Applying Blockchain as a Decentralized Cybersecurity Framework

Fahad F. Alruwaili

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

Abstract
The blockchain applications have attracted a larger interest in the research community following its recent success in the financial industry of cryptocurrencies. Blockchain is a decentralized and distributed ledger technology in which, all transactions or events take place in a trustless peer-to-peer network without involving intermediaries. Considering the recent technological advancements, blockchain has the potential to revamp heterogeneous business models across different industries. Though it promises a secure distributed framework to smoother the exchanging, sharing and integration of information across all the users and third parties, it is important for the planners and decision-makers to carefully analyze it's secure application and suitability in different industry and business. The blockchain should be considered only where applicable and provides a better security and opportunities in cost reduction and obtaining increased revenues. Therefore, this paper proposes the blockchain as a decentralized cybersecurity framework by employing the Design Science Research (DSR) methodology for innovative information systems. This methodology employs a specific set of concepts and principles to develop IT based solutions. The proposed Threat and Vulnerability Blockchain (TVB) framework is suitable for encouraging mass security experts to discover new threats and vulnerabilities. This article also presents an overview of this technology for realization of security across distributed parties in an impregnable and transparent way.

Key words:
Cybersecurity, Distributer Ledger Technology (DLT), Smart Contract, Blockchain, Privacy, Compliance, Decentralized Systems.

1. Introduction

The blockchain is one of the most emerging technologies of cybersecurity [1, 11]. This technology has successfully replaced economic transaction systems in various organizations and has the potential to revamp heterogeneous business models in different industries. It promises a secure distributed framework to facilitate sharing, exchanging, and the integration of information across all users and third parties, it is also important for the planners and decision maker to analyse it in depth for its suitability in their industry and business applications [2-4]. Blockchain is a decentralized ledger technology and a different but innovative data structure. It can be referred to as a sequence of blocks in a chain where the corresponding blocks point to the prior blocks in a chronological order. Once the details of the transactions or events are fed into the Blockchain, it is impossible to tamper with as same details are shared across all members of the network. Users of the Blockchain network should be completely aware of the transactions taking place since they are having a copy of the same ledger, hence distributed ledger technology (DLT). We will draw an analogy to simplify the concept. Consider the blockchain as a textbook where each page of the book refers to its previous page by a page number. Pages in the book refer to the blocks and an entry in any page refers to the blockchain transaction. It is easy to detect whether a page or a block has been tampered with or altered. In blockchain, each block is built on top of the previous block and it uses the latter's nonce and signature as a key for going into the next block.

Since blockchain is one of the new technologies in financial industry, some users are very concerned about its security. Some security vulnerabilities and attacks have been recently reported. Loi et al. discover that 8,833 out of 19,366 existing Ethereum contracts are vulnerable [12]. Note that smart contracts with security vulnerabilities may lead to financial losses. For instance, in June 2016, the criminals attacked the smart contract DAO [18] by exploiting a recursive calling vulnerability, and stole around 60 million dollars. As another example, in March 2014, the criminals exploited transaction mutability in Bitcoin to attack MtGox, the largest Bitcoin trading platform. It caused the collapse of MtGox, with a value of 450 million dollars Bitcoin stolen [19].

Although there are some recent studies on the security of blockchain, none of them performs a systematic examination on the risks to blockchain systems, the corresponding real attacks, and the security enhancements. The closest research work to ours is [21] that only focus on Ethereum smart contracts, rather than popular blockchain systems. From security programming perspective, their work analyzes the security vulnerabilities of smart contracts, and provides a taxonomy of common programming pitfalls that may lead to vulnerabilities [21]. Although, a series of related attacks on smart contracts are listed in [21], there lacks a discussion on security enhancement. This paper focuses on the security of blockchain from more comprehensive perspectives.

The main contributions of this paper are as follows:

Manuscript received February 5, 2020
Manuscript revised February 20, 2020

(1) Initially, a systematic examination on security risks to popular blockchain systems is conducted to the best of author's knowledge.
(2) Real attacks on popular blockchain systems from the past researchers were examined, in addition to an analysis on the related vulnerabilities has been considered.
(3) Practical achievements for enhancing the security of blockchain is performed by proposing a new TVB framework and suggests a few future directions in this area.
Remainder of this paper is organized as follows. Section 2 depicts the works done in the field of cybersecurity techniques and blockchain. Section 3 introduces the concept of blochchain technologies along with its key characteristics. Section 4 shows the main technologies used in the proposed system with the Threat and Vulnerability Blockchain (TVB) Framework and its architecture. Finally, section 5 depicts the conclusion of this paper.

