Blockchain-Based Solutions for Cybersecurity: Architecture, Applications, and Review

Tushar Bhardwaj, Vivek Anand Kamat, and Gaurav Dwivedi

Abstract In recent times, blockchain technology has gradually come out to be the most frequent leveraged mechanism for securing the data storage and transfer via the trustless, decentralized, and peer-to-peer ecosystems. Blockchain is essentially a distributed ledger that operates in a peer-to-peer network and contains a record of all the transactions that have been executed or confirmed among the participants or nodes. In this book chapter, the authors have explained the detailed architecture of blockchain technology and its integration with cybersecurity applications. This integrated architecture delivers a clear understanding to the readers about the working mechanism of blockchain technology in empowering the security and privacy of the user data in various cybersecurity domains. This book chapter talks about the roles and responsibility of blockchain technology in transforming the cybersecurity applications such as privacy, security, accountability, and integrity of data in various security domains such as mitigating DDoS attacks, biometric private keys, Securing DND, and data veracity. In addition, in this book chapter, the authors have discussed various applications of blockchain to cater cybersecurity, such as data storage and sharing, IoT, Network Security, Utility of World Wide Web (WWW), and Private user data.

Keywords Blockchain · Cyber security · Blockchain architecture · Integration of machine learning and cybersecurity

T. Bhardwaj (✉)
Applied Research Center, Florida International University, Miami, USA
e-mail: tushar.bhardwaj@fiu.edu

V. A. Kamat · G. Dwivedi
Florida International University, Miami, USA
e-mail: vkamat@fiu.edu

G. Dwivedi
e-mail: gdwiv001@fiu.edu

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_3

1 Introduction

Blockchain is a decentralized cryptocurrency data management and transaction technology developed in 2008 [1]. The interesting attributes that ensures security, anonymity without a control by any organization makes this technology interesting [2, 3]. These qualities have led to an exponential growth in creation and implementation of several cryptocurrency and their rapid adoption by financial institutions due to the ledger structure. The structure processes a digital ledger of transactions that is generated and distributed to computers on a network. This ledger is not controlled or owned by any central authority and can be viewed by all users. Since the data is distributed in many interlocked systems, at least 50% of these systems in the network need to be compromised for successful hacking. This might not be successful as an attempt to hack the network or secure the currency from another account might fail as there are multiple identical copies of same ledger stored as backups. These backup copies can in turn deliver the funds in the compromised or hacked account. Blockchain technology has the potential to prevent these attacks maintaining security and privacy of the network. There have been reports that bitcoin transaction had been compromised [4]. Most of the reported cases of hacking have been due to unsecure holding and storage of bitcoin private keys which were leaked or misplaced. Since the development of bitcoin several blockchain systems, predominantly "ethereum" have emerged and grown allowing secure network and transactions to public and private entities. There are various domains of cybersecurity where blockchain can be very useful, such as mitigating DDoS attacks, biometric private keys, Securing DND, and data veracity, as shown in Fig. 1. The unique security characteristics has also been a major subject of scientific researcher raising interest among individual developers, programmers, and large industrial partners.

Blockchain is publicized as a technology that has the capability to provide a robust cybersecurity solution with a better privacy and data management. Due to the

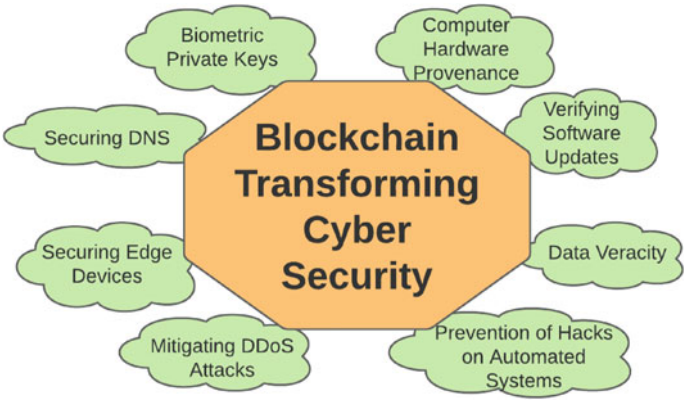

Fig. 1 Blockchain solutions for cybersecurity

growing trend in cryptocurrency transactions, the blockchain could now enable newer decentralized applications. These applications can further provide the foundation for major Internet security platforms. The advent of multi-signature (multisig) protection in development has great potential in improving security and privacy. The rapid growth potential in crypto currency technology has thus created enormous research potential especially in the area of security and privacy [5]. Therefore, it is important to identify the implications and limitations of existing research specifically in the area of blockchain security, to understand emerging cyber security threats and find relevant practical solutions. An in-depth literature review is therefore necessary to understand current practice and research relevant to the cyber security aspects of blockchain which this chapter covers [6]. Our goal is to provide an unbiased review of these technologies to a larger community to better understand the concepts of block chain and its close interaction with principles of cyber security.

