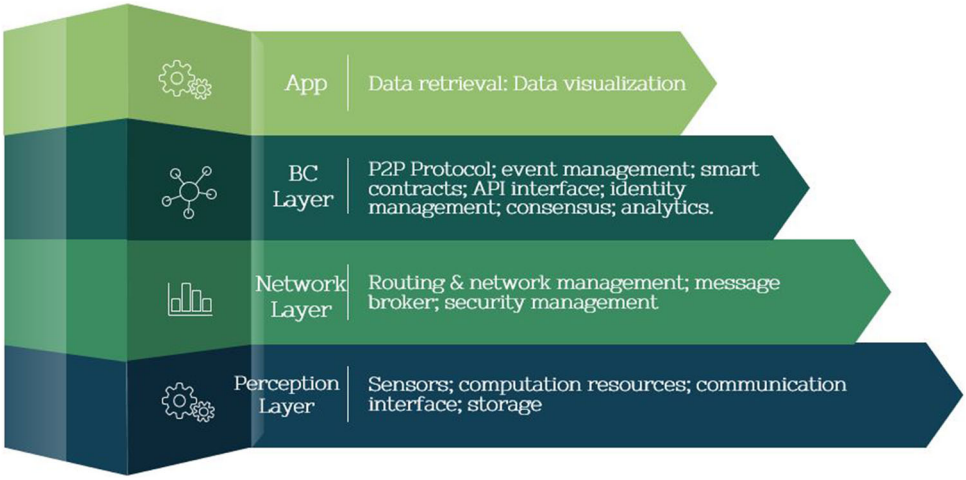

Fig. 1 Proposed Blockchain-based IoT Framework

6 Conclusion

Along with the pervasive growth in technology there might be some critical security and applicability issues while integrating blockchain in IoT systems. Therefore, this research paper analyzes IoT security requirements based on its 4-tier architecture to identify possible security and privacy vulnerabilities and to mitigate such risks through adopting blockchain technology. Moreover, the research paper highlights new security challenges imposed while adopting blockchain in IoT systems that are most predominant and require to stir the research focus on its solutions. The proposed framework draws our recommendations for efficient and secure integration of blockchain and IoT to guarantee the proliferation of its services.

Acknowledgements This research is supported by Zayed University cluster research award R19046.

References

1. Kumar, N.M., Mallick, P.K.: Blockchain technology for security issues and challenges in IoT. Procedia Comput. Sci. **132**, 1815–1823 (2018)
2. Hung, M.: Leading the IoT, gartner insights on how to lead in a connected world. https://www.securityweek.com/mirai-based-botnet-launches-massive-ddos-attack-streaming-service (2017). Accessed Sept 2019
3. Lewis, T., Liwen, W., Safa, O., Moayad, A., Jalel Ben, O.: Blockchain for managing heterogeneous internet of things: a perspective architecture. IEEE Netw. **34**(1), 16–23 (2020)
4. Ali, F., Aloqaily, M., Alfandi, O., Ozkasap, O.: Cyberphysical blockchain-enabled peer-to-peer energy trading. In: Computer IEEE (2020)
5. Aloqaily, M., Boukerche, A., Bouachir, O., Khalid, F., Jangsher, S.: An energy trade framework using smart contracts: verview and challenges. IEEE Netw. 1–7 (2020)
6. Hassan, W.H.: Current research on internet of things (IoT) security: a survey. Comput. Netw. **148**, 283–294 (2019)
7. Kushner, D.: The real story of stuxnet. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (2013). Accessed Sept 2019
8. Arghire, I.: Mirai-based botnet launches massive DDOS attack on streaming service. (2019). Accessed Sept 2019
9. Subramanian, H.: Decentralized blockchain-based electronic marketplaces. Commun. ACM **61**(1), 78–84 (2018)
10. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016)
11. Lee, I.: The internet of things for enterprises: an ecosystem, architecture, and IoT service business model. Internet Things **7**, 100078 (2019)
12. Radoglou Grammatikis, P., Sarigiannidis, P., Moscholios, I.: Securing the internet of things: challenges, threats and solutions. Internet Things **5**, 41–70 (2019)
13. FIDO Alliance. How fido works. https://fidoalliance.org/how-fido-works/. Accessed Feb 2020
14. Tewari, A., Gupta, B.: Security, privacy and trust of different layers in internet-of-things (IOTS) framework. Future Gener. Comput. Syst. (2018)
15. Salman, T., Zolanvari, M., Erbad, A., Jain, R., Samaka, M.: Security services using blockchains: a state of the art survey. IEEE Commun. Surv. Tutor. **21**(1), 850–880 (2019)
16. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf (2008). Accessed Sept 2019
17. Antonopoulos, A.M.: Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media Inc., New York (2014)
18. Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. **18**(3), 2084–2123 (2016)
19. Ethereum blockchain app platform. www.ethereum.org/ (2017). Accessed Sept 2019
20. Bitcoinwiki. Proof of work. Accessed Sept 2019

