Peer-to-Peer Networking and Applications (2021) 14:392–402
https://doi.org/10.1007/s12083-020-00971-w

Security improvement in block chain technique enabled peer to peer network for beyond 5G and internet of things

S. Perumal Sankar[1] · T. D. Subash[2] · N. Vishwanath[1] · Deepa Elizabeth Geroge[1]

Received: 1 April 2020 / Accepted: 21 July 2020 / Published online: 1 August 2020

Abstract

Secured data transmission and data sharing have always been a challenge on the Internet of things-based networks. Blockchain-enabled peer to peer (P2P) networks are suitable infrastructure for the Internet of Things (IoT) and Beyond 5G (B5G) applications. The advantage is that the distributed nature of architecture and security services provided by this network extends its use in all sort of financial transactions. There are many issues related to IoT based networks; Heterogeneous IoT devices, security, energy issues. This paper implements data security by employing private blockchain in SDN and public blockchain for peer to peer communication and a secured authentication method to validate the blocks in the network. To increase confidentiality and non-repudiation, it implements an additional component; here, the sender signs the particular operation while transferring the data from one user to another user. It is published with a public key and Public-key value-based signature generated with the private key of the transaction. Nodes authenticate this operation based on Public key value-based signature thus generated. The cryptography with hashing process provides better immutability. The results show enhanced security during data transmission and improved throughput, response time, reduction in end-to-end delay and overhead when compared to the existing methods. This work uses Pyethereum tester tool under the Ethereum platform.

Keywords Blockchain · Peer to peer network · Software DefinedNetworks · D2D communication · Internet of things · 5G services · Secure network

1 Introduction

The advent of 5G and Beyond 5G technologies provides faster speeds and improved reliability. Usage of the Internet has seen phenomenal growth with the implementations of these technologies. Communication engineering has been exploring its high technical intelligence to cover the entire applications, namely 5G and B5G. The world witnesses massive changes, for the benefit of humans, in the name of information services and IoT, courtesy these technologies. The Technology, IOT which connect all appliances with wireless (CAW) has introduced the change in the whole scenario of the society, fetch everything in its place in a jiffy. This technology helps in presenting smartness everywhere to meet the futuristic requirements of All Time Connectivity (ATC) with the amplest capacity and extensive coverage. But, with the heterogeneity of IoT devices, the vulnerability in data security and non-availability of the central controller, communication among IoT devices in the network face more significant challenges. These new generation networks shall have to find solutions to all sort of problems in communication with an assured security level, guaranteed bandwidth and no latency (Table 1).

The solution for the issues could be achieved by involving novel multi-skilling techniques to a common platform and integrate with advance technologies. We have to propose an architecture that ensures data security and availability of the central controller. Over the years, peer to peer networking has crafted an exact network configuration by offering shared network nodes with equal responsibilities without a central server to share the files in both directions. The association of blockchain technology with peer to peer network still deeply entrench the security level of the P2P network, making it the most popular and trusted network for sharing the critical files. In such a scenario, we have to provide a network connecting

This article is part of the Topical Collection: *Special Issue on P2P Computing for Beyond 5G Network and Internet-of-Everything*
Guest Editors: Prakasam P, Ajayan John, Shohel Sayeed

✉ S. Perumal Sankar
spsankar2004@yahoo.co.in

[1] Toc H Institute of Science and Technology, Ernakulam, Kerala, India

[2] Mangalam College of Engineering, Kottyam, Kerala, India

Table 1 Stimulation Parameters Values

Emulator –SDN	EstiNet network simulator-wifi
Source controller Emulator	POX
Private and public blockchain	Ethereum / Pyethereum
Protocol	OpenFlow protocol
No of SDN controllers	six
No. of SDN Domains	six
Nodes	Ninety
Simulation time	100 s
IoT devices speed	10 m/s
Mobility model	Random waypoint model Traffic

IoT devices. We propose to use a P2P system for communication and data sharing and blockchain technology for security. The member nodes in Peer-to-peer architecture (P2P architecture) share their contribution and responsibilities during file transmission at any state without centralized server in the network. Moreover, it helps reduce bandwidth issues and communication delays. Further, it avoids a single point of network failures. Distributed nature of this network reduces the cost of data transmission among peer nodes, increases the data transmission rate and lessens the loading capacity of nodes. The work process happens simultaneously in the network that allows us to reduce a load of each peer when several peers are involved. Further, there will be a reduced impact on the system when some peers move away from the network. One disadvantage is that it does not have a centralized server.

A sound security system has to exhibit the three essential characteristics, namely availability of resources when needed, confidentiality- only authorized access the data and integrity. Blockchain technology provides all the required features. P2P provides distributed connectivity. To provide the central controller for the network, we delve into the concept of Software Defined Network (SDN). There are two essential components in SDN, namely controller and switch. As SDN separates the data plane from the control plane, we propose to use the SDN as a central controller.

The blockchain-enabled P2P network offers completely decentralized verification, validation and updating of transactions. It ensures autonomy, concealment of data, with consensus mechanism and immutability. Despite the newer strategies provided by the blockchain-enabled P2P network, it is vulnerable to frequent attacks. Sibyl attack is one among them. It happens when an attacker possesses many nodes, and he could easily compromise the system when he achieves a majority. Thus, it poses a threat in the public blockchain. Hence, to further strengthen the data security and meet the challenges, a new cut in edge technique is required to enhance the security level of the network. This paper explores various existing approaches to improve the security level of Blockchain-enabled P2Petwork, and it proposes a new technique that enhances the security system without third party intervention in communication. This significant improvement in data security will allow the use of the system for more applications in B5G technology.

New threats are largely evolving, and data hacking is still driven mainly by the intrusion of malicious nodes. The continuous effort of passive attackers to steal the information of the nodes are always a challenge and reduce the efficacy of the network. Mainly the blockchain technology makes a favourable impression in situations that required employing most reliable tight cybersecurity systems for data transmissions. New P2P networks support confidentiality and privacy.

The importance of this work is to come up with a most secured system that shows resilience against all possible attacks like Sybil attack, selfish mining, DNS Attack, DOS attack, Consensus delay and double-spending attacks. Selfish mining is a dishonest attempt to compromise the integrity of the network. Typically, all these attacks are due to the admission of new nodes without proper examination / no measures to find out their troths of pseudonymous of the nodes/failure to identify intruder nodes. Although the technologies are emerging to weed out some of these problems, still secure communication suffers from the attack of intellectual hackers who uses better ideas than anti hackers.

Blockchain Technology In general, security in peer to peer network needs improvement considering the decentralized architecture and the distributed protocols-dependent services. Some entities need secured data transfer; we need advance protection to data from threats. Blockchain technology implemented using P2P network provides accountability and validation of the nodes. This technology overcomes the MITM attack and EFAIL attack in electronic messaging and maintains the track records of complete transactions [1]. Initially, the purpose behind blockchain was to create the time records of the digital documents; it ensured that the documents could not be malformed. It is difficult to alter the data by meddling in-network since the validation process takes time because of the action happens in individual networks. Developing new applications using blockchain possesses new menaces like scalability, possible breach of privacy etc. These impediments need proper solutions [2].