2. Related Work

Many novel cybersecurity techniques have been used in website security [13] [14], application security [15] and blockchain security [15]. For example, Nikolic et al. [16] present the first tool for precisely specifying and reasoning about trace properties, which employs inter-procedural symbolic analysis and concrete validator for exhibiting exploits. Tsankov et al. [8] present a security analyzer for smart contracts that is scalable, and able to prove contract behaviors as safe/unsafe with respect to a given property. Recently, blockchain technology has made significant contributions to cybersecurity due to its immutability, traceability, decentralization, and transparency [13-17].
Zyskind et al. [18] propose a blockchain based approach to protect application data, which separates data from permissions, records permission settings and data access in blockchain, enabling full control of data access permissions and transparent access procedures. Azaria et al. [19] propose a medical data management model based on blockchain and smart contract, which records data permissions and operations in the blockchain, and is executed by smart contracts to implement data authentication, confidentiality, auditing, and sharing. Buldas et al. [20] highlight a blockchain based keyless signature framework, which records the root hash value in the chain and performs multi-file signature, which increases the overhead of falsifying signature files, ensuring the integrity of the file. Ali et al. [21] suggest a distributed domain name resolution system based on blockchain, where this system can effectively resist DDoS attacks by layering the domain name resolution logic and the underlying consensus mechanism.
The below three blockchain generations are classified in accordance to advancements made towards accessibility, speed, scalability, and improved consensus algorithms:
(a) The first generation public blockchain (blockchain 1.0),
(b) The second generation public blockchain (blockchain 2.0), and
(c) The third generation private blockchain (blockchain 3.0).
Blockchain 1.0 deploys cryptocurrencies in applications related to cash, such as currency transfers, currency settlements, and digital payments. Blockchain 2.0 includes smart contracts for economic markets and financial applications. This category handles more than simple cash transactions. It includes stocks, bonds, loans, mortgages, titles, smart properties, and smart contracts. The third category applies to applications beyond currencies, finance, and markets. It includes areas, such as government, health, science, literacy, culture, and art. Therefore, blockchains within this category are considered private or semi-private i.e. a mixture of private and public use [5]. Blockchain is a promising technology that may alleviate the risk of cyberattack directed to a single point, which could bring down the entire network [6]. However, a coded intrusion or system vulnerability could allow more negative consequences to the security of the system. For example, if successful, an attacker could gain access not only to the information stored at the point of attack but also to all information recorded in the ledger. Thus, security issues related to blockchain are critical in terms of cybersecurity. In this sense, security experts need to fully understand the scope and impact of the security and privacy challenges related to blockchain before predicting the potential damage from an attack, and verify whether the current technology can withstand persistent hacking attempts.
Previous studies have explored the technical architecture of Blockchain technology in relation to cryptocurrency [7]. Although some studies have focused on the security aspects of Blockchain technology owing to the increasing demand for cryptocurrency with its current security challenges, these studies have focused little on Blockchain technology based cybersecurity threats and vulnerabilities. Among these studies, Conti et al [8] focused on the fundamental background of Bitcoin cryptocurrency, overviews of its use and functionalities, and its privacy aspects. Atzei et al [10] analyzed the smart contracts and offered taxonomy of general programming pitfalls and bugs related to Blockchain technology vulnerabilities. With the emergence of highly sophisticated and dynamic attacks, the existing approaches to security are becoming outdated and less effective. Based on such grounds, our study presents a comprehensive and novel approach using Blockchain to enable exploring and reporting attack vectors that focus on user security and its vulnerabilities.

3. Blockchain Concept

A blockchain is a distributed digital record of transactions. The terminology comes from its structure, where, the individual records called blocks. These blocks are linked

together with each other, and in accordance with the implemented consensus protocol, in single list which is called a chain. The current implementation of blockchains are now seeing in recording crypto currencies transactions. The notion of decentralization is core component, hence, any involved transactions cannot be altered without the alteration of all concurrent blocks.

