Applying Distributed Ledger Technology as a Cybersecurity Layer

Fahad F. Alruwaili

College of Computing and Information Technology, Shaqra University
P.O. Box 33, Shaqra 11961 Saudi Arabia

Abstract

Since its inception, Blockchain has drawn lots of attention to the next generation of decentralized economies due to its structure that suits the digital transformation era. It has successfully changed many financial transaction systems in different organizations and has the potential to innovate current business models across different industries. One of blockchain important building blocks is the activity of applying transparency and security with cryptography and authentication of distributed peers. In this work, an overview of current blockchain protocols is demonstrated along with how it can potentially tackle current security and transparency concerns in cloud storage services. Further, a novel TSS Model of applying blockchain to cloud services to address transparency and secure access issues is presented and suggest future directions to advance research efforts into this field.

Key words:

Cybersecurity, Distributed Ledger Technology (DLT), Smart Contract, Blockchain, Privacy, Cloud Computing, Compliance, Decentralized Systems.

1. Introduction

Global financial industry expects that blockchain security solutions could grow to 20 billion dollars by the year of 2020. The blockchain is one of the recent emerging technologies that benefits the cybersecurity industry [1, 7]. This technology has successfully replaced many economic transaction systems in different countries and has the potential to innovate diverse business models in different industries. It enables trustless and secure distributed framework to facilitate exchanging, sharing, and the incorporation of information across all users and third party participants. However, it is also substantial for decision makers to rigorously review its suitability in their industry and business applications [2-4]. Blockchain utilizes decentralized ledger technology (DLT) as new and innovative data structure. It is a series of blocks in a chain where each corresponding block point to the prior one in a chronological order i.e. via the latter's nonce signature. Once the transactions or events are verified via consensus mechanism, then the information is committed into the Blockchain. Now it will be impossible to tamper with the committed block as copy of the details are shared across all participating network nodes i.e. a shared copy the DLT registry. Since copies of the same ledger are distributed, users and network participants will be aware of the transactions taking place and/or any unauthorized attempts. To simplify the notion, consider the analogy of a "book" where each page refers to its previous page by a page number. Pages in a textbook counterpart with blocks in blockchain network, and an entry in a page refers to committed event or transaction. As a result, threats and unauthorized access are easily detected if a page or a block has been tampered with or altered [8].

Since blockchain is a new emerging technology in financial industry, some users are very concerned about its security. While security vulnerabilities have been recently reported, some are unforeseen. Loi et al. reported that 8,833 out of 19,366 smart contracts run on Ethereum blockchain are somewhat vulnerable [12]. Such security vulnerabilities may not only lead to potential financial losses but also to blockchain migration issues. Further in June 2016, criminals were able to compromised the smart contract of decentralized Autonomous Organizations (DAO) [18] by exploiting a recursive calling vulnerability, resulting in roughly USD ~60 million fraud. Also back in March 2014, hackers took advantage of transaction mutability in Bitcoin network to attack MtGox currency exchange, which led to the collapse of MtGox, and a loss of USD 450 million dollars in Bitcoin currency [19].

Cloud computing technology as well has attracted many IT organizations due to flexibility, availability, and efficiency. However, many of which are reluctant to offloading their data to the cloud due to security and privacy issues; in particular, issues related to confidentiality, integrity, secure storage, and strong access controls [9].

The main contributions of this paper are as follows:

1. A systematic investigation of blockchain technology and survey the trends on security risks to blockchain systems and cloud computing services are conducted to the best of authors knowledge.
2. Practical achievements for enhancing the security and transparency of cloud storage is performed by proposing a new TSS model and suggests a few future directions in this area.

The rest of the paper is organized as follows: Section 2 depicts the prior works found in the field of cybersecurity,

Manuscript received July 7, 2020
Manuscript revised July 20, 2020

cloud computing, and blockchain. Section 3 highlights the notion of blockchain technologies along with its key features. Section 4 points the research methods and motivations. Section 5 explains the proposed system with the transparent and secure (TSS) Framework and its architecture. Finally, section 6 concludes the study of this paper.