Generally, the blockchain architecture consists of the infrastructure layer, platform layer, distributed computing layer, and application layer [3]. Infrastructure layer consists of storage facilities, simple nodes, mining nodes and full nodes, and network facilities. Platform layer helps the clients to access the application developed on top of a blockchain network. Platform layer assists Remote Procedure Calls [4], Web API [5], and Representational State Transfer (REST) API. Distributed computing layer guarantees fault tolerance, accessing data locally, privacy-preserving, immutability, authenticity, and security for the transaction data.

Immutability ensures tamper-proof of stored record in the ledger and updates it with consensus agreement; miner ensures new block generation. Also, the encryption technique provides user authentication [6], and the hashing technique provides data privacy [7]. Introduction of smart devices within the distributed computing layer offers privacy protection and energy security [8]. The application layer provides a digital asset transaction and smart contract execution. Blockchain is a critical technology in 6G applications which helps spectrum sharing [9] and terrestrial communication [10].

1.1 Aim of the research

To develop a new secure data transmission method between heterogenous IoT devices for an existing blockchain-enabled architecture for IoT devices. This network uses an SDN Controller. The proposed method would provide a secure method for transfer-of-files and its data.

The Paper organisation is given as under: Section 2gives a detailed account of the related works happened. In Section 3we define the problem. Section 4 provides proposed mechanism for secure transmission of transfer of files and its data between nodes of IoT networksSection 5 talks about results and discussion. Section 6 provides conclusion.

2 Related works

In related works, we analyze existing research papers that explore the Internet of Things, software-defined networks and blockchain and the integration of these technologies, their usefulness and challenges. The advantage is that the distributed nature of architecture and security services provided by this network extends its use in all sort of financial transactions.

The blockchain technology provides security and immutability. It needs implementation using a programming language. It allows agreement between nodes and ensures the trust of using the underlying platform. The programming practices of implementing blockchain related to different domains and platforms, related security issues are emphasized by the authors R. M. Parizi et al. [11] in their paper. The authors of [12] and [13] illustrated the uses of blockchain technology in intelligent accountings, e-government and medical data gatherings. In [14], the researches contributed an empirical evaluation of open-source automatic security analysis tools for the security vulnerability detection of Ethereum smart contracts written in Solidity. In the research paper [15], the authors suggested the utilization of blockchain for cybersecurity applications. The references [16, 17] described the details of the chain of blocks in the blockchain, how it records the details of transactions carried out and uses that for secure P2P network management without the help of intermediaries. S. Huh et al. [18] used Ethereum based blockchain to build the IoT configuration. In their research, the author did not consider the memory of the IoT devices to keep the records of the whole chain. In another paper [19], A. Dorri et al. elucidates the development of IoT applications using a developed blockchain, where clustered architecture is involved in minimizing the delay and other issues.

Abbas Yazdinejad et al. [20] proposed a novel Blockchain-enabled Packet Parser (BPP) architecture that depends on the features used in security. They employed a multivariate correlation approach on the packets in traffic to detect the attack. The authors Reza M. Parizi et al. [21] addressed Privacy Enhancing Techniques - Enabled with Side-chain (PETES) using Garlic Routing and Onion Routing (GOR) framework in blockchain structure. Abbas Yazdinejad [22] illustrated an SDN architecture using public and private blockchains enabled in P2P network communication for IoT applications. This document suggested a new routing protocol with a clustered structure to increase energy efficiency.

Intruders intrude in the stream of working architecture with a fake identity and try to grasp the data or damage the data in the regular-stream. Authentication is an essential tool to trust the devices/ nodes which sink/source the data from the protected set of network architecture. IoT research promoters advocate various valuable novel ideas for authentication to increase the security level of the complete architecture and defend it from destructive actions. SanazKavianpour et al. [23] reviewed the different authentication approaches to secure the IoT security and discussed the problems and opportunities of each approach. J. Wang et al. [24]. Suggested a blockchain for edge empowered smart grid using a mutual authentication protocol. L. Xiong et al. [25] introduced a new authentication method to enhance privacy in-network.

J. Wan et al. [26] recommended a decentralized blockchain structure for industrial IoT applications and the authors Z. Lu et al. of [27] contributed a privacy maintaining authentication framework. The authors L. Li et al. [28] initiated another privacy maintaining technique for credit coin application. Day by day, attackers follow new tactics to attack the network, which deteriorate the nature of the system and to reduce its importance. So the purpose of the design of the new architecture of the network will not be solved, and the designers try to introduce new anti-attacking strategies/ strengthen the securities in the network. Many authors concentrated their attention on network security. They initiated the research to maintain the privacy management architecture using blockchain M. U. Hassan et al. [29] proposed a privacy maintaining technique in mobile networks and services, particularly for 5G IoT systems.

Exploits the advantages of blockchain technology in access control mechanisms of resources, makes it very efficient in IoT and other applications. In this direction, the authors M. Ma et al. [30], S. Ding et al. [31], Z. Liu et al. [32] and M. Yang et al. [33] conducted their research and proposed their individual blockchain-based access control techniques. These expedited the study on the blockchain and invigorated the attention of scientist to find out more application using blockchain with P2P networks. Blockchain provides distributed ledger and decentralized resource allocation. Hence it is an appropriate technology for communication networks to solve the key issues and provide better solutions. Blockchain helps to maintain reliable resource allocation for video transcoding and delivery, as suggested by the author Y. Liu et al. [34], and for the purpose of efficient spectrum management by the researchers M. B. Weiss et al. [35]. Dynamic spectrum access using blockchain technology was described btK.Kotobi and S. G. Bilen [36].

Data transmission, Data storage and Data sharing are essential processes in IoT networks. Here, security challenges, data centre cost management and less complexity in computations are the bottlenecks. W. Liang et al. [37], contributed their work to propose a secure data transmission technique and C. H. Liu et al. [38] suggested a secure data collection technique for Industrial IoTs using blockchain. D. Li et al. [39] encouraged the blockchain decentralized architecture to secure data storage, and K. Fan et al. [40] discussed the blockchain-based data sharing techniques. Moreover, new methods to handle the problems of delay due to procrastination in auditing was addressed by Y. Zhang et al. [41] and they proposed a solution for cloud storage using blockchain.