The key characteristics of the blockchain include

- Decentralization
- Persistency
- Anonymity and
- Auditability

The key advantages and features of Blockchain technologies, includes:

1. Immutability: It means one-way writing to the ledger, hence difficult to tamper or alter a block or committed transaction.
2. Irreversibility: It prevents double spending.
3. Distribution of records: It means that a copy of the ledger is present with all its members.
4. No Centralized Authority or third party: It is a peer-to-peer network.
5. Resiliency: It is not prone to any sort of major attacks.

4. Blockchain Technologies

Blockchain is considered to be the next big technological revolution, as it is reinventing the way we work and live. The structure of blockchain is shown in figure 1. The idea of the blockchain was first introduced by a researcher who implemented the digital crypto currency known as Bitcoin. Blockchain has become an integral part of bitcoin's operation. For several decades, researchers have been dealing with information exchange and the transfer of money and other assets through online transactions via the Internet, where each of these transactions involved a trusted intermediary. It is provides a secure exchange and traceability in the event of any failures or security breaches. In a paradigm shift, the blockchain eliminates the need for any central authority between multiple parties executing financial and data transactions by using an incorruptible, immutable, and decentralized public ledger.

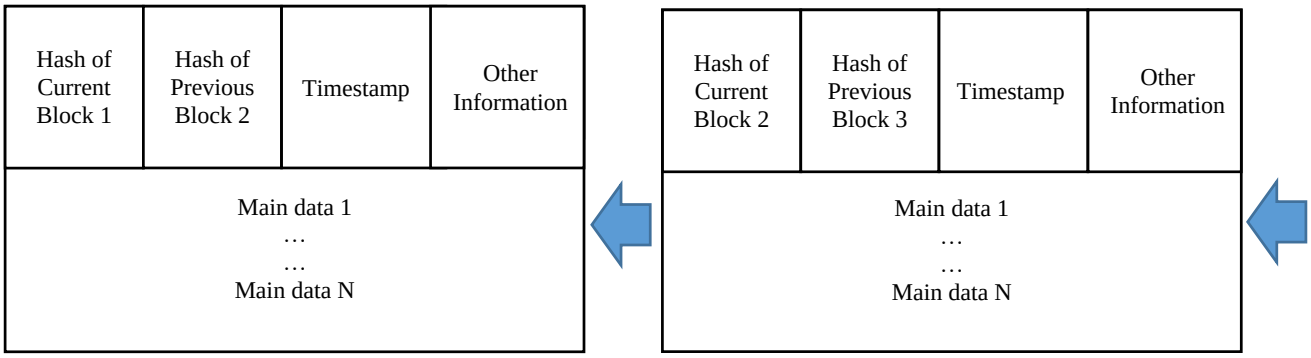


Fig. 1 Structure of Blockchain

Blockchain are working on different kind of technologies. Few of them are listed below:

4.1. Colored Coins

Protocols that allow digital assets other than Bitcoin to be transferred in across different blockchains as "tokens or coins". Those coins and/or tokens can be used to a transfer digital assets where they can be regarded as a meta data for representation of shares, property and other instances.

4.2. Ethereum Blockchain

It is a new developed Blockchain and it operates using digital contracts known as "Smart Contracts". The protocol for Ethereum is different from Bitcoin Blockchain. Smart Contracts are basically small computer programs that accounts for a deal between a client and an end user. Blockchain has a wide range of financial and non-financial applications. It has been used largely by Multinational companies like IBM, Amazon etc. and many other and innovative use cases will evolve in the coming years. Many banks and governments have already collaborated in order to explore the implementation of blockchain technologies in their system.

4.3. Alternative Blockchains

This is also termed as "Sidechains". In the Alternative Blockchain feature, transactions across different blockchains can form new business case. This ensures scalability by providing lesser time for validation, more

easily programmable and most importantly, a separate consensus mechanism.

4.4. Hyperledger Blockchain

It is an umbrella project of Open Source Blockchain and related tools started in 2015 by Linux Foundation to support the collaborative development of Blockchain based Distributed ledgers. It has four platforms like Iroha, Fabric, Sawtooth and Burrow. IBM owns the Hyperledger Fabric and Intel holds and supports the Sawtooth project of Hyperledger [11].