2. Existing Research

Several methods of cybersecurity have been used in website security [13] [14], application security [15] and blockchain security [16]. Zikratov et al. [17] present hashing based method for checking the integrity of verification in the cloud. Their proposal flows the blockchain structure in terms of block creation.

Zyskind et al. [19] propose a blockchain based system to improve application data protection, which separates data from permissions, records permission settings and data access in blockchain, enabling full control of data access permissions and transparent access procedures.

Tschorsch et al. [7] present a security-analyzing tool to monitor smart contracts that is scalable, and able to prove contract behaviors with respect to a given property.

Azaria et al. [20] propose a medical data management model using blockchain and smart contracts. Their model logs data permissions and operations in the distributed ledger, and is executed by smart contracts to implement data authentication, cryptography, checking, and exchanging of patient records.

Buldas et al. [21] highlight a blockchain based keyless signature framework, which allows recording the root hash value in the chain and performs multi-file signature. Their work increases the overhead of falsifying signature files, ensuring the integrity of the file.

Karaarslan et al. [22] suggest a distributed domain name resolution system (DNS) based on blockchain. Its goal is to effectively counterfeit the distributed denial of service (DDoS) attacks by layering the domain name resolution logic and the underlying consensus mechanism.

Recently, blockchain technology has made significant contributions to cybersecurity due to its immutability, traceability, decentralization, and transparency [10-17]. In addition, many ongoing studies to improve security leveraging the characteristics of blockchain are work in progress. The work of this paper addresses the transparency and security of cloud storage in a new approach that hasn't been address in current research.

3. Background Concepts on Blockchain Technology

A blockchain is a distributed digital registry of transactions that is managed by different participants i.e. peer-to-peer network [23, 24].

