Computer Communications 181 (2022) 274–283

Contents lists available at ScienceDirect

Computer Communications

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

AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems

Sohaib A. Latif [a], Fang B. Xian Wen [a], Celestine Iwendi [b], Li-li F. Wang [a], Syed Muhammad Mohsin [c], Zhaoyang Han [d,*], Shahab S. Band [e,*]

[a] *Department of Computer Science, Anhui University of Science and Technology, Huainan, Anhui, 232001, Republic of China*
[b] *The Centre for Applied Computer Science School of Arts and Creative Technologies University of Bolton, Bolton BL3 5AB, United Kingdom*
[c] *Department of Computer Science, COMSATS University Islamabad, 45550, Pakistan*
[d] *Division of Computer Science, University of Aizu, Fukushima 965–8580, Japan*
[e] *Future Technology Research Center, College of Future, National Yunlin University of Science and Technology, 123 University Road, Section 3, Douliou, Yunlin 64002, Taiwan, ROC*

ARTICLE INFO

Keywords:
Internet of things
SDN
Blockchain
Security
Energy efficiency
Cyber physical systems
Industry 4.0

ABSTRACT

Internet of things (IoT) is one of the most emerging technologies nowadays and it is one of the key enablers of industrial cyber physical system (CPSs). It has started to participate in almost every aspect of our social life, ranging from financial transactions to the healthcare system, communication to national security, battlefield to smart homes, and so on. However, the wide deployment of IoT suffers certain issues as well, such as interoperability, compatibility, heterogeneity, large amount of data, processing of heterogeneous data etc. Among others, energy efficiency and security are the utmost prominent issues. Scarce computing resources of IoT devices put hindrances on information sharing across edge or IoT network. Indeed, unintentional or malicious interference with IoT data may lead to severe concerns. In this study, the researcher exploits the potential benefits of a blockchain system and integrates it with software-defined networking (SDN) while justifying energy and security issues. More in detail, the researcher proposed a new routing protocol with the cluster structure for IoT networks using blockchain-based architecture for SDN controller. The proposed architecture obviates proof-of-work (PoW) with private and public blockchains for Peer-to-Peer (P2P) communication between SDN controllers and IoT devices. In addition to this, distributed trust-based authentication mechanism makes blockchain even more adoptive for IoT devices with limited resources. The experimental results show that the proposed cluster structure based routing protocol outperforms the state-of-the-art Ad-hoc On-demand Distance Vector (AODV), Destination-Sequenced Distance Vector (DSDV), Secure Mobile Sensor Network (SMSN), Energy efficient secured cluster based distributed fault diagnosis (EESCFD), and Ad-hoc On-demand Multipath Distance Vector (AOMDV), in terms of energy consumption, network throughput, and packet latency. Proposed protocol help overcome the issues especially, energy management and security of the next generation industrial cyber physical systems.

1. Introduction

Industrial automation leads to the concept of smart factory on the basis of artificial intelligence (AI) and internet of things (IoT). Adaptive supply chain management, human–robot integration, production quality and predictive maintenance are a few examples of the industrial automation and cyber physical systems (CPSs). A huge number of sensors are deployed in the field for effective and efficient industrial automation and such a vast deployment lead to the issues of interoperability, heterogeneity among devices, processing and dealing of big data, storage of data, energy management, safety and security.

Thanks to recent advancements in the internet and its related technologies such as IoT, SDN, and cloud computing, the realization of smart homes, smart healthcare systems, smart security, industry 4.0, cyber physical systems (CPSs) to name a few, became possible [1–4]. The compact size, low cost, and integrated features enable the wide deployment of IoT. According to the Cisco report 2018–23 [5], there will be almost 30 billion devices will be connected to the internet and

* Corresponding authors.
E-mail addresses: sohaiblatif095@gmail.com (S.A. Latif), xwfang@aust.edu.cn (F.B.X. Wen), celestine.iwendi@ieee.org (C. Iwendi), Wanglili198301@163.com (L.-l.F. Wang), syedmmohsin9@yahoo.com (S.M. Mohsin), d8212109@u-aizu.ac.jp (Z. Han), shamshirbands@yuntech.edu.tw (S.S. Band).

https://doi.org/10.1016/j.comcom.2021.09.029
Received 30 May 2021; Received in revised form 19 August 2021; Accepted 27 September 2021
Available online 11 October 2021

have started their operational life in the industry, commerce, and home appliances, etc. Such a huge deployment of IoT poses some serious concerns. Lack of industry-oriented standards causes interoperability, compatibility, heterogeneity issues. Residing at the top of the hierarchy, security, and privacy for confidential data of private and corporate users is the most important issue [6]. It is a top priority for all who rely on the Internet for business and personal online activities. Protecting digital assets and content encompasses an ever-expanding digital landscape. Organizations need actionable insights and scalable solutions to secure employees' devices, IoT connections, infrastructure, and proprietary data. Focusing on the importance of security, the research community has done a lot of work to improve important security aspects of mutual authentication [7], integrity and confidentiality [8], and privacy protection [9].

Apart from security, the energy optimization of IoT is an important issue as well. Focusing on the importance of energy optimization issue, authors of [10,11] have discussed congestion recognition problem and a framework to optimize edge cooperative network, respectively. The life of battery-powered IoT mainly depends on the utilization of their limited energy. Optimal energy utilization enhances the operation life of IoT and can be a viable solution in economic terms. Moreover, battery and processing constraints result in the potential barrier in communication and implementation of security solutions [12,13]. In recent; fog and edge computing have presented a viable architecture to resolve the resource scarcity problem in IoT [14]. There are, however, certain issues that remain unresolved. Aside from these, they adversely affect IoT network communication and energy optimization [15]. Confidentiality ensures that only the authorized IoT can access the network. Integrity demands for detection of any modification in transmitted data. Minimizing energy consumption without compromising network security or improving security without affecting energy consumption is an important consideration. Therefore, it is required to have a solution with the support of a new feature for integrity, confidentiality, extensive security, and energy efficiency while considering the low computational resources of IoT [16].

In general, we need to provide the architecture for IoT having capabilities to balance security enforcement with optimizing energy consumption. Fortunately, evolution in SDN will ease to provide a viable solution. SDN is an emerging technology that decouples the data and control plane [17,18]. The data plane is the lowest layer of SDN architecture and it is responsible for data forwarding. Whereas, the control plane is the core of the SDN system. It can manage network resources, make configuration agile and flexible, and able to update forwarding rules dynamically [19,20].

SDN controller is the brain of the control plane, which is responsible for controlling the communication between application and forwarding devices. SDN controllers, which act as Network Operating System NOS, is a logically centralized entity and manage the network resources [21]. It poses full control over network communication and can dynamically program the network. Indeed, the support for the global view of the network enables real-time monitoring and collecting of network configuration and programming data. The centralized architecture and real-time monitoring of the SDN controller allow to implementation of network management services, security, energy, and routing optimization [22]. The software-defined and easily extendable nature of SDN boasts to resolve the network management and program-ability issues of billions of IoT devices connected to the date and shortly. SDN functionality can be effectively and efficiently utilized to enhance the IoT network performance. IoT network communication suffers from a lack of centralized controlling agency, which leads to insecure communication, inappropriate routing with energy consumption at an adverse rate [23]. SDN controller can manage and control the dynamic network configuration caused by the diverse set of IoT devices.