The authors Aakanksha Tewari and B.B. Gupta [42], proposed an authentication method based on ECC mechanism involving RF ID tags for IoT applications. The novelty of this work is producing the new public and private key pseudo random number generator and ECE for every session. The authors proved security of RF ID authentication protocol used in this work through security analysis. The blockchain technology has been known for its robustness in securing the system. We have public and private blockchain. The blockchain is decentralised P2P networks. Online purchasers use to refer to the Reputation evaluation system. Typically, the system uses a third party to manage such systems. The use of the third party risks the privacy of the users. Haoxuan Li, et al [43] addressed the issue of privacy, blockchain stores the evaluation information instead of the third party. The consistent technological improvements in communication and the use of newer technologies with gaps endanger security while transmitting data. It is all the more relevant in securing IoT where we need to protect connected heterogeneous devices in the network. Christos Stergiou et al. [44] introduces one novel system which integrates IoT with cloud computing. It presents a new architecture wherein it places a security wall between the internet and the cloud which takes care of all the security issues. The cloud now takes care of the privacy issues.

Despite the usefulness of IoT, it is vulnerable to online attacks. To strengthen the IoT with due consideration to it having the limited resources, Aakanksha Tewari, *B. B. Gupta [45] investigate the security issues in all three layers of IoT and crosslayer heterogeneous integration issues. Researchers in [46] use new technique to handle the fairness. This technique controls the infidelity of transaction among the Leechers and improves the fairness; also solve the free-riding problems. Preserving user's anonymity has inherent difficulty in P2P networks, which is unstructured. Many solutions offered were in similar lines as given to the client-server method, which is structured. Authors A. Naghizadeh et al. [47] presents structural-based tunnelling (SBT) to provide anonymity for the peer to peer circular networks. The newly incorporated chords to SBT help manage designs for the applications. The disadvantage in this method is that there is a trade-off between performance and security. Authors Alireza Naghizadeh et al. in [48], propose a tunnelling method to offer receiver's anonymity in circular P2P architectures. This mechanism provides higher security by preserve the identity of receivers. Optimising the size of the tunnel reduces the routing cost.

3 Problem definition

The essential characteristics of blockchain-like distributed nature, secure communication and no intermediaries allow the Blockchain-enabled Peer to Peer network to be the right choice for Beyond-5G communication. Blockchain-enabled P2P network satisfies the anticipation of users in primary potential services like an intelligent way of managing security issues, processing the data and efficiently handling the resources. Among all these possible primary services, this work concentrates on secure services, discusses the challenges and suggests a new secure transmission for this network. Nodes in the blockchain-enabled networks perform similar kinds of work. While adding new blocks in the network, the blockchain protocols direct all nodes in the network to verify the node's information based on a cryptographic technique that ensures the immutability of information. The primary existence in the blockchain architecture is the distributed computing layer, in which the role of consensus protocols in the consensus sub-layer is an essential layer behind all Ethereum, Hyperledger, or any other blockchain. Ethereum and Bitcoin are some of the examples of permissionless blockchain. Here one can use probabilistic consensus. At the same time, Hyper ledger and fabric are permissioned-blockchains that employ deterministic consensus. The duty of consensus protocol is authenticating the blocks, ordering the blocks and ensuring the concordance of all other nodes. Proper authentication strategies introduce intensified screening methods to validate the block and eliminate the probable risks to enhance the security service. Consensus protocols (algorithms) make a particular set of indentures among nodes in the network, synchronize the nodes, ensure all nodes agreed to the truth, and ensure the confirmation that all transactions validations are as per the rule.

4 Proposed mechanism

The specific objective is to provide an elevated secure mechanism for data transferring between the users in a blockchain-enabled network. This work selected an existing cluster architecture, using peer to peer network-enabled by blockchain-based SDN controllers to execute and validate the proposed secure. The clustered architecture comprises of many SDN domains, in which, each cluster domain is connected to another using a public blockchain (P2P network between SDN Controllers. All SDN domains connect to cloud storage. In each SDN domain, each cluster head is an SDN controller. It is linked to one private blockchain. The IoT devices are connected to SDN Controllers. Network management is through IoT- based-blockchain. This network has private block chain in SDN Domain. The network shall have heterogeneous IoT devices are heterogeneous. The P2P network that connects the controller provides the security of the data.

This work concentrates on these points and intends topoint out a perfect method able to face chaotic situations using a new authentication strategy to validate the blocks in theblockchain-enabled P2P network. The organized structure of blockchain-enabled network shown in Fig. 1 always shows efficiency in its operation. The SDN controller is a cluster head coordinates the entire cluster, and this structure uses private and public blockchains. As it is a cluster structure, the public blockchain-enabled between the controllers in P2P keeps ledger at the small number and adds secure communication. New SDN domain can join in this structure by generating a new block and avail completed transactions of the particular controller. But private blockchain-enabled between the nodes and controllers requires validation as per paradigm set by the network. Figure 1 explains the new enhanced authentication method for file transfer through the SDN controller using a private and public key. While transferring data files from user A to B, the particular operation is signed by A. It will be published with the public key and Public-key value-based signature generated with the private key of the transaction. This is sent to the whole network; Nodes authenticate this operation based on Public key value-based signature generated with the private key. Now only the users know the value-based signature can decode the data from the File. The value-based signature approach is preventing the entire transaction from the attacks and malfunctioning of the data transfer operation. The encoding and decoding algorithms used in the above data transaction is given below to recognize the procedure in detail.

Figure 2 states the encoding and decoding flow of source A, SDN, destination B at the initiator end and the receiver end.

4.1 Encoding and decoding flow

4.1.1 File Signature and Encodeby A

- A wants to transfer its File to B
- Generate identity A (ID_A, N_A) and B (ID_B, N_B)
- Then Compute Hash value the $PW_A = h\ (N_A \,||\, N_B)$
- T1 is support value is calculated by $T1 = ID_A \oplus N_B$
- Public key value based signature generated $SA_A = h\ (T1 \| PW_A) \oplus ID_B$
- Private Key based Encoding $EF = Enc(F,PK)$
- Finally add the Public key based signature in the encoded file using

$$SA_{Enc} = E_{SDN}\ (ID_B, N_B, SA_A, T1,EF).$$

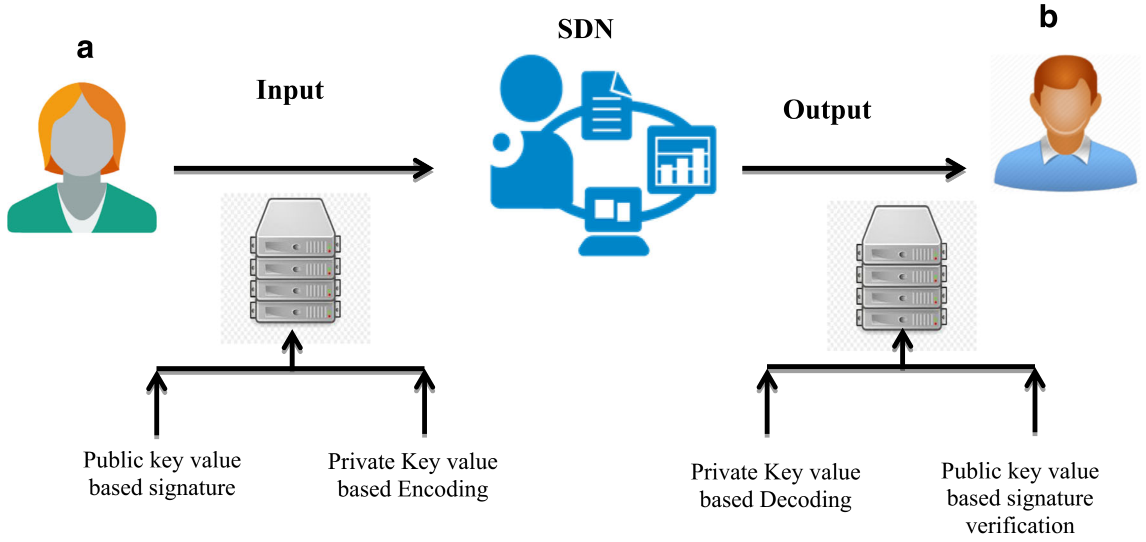

a
Input
SDN
Output
b
Public key value based signature
Private Key value based Encoding
Private Key value based Decoding
Public key value based signature verification