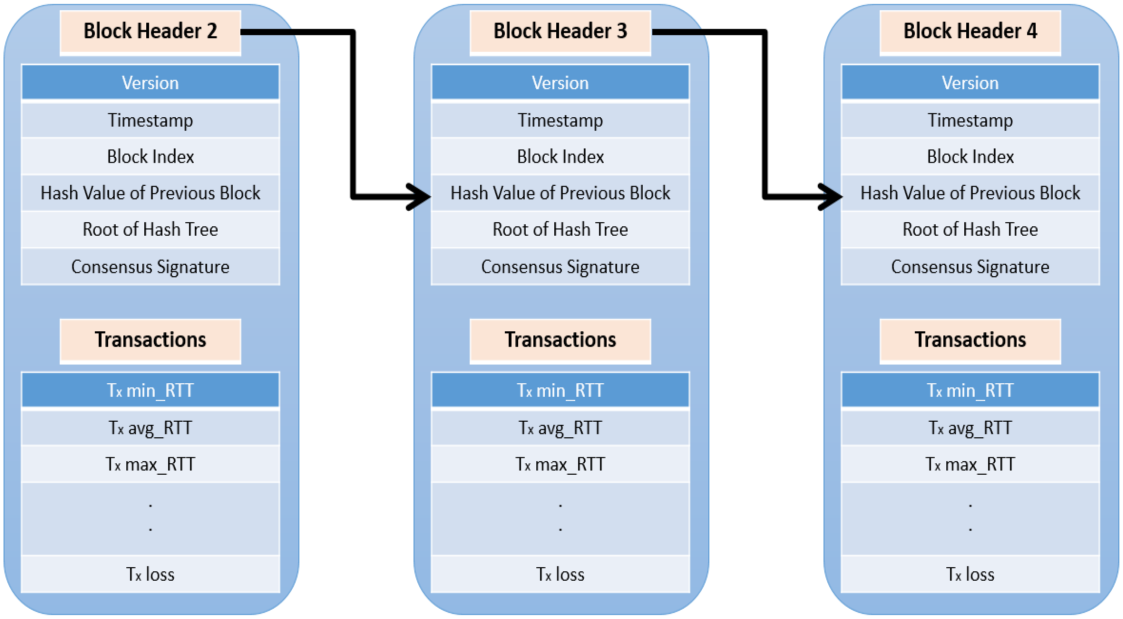


Fig. 1 Blockchain Structure

The terminology originates from its data structure, where, the individual records of transactions are registered as blocks. Each block is connected with the previous block and will be linked as well with the next block once it becomes part of the chain i.e. when verified, see Figure 1. Every block plays a key role to record, validate, and share transactions in a distributed fashion among other blocks [25]. Thus, data in these blocks are record of transactions and the exact same records are shared across all participating network nodes. The synced and decentralized ledger is a core component, hence, any involved transactions cannot be altered without the alteration of all concurrent blocks.

The key characteristics and features of Blockchain technologies, includes:

1. Immutability: It means one-way writing to the ledger, hence no participant be able to tamper or alter a block or committed transaction.
2. Irreversibility: It implements one-way writing to the block e.g. it prevents double spending attack.
3. Distribution of Records: It means that a copy of the ledger is present with all its members.
4. Provenance: the proof of ownership of a registered asset.
5. No Centralized Authority or third party: It is a peer-to-peer network.
6. Finality: single yet distributed ledger of records, which indicates one-place to check and trace transactions.
7. Consensus: in order for transaction to be valid as new entry, all participants/validators must agree on transaction validity.
8. Resiliency: It is not prone to any sort of major attacks.

4. Research Methodology and Motivation

In this paper, the design science research (DSR) methodology for crafting innovative information systems is employed. This methodology employs a specific set of concepts and principles to develop IT solutions [26]. The main DSR elements are summarized in Table 1. It begins with identifying the problem and setting the objectives. This is followed by designing, developing, and demonstrating the solution, which is presented in Sections 5 and 6.

Table 1: Design Science Research (DSR) Components.

Guideline		Description
1	**Design**	The TSS model is suitable for encouraging the transparency and security of cloud storage services.
2	**Problem Relevance**	It is relatively costly and difficult to ensure secure cloud storage which hinders many organizations from migrating their data and systems to the cloud services. It is also challenging many organizations to engage 3rd party experts in the monitoring and trusting cloud storage service providers. thus the need for efficient, transparent, and trustless model is critical, hence the TSS. The objective is to develop automated and distributed ledger of records solution that can be adopted as the next generation of secure automation of cloud storage access.
3	**Design Evaluation**	The TSS ecosystem is evaluated using an environment, which reflects real world situations as a suggested pilot.
4	**Contributions to Research**	The TSS model provides clear and significant contributions in the area of distributed ledger based cybersecurity of cloud services
5	**Research Rigor**	The proposed solution relies on rigorous blockchain technology and information security methods.
6	**Design as a Search Process**	The search for an effective transparent and secure cloud storage solution requires examining all available approaches to reach a solution.
7	**Research Communication**	The insights gained are disseminated to the blockchain technology and cloud cybersecurity communities.

This paper presents a TSS model that examines the cloud storage access and vulnerabilities discovered through verified proof of consensus among engaged participants. The selection of engaged participants requires an understanding of multiple factors and criteria to reach an agreement which then are lock in a digital and automated contract. Further, the model considers the selection of validators and referees using community voting to elect the most suitable subject matter experts in the field of cybersecurity and threat intelligence.

The motivation for this work is to address the current cloud storage security issues in a transparent and efficient approach. The model utilizes the structure of distributed ledger in blockchain architecture to allow trusted verification and authorization of cloud storage contracts. This method of distributed and automated and secure contracts based improves the status quo in cloud security mechanisms and enables many organizations to rethink their strategies in migrating to cloud storage services.

5. Transparent and Secure Storage (TSS) Model

In this section, architecture of the transparent and secure (TSS) blockchain-powered model is presented. The goal is to provide trustless, cost efficient, and secure cloud storage mechanism. The TSS architecture includes participants (cloud users, cloud service providers, validators), consensus algorithm, smart contract, cryptographic functions and digital signature. The main TSS components are shown in Figure 2 and described below.