Blockchain has been effectively used for transaction verification of the Bitcoins system [24]. Beyond Bitcoin's verification, it has also been adopted to automate the accounting process, e-government, information collection in the healthcare system, storage as a service in the distributed cloud [25]. It comprises blocks link together and is located in a distributive inflexible manner to form a chain where each block stores some specific information. Since the chain of block structure can easily detect any alteration or missing of one or more blocks without need of a central or intermediary entity.

By design security nature of blockchain permits to utilize it across the SDN platform because it provides security and ensures integrity and privacy from untrusted users in an energy-efficient manner [26–28]. Thus, we exploit the potential benefits of the blockchain system and integrate it with software-defined networking SDN while mitigating energy and security challenges in IoT communication. Unique characteristics of SDN and blockchain make them useful for incorporating into IoT networks. The peer-to-peer communication nature of this integration resolves the single point of failure problem along with protecting privacy and security.

In this article, we proposed a routing protocol with the cluster structure for IoT networks using blockchain-based architecture for the SDN controller. The proposed architecture eliminates PoW with private and public blockchains for Peer-to-Peer P2P communication between the SDN controller and IoT devices. The distributed trust-based authentication mechanism interacts in a verifiable manner and facilitates secure connection for IoT in each SDN domain (also known as a cluster) and makes blockchain even more appropriate for IoT devices with limited resources. However, certain blockchains, especially with PoW consensus protocols, could increase complications from the computation perspective and significantly increase bandwidth overhead and transmission delay [29,30]. Indeed, the inefficient and inappropriate handling of blockchain can even adversely affect the network performance and thus, may not be useful for resource-constrained IoT. Therefore, we proposed a customized blockchain for IoT in which the SDN controller provides a distributed authentication mechanism in each SDN domain and effectively reduces the overhead caused by traditional blockchain. In each SDN domain, IoT devices register themselves via a non-changeable distribution ledger, and it is the responsibility of the SDN controller to centrally manage that ledger. The use of cluster structure and optimizing PoW prevent the entry of selfish nodes and enhance the security and energy optimization of IoT devices.

The main contribution of the proposed architecture are given below.

- Provide IoT networks with a personalized blockchain-based software-defined network (SDN) controller architecture
- Using a blockchain-based SDN controller, provide distributed IoT network management with SDN cluster architecture
- Devise energy and computation sensitive private and public blockchain that is implemented to provide secure communication and access control to IoT data
- Propose a secure and energy-sensitive SDN cluster structure for transferring files among IoT devices

The rest of the manuscript is organized as follows: Section 2 highlights the state of the art literature review. The detailed working of the proposed architecture including energy and security improvement mechanism for IoT is described in Section 3. Experimental setup and results findings are discussed in Section 4 whereas, concludes the study.

2. Literature review

In the literature, several types of research on the integration of IoT with SDN and blockchain have been proposed in the literature. Traditional distributed architectures, protocols, and techniques, especially those related to security and energy, are no longer sufficient in the current era of information technology in the field of IoT [30,31]. Nowadays, Researchers and practitioners are much attracted to the implementation of blockchain and SDN solutions to solve the current problems in the field of IoT space [32,33].

Blockchain technology is used by DistBlockNet [34] model to confirm and distribute flow rules tables between IoT devices. The design works on the fundamental principle of distributed features in a software-defined network (SDN) to generate security and comparability-based plan in IoT-based networks. In this architecture, threats are automatically isolated based upon the updated flow rules tables using the blockchain technique. However, energy consumption and resource limitation of IoT devices is not considered to evaluate the performance of this architecture.

Blockchain security over SDN (BSS) is used in [35]. Files are securely transferred using blockchain to SDN. The use of the Ethereum platform, as well as the integration of the OpenDaylight controller with the OpenStack controller, indicates safe file movement among SDN devices using P2P distributed architectures. The technique is purely based upon secure transmission and does not address the core issues of IoT devices i.e. Energy and resource limitations.

An IoT-based solution for smart homes is optimized in [36]. The proposed method eliminates the classical overhead of blockchain's approach. Process time for authentication is reduced by using the distributed trust architecture. This method often ignores the limitations of IoT devices, such as energy and resource constraints. Routing plays a back-bone role in hierarchical structures. Lack of proper routing techniques in these structures may result in some security issues and more energy consumption.

The technique proposes by Dorri et al. [37] uses the principle of blockchain-based architectures for smart homes. Two types of blockchain were used in these solutions i.e. public and Local for communication and authentication purposes. Cooja simulator was used as a developing tool and the BC-based approach was used for comparison purposes. The results show that clustering nodes reduce network overhead and latency. This approach ignores the energy and availability concerns that are an essential part of IoT-based solutions.

A Three layers classical blockchain approach is discussed in [38,39], where the fog node is at the edge and connected through distributed controllers. The basic idea behind this approach is to provide low-cost, blockchain-based on-demand access across various layers of clouds, fog, and devices. The architecture presented in this paper lacks the consideration of challenges in the IoT i.e. Energy consumption, resource limitation, and communication among IoT devices.

Shama et al. [40] proposed a blockchain-based architecture for a smart city. The main architecture is divided into core and edge networks for efficiency purposes. It utilizes a centralized distributed architecture for efficiency whereas PoW design is used for privacy and security purposes. The key evaluation parameters used in this approach are; Delay, hash rate, and block. The hybrid approach discussed does not evaluate the performance of the network over key parameters of the IoT-based architecture which are energy and security issues. Two main problems in the discussed architecture are the effective implementation of edge nodes and the caching technique used by these nodes.

A block-VN-based car network implemented in smart-city is proposed by the authors in [41]. It is secure, reliable, and works in a distributed manner based upon a distributed management system. For data transmission, they use a centralized network infrastructure and a blockchain of vehicles. The main assessment focuses on the inter-vehicular network, but it neglects to address key IoT challenges.

Authors of [23] proposed BCTrust as an energy-efficient using blockchain authentication mechanism for energy computation and storage. It makes use of a clustered framework. The cluster head, dubbed CPAN, has an encryption key and transmits data using a blockchain technique. A combination of Ethereum blockchain and C language is used to evaluate the performance of this approach. This method also does not indicate and evaluate the energy parameter of IoT devices.

In [42], the blockchain method is used to control and configure IoT systems. Ethereum was used as a possibility of smart contracts. For easy setup and management, private keys are stored in Ethereum, while public keys are held and stored on separate computers. RSA is primarily used as an encryption method to secure keys. The limited memory of IoT devices, as well as their energy consumption, are not taken into account in this process.

Security and safety model of cyber physical systems (CPSs) is discussed on detail by the authors of [43]. Traditionally, the computer scientists perceive the security as data or communication security issue only. Whereas, emergence of CPSs and integration of internet of things with CPSs demand unified efforts to deal with concerned safety and security issues. Authors urged upon the need of development of diligent application effective at both run time and design time.

Industry 4.0 is based upon connectivity, interoperability, smart decision, resource optimization and interactivity of the entities. Authors of [44] stated that industrially internet of things and artificial intelligence have major role in development of industry 4.0. In this context, industries are using cyber physical system powered with intent of things for better, reliable and safe production. Authors have reviewed prominent CPS models with special emphasis on their characteristics and technologies. Challenges and gaps to improve the industries are also discussed in this study.