The chapter highlights the security and privacy considerations and challenges associated with the environment discussing new approaches in improving privacy protection and cyber security. In this book chapter, the authors have explained the detailed architecture of blockchain technology and its integration with cybersecurity applications. This integrated architecture delivers a clear understanding to the readers about the working mechanism of blockchain technology in empowering the security and privacy of the user data in various cybersecurity domains. This chapter also focuses on the superior implications of the decentralized blockchain-based solutions as compared to the current IoT ecosystem which operates on a centralized cloud server through service providers [7]. Each aspect is critically examined which encompasses the existing research and prospects on blockchain cyber security. This book chapter talks about the roles and responsibility of blockchain technology in transforming the cybersecurity applications such as privacy, security, accountability, and integrity of data in various security domains such as mitigating DDoS attacks, biometric private keys, Securing DND, and data veracity. In addition, in this book chapter, the authors have discussed various applications of blockchain to cater cybersecurity, such as data storage and sharing, IoT, Network Security, Utility of World Wide Web (WWW), and Private user data. With the rapid technological advancement, the key mechanisms governing the blockchain's interaction with the cloud platform and influences on the Internet of Things (IoT) are also covered. Finally, the chapter argues on real scenarios discussing future outcomes of blockchain's decentralized feature and the possibilities of misuse by malicious participants and how these security aspects will play a critical role in the success of blockchain technology.

2 Blockchain-Based Architecture for Improved Cyber Security Solutions

The need for robust Blockchain technology is mandatory with the advent of the Internet of Things (IoT) having its aim for more engaging and dynamic devices to

enhance the quality of daily life. Billions of these constantly engaging and responsive devices entail decentralized and distributed management solutions for securing user's private information. The concept of blockchain has emerged over the last few years and attracted a lot of researchers to study its features and applications in cyberspace.

A block is the smallest entity of a blockchain. It holds data and the previous block's hash information. In addition to it, a block contains the hash of the data and its previous hash. Blockchain transactions are immutable which helps in ensuring the integrity of the complete blockchain [8]. Any change associated with any block will ultimately lead to a completely new hash value. The adjacent block gets a new hash value as soon as its neighboring block hash is changed. This immutable property of blockchains is highly regarded to establish enhanced cybersecurity.

It is possible to add a new block to an existing node. The method of augmenting a new block is achieved by broadcasting to other available nodes. The process permits the node to view the entire blockchain at the very moment. Basically, there are two main types of consensus mechanisms associated with the technology in block augmentation. Proof of Stake (PoS) was an alternate to the original algorithm Proof of Work (PoW). In the case of PoW, successful block augmentation is the result of the validation of complex computation work [9]. Miners are responsible for this extensive work. Results are validated by the nodes which afterward accept the block to join. On the other hand, PoS must verify their stake in blockchain for approval of a new block to be added. These are achieved by the owners of the stake.

There are various segments of blockchain architecture governing the security of an IoT environment, as shown in Fig. 2. It starts with a client which requests resources over the network. Resources are stored in Resources Servers and legally owned by