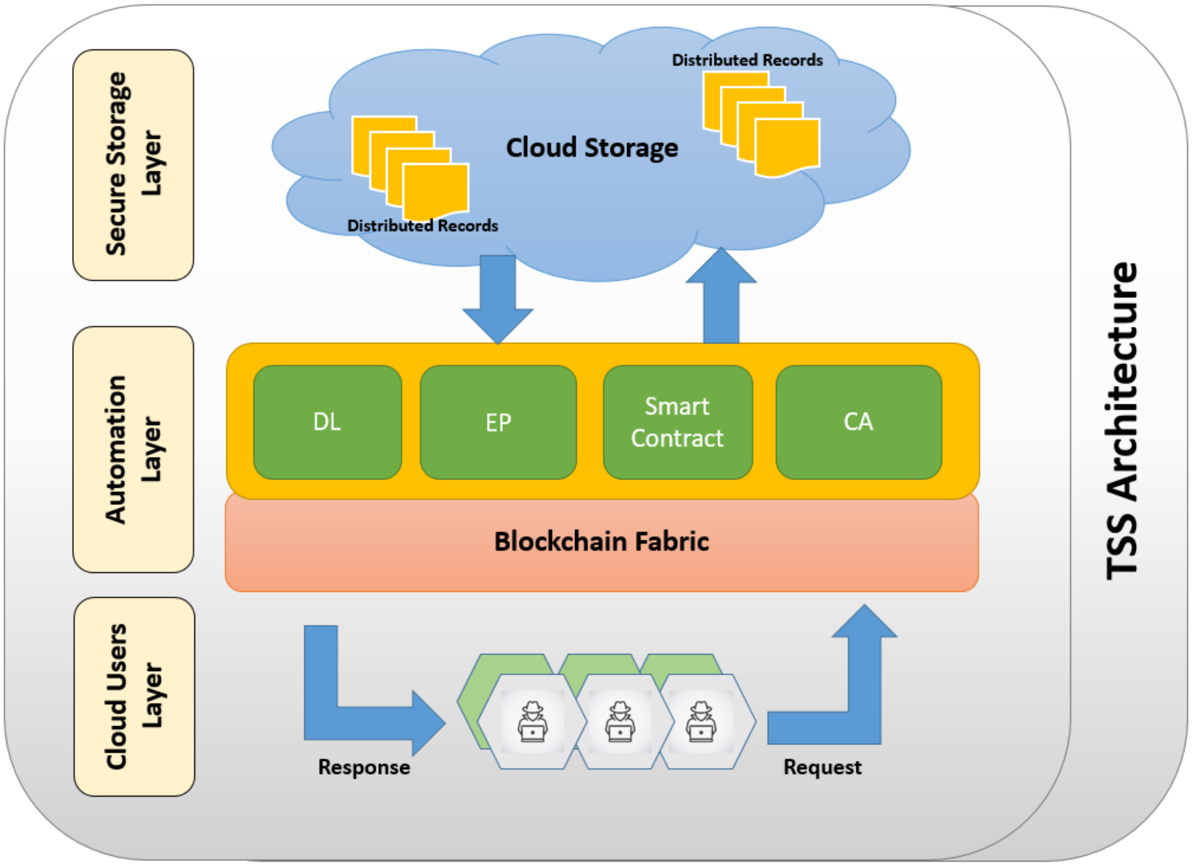


Figure 2. The Transparent and Secure Storage (TSS) Architecture

5.1. Blockchain Fabric (BF)

The BF function is to automate the transactions across the blockchain and cloud storage from and to the validated participants. It also facilitates the requests from different users to and from the cloud operational model i.e. blockchain-as-a-service. The BF role is to abstract the underlying physical and logical architecture in order to enable the aforementioned blockchain-as-a-service which is a platform-as-a-service (PaaS) deployment model, to interact with the cloud services. The BF operates in an automation layer of TSS model to enable transparent and scalable services in a distributed network of storage i.e. cloud storage.