21. Khalilov, M.C.K., Levi, A.: A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Commun. Surv. Tutor. (2018)
22. Baraniuk, C.: Bitfinex users to share 36% of bitcoin losses after hack. BBC News. https://www.bbc.com/news/technology-37009319 (2019). Accessed Oct 2019
23. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., Mohaisen, A.: Exploring the attack surface of blockchain: a systematic overview. arXiv preprint arXiv:1904.03487 (2019)
24. Hyperledger. https://www.hyperledger.org (2017). Accessed Oct 2019
25. Castro, M., Liskov, B.: Practical byzantine fault tolerance. Osdi. OSDI **99**, 173–186 (1999)
26. Sachs, G.: Blockchain' putting theory into practice. the-blockchain.com, pp. 25–32 (2016)
27. Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., Wang, Z.: Consortium blockchainbased malware detection in mobile devices. IEEE Access **6**, 12118–12128 (2018)
28. Zhang, A., Lin, X.: Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. J. Med. Syst. **42**(8), 140 (2018)
29. Tao, F., Wang, Y., Zuo, Y., Yang, H., Zhang, M.: Internet of things in product life-cycle energy management. J. Ind. Inf. Integr. **1**, 26–39 (2016)
30. Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., Sassone, V.: Blockchain-based database to ensure data integrity in cloud computing environment. (2017)
31. Xie, S., Zheng, Z., Chen, W., Wu, J., Dai, H.N., Imran, M.: Blockchain for cloud exchange: a survey. Comput. Electr. Eng. **81**, 106526 (2020)
32. Zyskind, G., Nathan, O., Pentland, A.: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE security and privacy workshops, pp. 180–184 (2015)
33. Xia, Q., Sifah, E.B., Smahi, A., Amofa, S., Zhang, X.: BBDS: blockchain-based data sharing for electronic medical records in cloud environments. Information **8**(2), 44 (2017)
34. Peterson, K., Deeduvan, R., Kanjamala, P., Boles, K.: A blockchain-based approach to health information exchange networks. Proc. NIST Workshop Blockchain Healthc. **1**, 1–10 (2016)
35. Popov, S.: The tangle, iota whitepaper
36. Valenta, M., Sandner, P.: Comparison of ethereum, hyperledger fabric and corda. ebook Frankfurt School, Blockchain Center (2017)
37. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Muralidharan, S.: Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Thirteenth EuroSys Conference, ACM, p. 30 (2018)
38. Lee, B., Lee, J.H.: Blockchain-based secure firmware update for embedded devices in an internet of things environment. J. Supercomput. **73**(3), 1152–1167 (2017)
39. Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., Sirdey, R:. Towards better availability and accountability for IoT updates by means of a blockchain. In: IEEE European Symposium on Security and Privacy Workshops (EuroS and PW), pp. 50–58 (2017)
40. Leiba, O., Yitzchak, Y., Bitton, R., Nadler, A., Shabtai, A.: Incentivized delivery network of IoT software updates based on trustless proof-of-distribution. In: IEEE European Symposium on Security and Privacy Workshops (EuroS and PW), pp. 29–39 (2018)
41. Zhao, Y., Liu, Y., Tian, A., Yu, Y., Du, X.: Blockchain based privacy-preserving software updates with proof-of-delivery for internet of things. J. Parallel Distrib. Comput. **132**, 141–149 (2019)
42. Ruffing, T., Kate, A., Schröder, D.: Liar, liar, coins on fire!: penalizing equivocation by loss of bitcoins. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 219–230 (2015)