Authors of [45] have presented a survey to discuss design, technologies, principles and policies for cyber physical systems. They have reviewed the literature on CPSs and IoT from 2010 to 2021. This study has focused on automation of AI empowered CPSs. Integration of IoT and CPSs with special focus on cybersecurity is discussed in detail by the authors. Both technical and social level automation of CPSs is the primary focus of this study.

3. Proposed system model

This section describes the in-depth working of our proposed model. We implemented the IoT-supported blockchain and cluster structure of SDN for distributed network management of IoT. Fig. 1 shows the high-level architecture of the proposed model. A blockchain is attached to each SDN controller for IoT communication. Analogous to Bitcoin's system, SDN controllers are connected in a P2P topology. The proposed architecture has two key objectives: (a) improve communication security for IoT devices and (b) optimize their energy consumption to enhance their lifetime.

Indeed, large network structures without organized effort will lead to chaos. A well-organized structure for a large network is required for its efficient operation. In the proposed model, we organized the large SDN architecture for IoT in different clusters where each cluster refers to a SDN domain. SDN controller plays the role of cluster head in each SDN domain to coordinate the intra-cluster communication, reduce the network delay, and mitigate overhead. It is also responsible for the registration of a heterogeneous set of IoT devices. It monitors the IoT devices connected in its domain, satisfies their needs, and enforces regulation policies. Cloud storage is also a part of the proposed model and is used for keeping records of transactions and acts as storage for data of IoT. It has also been used for storing public blockchain for SDN controllers. The systems with a central controlling agent are much prone to cyber-attacks. They become a single point of failure. The blockchain with P2P nature creates an opportunity for utilizing blockchain features for the SDN controller and protects the integrity and security of data while eliminating a single point of failure. The proposed model maintains the P2P connection for IoT devices in a cluster domain and also for the blockchain SDN controller for inter-domain communication. As shown in Fig. 2, public blockchains are used for inter-domain and intra-domain security respectively. Both forms of blockchain follow the same decentralized ledger technology principle, under which each user keeps a copy of a shared block digitally signed transaction ledger. Public blockchains are managed by the SDN controller, while private blockchains are maintained by IoT devices in each domain.

As for the public blockchain, a new block of the chain is generated when SDN controller with IoT devices is added into the network, and the complete transaction history of the SDN controller is available for it. Any SDN domain can join and share the distributed network since the public blockchains networks are completely open. As mentioned in Section 1 that one of the major issues with public blockchain is its high computation complexity which is caused by a distributed ledger management system. This significantly consumes computational and communication resources. The computational complexity can be resolved using a cluster structure for SDN and eliminating PoW through the SDN controller. The blocks of public blockchain i.e. SDN controller along with their associated IoT devices are added into the chain without necessity of the PoW process.

Thus, the use of cluster structure and elimination of the PoW process reduces a substantial amount of computational overhead and energy consumption. The constrained resources of IoT devices prohibit them to implement complex security procedures. In the proposed architecture, we place the private blockchain between IoT devices and the SDN controller in each SDN domain. As shown in Fig. 3, IoT devices make P2P connections, and blocks of the chain are maintained jointly by SDN controllers and IoT devices. A registration process is required to participate in private blockchain and must be verified by certain rules set up by the network starter. Authentication and verification are the core responsibility of the SDN controller to ensure that only the legitimate user becomes part of the domain. Since the identity of each device involving in the transaction is clear, access is granted only to the relevant section of data. Blockchain maintained in each SDN domain keeps a record of all incoming and outgoing transactions and enforces policies for IoT devices. A unique key is associated with every SDN controller and shared with other controllers in the same network. The key is specifically used for authorization of newly generated SDN domain or blocks of the existing chain.

After successful authentication of an IoT device in an SDN domain, the SDN controller registers its identity with a transaction in the public blockchain and shares the public and private key with other IoT devices to exchange data and carry out transactions. IoT devices connected with the SDN controller have the right to change their domain if they observe excessive delay and energy consumption. When an IoT device decided to migrate to another SDN domain, it re-initializes the registration process with a new SDN controller. The destination controller verifies the device identity via public blockchain and sends a request to obtain the public key of that device from the previous controller. Once the key is received, a confirmation is sent to the device, and transactions device related to devices are incorporated in the public blockchain.

3.1. Data transfer mechanism in SDN domain

IoT devices in an SDN domain keep the private and public keys according to rules and policies defined by the SDN controller to carry out secure transactions in the blockchain. Whenever an IoT device intends to send data over the SDN domain; it signs in with a private key and publishes the message using its public key. The domain members consider the sender's public key and verify the validity of the block format message sent. The block is stored in a private blockchain and the file is passed to the receiver if the sender node is allowed to share data. If data is to be sent to the device located in other SDN domains, after publishing its public key, the SDN controller sends a membership request to the controller of the destined device. On the successful completion of the registration and authentication process, the file is transferred to the recipient.

To fully comprehend the proposed public and private blockchain-based SDN architecture for IoT, an illustration is provided using the case scenario of file transfer between IoT devices. Let assumes that there are five SDN domains named A1, A2, A3, A4, and A5, a device in A1 intend to transfer a file to the device located in A5 as shown in Fig. 4. The following steps are to be followed for exchanging data file:

1. **Step 1:** SDN controller in A1 signed the transaction using the private key and publish it with the public key across the network
2. **Step 2:** If the destined device is in the other SDN domain (A5 for stated case), the file is the controller in A1 will send it to the controller in A5
3. **Step 3:** A block is added to the blockchain and broadcast in the SDN domain. The transaction is authenticated based on the public key
4. **Step 4:** On the receipt of the file, only the intended receiver can decode it

3.2. Customizing blockchains to improve security and energy efficiency

Proof-of-Work (PoW) is used in blockchain as a consensus algorithm when it commits to add new transactions into the ledger. PoW first aims to verify transactions and generate new blocks to the chain. With PoW, participants strive for each other to complete transactions on the network and get rewarded.

The participant is known as a miner and the process is termed as mining. Miners send digital tokens to each other in the network. A decentralized ledger gathers all the transactions into blocks. However, care should be taken to confirm the transactions, arrange blocks, and resolve consensus among miners. The complex and resource-hungry nature of the PoW algorithm does not suit the resource-constrained IoT devices and becomes almost impractical. Moreover, resolving consensus among miners introduces additional delays. The proposed model shown in Fig. 5 is SDN cluster-based IoT network aimed to reduce the proposed architecture's overhead associated with PoW. The distribution trust base authentication mechanism resolves the PoW complexity issue. To be more precise, blocks are inserted into chains without the need for PoW consensus, reducing the initial PoW's overhead to zero. When you create a block, the SDN controller creates its hash. The controller recalculates the hash whenever the data changes. Linking the hash of the block each other build a chain and this whole process ensures the security of the network. The proposed architecture applies to a diverse set of IoT devices, which generate and share data, perform transactions, and perceive smart contract features. Besides, we also have heterogeneous resources with various security and energy capabilities.