5.2. Distributed Ledger (DL)

The DL role in TSS is to keep an immutable log of transactions. It is designed to have one-way cryptographic writing to the records. Therefore, these records are immutable and cannot be reversible nor repudiable. Moreover, DL records and transactions are committed only once the consensus among blockchain “validators” is confirmed, hence DL transactions driven by CA component. The governance and transparency are addressed by having distributed copies of DL records across all blockchain nodes. Further, with the DL the cloud data access is mutualized. Thus and in the case of highly sensitive data, it is important to implement a permissioned DL in order to ensure stronger security mechanism. The DL implementation resolves storage trust issues associated with a centralized approach of managing cloud storage services.

5.3. Encryption Protocol (EP)

Cryptography is an integral part of the blockchain technology. The EP in TSS adapts hash functions and asymmetric cryptography to ensure data protection is maintain whenever data at rest, transit, or in processing. Current business practice underutilizes encryption in that mostly used during the log-in procedures and once logged-in there is almost little security implemented on data access [27]. The EP promises secure transactions to access and update data in the ledger but coupling the EP with automated execution (5.4) results in not only a better security measures to cloud storage access but also efficient and greater benefits to reducing cost and time.

5.4. Smart Contract (SC)

The automated execution of transactions i.e. SC, is used in TSS which contains logic and algorithms that govern the cloud access among participants by executing code and triggering certain events. These are recorded in the DL for transparent tracking of access and edits events in cloud storage. The SC contains the following sections:

- Logic: verifiable rules and conditions among the participants e.g. details of access control such as date, time and location. These rules are agreed upon cloud service providers and prospective participants of TSS.
- Involved Parties: blockchain and contract participants (people, organizations, Internet of things (IoT), etc.) agreeing on certain terms and conditions to cloud storage. The execution of the contract authenticated using digital signature and asymmetric keys. The contract only becomes locked and active once both parties sign the contract and become legally binding.
- Schema: these are variables and changing values linked with certain conditions. The Schema contains data elements needed for the fulfillment of the SC obligations.
- External Sources: these are inputs from different systems required to facilitate the execution of the contract e.g., via application programming interface (API) a biometric scan stored in national database is linked to verify and, if successful, allows automated access to cloud storage via TSS ecosystem. The EP with SC collaborate to establish a cryptographic proof of authenticity among external resources.

5.5. Consensus Algorithm (CA)

Consensus piece is one of the critical components of TSS model aims at providing agreement on the state of data and regulated transaction on a peer-to-peer basis. The CA helps monitoring the state of data from unauthorized access and prevents malicious blockchain nodes from changing the data in a distributed environment. The consensus model can be a proof-of-work (PoW), proof-of-stake (PoS), proof-of-authority (PoA) or even a voting based on permissioned and selected blockchain participants and validators.

Due to decentralization of TSS architecture, the validators agree on exchanging the information and its validity without the use of intermediary or trusted third party to ensure secure storage, data accountability and management. This is accomplished via the use of a CA. TSS may utilize this algorithm to ensure greater security, accuracy and, if applicable i.e. permission-less or public blockchain, reward to those validators is expected.

5.6. TSS Client Onboarding and Request Validation Process

In this piece the cloud storage participants i.e. users of cloud storage and validators, are registered via a structured process. This process is called “client onboarding” where users go through a set of required information in order to define the ongoing relationship among users, cloud storage service providers, and validators. Participants are granted a digital identity and then need to lock their agreement into the smart contract.

The validator verifies the ownership of registered users using a copy of this agreement and ensures all necessary security and identification requirements are in place and maintained by cloud storage providers. The decision for acceptance or rejections of user requesting access is based on the parameters set in the smart contract and the consensus algorithm. Once the validators consensus is confirmed then transaction becomes a valid blockchain ledger record. Then the updated DL records are propagated to ensure the exact copy distribution throughout the chain of TSS, see Figure 3.