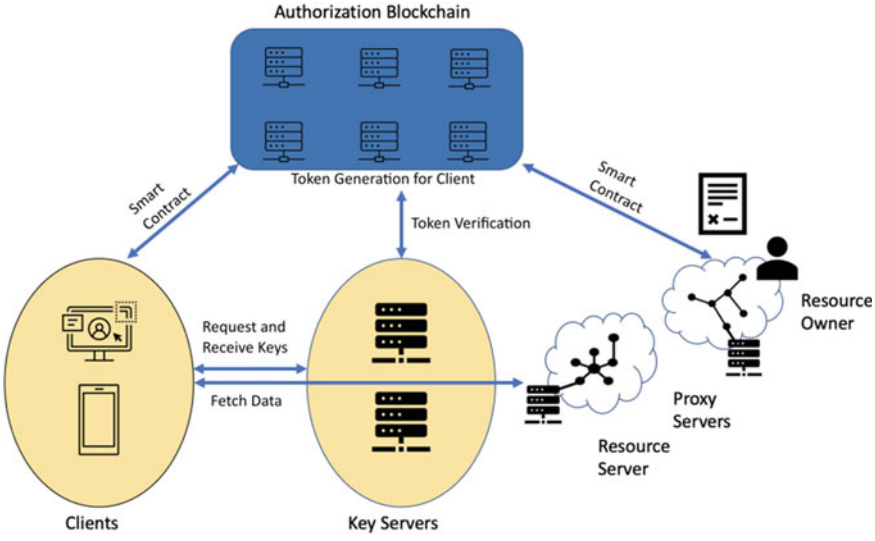

Fig. 2 Blockchain architecture solutions for IoT cybersecurity [10]

entities called Resource Owners. Resources are protected via encryption on Key Servers. Key Servers are the nodes for providing decryption keys associated with a resource to the client. Authorized Servers are responsible for generating Access Tokens. Provision of access and rights of clients corresponding to the resources are determined by Access Tokens. Every definition counts useful for the authorization blockchain element. All the above participants act as nodes in defined architecture. Nodes that store complete information about the blockchain are called full nodes, e.g., key and authorization servers. Blockchains are basically any transaction logs that are occupied in the form of blocks. PoS and PoW come into play for appending blocks to the blockchains [10, 11]. Client and resource owners share and are recognized by an asymmetric key pair. Transactions are the interaction between the client and resource servers.

3 Blockchain Solutions for Cybersecurity

The blockchain technology is used to strengthen the already existing mechanisms to secure data, networks, and communications. The backbone technology of blockchain is encryption and hashing which stores the records (immutable) and most of the existing "cybersecurity" solutions which leverages the similar workflows. Most of the published research relies on the "single trusted authority" for the verification of the stored data in encrypted format. The aforementioned scenario is prone to attack and allows the cyber attackers to focus toward a single target to commit various attacks such as "denial of service attacks, inject malicious information and extort data through theft or blackmail". To overcome the limitations of the existing security measures, blockchain has the decentralized architecture and hence omits the requirement of trusting the single member of the group or the network. In this system, the model is not required to the "trust" factor, as on each node, or actor, possesses the overall replication of the most of the historical information. This architecture presents better security measures, as most of the member of a particular group having access to the same information will secure that particular group way better than the other group which is having one master (leader) and a host member who rely on the master's information. In case, when the bad users join the group members and also the leaders themselves. In this book chapter, the authors have focused on the following blockchain applications for the cybersecurity measures: data storage and sharing, IoT (Internet of Things) Network Security, Private user data, and Utility of World Wide Web (WWW).

- **Data sharing and storage**:
  To overcome and prevent the single point of failure cyber-attacks and achieve data protections to avoid data tampering, the public and private distributed ledgers are leveraged. The blockchain technology allows the data to be stored in cloud environments which are resistant to both unauthorized access and modifications [12–14]. Also, the use of hash lists enables the data search more feasible and

secure in terms of storage and exchange are supposed to be verified [15–17]. To summarize, the blockchain helps in the improvement of data storage and sharing in a secure manner by generating the decentralized network which leverages the client-side encryption. The blockchain technology is sitting in the form of a protocol between the application and the transport layers of the network. In order to track the data management and prevention of the malicious access, one class of the private blockchains such as "Hyperledger Fabric" are leveraged to implement the "permitted access control for devices" for the network [18–20]. On the other hand, in order to deliver IoT device authentication, identification, and seamless (secure) data transfer, the other class of blockchain technology is leveraged to secure the deployment of the firmware via "peer-to-peer propagation" [21–23]. Researchers are working toward the application of blockchain to secure the IoT connections and sessions to detect the malicious behavior [24, 25]. Looking at this potential cyber threat there needs to be some technology which can provide strong security to protect the sensitive data. Blockchain Technology is one such methodology which can make this possible. By the name itself these are a series of blocks that are joined together, and each block contains some confidential information, e.g., payment transactions, medical records, or private logs. All the blocks are immutable which provided strong security and are difficult to crack the key. Each block has its own hash code and contains the hash code of next block which makes it immutable. These features allow for advanced data storage and sharing options with high security and encryption.