5. Research Methodology and Motivation

In this paper, the DSR methodology for information systems is employed. This methodology employs a specific set of concepts and principles to develop IT solutions [23]. The main DSR elements are summarized in Table 1. It begins with identifying the problem and setting the objectives, which are discussed in Section 4.1. This is followed by designing, developing, and demonstrating the problem, which is presented in its architecture.

Table 1: Design Science Research (DSR) Components.

	Guideline	Description
1	Design	The TVB framework is suitable for encouraging mass security experts to discover new threats and vulnerabilities.
2	Problem Relevance	Despite the benefits of blockchain technologies, it is costly and difficult to find cybersecurity experts to address organizations' related threats and vulnerabilities. It is also challenging many organizations to engage experts in the ongoing discovery of unknown and new threats and security gaps, thus the need for efficient, transparent, and trusted approach is critical. The objective is to develop a distributed and engaging solution that can be adopted and driven by the cybersecurity community.
3	Design Evaluation	The TVB ecosystem is evaluated using an environment which reflects real world situations as a proof of concept.
4	Contributions to Research	The TVB framework provides clear and significant contributions in the area of distributed and blockchain based cybersecurity.
5	Research Rigor	The proposed solution relies on rigorous information security methods.
6	Design as a Search Process	The search for an effective threat and vulnerability discovery and verification solution requires examining all available approaches to reach a solution.
7	Research Communication	The insights gained are disseminated to the blockchain technology and cybersecurity management communities.

This paper presents a TVB framework that examines the threats and vulnerabilities discovered through verified proof of work of participants and engaged community. The selection and validation of the discovered vulnerabilities and threats require an understanding of multiple factors and criteria from diverse perspectives. Further, the framework considers the selection of validators and referees using community voting to elect the most suitable subject matter experts in the area of cybersecurity and threat intelligence.
The motivation for this work is to address the undiscovered cybersecurity security threats and vulnerabilities in a transparent and efficient approach. It enables everyone from anywhere to get incentivized to participate in the discovery of security concerns and protection of digital assets. The model utilizes the structure of distributed nodes in blockchain architecture to allow trusted communication and discovery. This method of community based driven security and intelligence services improves the status quo in tackling threats, cybercrimes, and optimizes the defense in depth found in many organizations.

6. Threat and Vulnerability Blockchain (TVB) Framework

In this section, architecture of the threat and vulnerability blockchain (TVB) is presented. The goal is to provide cost effective and transparent threat and vulnerability detection and prevention mechanism. The TVB architecture includes cybersecurity professionals (participants of the discovery, validators, consumers of the information, etc...), consensus algorithm, peer-to-peer and distributed communication, cryptographic functions and digital signature. The TVB components are shown in Figure 2 and described below.