43. Chen, X., Li, J., Huang, X., et al.: Secure outsourced attribute-based signatures. IEEE Trans. Parallel Distrib. Syst. **25**(12), 3285–3294 (2014)
44. Naik, N.: Choice of effective messaging protocols for IoT systems: MQTT, COAP, AMQP and HTTP. In: 2017 IEEE International Systems Engineering Symposium (ISSE), pp. 1–7 (2017)
45. Fakhri, D., Mutijarsa, K.: Secure IoT communication using blockchain technology. In: 2018 International Symposium on Electronics and Smart Devices (ISESD), pp. 1–6 (2018)
46. Puthal, D., Mohanty, S.P.: Proof of authentication: IoT-friendly blockchains. IEEE Potentials **38**(1), 26–29 (2019)
47. Al Ridhawi, I., Aloqaily, M., Boukerche, A.: Comparing fog solutions for energy efficiency in wireless networks: challenges and opportunities. IEEE Wirel. Commun. **26**(6), 80–86 (2019)
48. Zhao, H., Bai, P., Peng, Y., Xu, R.: Efficient key management scheme for health blockchain. CAAI Trans. Intell. Technol. **3**(2), 114–118 (2019)
49. Tomescu, A., Devadas, S.: Catena: Efficient non-equivocation via bitcoin. In: 2017 38th IEEE Symposium on Security and Privacy (SP), pp. 393–409 (2017)
50. Dorri, A., Kanhere, S.S., Jurdak, R.: Mof-bc: a memory optimized and flexible blockchain for large scale networks. Future Gener. Comput. Syst. **92**, 357–373 (2019)
51. Si, H., Sun, C., Li, Y., Qiao, H., Shi, L.: IoT information sharing security mechanism based on blockchain technology. Future Gener. Comput. Syst. **101**, 1028–1040 (2019)
52. Dittmann, G., Jelitto, J.: A blockchain proxy for lightweight IoT devices. In: Crypto Valley Conference on Blockchain Technology (CVCBT) (2019)
53. Rathore, S., Wook Kwon, B., Park, J., Blockchain-based decentralized security architecture for IoT network: BlockSecIoTNet: blockchain-based decentralized security architecture for IoT network. J. Netw. Comput. Appl. **143**, 167–177 (2019)
54. Bouachir, O., Aloqaily, M., Tesng, L., Boukerche, A.: Blockchain and fog computing for cyber-physical systems: case of smart industry. In: Computer IEEE (2020)
55. Son, M., Kim, H.: Blockchain-based secure firmware management system in IoT environment. In: International Conference on Advanced Communications Technology (ICACT) (2019)
56. Dukkipati, C., Zhang, Y., Cheng, L.C.: Decentralized, blockchain based access control framework for the heterogeneous internet of things. In: Proceedings of the Third ACM Workshop on Attribute-Based Access Control, pp. 61–69 (2018)
57. Maesa, D.D.F., Mori, P., Ricci, L.: Blockchain based access control. In: IFIP International Conference on Distributed Applications and Interoperable Systems. Springer, Cham, pp. 206–220 (2017)
58. Ouaddah, A., Abou Elkalam, A., Ait Ouahman, A.: Fairaccess: a new blockchain based access control framework for the internet of things. Secur. Commun. Netw. **9**(18), 5943–5964 (2016)
59. Alfandi, O., Otoum, S., Jararweh, Y.: Blockchain solution for IoT-based critical infrastructures: byzantine fault tolerance. In: Network Operations and Management Symposium, IEEE/IFIP (2020)
60. Outchakoucht, A., Hamza, E.S., Leroy, J.P.: Dynamic access control policy based on blockchain and machine learning for the internet of things. Int. J. Adv. Comput. Sci. Appl. **8**(7), 417–424 (2017)
61. Gilad, Y., Hemo, R., Micali, S., Vlachos, G., Zeldovich, N.: Algorand: scaling byzantine agreements for cryptocurrencies. In: 26th Symposium on Operating Systems Principles. ACM, pp. 51–68 (2017)