- **Internet of things (IoT) environment**:
  As the evolution of Internet of Things (IoT) came into existence, the challenge in handling large data became easier [26]. IoT has specialized in many fields taking from smart devices to smart applications to smart cities [27]. The need of IoT is expected to exponentially increase within the next couple of years and projected 50 billion devices will be equipped and connected with IoT [28]. IoT devices implement sensors and actuators which are embedded with hardware, software and are able to share, communicate the data among the devices. The enormous date generated from IoT devices has lead to expansion of data storage and new technologies to protect the data from several growing cyber threats [29].

  Current IoT devices such as smart wearable devices tracking health and health conditions generated tremendous records which need an efficient encryption and security protocol. Smart devices such as smart homes and electric vehicles rely on IoT protocols for connectivity, sensing, and communicating, these devices are more vulnerable to hacking and cyber threats which can be strengthened using blockchain architecture. Another major area of implementing blockchain with IoT devices (wearable/self-monitoring/smart devices) is to improvise medical data generated from these devices [30]. With the advent of blockchain medical data recording such as personal records can be secured this is also known as Remote Patient Care (RPC). Because of IoT, the medical sector can now make data processing and the generated data, i.e., patient data or any important information to store in electronic health records and send over the cloud. EHR contains many confidential information and transferring the data to EHR can make the risk of

a cyber threat. Hackers can penetrate inside the network and can hamper the information or leak the data.

- **Network Security**:
  In the network security domain, most of the research is focused around the usage of blockchain technology for the improvement of "Software Defined Networks (SDNs)". Blockchain technology leverages the containers for the authentication of the critical data which is supposed to be stored in the decentralized and robust fashion [31–33]. In these types of mechanisms, the SDN controllers leverage the blockchain-enabled architectures which use the cluster structure model. This architecture takes the advantage of both public and private blockchains for the nodes to communicate with each other in a network with P2P manner. Currently several methods are being under development and implemented with cloud integrated blockchain technology to provide extra security of data. Strong encryptions are implemented to avoid data loss, data leakage from the cloud. The use of Intrusion Detection System (IDS) deployed over cloud can make cloud security more secure. If any intruder tries to break the network IDS stops the cyber-attack and sends an alert. Making the firewall and IDS rules strong has helped prevent data loss. Today traditional IDS are used but in the future more customized and modernized IDS will be implemented with the help of machine learning and blockchain. Another aspect is using HMAC (Hash-Based Message Authentication Code) over cloud data. HMAC provides more strong security (using MD5, SHA 256) for the data. Applying such strong hash codes can help data security become more secure. HMAC could be imposed on blockchain though each block has its hash and others block hash. Using HMAC on top of that will make attacker exceedingly difficult to crack the keys.
- **User's Private Data**: There are still limitations in blockchain technology, which makes it quite difficult in delivering the data protection and privacy measures. One of the major reasons for the aforementioned scenario is the "the irreversibility nature of blockchain (everybody has a copy of the ledger)". The existing research revolves around the preferences given to the device for the encryption and storage on the blockchain for the retrieval of the data only by a particular user [34–36]. In addition, the researchers are trying to differentiate between the "blockchain PoW" and "proof-of-credibility consensus mechanisms". Many organizations have equipped with new blockchain cloud storage which provides necessary computing power. Though IoT mainly plays with cloud deployment such personal medical data or the EHR when stored over the cloud would also be a cyber threat. For example, attacker can alter user personal medical data over the cloud and the data can be stolen or lost. Blockchain has the potential to securely encrypt the data and store in a secure and protected environment.

  Integration of IoT Blockchain in health care has massive implementation in the future. In this case (Fig. 3) the patient is at home under remote monitoring. All body parameters are sensed and transmitted by IoT-enabled devices. The data stream is archived in the private cloud storage of the hospital. The data stream can be retrieved for analysis using Unique Patient Identifier (UPI) which is secured on cloud blockchain. The doctor needs to visit each remotely patient's record