Fig. 1 File Transfer Technique through SDN controller using private and public key

4.1.2 SDN Block chain

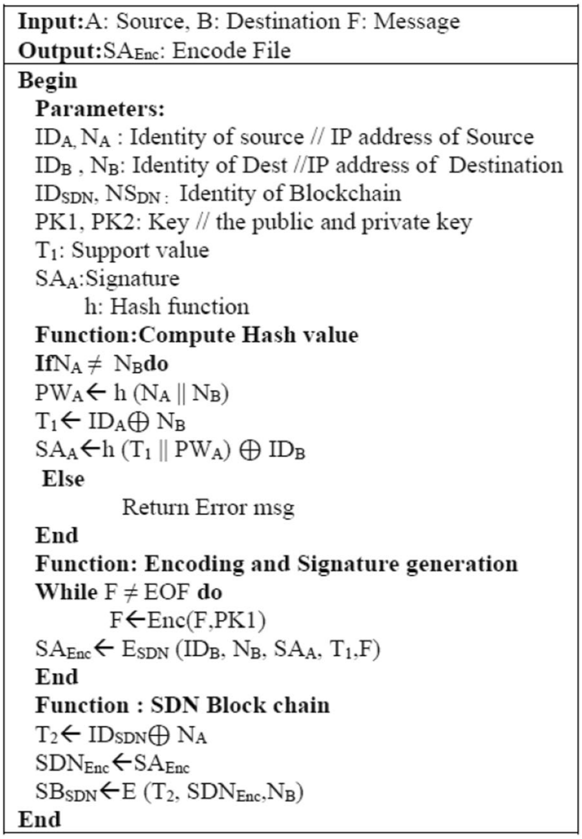
- A sends SA_{Enc}that are received from A to SDN.
- Generate identity of block chain ID_{SDN}, NS_{DN}
- Support value is calculated $T2 = ID_{SDN} \oplus N_A$
- Assign the encoded file to the blocks using $SDN_{Enc} = SA_{Enc}$
- Add Authentication to the SDN $SB_{SDN} = E\ (T2, IDB, NB)$

4.1.3 File Signature verifies and Decode by B

- After receiving the message, B first decrypts $S_{\ SDN} = D\ (SB_{SDN})$ to reveal $S_{\ SDN}$, SDN_{En}, T2.
- Then calculate $T2 = T1 \oplus N_B$ and $SA_A = h\ (T2 \parallel PW_A) \oplus ID_B)$, Then SA_A checks whether $SB_{FA} = SB_{FA}$If they are equal, File is decode otherwise not
- The file is decoded using private key $S = D\ (SDN_{Enc})$

4.2 Encoding and decoding algorithms

Algirithm 1: Encoding.



```
Input:A: Source, B: Destination F: Message
Output:$SA_{Enc}$: Encode File
Begin
  Parameters:
  $ID_A$, $N_A$ : Identity of source // IP address of Source
  $ID_B$ , $N_B$: Identity of Dest //IP address of  Destination
  $ID_{SDN}$, $NS_{DN}$ :  Identity of Blockchain
  PK1, PK2: Key // the public and private key
  $T_1$: Support value
  $SA_A$:Signature
       h: Hash function
  Function:Compute Hash value
  If$N_A \neq N_B$do
  $PW_A \leftarrow h\ (N_A \parallel N_B)$
  $T_1 \leftarrow ID_A \oplus N_B$
  $SA_A \leftarrow h\ (T_1 \parallel PW_A) \oplus ID_B$
   Else
            Return Error msg
  End
  Function: Encoding and Signature generation
  While $F \neq EOF$ do
          $F \leftarrow Enc(F,PK1)$
  $SA_{Enc} \leftarrow E_{SDN}\ (ID_B, N_B, SA_A, T_1,F)$
  End
  Function : SDN Block chain
  $T_2 \leftarrow ID_{SDN} \oplus N_A$
  $SDN_{Enc} \leftarrow SA_{Enc}$
  $SB_{SDN} \leftarrow E\ (T_2, SDN_{Enc},N_B)$
End
```

Algorithm 1 is a description of the blockchain-based data Encoding and Signature generation. The process sequence for proposed blockchain P2P networks as follows:

Step1 : Compute the Hash value

- First check the identity of the source and destination $\mathbf{N_A \neq N_B}$ if there is equal terminate the combination otherwise Compute the values $\mathbf{PW_A, T_1, SA_A}$.

Step2 : Encoding and Signature generation

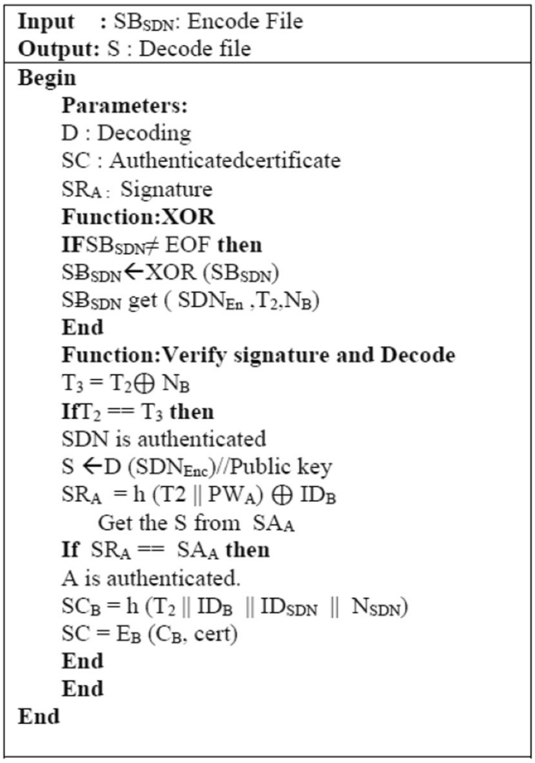
- Check the condition End of Packet (EOP) if it is true to do encoding and signature generation process.
- Source **A** generate the data and send to the destination **B**
- Source **A** encrypts the diagnosis data **F** into cryptograms using the private key **PK1**.
- The **F** cryptograms the analysis data from the ring signature as **SAEnc.** It can be taken as a pattern to check the same data kept twice in blockchain storage. The **SAEnc** sends the series of data to the blockchain network.