62. Yu, J., Kozhaya, D., Decouchant, J., Verissimo, P.: Repucoin: your reputation is your power. IEEE Trans. Comput. **68**(8), 1225–1237 (2019)
63. Dorri, A., Kanhere, S. S., Jurdak, R., Gauravaram, P.: Lsb: a lightweight scalable blockchain for IoT security and anonymity. J. Parallel Distrib. Comput. (2019)
64. Ali, M. H., Fadlizolkipi, M., Firdaus, A., Khidzir, N.Z.: A hybrid particle swarm optimization-extreme learning machine approach for intrusion detection system. In: IEEE Student Conference on Research and Development (SCOReD) (2018)
65. Aloqaily, M., Otoum, S., Ridhawi, I., Jararweh, Y.: An intrusion detection system for connected vehicles in smart cities. Ad Hoc Netw. **90**, 101842 (2019)
66. Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., Kumar, R.: A blockchain framework for securing connected and autonomous vehicles. Sensors **19**(14), 3165 (2019)
67. Zhang, X., Chen, J.: Deep learning based intelligent intrusion detection. In: IEEE 9th International Conference on Communication Software and Networks (ICCSN) (2017)
68. Otoum, S., et al.: On the feasibility of deep learning in sensor network intrusion detection. IEEE Netw. Lett. **1**(2), 68–71 (2019)
69. Anish, A., Sundarakantham, K.: Machine learning based intrusion detection system. In: Proceedings of 2019 3rd International Conference on Trends in Electronics and Informatics, vol. 10.1109, pp. 916–920 (2019)
70. Taher K.A., Jisan, B.M., Rahman, M.M.: Network intrusion detection using supervised machine learning technique with feature selection. In: 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (2019)
71. Laufenberg, D., Li, L., Shahriar, H., Han, M.: An architecture for blockchain-enabled collaborative signature-based intrusion detection system. In: Proceedings of the 20th Annual SIG Conference on Information Technology Education—SIGITE 19 (2019)
72. Chen, Y., Liu, J.: Distributed community detection over blockchain networks based on structural entropy. In: Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure—BSCI 19 (2019)
73. Kim, S., Kim, B., Kim, H.J.: Intrusion detection and mitigation system using blockchain analysis for bitcoin exchange. In: Proceedings of the 2018 International Conference on Cloud Computing and Internet of Things—CCIOT 2018 (2018)
74. Chen, X., Ji, J., Luo, C., Liao, W.: When machine learning meets blockchain: a decentralized, privacy-preserving and secure design. In: 2018 IEEE International Conference on Big Data (Big Data), pp. 1178–1187 (2018)
75. Dheeru, D., Karra, E.: Taniskidou. UCI machine learning repository. http://archive.ics.uci.edu/ml. Accessed Feb 2020
76. LeCun, Y., Cortes, C.: MNIST handwritten digit database. http://yann.lecun.com/exdb/mnist/. Accessed Feb 2020
77. Blanchard, P., Mhamdi, E.M.E., Guerraoui, R., Stainer, J.: Byzantine-tolerant machine learning
78. Dey, S.: Securing majority-attack in blockchain using machine learning and algorithmic game theory: a proof of work. In: 2018 10th Computer Science and Electronic Engineering (CEEC). pp. 7–10. IEEE (2018)
79. Bravo Marquez, F., Reeves, S., Ugarte, M.: Proof-of-learning: a blockchain consensus mechanism based on machine learning competitions. In: IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), pp. 119–124 (2019)
80. Rathore, S., Pan, Y., Park, J.H.: Blockdeepnet: a blockchain-based secure deep learning for IoT network. Sustainability **11**, 3974 (2019)
81. Everingham, M., Eslami, S.A., Van Gool, L., Williams, C.K., Winn, J., Zisserman, A.: The pascal visual object classes challenge: a retrospective. International J. Comput. Vis. **111**(1), 98–136 (2015)
82. Sankar, L. S., Sindhu, M., Sethumadhavan, M.: Survey of consensus protocols on blockchain applications. In: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, pp. 1–5 (2017)
83. Wang, Q., Zhu, X., Ni, Y., Gu, L., Zhu, H.: Blockchain for the IoT and industrial IoT: a review. Internet Things, 100081 (2019)
84. Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K., Shieh, S.: Iot security: ongoing challenges and research opportunities. In: IEEE 7th International Conference on Service-Oriented Computing and applications, pp. 230–234 (2014)
85. Apte, S., Petrovsky, N.: Will blockchain technology revolutionize excipient supply chain management? J. Excip. Food Chem. **7**(3), 910 (2016)
86. Miraz, M.H., Ali, M.: Applications of blockchain technology beyond cryptocurrency. arXiv preprint arXiv:1801.03528 (2018)
87. Tasatanattakool, P., Techapanupreeda, C.: Blockchain: challenges and applications. In: International Conference on Information Networking (ICOIN). IEEE, pp. 473–475 (2018)
88. Dorri, A., Kanhere, S.S., Jurdak, R.: Towards an optimized blockchain for IoT. In: 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 173–178 (2017)
89. Abbasi, A.G., Khan, Z.: Veidblock: verifiable identity using blockchain and ledger in a software defined network. In: Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 173–179 (2017)
90. Kravitz, D.W., Cooper, J.: Securing user identity and transactions symbiotically: Iot meets blockchain. 2017 Global Internet of Things Summit (GIoTS), pp. 1–6 (2017)
91. Liu, B., Yu, X.L., Chen, S., Xu, X., Zhu, L.: Blockchain based data integrity service framework for IoT data. In: 2017 IEEE International Conference on Web Services (ICWS), pp. 468–475 (2017)
92. Steichen, M., Hommes, S., State, R.: Chainguard—a firewall for blockchain applications using SDN with openflow. In: 2017 Principles, Systems and Applications of IP Telecommunications (IPTComm), pp. 1–8 (2017)
93. Basnet, S.R., Shakya, S.: BSS: blockchain security over software defined network. In: 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 720–725 (2017)
94. Baker, T., Asim, M., MacDermott, A., Iqbal, F., Kamoun, F., Shah, B., Alfandi, O., Hammoudeh, M.: A secure fog-based platform for SCADA-based IoT critical infrastructure. Practice and Experience, Software (2019)