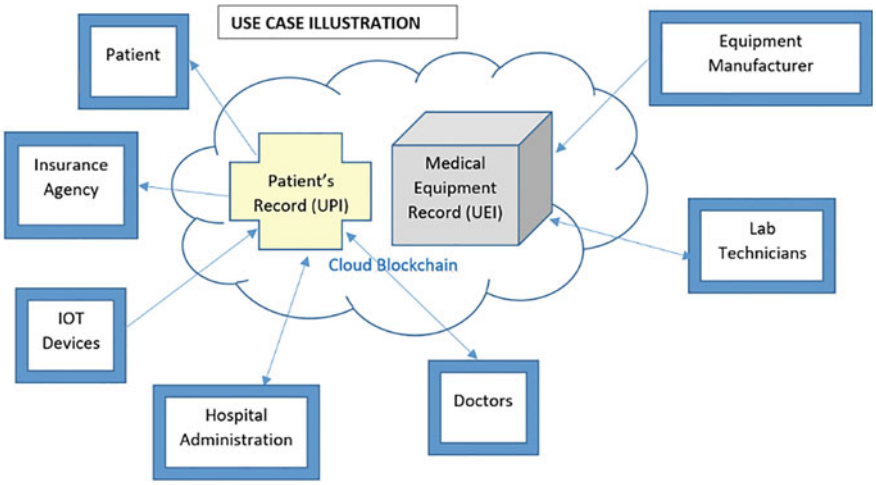

Fig. 3 Schematic of cloud blockchain environment for securing medical records

like a ward tour. Day #1, the doctor notices that heart rate is faster than usual. Doctor calls the patient and enquires to find any specific reason. Upon enquiry notices that the patient has underwent anxiety event a day before in real life. Since the higher heartbeat rate prevailed for almost one full day and that can be dangerous to patient's health, the doctor prescribes additional medication and ensures delivery of medicine to patient's home. Doctor updates medical record of the patient. Doctor then reviews another patient's record. With billions of people in this world using IoT sensors and wearable sensors the amount of information storage is beyond the limits of prevailing storage devices. There are certain tools that harness blockchain like the blockchain-based DB tool which can provide increased efficiency in terms of security of the data stored via hash codes and performance of the entire blockchain environment.

- **Accessibility of World Wide Web (WWW)**:
  In order to improve the validity of the wireless Internet access points, blockchain technology is leveraged by monitoring and storing the access control data and local ledger [37]. In addition, the blockchain is used to facilitate the navigation to the correct URLs with the help of correct DNS database records [38, 39], and also safer communication with others via secure and encrypted methods [40, 41]. There are many benefits of using cloud and blockchain the most important being cloud servers can be deployed where encrypted data blocks can be stored [42–45]. It provides increased information security where P2P encryption helps keep transactions and data secure which adds a third layer of security. If any transactions are done private keys are used (One factor Authentication) which can have some cyber threat. By using cloud computing with blockchain two-step verification can be authorized which provides improved security of private keys [46–49]. Bringing blockchain with cloud storage solutions is also beneficial. It

helps user data to pipe into small pieces. After the data is broken into small pieces an extra layer of security is added and is distributed over the network. Looking at the hash algorithm, transactions' ledgers can make this function operate. Such encryption using cloud platform can be easily possible without worry of any cyber threat.

4 Future Prospects

Though blockchain technology is strong it has not fully been developed in terms of efficiency, storage, processing power. Blockchain to be made more mature is a future research domain where all the benefits such as improved power, improved storage space, strong security can be used by this technology. Looking at the methods to secure data there is still more gaps to be researched which would make the whole IoT landscape more secure by implementing blockchain. Blockchain technology can be perfectly implemented along with the cloud to generate information and simultaneously segregated for private cloud and public cloud application consumption.

References

1. Lin IC, Liao TC (2017) A survey of blockchain security issues and challenges. IJ Netw Secur 19(5):653–659
2. Bhanot K, Peddoju SK, Bhardwaj T (2015) A model to find optimal percentage of training and testing data for efficient ECG analysis using neural network. Int J Syst Assur Eng Manag. https://doi.org/10.1007/s13198-015-0398-7
3. Bhardwaj T (2014) End-to-end data security for multi-tenant cloud environment. J Comput Technol Appl ISSN: 2229–6964
4. Möser M, Böhme R, Breuker D (2014, March) Towards risk scoring of Bitcoin transactions. In: International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, pp 16–32
5. Dasgupta D, Shrein JM, Gupta KD (2019) A survey of blockchain from security perspective. J Bank Financ Technol 3(1):1–17
6. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KKR (2020) A systematic literature review of blockchain cyber security. Digital Commun Netw 6(2):147–156
7. Zhang R, Xue R, Liu L (2019) Security and privacy on blockchain. ACM Comput Surveys (CSUR) 52(3):1–34
8. Seok B, Park J, Park JH (2019) A lightweight hash-based blockchain architecture for industrial IoT. Appl Sci 9(18):3740
9. Duong T, Fan L, Katz J, Thai P, Zhou HS (2020, September) 2-hop blockchain: combining proof-of-work and proof-of-stake securely. In: European symposium on research in computer security. Springer, Cham, pp 697–712
10. Alphand O, Amoretti M, Claeys T, Dall'Asta S, Duda A, Ferrari G, … Zanichelli F (2018, April) IoT Chain: a blockchain security architecture for the Internet of Things. In: 2018 IEEE wireless communications and networking conference (WCNC). IEEE, pp 1–6