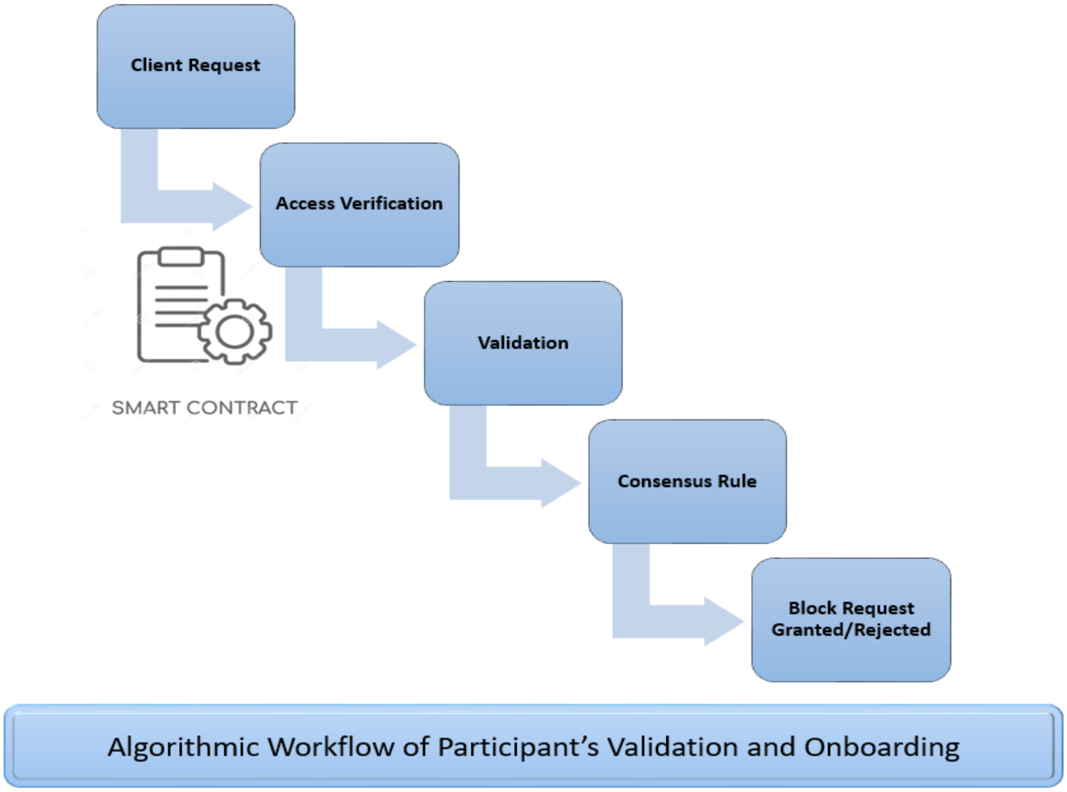

Client Request
Access Verification
Validation
Consensus Rule
Block Request Granted/Rejected
SMART CONTRACT
Algorithmic Workflow of Participant's Validation and Onboarding

Fig. 3 Validation and Onboarding Process

6. Concluding Remarks

The current blockchain implementation has shown an effective solution to secure transactions and clients' data. The use of cryptographic keys and hash function in a decentralized data indicates promising improvements in regards to security and transparency of cloud services [28-31]. One of main issues than hinder organizations from adopting the cloud services is economies is the cybersecurity industry with its ongoing and challenging issues to overcome zero-day threats and cyber-attacks. The consensus and decentralization aspects of the blockchain allow effective cybersecurity application to counter or minimize such issues. The proposal provided in this paper, a novel TSS model enables transparent and efficient cybersecurity implementation for accessing and monitoring cloud storage. After providing a general methodology on the appropriate implementation of TSS model to counter unauthorized cloud storage access, some of the most relevant and recent work were examined. The TSS architecture is highlighted were trusted participants are governed via automation of digital contracts where information and distributed records are shared among the authorized participants. Because of TSS nature was built on decentralized ledger and consensus algorithm, there was no need to engage centralized third party for the purpose of auditing and monitoring. TSS model offers many opportunities for better transparency and security of distributed cloud storage services. Participants, such as clients and validators, around the world can take part in the mission of storage security and reward mechanism of the TSS. Author believes that the presented model will not only increase the authenticity, transparency, access automation, but creates a disruptive dimension of how cloud storage security are managed, monitored, and indeed rewards those talents in the TSS model.