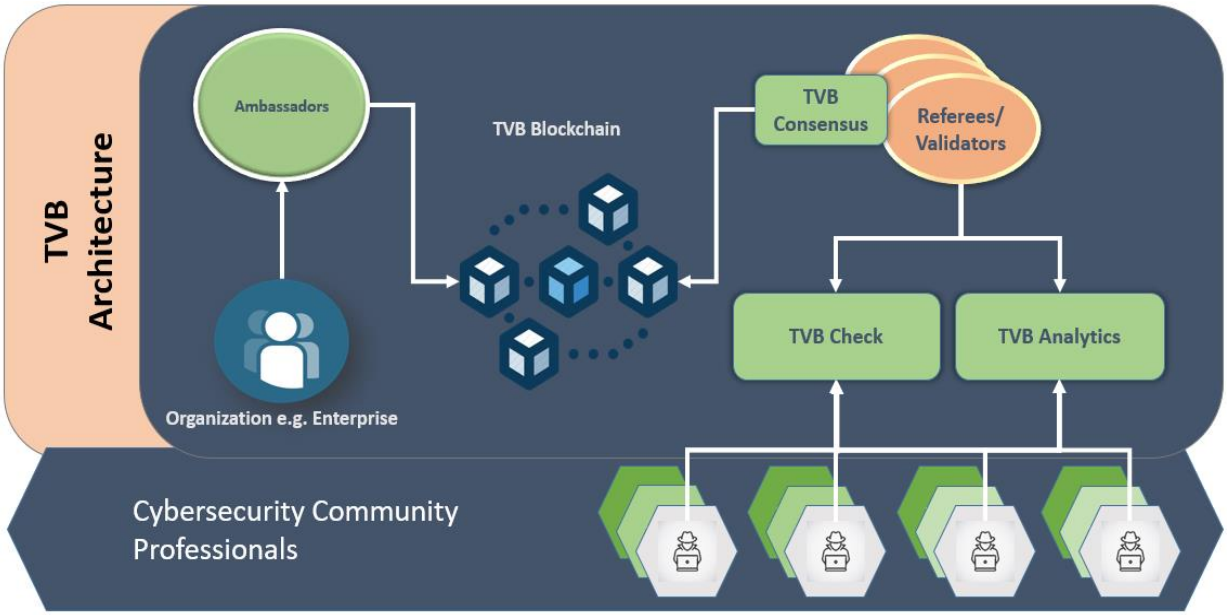


Fig. 2 The Threat and Vulnerability Blockchain (TVB) Architecture.

6.1. TVB Consensus

The Consensus piece is one of the critical components of TVB framework aims at providing regulated transaction of any reported threats and vulnerabilities on a peer-to-peer basis. Due to decentralization of TVB architecture, the community participants agree on exchanging the information and its validity without the use of intermediary or trusted 3rd party to ensure secure storage, data accountability and management. This is accomplished via the use of a protocol called "Consensus Algorithm". TVB may utilize this algorithm to ensure greater security, accuracy and reward to those participants with valid threat/vulnerability findings.

The process begins when one of the community members uploads a new threat or vulnerability providing all relevant details to the newly discovered file and/or signature. This then gets into TVB block which is broadcasted to all participants to be audited by a group of cybersecurity referees across the world. The referee with the longest chain of trusted records in TVB can commit the validity of the new proof of work i.e. the new threat/vulnerability transaction. Finally, a new block is created and committed to TVB chain which has the finding details e.g. description, threat type, impact factor, signature, potential mitigation, etc.

6.2. TVB Network Participants

The participants of the proposed structure can range from cybersecurity individuals who wants to upload a new threat/vulnerability finding or who wants to consume new threat/vulnerability findings to those organizations and or institutions wanting to share information and the distributed ledger that contains valid transitions of threat/vulnerability discovered in a chronological order. Depending on the deployment of TVB blockchain i.e. public or hybrid blockchain, there should be some form of incentives to those network participants. New discovery of threat/vulnerability should be recognized and accredited to ensure the continuity of such needed work. Similarly, referees/validators are at other edge playing a key role in ensuring the integrity and relevancy of the threat/vulnerability discovery process, hence should be recognized and rewarded. TVB categorizes participants as follows:

Cybersecurity Professionals: individuals, institutes, research centers and other participants who detect and reports new threat/vulnerability signature as new block in TVB.

Referees: individuals, institutes, research centers, and other participants who can be elected as master nodes and validators of the new threat/vulnerability findings detects and reports new threat/vulnerability signature as new block in TVB.

Ambassadors: individuals, organizations, commercial companies/vendors, institutes, and research centers who can act as a representative of the beneficiary of the TVB service. The representative of an organization X logs into the systems to search for or get the latest threats reports.

6.3. TVB Governance Model

In order to ensure compliance and transparency, TVB governance model is proposed. The model is regulated and executed via the use of smart contract where results are logged into TVB blockchain. The governance model contains:
Voting authority model to select the most suitable Referee/validator. It provides an immutable, transparent and decentralized voting procedure
The security checks and audits are governed by smart contract against compliance with threat/vulnerability reporting security checks, standards and formats such as The Common Vulnerability Reporting Framework (CVRF) [22].

6.3.1. TVB Check

This component is suggested for professional services provided by the community participants and uploaded to TVB. Services such as security audits, penetration testing, vulnerability assessment, can be offered to ambassadors in need for conducting such security checks/services to their organizations. Validators review the authenticity of submitted reports and authorize its blockchain transactions.