Step3 : SDN Blockchain.

The analysis data from the Source A along with **SAEnc** of the files are then sent to the blockchain network Add one more signature for the blockchain using T_2, SB_{SDN} to be data are stored in an SDN.

Algorithm 2 is a portrayal of the entire blockchain-based data Signature verifies and decode. The process of blockchain decoding and verification of P2P networks as follows:

Algorithm 2: Signature verifies and decode.



```
Input    : $SB_{SDN}$: Encode File
Output: S : Decode file
Begin
      Parameters:
      D : Decoding
      SC : Authenticatedcertificate
      $SR_A$ :  Signature
      Function:XOR
      IF$SB_{SDN} \neq$ EOF then
      $SB_{SDN} \leftarrow XOR\ (SB_{SDN})$
      $SB_{SDN}$ get ( $SDN_{En}$ ,$T_2$,$N_B$)
      End
      Function:Verify signature and Decode
      $T_3 = T_2 \oplus N_B$
      If$T_2 == T_3$ then
      SDN is authenticated
      $S \leftarrow D\ (SDN_{Enc})$//Public key
      $SR_A\ = h\ (T2 \parallel PW_A) \oplus ID_B$
          Get the S from  $SA_A$
      If  $SR_A ==\ SA_A$ then
      A is authenticated.
      $SC_B = h\ (T_2 \parallel ID_B\ \parallel ID_{SDN}\ \parallel\ N_{SDN})$
      $SC = E_B\ (C_B, cert)$
      End
      End
End
```

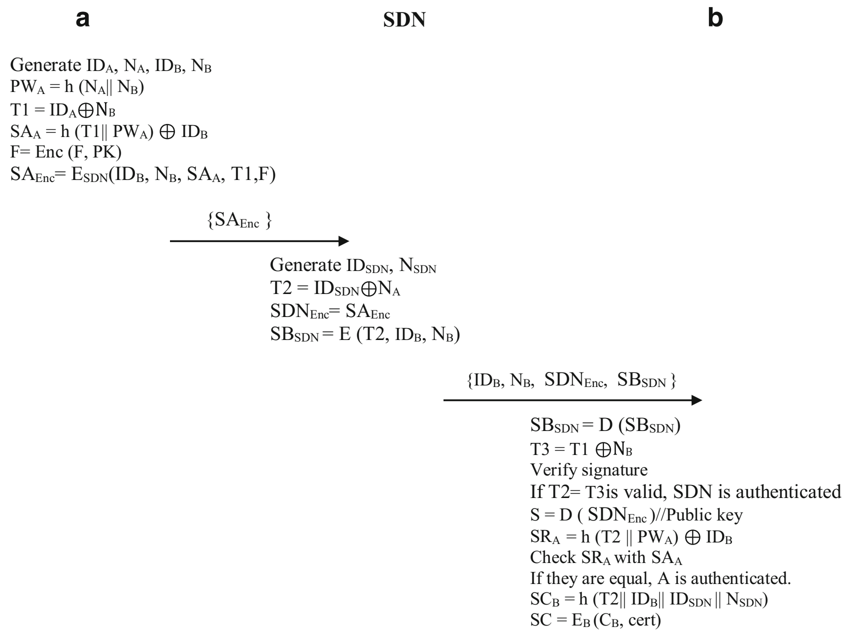

a
SDN
b
Generate ID_A, N_A, ID_B, N_B
$PW_A = h (N_A|| N_B)$
$T1 = ID_A \oplus N_B$
$SA_A = h (T1|| PW_A) \oplus ID_B$
F= Enc (F, PK)
$SA_{Enc}= E_{SDN}(ID_B, N_B, SA_A, T1,F)$
$\{SA_{Enc} \}$
Generate ID_{SDN}, N_{SDN}
$T2 = ID_{SDN} \oplus N_A$
$SDN_{Enc}= SA_{Enc}$
$SB_{SDN} = E (T2, ID_B, N_B)$
$\{ID_B, N_B, SDN_{Enc}, SB_{SDN} \}$
$SB_{SDN} = D (SB_{SDN})$
$T3 = T1 \oplus N_B$
Verify signature
If T2= T3is valid, SDN is authenticated
$S = D (SDN_{Enc})$//Public key
$SR_A = h (T2 || PW_A) \oplus ID_B$
Check SR_A with SA_A
If they are equal, A is authenticated.
$SC_B = h (T2|| ID_B|| ID_{SDN} || N_{SDN})$
$SC = E_B (C_B, cert)$

Fig. 2 Encoding and Decoding flow of source A, SDN, destination B

Step1 **: XOR**

- Check the condition ***$SB_{SDN} \neq EOP$*** if it is true XOR the ***SB_{SDN}*** and separate the all values using ***S_{SDN} get (SDN_{En}, T_2, N_B)*** otherwise stop the decoding process of ***B***

Step2 **:** Verify signature and Decode

- First, calculate verifying signature generation using ***$T_3 = T_2 \oplus N_B$***
- Check the identity of SDN authentication using ***$T_2 == T_3$*** if there is not equal terminate the combination otherwise Compute the values **S, SR_A,** get the **S** from **SA_A**.

Check the identity of ***B*** authenticated using ***SR_A***

- ***$== SA_A$*** if there is not equal terminate the destination otherwise access the decoding packet and set the certification to the B is authentication using ***SC_B, SC.***

4.3 Analytical evaluation of the proposed method

This part talks about the analytical evaluation. It helps to analyse and estimate the performance based on parameters namely Throughput, Time overhead. Latency and bandwidth. For this we use queing model M/H/2/1.

Let λ_i, be Packet arrival rate at the i^{th} device, The arriving rate λ follows the poison distribution.

Let μ represent the service rate. It follows the exponential distribution.

Arrival rate given value = λ_i at the i^{th} node,

Arrival time given value = $1/ \lambda_i$.

Service rate given value = μ,

Service time given value = $1/ \mu$.

The incorrect packets reaching the SDN controller $\rho = \lambda/ \mu < 1$, to find probability of n packets in the system, when $n = 0$, $p(0) =$ idle rate = $1-(\lambda/ \mu)$,

$n = 1$, $p(1) = \rho x p(0) = (\lambda/ \mu) [1-(\lambda/ \mu)]$.

$p(n) = (\lambda/ \mu)^n [1-(\lambda/ \mu)]$, gives the probability of n packets in the system.

Average number of packets in the system (Ls) = utilisation rate /idle rate = $\lambda/ (\mu- \lambda)$.

Average number of packets in the Queue (Lq) = $[\lambda/ (\mu- \lambda)] = [\lambda/ \mu]$ Ls.

Average waiting time for a packet in the system $W_s = 1/ (\mu- \lambda)$.