Hence, it is pertinent to have a secure and energy-efficient mechanism to prevent unauthorized access in each SDN domain. Since the SDN controller act as a cluster head in each domain, permission to avail the network services by IoT devices is granted by the controller. It enables to prevent the selfish or malicious node to become part of the SDN domain. Once, the malicious joins the network, it compromises the network security and causes to deplete the device's energy abruptly. The energy-efficient and secure flow of information are depicted in Fig. 5. The flow begins when IoT devices register with the SDN controller. After registration, the controller assigns a unique IP address (since it also acts as a Dynamic Host Configuration Protocol server) to each device in the SDN domain. It also allocates the private and public keys for IoT devices.

It also allocates the private and public keys for IoT devices. It keeps an eye on all activities and transactions of devices and is well aware of the computational and energy resources of these devices. IoT devices can detect the remaining energy from packets transmitted to/from their neighbors in the private blockchain of each SDN domain. They send a packet to the other IoT devices based on the amount of their remaining energy. If the energy falls below a certain threshold, it switches the path and chooses another neighbor for transferring packets. Since the controller is monitoring every device, it can detect any malicious or selfish behavior of nodes using its energy profile. It then blocks the malevolent node and shares its ID with other controllers so that it cannot be registered in other domains and remain blocked even in public blockchains. The public key of devices registered with SDN controllers remains valid for a public blockchain and allows them to authenticate in other SDN domains. For the IoT devices not listed in the

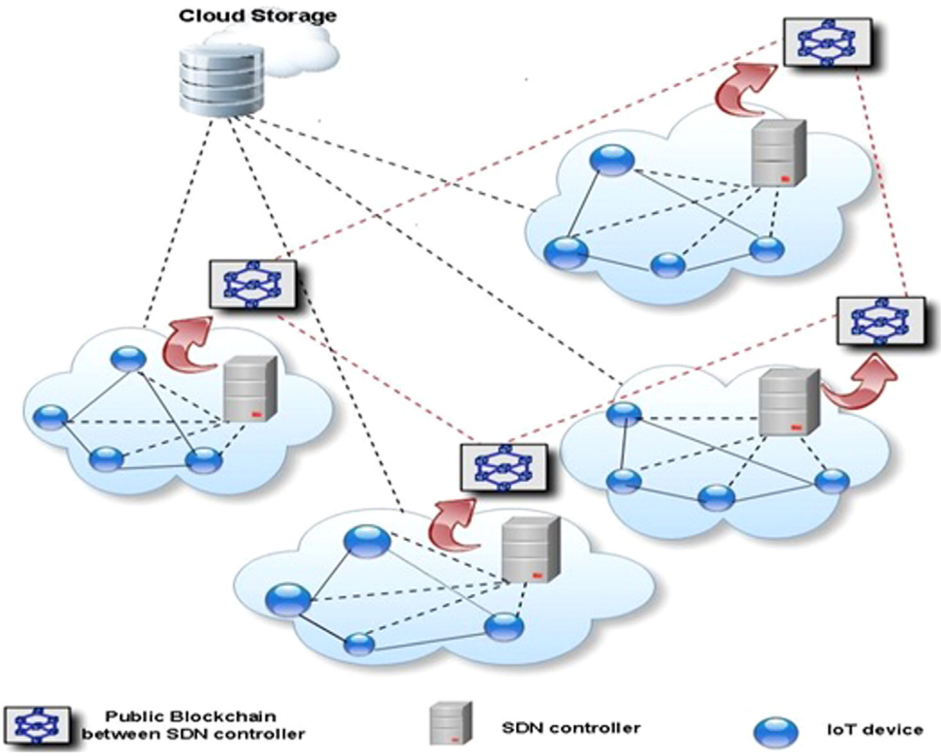

Fig. 1. Cluster-based proposed model with blockchain-enabled SDN controllers.

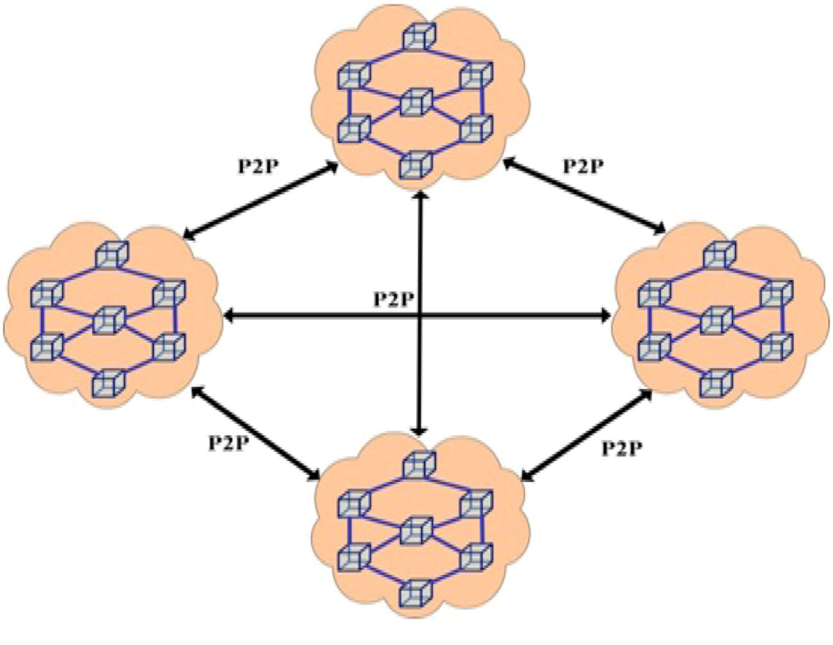

Fig. 2. Private blockchain between IoT devices and SDN.

blacklist and whose energy becomes as low as the defined threshold, they can migrate to other SDN domains to save their energy and prolong their lifetime. For the sake of making transactions, they receive a private key from their new SDN controller.

In the proposed architecture, we make the network efficient by enabling the SDN controller to provide various services to IoT devices. It enables IoT devices to migrate on a need basis and communicate in different domains. The network will protect and detect compromising nodes by combining public and private blockchains with peer-to-peer communication. The SDN controller monitors the IoT devices in his area of responsibility and detects selfish parties and prohibits them from registering in other SDN domains.

4. Experiments and results

In this section, a description of the experimental setup is provided followed by performance evaluation and analysis. The performance of the proposed model is evaluated against state-of-the-art AODV, DSDV, SMSN, EESCFD, and AOMD, in terms of energy consumption, network throughput, and packet latency.

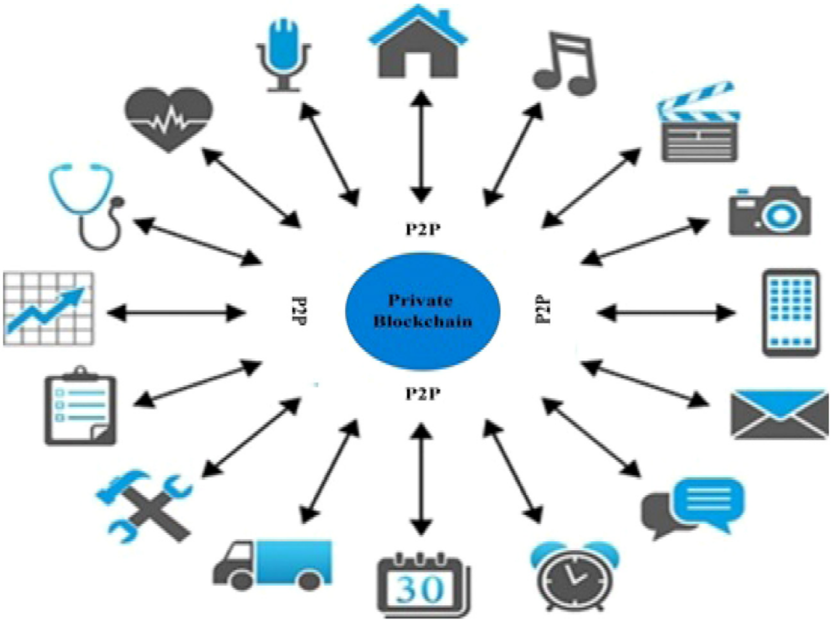

Fig. 3. Inter-controllers public blockchains.