6.3.2. TVB Analytics

The analytics component acts as a community driven threat intelligence function. It enables reporting and registering zero-day threats and vulnerabilities. Active participants around the world log their findings continuously to TVB ledger for review and reward. Referees then cast their votes on the most accurate, relevant and authentic threat and vulnerability transaction.

7. Conclusion

Blockchain technology has shown a promising benefit towards enabling trustless digital transformation in different economies. One of these 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. This paper provided a novel TVB framework that enables smarter and efficient cybersecurity threat intelligence reporting. After providing a general methodology on the appropriate implementation of TVB framework to threat and vulnerability detection and reporting, some of the most relevant and recent work were examined. The TVB architecture is highlighted were trusted source of threat and vulnerability information and can shared among the community. Because of TVB nature was built on decentralized ledger and consensus algorithm, there was no need to a centralized third party to be involved in the operations. TVB model offers many opportunities for better discovery and mitigation of cybersecurity threats and vulnerabilities. Many participants around the world can take part in the discovery and reward mechanism of the TVB. Author believes that the presented model will not only increase the authenticity of threat finding and reporting, but creates a disruptive dimension of how security vulnerabilities got discovered, reported, and indeed rewards those talents in the TVB community.

References

[1] 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.

[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] 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.

[4] 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’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), IEEE international congress on. IEEE, pp. 557-564, 2017.

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

[7] Tschorsch F, Scheuermann B. “Bitcoin and Beyond: a Technical Survey on Decentralized Digital Currencies.” IEEE Commun Surv Tutorials, Vol. 18, 2016.

[8] P. Tsankov, A. Dan, D. D. Cohen, A. Gervais, F. Buenzli, and M. Vechev, “Securify: Practical Security Analysis of Smart Contracts”, arXiv preprint arXiv: 1806.01143, 2018.

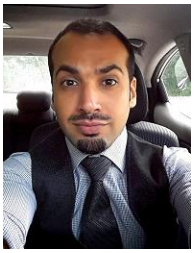
[9] Conti M, Lal C, Ruj S. “A Survey on Security and Privacy Issues of Bitcoin.” IEEE Commun Surv Tutorials https://doi.org/10.1109/ COMST.2018.2842460, Vol. 20, No. 4, pp. 3416-3452, 2018.

[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, (2017) "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, pp. 580–584, 2017.
[14] R. Kachhwaha and R. Purohit, (2019) "Relating Vulnerability and Security Service Points for Web Application through Penetration Testing", In Progress in Advanced Computing and Intelligent Engineering. Springer, pp. 41–51, 2019.
[15] Y. K. Lee, P. Yoodee, A. Shahbazian, D. Nam, and N. Medvidovic, (2017) "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] I. Nikolic, A. Kolluri, I. Sergey, P. Saxena, and A. Hobor, "Finding the Greedy, Prodigal, and Suicidal Contracts at Scale", arXiv preprint arXiv: 1802.06038, 2018.
[17] Q. Shao, C. Jin, Z. Zhang, W. Qian, A. Zhou et al., (2018) "Blockchain Technology: Architecture and Progress", Journal of Computer, Vol. 41, No. 5, pp. 969–988, 2018.
[18] G. Zyskind, O. Nathan et al., "Decentralizing Privacy: Using Blockchain to Protect Personal Data", In Security and Privacy Workshops (SPW), 2015 IEEE, pp180–184, 2015.
[19] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, (2016) "Medrec: Using Blockchain for Medical Data Access and Permission Management", In Open and Big Data (OBD), International Conference on. IEEE, pp. 25–30, 2016.
[20] 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.
[21] Ali, M., Nelson, J. C., Shea, R., and Freedman, M. J. "Blockstack: A Global Naming and Storage System Secured by Blockchains." In USENIX Annual Technical Conference, pp. 181–194, 2016.
[22] 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.
[23] Hevner, Alan, and Samir Chatterjee. "Design Science Research in Information Systems." In Design research in information systems Springer, Boston, MA,pp. 9-22, 2010.



Fahad F. Alruwaili is an Assistant Professor in the College of Computing and Information Technology, University of Shaqra, Saudi Arabia. He is an information security and risk management consultant with over twelve 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 information security and data privacy.