11. Sriman B, Kumar SG, Shamili P (2021) Blockchain technology: consensus protocol proof of work and proof of stake. In: Intelligent computing and applications. Springer, Singapore, pp 395–406
12. Bhardwaj T, Upadhyay H, Sharma SC (2019) An autonomic resource allocation framework for service-based cloud applications: a proactive approach. In: 4th international conference on soft computing: theories and applications (SoCTA–2019). Advances in intelligent systems and computing (AISC). Springer. Scopus Indexed. 27th–29th Dec 2019, India
13. Bhardwaj T, Upadhyay H, Sharma SC (2019) Autonomic resource allocation mechanism for service-based cloud applications. In: IEEE international conference on computing, communication, and intelligent systems (ICCCIS-2019). 18th–19th Oct 2019, India
14. Bhardwaj T, Upadhyay H, Sharma SC (2020) Framework for quality ranking of components in cloud computing: regressive rank. In: IEEE 10th international conference on cloud computing, data science & engineering (CONFLUENCE-2020). 29th–31st Jan 2020, India
15. Ali M et al (2016) Blockstack: a global naming and storage system secured by blockchains. In: USENIX annual technical conference, p 181194
16. Yue L, Junqin H, Shengzhi Q, Ruijin W (2017) Big data model of security sharing based on blockchain. In: 2017 3rd international conference big data computing communications, p 117121
17. Cai C, Yuan X, Wang C (2017) Hardening distributed and encrypted keyword search via blockchain. In: 2017 IEEE symposium privacy-aware computing, p 119128
18. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE international conference pervasive computing communications work. PerCom Work, p 618623
19. Pinno OJA, Gregio ARA, De Bona LCE (2017) Controlchain: blockchain as a central enabler for access control authorizations in the IoT. In: GLOBECOM 2017—2017 IEEE Global Communications Conference, p 16
20. Huang Z, Su X, Zhang Y, Shi C, Zhang H, Xie L (2017) A decentralized solution for IoT data trusted exchange based-on blockchain. In: 2017 3rd IEEE International Conference on Computing Communications, p 11801184
21. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:22922303
22. Kshetri N (2017) Blockchains roles in strengthening cybersecurity and protecting privacy. Telecomm Policy 41(10):10271038
23. Banerjee M, Lee J, Choo K-KR (2018) A blockchain future to internet of things security: a position paper. Digit Commun Netw 4(3):149–160
24. Gu J, Sun B, Du X, Wang J, Zhuang Y, Wang Z (2018) Consortium blockchain-based malware detection in mobile devices. IEEE Access 6:1211812128
25. Gupta Y, Shorey R, Kulkarni D, Tew J (2018) The applicability of blockchain in the Internet of Things. In: 2018 10th international conference on communications system networks, p 561564
26. Bhardwaj T, Sharma SC (2018) An autonomic resource provisioning framework for efficient data collection in cloudlet-enabled wireless body area networks: a fuzzy-based proactive approach. Soft Comput
27. Bhardwaj T, Sharma SC (2018) Fuzzy logic-based elasticity controller for autonomic resource provisioning in parallel scientific applications: a cloud computing perspective. Comput Electr Eng 70:1049–1073
28. Bhardwaj T, Sharma SC (2018) Cloud-WBAN: an experimental framework for cloud-enabled wireless body area network with efficient virtual resource utilization. In: Sustainable computing, informatics and systems, vol 20, pp 14–33
29. Bhardwaj T, Sharma SC (2015) Internet of things: route search optimization applying ant colony algorithm and theory of computation. In: Proceedings of fourth international conference on soft computing for problem solving. Advances in intelligent systems and computing, vol 335. Springer, New Delhi
30. Bhushan P et al (2020) (Sensor Division Outstanding Achievement Award Address) Towards biosensor enabled smart dressings for management of chronic wounds: advances and perspectives. ECS Meeting Abstracts. No. 66. IOP Publishing