Average waiting time for a packet in the queue $W_q = (\lambda/ \mu) 1/ (\mu- \lambda) = (\lambda/ \mu) W_s$.

The expected length of the non-empty queue = Lq' = Lq/ $p(n > 1) = \mu/ (\mu- \lambda)$, Where $\rho = \lambda/ \mu < 1$.

By little law, expected time for an IoT device to process the packets = $1/ (\mu- \lambda)$.

5 Results and discussions

This study carried out a systematic evaluation to verify the performance metrics like throughput, end to end delay, latency, Time overhead and response time to prove the pieces of evidence of the proposed research. This work used the Pyethereum tester tool under the Ethereum platform to execute and test the public and private blockchains. This work also has evaluated routing and compared with familiar routing protocols. For simulation purpose, this study employs six open daylight SDN controllers

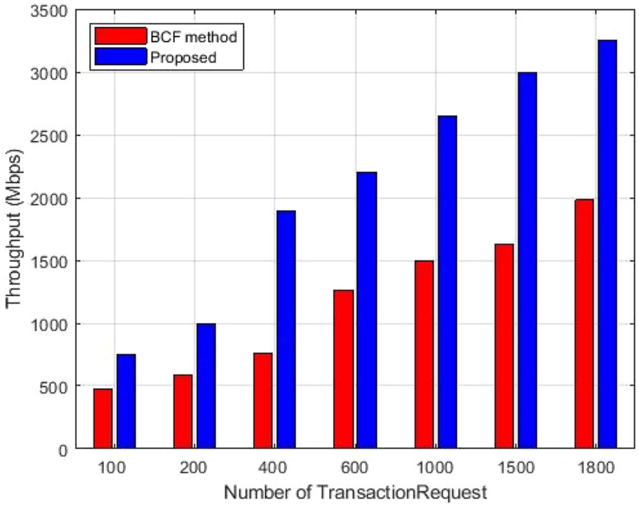


Fig. 3 Throughput-comparison

with 90 nodes using the random waypoint mobility model and simulation runs for 100 s.

5.1 Performance evaluation

Here we provide the details of implementation, the environment under which we test the proposed method. The metrics for evaluation of the results are immutability, throughput and time overhead, bandwidth and latency, response time and an end to end delay. To implement the Software-Defined Network (SDN), We used wifi simulator EstiNet network simulatortogether with the open-source controller pox. Each node on the EstiNet represents a process. It allows many applications to run on it. This method is applied in cluster architecture using SDN controller as a cluster head and executed, tested using Pyethereum tester tool (for implementing blockchain) under the Ethereum platform. The controller which contains blockchain, connects to cloud. The system uses Blockchain-Fundamental (BCF) to compare the performance. BCF uses hashing algorithm. Further it uses proof of work. These are some of the overheads.

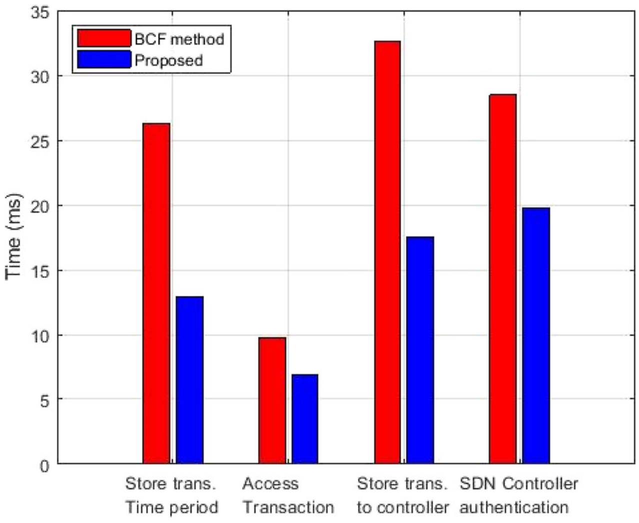


Fig. 4 Time overhead

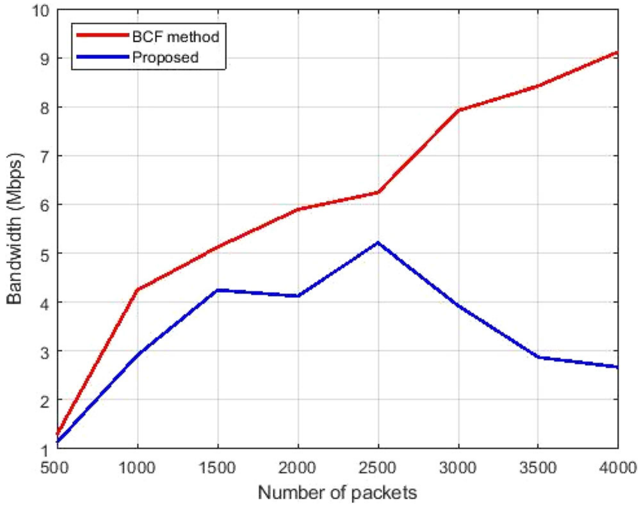


Fig. 5 Bandwidth requirements

We implement private and public blockchain and test them and do our evaluation using Pyethereum. Simulation of data sharing, transmitting of document files in the integrated environment of SDN and blockchain is done. With the help of Pyethereum tester tool installed in a virtual machine and EstiNet, we create different SDN networks with different IP addresses. We used open-daylight protocol. For simulation purpose, this study employs six open daylight SDN controllers with 90 nodes using the random waypoint mobility model and simulation runs for 100 s.

5.2 Evaluation metrics

5.2.1 Immutability

There is no possibility to tamper the block in this blockchain and provides better immutability. Many attempts have been