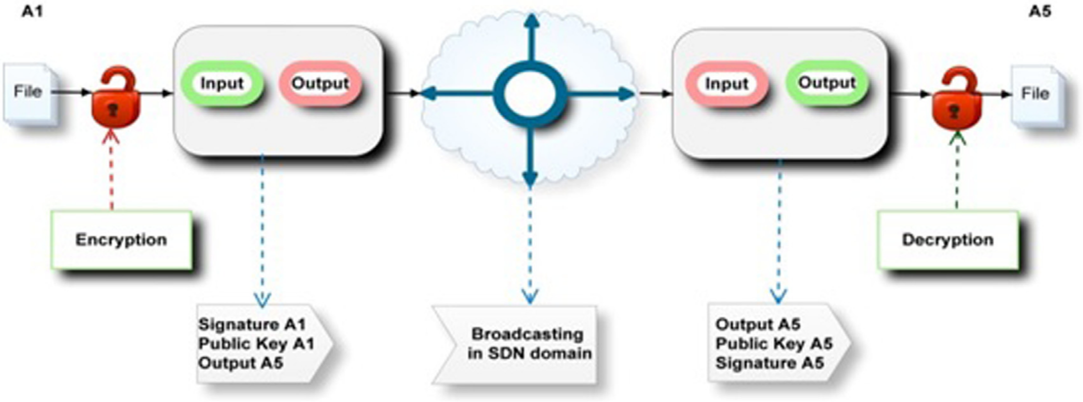

Fig. 4. File transfer between two users A1 and A5 in SDN domain.

Table 1
Simulation parameters.

Parameter	Value
Network Simulator	mininet-wifi/ Ethernet
SDN Controller type	Opendaylight
Number of SDN Controllers	6
Number of SDN Domains	6
Number of IoT devices	100
Initial Energy value of IoT device	10–14 j
Simulation Time	120 s
Mobility Model	Random Waypoint
Device Velocity	10 m/s
Routing protocol	AODV, DSDV, SMSN, EESCFD, AOMDV
IEEE standard	802.11p
Data traffic	Constant bit rate
Packet size	512 Bytes
Number of Transactions	1824

4.1. Experimental setup

This section details the implementation and experimental setup used to assess the proposed model's efficiency. SDN domain is simulated using open daylight controller [27] and mininet-wifi simulator [22] in this work. The blockchain part is implemented with the Pyethereum tester tool [18] under the utilization of the Ethereum platform. The Ethereum platform was installed in Ubuntu 18.04 LTS. Pyethereum is used for experimental purposes to evaluate the performance of private and public blockchains without interfering with the blockchain itself. SDN and blockchain are integrated for the secured sharing of a document or file among IoT devices across SDN domains. Virtual machines (VMs) are installed with unique IP addresses in the Ethereum, and SDN domains are created with a mininet-wifi simulator.

The open daylight SDN controller has connected with SDN topology remotely. The simulated environment is divided into six SDN domains, with each domain having an open daylight controller acting as a cluster head. It is connected to IoT devices that have been registered in its domain. In each SDN domain, we assume that there exist fifteen IoT devices with varying levels of residual energy. They are free to move their domain once they observe prolonged delay, reduction in throughput, and increase in energy consumption rate. The mobility of nodes is also taken into account and maximum speed is set to 10 m/s and nodes follow the random waypoint model. The open daylight controller is directly connected with cloud storage where data and blockchains are stored. 1824 transactions were being generated during the simulation period of 120 s. We compute the average results of 10 simulations. The summary of simulation parameters is enlisted in Table 1.

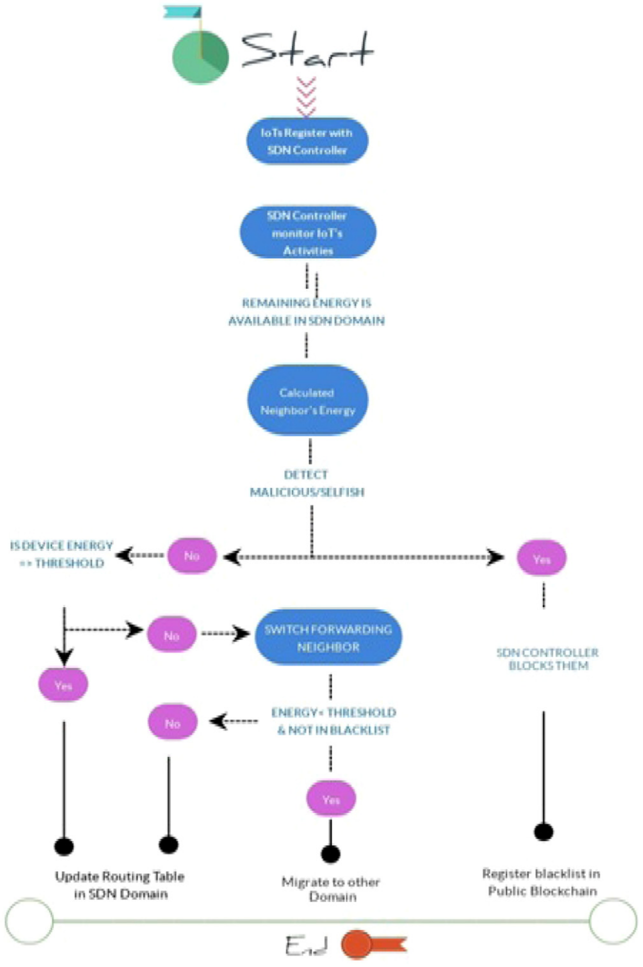
Start
IoTs Register with SDN Controller
SDN Controller monitor IoT's Activities
REMAINING ENERGY IS AVAILABLE IN SDN DOMAIN
Calculated Neighbor's Energy
DETECT MALICIOUS/SELFISH
IS DEVICE ENERGY >= THRESHOLD
No
Yes
No
SWITCH FORWARDING NEIGHBOR
Yes
SDN CONTROLLER BLOCKS THEM
No
ENERGY< THRESHOLD & NOT IN BLACKLIST
Yes
Update Routing Table in SDN Domain
Migrate to other Domain
Register blacklist in Public Blockchain
End

Fig. 5. Flow mechanism of secure and energy efficient proposed model.