31. Basnet SR, Shakya S (2017) BSS: blockchain security over software defined network, Ieee Iccca, p 720725
32. Bozic N, Pujolle G, Secci S (2017) Securing virtual machine orchestration with blockchains. In: 2017 1st cyber security network conference, p 18
33. Alvarenga ID (2018) Securing configuration, management and migration of virtual network functions using blockchain
34. Fu D, Liri F (2017) Blockchain-based trusted computing in social network. In 2016 2nd IEEE international conference on computing communication ICCC 2016—Proceedings, p 1922
35. Cha SC, Chen JF, Su C, Yeh KH (2018) A blockchain connected gateway for BLE based devices in the internet of things. IEEE Access 3536 no. c
36. Sharma TK, Pant M, Bhardwaj T (2011) PSO ingrained artificial bee colony algorithm for solving continuous optimization problems. In: Proceedings of IEEE international conference on computer applications and industrial electronics (ICCAIE 2011), Malaysia, pp 108–112
37. Niu Y, Wei L, Zhang C, Liu J, Fang Y (2017) An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the Bitcoin blockchain. In: 2017 IEEE/CIC international conference on communications China, no. Iccc, p 16
38. Benshoof B, Rosen A, Bourgeois AG, Harrison RW (2016) Distributed decentralized domain name service. In: Proceedings—2016 IEEE 30th international parallel and distributed processing symposium IPDPS 2016, 2016, p 12791287
39. Wang X, Li K, Li H, Li Y, Liang Z (2017) Consortium DNS: a distributed domain name service based on consortium chain. 2017 IEEE 19th Int Conf High Perform Comput Commun. IEEE 15th Int Conf Smart City; IEEE 3rd Int Conf Data Sci Syst 617620
40. Qin B, Huang J, Wang Q, Luo X, Liang B, Shi W (2017) Cecoin: a decentralized PKI mitigating MitM attacks. Futur Gener Comput Syst
41. Alphand O et al (2018) IoTChain: a blockchain security architecture for the internet of things. In: IEEE wireless communications and networking conference (WCNC), pp 1–6
42. Bhardwaj T, Upadhyay H, Sharma SC (2020) Autonomic resource provisioning framework for service-based cloud applications: a queuing-model based approach. In: IEEE 10th international conference on cloud computing, data science & engineering (CONFLUENCE-2020). 29th–31st Jan 2020, India
43. Bhardwaj T, Sharma SC, An efficient elasticity mechanism for server-based pervasive healthcare applications in cloud environment. In: 19th IEEE international conference on high performance computing and communications workshops (HPCCWS 2017), Bangkok, Thailand
44. Kadarla K, Sharma SC, Bhardwaj T, Chaudhary A (2017) A simulation study of response times in cloud environment for IoT-based healthcare workloads. In: 14th IEEE international conference on mobile ad hoc and sensor systems (MASS-2017), vol 00, pp 678–683. https://doi.org/10.1109/MASS.2017.65
45. Bhardwaj T, Kumar M, Sharma SC (2016) Megh: a private cloud provisioning various IaaS and SaaS. In: Soft computing: theories and applications. Advances in intelligent systems and computing, vol 584. Springer, Singapore
46. Pandit MR, Bhardwaj T, Khatri V (2014) Steps towards web ubiquitous computing. In: Proceedings of the second international conference on soft computing for problem solving (SocProS 2012), December 28–30, 2012. Advances in intelligent systems and computing, vol 236. Springer, New Delhi
47. Bhardwaj T, Pandit MR, Sharma TK (2014) "A safer cloud", Data isolation and security by Tus-Man protocol. In: Proceedings of the second international conference on soft computing for problem solving (SocProS 2012), December 28–30, 2012. Advances in intelligent systems and computing, vol 236. Springer, New Delhi
48. Bhardwaj T, Sharma TK, Pandit MR (2014) Social engineering prevention by detecting malicious URLs using artificial bee colony algorithm. In: Proceedings of the third international conference on soft computing for problem solving. Advances in intelligent systems and computing, vol 258. Springer, New Delhi
49. Bhardwaj T, Pandit MR (2012) Analysis of cloud security problem and proposed igloo solution. In: Asia Pacific & MEA students' conference, March 14–16, Hong Kong