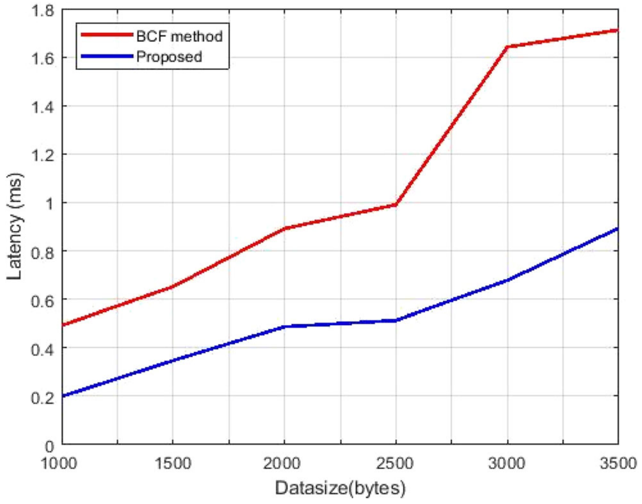


Fig. 6 Latency of data transmission

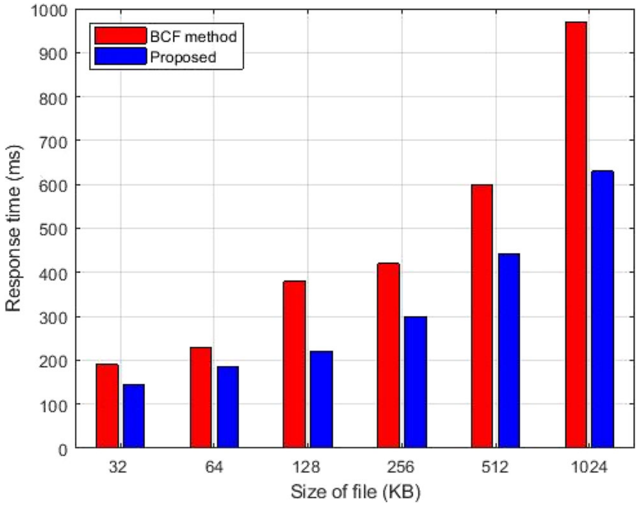


Fig. 7 Comparison of Response time

taken, and the network has been given considerable importance to immutability due to the new type of cryptography with blockchain hashing process used in this network. While transferring the data between the nodes, the sender signs the particular operation and the system publishes it with the public key; it generates a peer Public key value-based signature with the private key of the transaction.

5.2.2 Throughput and time over head

In the network, the IoT devices request for transaction among themselves. The number of such transaction in a network is the throughput time. Figure 3 shows the comparison of throughput by this process and BCF method. In this verification, several transaction requests up to 1800 are recorded, and it displays a better result. Even while enhancing the security level, this work did not compromise with the throughput. Each node in the blockchain-enabled to peer network using SDN controller gets support for a better transaction through this process. As a continuation of this result discussion, this paper discusses the time overhead also. From Fig. 3, one could notice the development in throughput at every set of transaction. Figure 4 shows the comparisons of time overhead with the BCF method. The result shows that there is no much change in the time overhead; even a small difference is there in milliseconds.

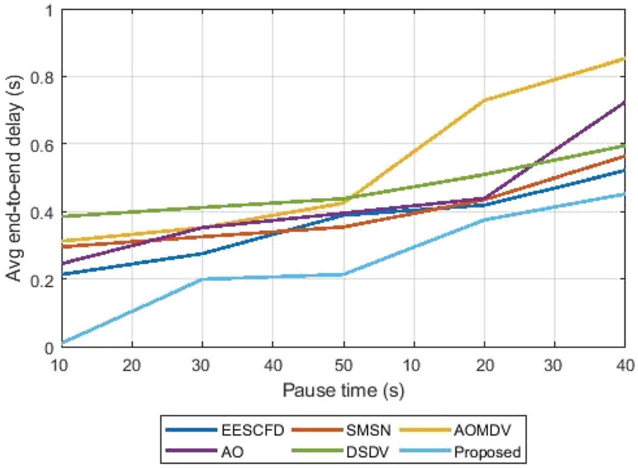


Fig. 8 Comparison of end-to-end delay

5.2.3 Bandwidth and latency

After including the proposed authentication method, the bandwidth and latency in the file transfer are evaluated and plotted in Figs. 5 and 6, respectively. As noted earlier, this simulation follows the random waypoint mobility model for assessing random paths used for file transfer. Through this work, the bandwidth and latency are less compared with the BCF method. There is no much difference in the latency of data transfer between using this process and the BCF method. The noteworthy point is, after authenticating this operation based on Public key value-based signature generated with the private key, the latency in data transfer is comparable with the BCF method. Regarding bandwidth, after 2500 data packets, there will be a reduction in bandwidth as the SDN controller choose the most efficient paths for the data transfer.

5.2.4 Response time and end to end delay

Figures 7 and 8 reveals the metrics like response time and an end to end delay of the network on data transfer from one node to another node. This fast response reduces energy consumption and increases the performance of this network. This structure takes almost a little bit lesser response time even after introducing a new security strategy to validate the blocks. Figure 8 compares the end-to-end delay of this network with those familiar network routing protocols like AODV, DSDV, AOMDV, SMSN and EESCFD [22].

6 Conclusion

Today, we face extreme challenges in terms of preserving privacy, data security and integrity with the ever-increasing usage of IoT devices and demand for smart services. Addressing these issues should be the immediate priority of the researchers. To address this issue, we presented a new authentication method to validate the block in the blockchain-enabled peer to peer network with SDN controller. This method is applied in cluster architecture using SDN controller as a cluster head and executed, tested using Pyethereum tester tool under the Ethereum platform. The inclusion of the validation strategy makes our proposed method doing far better when compared to the existing method like BCF, and existing DSDV, SMSN, AODV concerning the metrics like throughput, end to end delay, latency, Time overhead and response time.

The new strategy provides the solution to the growing challenges in the security of data transfer in IoT and financial applications. As a future process, we plan to reinforce the dynamic biometric signals in this new validation strategy; will be applied to the high-level architecture to enable the transaction more secure through the service of a blockchain-enabled peer to peer network.