References

[1] A. Gervais, G. O. Karame, K. W¨ust, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the Security and Performance of Proof of Work Blockchains," in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 3–16, New York, NY, USA, 2016.

[2] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, Sok "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," in IEEE Symposium on Security and Privacy, pp. 104– 121, May 2015.

[3] W. T. Tsai, R. Blower, Y. Zhu, and L. Yu, "A System View of Financial Blockchains," in IEEE Symposium on Service-Oriented System Engineering (SOSE'16), pp. 450–457, Mar 2016.

[4] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, Hawk, “The Blockchain Model of Cryptography and Privacy-preserving Smart Contracts,” in IEEE Symposium on Security and Privacy (SP’16), pp. 839–858, May 2016.

[5] Zheng Z, Xie S, Dai H, Chen X, Wang H. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.” In Big data (BigData congress), 2017 IEEE international congress on. IEEE; 2017:557-564.

[6] Sinha SR, Park Y. “Dealing with Security, Privacy, Access Control, and Compliance.” In Building an Effective IoT Ecosystem for Your Business. Cham: Springer, 2017:155-176, 2017.

[7] Tschorsch F, Scheuermann B. “Bitcoin and Beyond: a Technical Survey on Decentralized Digital Currencies.” IEEE Commun Surv Tutorials, No. 18, 2016.

[8] Conti M, Lal C, Ruj S. “A Survey on Security and Privacy Issues of Bitcoin.” IEEE Commun Surv Tutorials https://doi.org/10.1109/ COMST.2018.2842460. 20(4):3416-3452.

[9] Park, Jin Ho, and Jong Hyuk Park. “Blockchain security in Cloud Computing: Use Cases, Challenges, and Solutions.” Symmetry 9, No. 8, pp. 164, Aug 2017.

[10] Atzei N, Bartoletti M, Cimoli T. “A Survey of Attacks on Ethereum smart Contracts (SoK).” In International Conference on Principles of Security and Trust. Springer, pp. 164-186, 2017.

[11] Ahmed K, Andrew M, Elaine S, Zikai W, Charalampos P. Hawk “The Blockchain Model of Cryptography and Privacy Preserving Smart Contracts.” Proc. IEEE Symp. Secur. Privacy (SP), pp. 839-858, 2016.

[12] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, “Making Smart Contracts Smarter,” in The ACM SIGSAC Conference on Computer and Communications Security, pp. 254-269, 2016.

[13] A. Akkiraju, D. Gabay, H. B. Yesilyurt, H. Aksu, and S. Uluagac, Cybergrenade: Automated exploitation of local network machines via single board computers, in Mobile Ad Hoc and Sensor Systems (MASS), 2017 IEEE 14th International Conference on. IEEE, pp580–584, 2017.

[14] R. Kachhwaha and R. Purohit, “Relating Vulnerability and Security Service Points for Web Application through Penetration Testing,” in Progress in Advanced Computing and Intelligent Engineering. Springer, pp41–51, 2019.

[15] Y. K. Lee, P. Yoodee, A. Shahbazian, D. Nam, and N. Medvidovic, Sealant “A Detection and Visualization Tool for Inter-app Security Vulnerabilities in Androic,” in Automated Software Engineering (ASE), 2017 32nd IEEE/ACM International Conference on. IEEE, pp. 883–888, 2017.

[16] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, Hawk “The Blockchain Model of Cryptography and Privacy-preserving Smart Contracts,” in 2016 IEEE symposium on security and privacy (SP). IEEE, pp. 839–858, 2016.

[17] Zikratov, Igor, Alexander Kuzmin, Vladislav Akimenko, Viktor Niculichev, and Lucas Yalansky. “Ensuring Data Integrity using Blockchain Technology.” In 2017 20th Conference of Open Innovations Association (FRUCT), pp. 534-539. IEEE, 2017.