Omar Alfandi is an Assistant Dean for Students Affairs (AUH) and Associate Professor at the College of Technological Innovation at Zayed University. He holds a Doctoral degree (Dr. rer. nat.) in Computer Science and Telematics from the Georg-August-University of Goettingen—Germany in 2009. He received his M.Sc. degree in Telecommunication Engineering in 2005 from the University of Technology Kaiserslautern—Germany.

Salam Khanji is the CTO of Green Tomorrow for Smart Sustainable Solutions and a research assistant at the College of Technological Innovation at Zayed University, Abu Dhabi, UAE. She received the Master's degree in Information Technology (Specialization in Cyber Security) from Zayed University, UAE in 2016. She received her Bachelor's degree in Computer Science from University of Jordan, Jordan in 2003.

Liza Ahmad is an instructor at the College of Technological Innovation at Zayed University, Abu Dhabi, UAE. She received the Master's degree in Information Technology (Specialization in Cyber Security) from Zayed University, UAE in 2016. She received her Bachelor's degree in Computer Science from the American University of Sharjah, UAE in 2009.

Asad Khattak is an associate professor at the College for Technological Innovation, Zayed University in Abu Dhabi that he joined in August 2014. He received his M.S. in Information Technology from National University of Sciences and Technology, Islamabad, Pakistan in 2008. He got his Ph.D. degree in Computer Engineering from Kyung Hee University, South Korea in 2012.