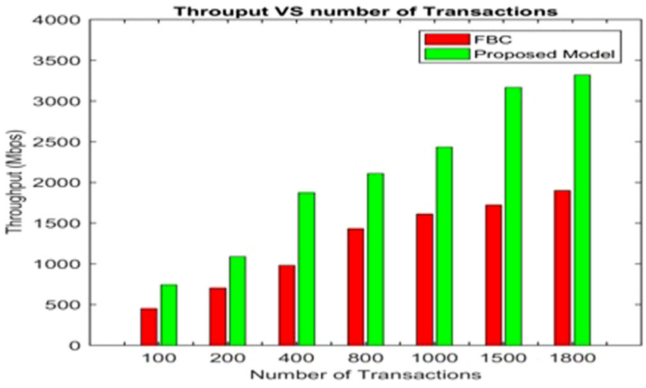

Fig. 6. Throughput comparison of the proposed model with FBC.

4.2. Performance evaluation

The proposed model revolves around the cluster structure to improve the security features in SDN with public and private blockchains while considering the resource limitations of IoT. The responsibility of authentication and validation of IoT devices rests with the SDN controller. The proposed model is flexible enough to accept changes in the cluster structure or neighboring clusters. Overhead of the proposed architecture is compared with fundamental blockchain FBC having PoW and hashing methods. Routing flow is also compared against well-known references AODV, DSDV, and AOMDV protocols [21]. Since the proposed model uses the cluster-based approach, it is also evaluated against two energy-aware clustering algorithms i.e. Secure Mobile Sensor Network (SMSN) [5] and Energy Efficient Secured Cluster-based Distributed Fault Diagnosis protocol (EESCFD) [12].

Table 2
Notations and their description.

Notations	Description
E_{tot}	Total energy consumption
N_{trans}	Number of transactions
T_{trans}	Transaction time
N_{cont}	Number of SDN controllers
E_{cont}	Energy consumed by each SDN controller
N_{iot}	Number of IoT devices
E_{iot}	Energy consumed by each IoT device

4.2.1. Throughput

The amount of data transferred successfully from the source to the destination is termed throughput. It can be linked with the total number of transactions carried out in the network. Fig. 6 shows the throughput of the proposed model and compares it with flow base configuration (FBC). A significant amount of throughput difference can be observed from the figure. The main reason for this improvement is the utilization of cluster structure. Throughput has also been improved because of reduced overhead which was originated by PoW in FBC. Throughput comparison with other routing protocols is also shown in Fig. 7. The average throughput of the proposed model is higher than the others. The possible cause of this lead is the detection and rectification of selfish nodes that become the major cause of packet drop. Moreover, the probability of link failure increases with an increase in the number of connections. The proposed SDN model efficiently handles the connections.

4.2.2. End-to-end delay

End-to-end is a term that refers to the process from beginning to end Delay, also known as latency, is the time it takes for a packet to pass from its source to its destination. It is the combination of processing time T_{proc}, transmission time T_{trans}, and queuing time T_{queue} i.e. shown in Eq. (1).

$$Delay = T_{proc} + T_{trans} + T_{queue} \tag{1}$$

The distance between source and destination, the number of packets in the output buffer, and the processing speed of nodes all influence the delay. For the sake of the evaluation, we set the traffic type as cluster based routing (CBR) with varying number of packets and packet size to 500 to 4000 and 1000 to 3500 bytes respectively. Fig. 8 shows the delay comparison of the proposed model with FBC. The proposed model observes low delay and it is not affected by the amount of traffic in each cluster. Delay value increases from 0.5 to 1.6 nanoseconds with increasing the packet size. This is because buffer capacity reduces with an increase in packet size, which ultimately increases delay. Fig. 9 illustrates the delay performance as a function of time against AODV, DSDV, AOMDV, SMSN, and EESCFD. The proposed model outperforms the other protocols. Since the number of packets generated by each node increases as time passes, the amount of delay also increases proportionally.

4.2.3. Energy consumption

Energy consumed in SDN based IoT network is the sum of energy consumed by each IoT device and SDN controller. The total energy consumption can be computed with the help of Eq. (2). Notations and their description is given in Table 2 of this study.

$$E_{tot} = N_{trans} * T_{trans} + [(N_{cont} * E_{cont}) + (N_{iot} * E_{iot})] \tag{2}$$

The above equation dictates that the more and larger the number of packets sent, and high the degree of connectivity, the higher will be

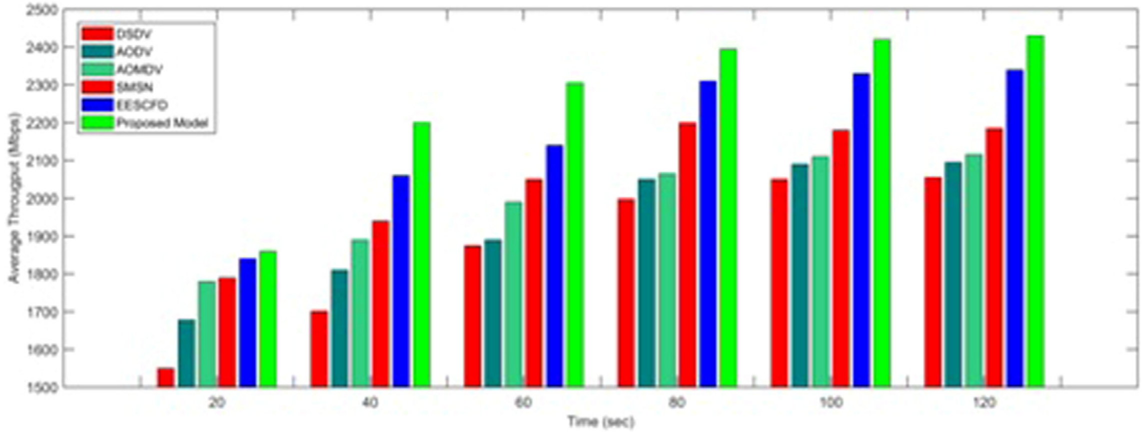

Fig. 7. Throughput comparison of the proposed model with routing protocols of the same category following the random waypoint mobility model.

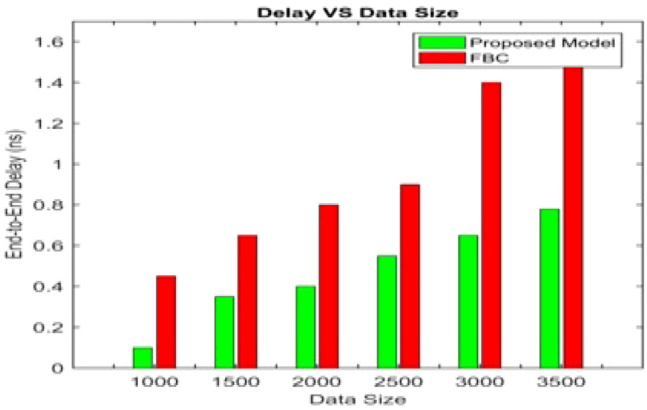

Fig. 8. Delay comparison of the proposed model with FBC with various size of the data file.

the energy consumption. The energy profile against other routing algorithms is shown in Fig. 10. Well-known protocols consume more energy whereas the proposed model saves the nodes energy and prolongs their lifetime. The proposed protocol uses an energy-efficient technique in which routing tables are modified via the SDN controller based on the energy profiles of nodes in each SDN domain. To summarize the findings, the proposed routing protocol outperforms the referenced routing protocols. This may mean that the protocol is suitable for use in the proposed IoT system architecture.