References

1. Kahina Khacef, Guy Pujolle, (2019), "Secure Peer-to-Peer communication based on Blockchain",Workshops of the International Conference on Advanced Information Networking and Applications WAINA 2019: Web, Artificial Intelligence and Network Applications pp 662-672
2. Irani Acharjamayum, Ripon Patgiri, Dhruwajita Devi,"Blockchain: A Tale of Peer to Peer Security",IEEE Symposium Series on Computational Intelligence SSCI 2018,978–1–5386-9276-9/18/ $31.00c 2018 IEEE
3. Leila Ismail, Huned Materwala, Symmetry-MDPI, 2019, doi: https://doi.org/10.3390/sym11101198, Article A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions
4. B. Remote Procedure Call—Wikipedia.Available online: https://en.wikipedia.org/wiki/ Remote procedure call. (accessed- November 2019)
5. Web API—Wikipedia. Available online: https://en.wikipedia.org/wiki/Web_API (accessed -November 2019)
6. Merkle RC (1988) "A Digital Signature Based on a Conventional Encryption Function", Proceedings of the Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, CRYPTO 87, Santa Barbara, CA, USA, 23–27 August 1988. Springer, London, pp 369–378
7. Swan F, Blockchain M (2015) Blueprint for a new economy. O'Reilly Media, Inc., Newton
8. K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks", IEEE Internet of Things Journal, 2019, Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks
9. Zhang Z, Xiao Y, Ma Z, Xiao M, Ding Z, Lei X, Karagiannidis GK, Fan P (2019) 6G wireless networks: vision, requirements, architecture, and key technologies. IEEE Veh Technol Mag 14(3):28–41
10. J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned aerial vehicle assisted cellular networks: an operators perspective", IEEE Internet of Things Journal,2019
11. R. M. Parizi, Amritraj, and A. Dehghantanha, "Smart contract programming languages on blockchains: An empirical evaluation of usability and security", in International Conference on Blockchain, pp. 75–91, Springer, 2018
12. M. Mettler, "Blockchain technology in healthcare: The revolution Starts Here", in 2016 IEEE 18th International Conference on e-HealthNetworking, Applications and Services (Healthcom), pp. 1–3, IEEE, 2016
13. M. Pilkington, "11 blockchain technology: principles and applications," Research handbook on digital transformations, vol. 225, 2016
14. R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and A. Singh, "Empirical vulnerability analysis of automated smart contractssecurity testing on blockchains", in Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering, pp. 103–113, IBM Corp., 2018
15. P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.- K. R. Choo, "A systematic literature review of blockchain cybersecurity", Digital Communications and Networks, 2019
16. R. M. Parizi and A. Dehghantanha, "On the understanding of gamification in blockchain systems",in 2018 6th International Conferenceon Future Internet of Things and Cloud Workshops (FiCloudW), pp. 214–219, IEEE, 2018
17. S. R. Basnet and S. Shakya, "Bss: Blockchain security over software defined network", 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 720–725, IEEE, 2017
18. S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," 2017 19th International Conference on Advanced Communication Technology (ICACT), pp. 464–467, IEEE, 2017
19. A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT", Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, pp. 173–178, ACM, 2017
20. Abbas Yazdinejad, Reza M. Parizi, Ali Dehghantanhaand, Kim-Kwang Raymond Choo, "P4-to-Blockchain: A Secure Blockchain-enabled Packet Parser for Software Defined Networking", Computers & Security 2019, doi: https://doi.org/10.1016/j.cose.2019.101629
21. Reza M. Parizi, Sajad Homayoun, Abbas Yazdinejad, Ali Dehghantanha, Kim-Kwang Raymond Choo,"integrating privacy enhancing techniques intoBlockchains using Sidechains", proceedings of the 32nd IEEE candian conference on electrical and computer engineering, 2019
22. Abbas Yazdinejad, Reza M. Parizi, Ali Dehghantanha, Qi Zhang, Kim-Kwang Raymond Choo,"an energy-efficient SDN controller architecture for IoT networks with Blockchain-based security", IEEE Trans Serv Comput, 2020
23. SanazKavianpour BS, Azam S, Zamani M, Samy GN, De Boer F (2019, Article ID 5747136, 14 pages) A Systematic Literature Review of Authentication in Internet of Things for Heterogeneous Devices. J Comput Netw Commun. https://doi.org/10.1155/2019/574713
24. J. Wang, L. Wu, K.-K. R. Choo, and D. He, "Blockchain based anonymous authentication with key management for smart grid edge computing infrastructure", IEEE Transactions on Industrial Informatics, 2019
25. L. Xiong and L. et al., "A blockchain-based privacy-awareness authentication scheme with efficient revocation for multi-server architectures", IEEE Access, vol. 7, pp. 125 840–125 853, 2019
26. J. Wan, J. Li, M. Imran, D. Li et al., IEEE Transactions on Industrial Informatics, 2019, A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory
27. Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for vanets," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019
28. Li L, Liu J, Cheng L, Qiu S, Wang W, Zhang X, Zhang Z (2018) Creditcoin: a privacy-preserving blockchain-based incentive announcementnetwork for communications of smart vehicles. IEEE Trans Intell Transp Syst 19(7):2204–2220
29. Hassan MU, Rehmani MH, Chen J (2019) Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions. Futur Gener Comput Syst 97: 512–529
30. M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario", IEEE Access, vol. 7, pp. 34 045–34 059, 2019

31. S. Ding, J. Cao, C. Li, K. Fan, and H. Li, “A novel attribute-based access control scheme using blockchain for IoT,” IEEE Access, vol. 7,pp. 38 431–38 441, 2019
32. Z. Liu, L. Gao, Y. Liu, X. Guan, K. Ma, and Y. Wang, IEEE Transactions on Industrial Informatics, 2019, Efficient QoS Support for Robust Resource Allocation in Blockchain-based Femtocell Networks
33. Yang M, Margheri A, Hu R, Sassone V (2018) Differentially private data sharing in a cloud federation with blockchain. IEEE Cloud Computing 5(6):69–79
34. Y. Liu, R. Yu, X. Li, H. Ji, and V. C. Leung, IEEE Transactions on VehicularTechnology, 2019, Decentralized Resource Allocation for Video Transcoding and Delivery in Blockchain-Based System With Mobile Edge Computing
35. M. B. Weiss, K. Werbach, D. C. Sicker, and C. Caicedo, IEEE Transactions on Cognitive Communications and Networking, 2019, On the Application of Blockchains to Spectrum Management
36. Kotobi K, Bilen SG (2018) Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networksenhances security and user access. IEEE Veh Technol Mag 13(1):32–39
37. W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, “A securefabric blockchain-based data transmission technique for industrial internet-of-things”,IEEE Transactions on Industrial Informatics, 2019
38. C. H. Liu, Q. Lin, and S. Wen, “Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning”, IEEETransactions on Industrial Informatics, 2018
39. Li D, Du R, Fu Y, Au MH (2019) Meta-key: a secure data-sharing protocol under blockchain-based decentralized storage architecture. IEEE Networking Lett 1(1):30–33
40. Fan K, Ren Y, Wang Y, Li H, Yang Y (2017) Blockchain-basedefficient privacy preserving and data sharing scheme of content-centric network in 5G. IET Commun 12(5):527–532
41. Y. Zhang, C. Xu, X. Lin, and X. S. Shen, IEEE Transactions on Cloud Computing, 2019, Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors
42. Aakanksha Tewari and B.B. Gupta, "A novel ECC-based lightweight authentication protocol for internet of things devices", Int. J. High Performance Computing and Networking, Vol. 15, Nos. 1/2, 2019
43. Haoxuan Li, Hui Huang, Shichong Tan, Ning Zhang and Xiaotong Fu,"A new revocable reputation evaluation system based on blockchain", Int. J. High Performance Computing and Networking, Vol. 14, No. 3, 2019
44. Christos Stergiou, Kostas E.Psannis, Brij B. Gupta and Yutaka Ishibashi, "Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT",Sustainable Computing: Informatics and Systems,Volume 19, September 2018, Pages 174–184
45. Aakanksha Tewari BB (2020) Gupta, "security, privacy and trust of different layers in internet-of-things (IoTs) framework ". Future Generation Comput Syst 108:909–920
46. Berenjian SSaeed Hajizadeh and Reza Ebrahimi Atani, "an incentive security model to provide fairness for peer-to-peer networks", 2019 IEEE conference on application. Inform Netw Secur (AINS). https://doi.org/10.1109/AINS47559.2019.8968699
47. Naghizadeh A, Berenjian S, Meamari E, Atani RE (2016) Structural-based tunneling: preserving mutual anonymity for circular P2P networks. Int J Commun Syst 29:602–619
48. Alireza Naghizadeh; Samaneh Berenjian ; Behrooz Razeghi; Saghi Shahanggar ; Nima Razagh Pour, "Preserving receiver's anonymity for circular structured P2P networks”, 2015 12th Annual IEEE Consumer Commun Netw Conference (CCNC), https://doi.org/10.1109/CCNC.2015.7157949

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