[18] Q. Shao, C. Jin, Z. Zhang, W. Qian, A. Zhou et al., “Blockchain Technology: Architecture and Progress, Journal of Computer,” Vol. 41, No. 5, pp. 969–988, 2018.

[19] G. Zyskind, O. Nathan et al., “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” in Security and Privacy Workshops (SPW), IEEE, pp. 180–184, 2015.

[20] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, Medrec “Using Blockchain for Medical Data Access and Permission Management,” in Open and Big Data (OBD), International Conference on IEEE, pp. 25–30, 2016.

[21] A. Buldas, R. Laanoja, and A. Truu, “Keyless Signature Infrastructure and PKI: Hash-tree Signatures in Pre-and Post-quantum World”, International Journal of Services Technology and Management, Vol. 23, No. 1-2, pp. 117–130, 2017.

[22] Karaarslan, Enis, and Eylul Adiguzel. “Blockchain Based DNS and PKI solutions.” IEEE Communications Standards Magazine 2, No. 3, pp. 52-57, 2018.

[23] Beikverdi, A.; JooSeok, S. “Trend of Centralization in Bitcoin’s Distributed Network.” In Proceedings of the 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan, 1–3 June 2015.

[24] Esposito, Christian, Alfredo De Santis, Genny Tortora, Henry Chang, and Kim-Kwang Raymond Choo. “Blockchain: A Panacea for Healthcare Cloud-based Data Security and Privacy?.” IEEE Cloud Computing 5, No. 1, pp. 31-37, 2018.

[25] Huru Hasanova, Uijun Baek, Mugon Shin, Kyunghee Cho, MyungSup Kim, “A Survey on Blockchain Cybersecurity Vulnerabilities and Possible Countermeasures,” International Journal of Network management, Vol, 29, No. 2, 2019.

[26] Hevner, Alan, and Samir Chatterjee. “Design science Research in Information Systems.” In Design research in information systems, pp. 9-22. Springer, Boston, MA, 2010.

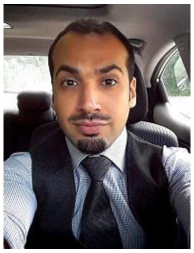
[27] Halaburda, H. “Blockchain revolution without the blockchain?.” Communications of the ACM, Vol. 61, No. 7, pp. 27-29, 2018.

[28] Ahmed S. Musleh, Gang Yao, S. M. Muyeen, "Blockchain Applications in Smart Grid–Review and Frameworks", Access IEEE, Vol. 7, pp. 86746-86757, 2019.

[29] Alexey V. Bataev, "Innovative Approaches in the Financial Sphere: Evaluation of the Implementation of Blockchain Technology", Soft Computing and Measurements (SCM) 2019 XXII International Conference, pp. 233-236, 2019.

[30] Jiaxi Hu, Debiao He, Qinglan Zhao, Kim-Kwang Raymond Choo, Parking Management: “A Blockchain-Based Privacy-Preserving System,” Consumer Electronics Magazine IEEE, Vol. 8, No. 4, pp. 45-49, 2019.

[31] Qiping Wang, Raymond Yiu Keung Lau, Xudong Mao, “Blockchain-Enabled Smart Contracts for Enhancing Distributor-to-Consumer Transactions,” Consumer Electronics Magazine IEEE, Vol. 8, No. 6, pp. 22-28, 2019.



Fahad F. Alruwaili is an Assistant Professor in the College of Computing and Information Technology, University of Shaqra, Saudi Arabia. He is a cybersecurity and risk management consultant with over thirteen years of practical experience and research development. He received the BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he received the MS degree in Computer, Information, and Network Security with first class honors from DePaul University, Chicago, IL USA, and in 2011 the MS degree in Information Systems and Technology with first class honors from Claremont Graduate University, Los Angeles, CA USA. In 2016, he received the PhD degree in Electrical Engineering from the University of Victoria, Victoria, BC Canada. His research interests are in the technical and theoretical views of cybersecurity, blockchain and digital transformation.