5. Conclusion and future work

Next generation industrial cyber physical systems (CPSs) require artificial intelligence (AI) empowered solutions to overcome the issues of heterogeneity of devices, big data generation by the sensors, data streaming, processing of heterogeneous unstructured data and the data security. The increasing trend of smart and intelligent services triggers the avalanche in the IoT network and their related services. To provide secure and efficient services, there is an urgent need to manage the computing and energy scarcity problem of IoT. This study focuses on mitigating some of the challenges related to IoT's network. By exploiting the power of AI, we have proposed architecture for IoT networks to enhance security and improve energy efficiency. We integrated the two emerging AI based technologies namely, blockchain and SDN, and leverage their potential benefits in terms of efficient data analysis, data security and efficient energy management. For the IoT network with blockchain support for the SDN controller, a cluster-based framework was introduced. On both public and private networks, the blockchain is used. The resource-hungry component of PoW is eliminated to tailor the blockchain for IoT capabilities. This method saves a large amount of energy, boosts data transfer rates, and reduces latency. Extensive testing has shown that the proposed model outperforms both the basic blockchain approach and current routing protocols. This study will In the IoT domain, we hope to develop a high-level P4 architecture with blockchain support in the future.

CRediT authorship contribution statement

Sohaib A. Latif: Conceptualization, Methodology, Software. **Fang B. Xian Wen:** Visualization, Investigation. **Celestine Iwendi:** Supervision. **Li-li F. Wang:** Software, Validation. **Syed Muhammad Mohsin:** Writing – review & editing. **Zhaoyang Han:** Innovation. **Shahab S. Band:** Grammarly check.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is partially supported by the Open Project Program of Key Laboratory of Embedded System and Service Computing of Ministry of Education, China (No. ESSCKF2018-04), the Foundation for Top-notch Academic Disciplines of Anhui Province, China (No. gxbjZD11), the National Natural Science Foundation of China (No. 61572035, No. 61902002, No. 61402011 and No. 61272153), the Anhui Provincial Big Data Foundation, China (No. 2017032), the Academic and Technology Leader Foundation of Anhui Province, China (No. 2019H239) and the Natural Science Foundation of Educational Government of Anhui Province of China (No. KJ2016A208). We also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentations.

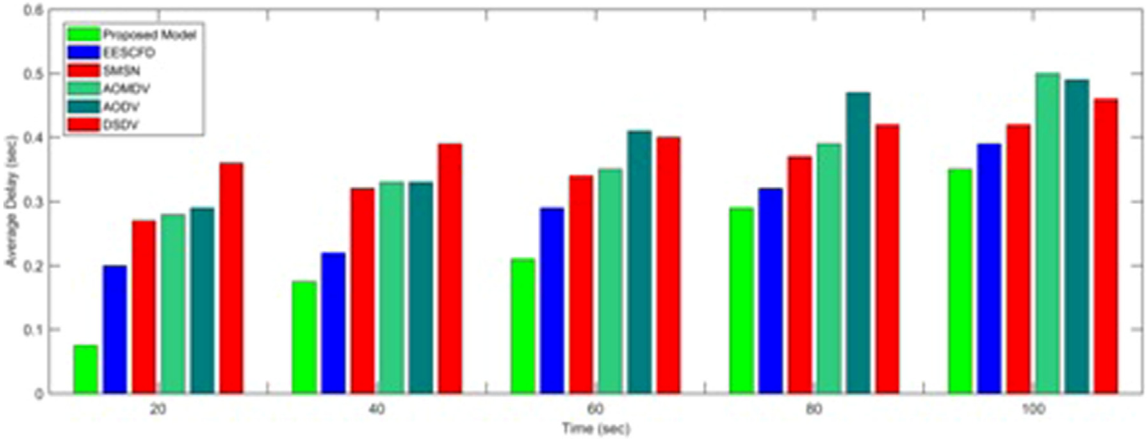

Fig. 9. Delay comparison of the proposed model with routing protocols of the same category following the random waypoint mobility model.

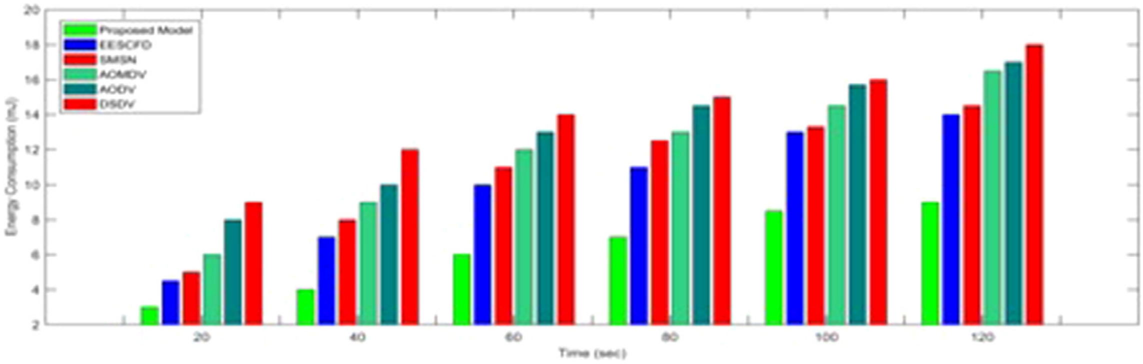

Fig. 10. Energy comparison of the proposed model with routing protocols of the same category following the random waypoint mobility model.

References

[1] W. Wang, F. Xia, H. Nie, Z. Chen, Z. Gong, X. Kong, W. Wei, Vehicle trajectory clustering based on dynamic representation learning of internet of vehicles, IEEE Trans. Intell. Transp. Syst. (2020).

[2] W. Wang, X. Zhao, Z. Gong, Z. Chen, N. Zhang, W. Wei, An attention-based deep learning framework for trip destination prediction of sharing bike, IEEE Trans. Intell. Transp. Syst. (2020).

[3] N. Shi, L. Tan, W. Li, X. Qi, K. Yu, A blockchain-empowered AAA scheme in the large-scale HetNet, Digit. Commun. Netw. (2020).

[4] L. Tan, K. Yu, F. Ming, X. Chen, G. Srivastava, Secure and resilient artificial intelligence of things: A HoneyNet approach for threat detection and situational awareness, IEEE Consum. Electron. Mag. (2021).

[5] G.-J. Ahn, G. Gu, H. Hu, S. Shin, Guest editors' introduction: Special section on security in emerging networking technologies, IEEE Trans. Dependable Secure Comput. 16 (6) (2019) 913–914.

[6] Y. Ai, M. Peng, K. Zhang, Edge computing technologies for Internet of Things: A primer, Digit. Commun. Netw. 4 (2) (2018) 77–86.

[7] S.M. Mohsin, I.A. Khan, S.M. Abrar Akber, S. Shamshirband, A.T. Chronopoulos, Exploring the RFID mutual authentication domain, Int. J. Comput. Appl. 43 (2) (2021) 127–141.

[8] I. Mustafa, I.U. Khan, S. Aslam, A. Sajid, S.M. Mohsin, M. Awais, M.B. Qureshi, A lightweight post-quantum lattice-based RSA for secure communications, IEEE Access 8 (2020) 99273–99285.

[9] I. Mustafa, H. Mustafa, A.T. Azar, S. Aslam, S.M. Mohsin, M.B. Qureshi, N. Ashraf, Noise free fully homomorphic encryption scheme over non-associative algebra, IEEE Access 8 (2020) 136524–136536.

[10] X. Han, G. Shen, X. Yang, X. Kong, Congestion recognition for hybrid urban road systems via digraph convolutional network, Transp. Res. C 121 (2020) 102877.

[11] X. Kong, S. Tong, H. Gao, G. Shen, K. Wang, M. Collotta, I. You, S. Das, Mobile edge cooperation optimization for wearable internet of things: A network representation-based framework, IEEE Trans. Ind. Inf. (2020).

[12] T. Ara, M. Prabhkar, P.G. Shah, Energy efficient secured cluster based distributed fault diagnosis protocol for IoT, Int. J. Commun. Netw. Inf. Secur. 10 (3) (2018) 539.

[13] S.M. Mohsin, I.A. Khan, S.M. Abrar Akber, S. Shamshirband, A.T. Chronopoulos, Exploring the RFID mutual authentication domain, Int. J. Comput. Appl. 43 (2) (2021) 127–141.

[14] S.R. Basnet, S. Shakya, BSS: Blockchain security over software defined network, in: 2017 International Conference on Computing, Communication and Automation, ICCCA, IEEE, 2017, pp. 720–725.

[15] M. Bilal, S.-G. Kang, An authentication protocol for future sensor networks, Sensors 17 (5) (2017) 979.

[16] D. Comer, A. Rastegarnia, Toward disaggregating the SDN control plane, IEEE Commun. Mag. 57 (10) (2019) 70–75.

[17] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of Things security and Forensics: Challenges and opportunities, Elsevier, 2018.

[18] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi, A Programmer's Guide to Ethereum and Serpent, 2015, URL: https://mc2-umd.github.io/ethereumlab/docs/serpent_tutorial.pdf.

[19] A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in internet of things: Challenges and solutions, 2016, arXiv preprint arXiv:1608.05187.

[20] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops, IEEE, 2017, pp. 618–623.

[21] R.R. Ema, M. Ashrafi Akram, A. Hossain, S.K. Das, Performance analysis of DSDV, AODV and AOMDV routing protocols based on fixed and mobility network model in wireless sensor network, Glob. J. Comput. Sci. Technol. (2014).

[22] R.R. Fontes, S. Afzal, S.H. Brito, M.A. Santos, C.E. Rothenberg, Mininet-WiFi: Emulating software-defined wireless networks, in: 2015 11th International Conference on Network and Service Management, CNSM, IEEE, 2015, pp. 384–389.

[23] M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of trust: A decentralized blockchain-based authentication system for IoT, Comput. Secur. 78 (2018) 126–142.

[24] S. Huh, S. Cho, S. Kim, Managing IoT devices using blockchain platform, in: 2017 19th International Conference on Advanced Communication Technology, ICACT, IEEE, 2017, pp. 464–467.

[25] M. Kantor, E. Biernacka, P. Boryło, J. Domżał, P. Jurkiewicz, M. Stypiński, R. Wójcik, A survey on multi-layer IP and optical software-defined networks, Comput. Netw. 162 (2019) 106844.

[26] G. Kumar, R. Saha, M.K. Rai, R. Thomas, T.-H. Kim, Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics, IEEE Internet Things J. 6 (4) (2019) 6835–6842.

[27] J. Medved, R. Varga, A. Tkacik, K. Gray, Opendaylight: Towards a model-driven SDN controller architecture, in: Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, IEEE, 2014, pp. 1–6.

[28] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, C. Qijun, A review on consensus algorithm of blockchain, in: 2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC, IEEE, 2017, pp. 2567–2572.

[29] B.A.A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, T. Turletti, A survey of software-defined networking: Past, present, and future of programmable networks, IEEE Commun. Surv. Tutor. 16 (3) (2014) 1617–1634.

[30] R.M. Parizi, A. Dehghantanha, On the understanding of gamification in blockchain systems, in: 2018 6th International Conference on Future Internet of Things and Cloud Workshops, FiCloudW, IEEE, 2018, pp. 214–219.

[31] R.M. Parizi, A. Dehghantanha, et al., Smart contract programming languages on blockchains: An empirical evaluation of usability and security, in: International Conference on Blockchain, Springer, 2018, pp. 75–91.

[32] R.M. Parizi, S. Homayoun, A. Yazdinejad, A. Dehghantanha, K.-K.R. Choo, Integrating privacy enhancing techniques into blockchains using sidechains, in: 2019 IEEE Canadian Conference of Electrical and Computer Engineering, CCECE, IEEE, 2019, pp. 1–4.

[33] P.K. Sharma, M.-Y. Chen, J.H. Park, A software defined fog node based distributed blockchain cloud architecture for IoT, IEEE Access 6 (2017) 115–124.

[34] P.K. Sharma, S.Y. Moon, J.H. Park, Block-VN: A distributed blockchain based vehicular network architecture in Smart City, J. Inf. Process. Syst. 13 (1) (2017).

[35] P.K. Sharma, J.H. Park, Blockchain based hybrid network architecture for the Smart City, Future Gener. Comput. Syst. 86 (2018) 650–655.

[36] P.K. Sharma, S. Singh, Y.-S. Jeong, J.H. Park, Distblocknet: A distributed blockchains-based secure SDN architecture for iot networks, IEEE Commun. Mag. 55 (9) (2017) 78–85.

[37] P.J. Taylor, T. Dargahi, A. Dehghantanha, R.M. Parizi, K.-K.R. Choo, A systematic literature review of blockchain cyber security, Digit. Commun. Netw. 6 (2) (2020) 147–156.

[38] C. Tselios, I. Politis, S. Kotsopoulos, Enhancing SDN security for IoT-related deployments through blockchain, in: 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN, IEEE, 2017, pp. 303–308.

[39] U. Cisco, Cisco annual internet report (2018–2023) white paper, 2020.

[40] Y. Wu, F. Tao, L. Liu, J. Gu, J. Panneerselvam, R. Zhu, M.N. Shahzad, A bitcoin transaction network analytic method for future blockchain forensic investigation, IEEE Trans. Netw. Sci. Eng. (2020).

[41] W. Xia, Y. Wen, C.H. Foh, D. Niyato, H. Xie, A survey on software-defined networking, IEEE Commun. Surv. Tutor. 17 (1) (2014) 27–51.

[42] H. Zheng, Q. Wu, J. Xie, Z. Guan, B. Qin, Z. Gu, An organization-friendly blockchain system, Comput. Secur. 88 (2020) 101598.

[43] M. Wolf, D. Serpanos, Safety and security in cyber-physical systems and internet-of-things systems, Proc. IEEE 106 (1) (2017) 9–20.

[44] D.G. Pivoto, L.F. de Almeida, R. da Rosa Righi, J. Rodrigues, A.B. Lugli, A.M. Alberti, Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review, J. Manuf. Syst. 58 (2021) 176–192.

[45] P. Radanliev, D. De Roure, R. Nicolescu, M. Huth, O. Santos, Artificial intelligence and the Internet of Things in Industry 4.0, CCF Trans. Pervasive Comput. Interact. (2021) 1–10.