Blockchain Techniques for Secure Storage of Data in Cloud Environment

Praveen Kumar Kollu[1], Monika Saxena[2], Khongdet Phasinam[3], Thanwamas Kassanuk[4], Malik Mustafa[5]

[1]Velagapudi Ramakrishna Siddhartha Engineering College
[2]Banasthali Vidyapith, Jaipur, Rajasthan 304022
[3]Faculty of Food and Agricultural Technology, Pibulsongkram Rajabhat University, Phitsanulok, Thailand
[4]Faculty of Food and Agricultural Technology, Pibulsongkram Rajabhat University, Phitsanulok, Thailand
[5]Center for foundation Studies, Gulf College

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract

The need for Blockchain advancement, as well as the importance of its use, has fueled ongoing research in a variety of theoretical and practical fields. Even as it is still in its early stages of development, the blockchain is being seen as a forward-thinking approach to modern technology issues such as decentralization, identification, confidence, character, data ownership, and information-driven decisions. The blockchain breakthrough offers major feedback when effectively searching for the optimal solution to storing and accessing cloud data. This essay examines the use of blockchain technologies to secure cloud computing. This research paper also presents a framework for secure storage of data in cloud computing environment. This framework makes use of smart contracts and access list for ensuring data security.

Keywords: Blockchain, Cloud Storage, Smart Contracts, Cloud Security, Access List

1. Introduction:

Cloud computing cannot be easily identified as the meteorological phenomenon from which it takes its name. The same common denominator is used in multiple definitions: the Internet. Cloud computing means using all the computer-installed tools, using the Internet in everyday life from a single computer or a single room. It is also capable of using pooled computer services with programs that handle local servers. The positioning and storage of their data do not bother cloud users. The programs are only being used anywhere and at any moment. Virtualization (Hypervisor) and virtual devices are the core drivers of this technology [1].

Virtualization is a way to distinguish physical devices by simulating software from the operating system and applications. Into the machine is the program known as hypervisor. The program also downloads files that describe a virtual machine. A virtual device is a program that consists of all the components needed to operate on an operating system. The device and operating systems virtualization masks the users' physical features. The hypervisor is a virtualization component that enables several virtual operating systems to instantly operate on the same physical computer [2].

Many instances of virtual servers, linked together through the virtual switch, may be installed on the same server hardware. The architecture enables a virtual data center to be set up with the same features as the actual rack device world. The redundancy of this framework helps users to access the apps anywhere and at any time. Definition of definition The cloud is a term that allows users to access a pool of computer services, such as software, CPUs, RAMs, database systems, virtual servers and network systems.

Cloud infrastructure is a model of a common pool of configurable computing tools (i.e. Networks, servers, storage, apps and utilities) that can be quickly supplied and released using limited

maintenance efforts or interference between providers provided by the US State Institute of Standards and Technology (NIST). This cloud architecture fosters availability and consists of five key features, three distribution models and four implementation models.

According to Cloud Security Alliance (CSA) the following are the top threats to cloud computing security. Data breaches, Data loss, Account or Service traffic hijacking, Insecure interfaces, Denial of service ranks, Insufficient due diligence, Shared technology vulnerabilities [3].

Cloud Control is a broad variety of issues from hardware and platform safety to cloud data safety and resource usage (through different end- user devices). Whilst cloud storage offers tremendous value, often cloud customers rely on security and privacy issues and discourage businesses and organizations from making wide-ranging adjustments.

2. Literature Survey

2.1 Cloud Storage

The supplier of web services uses a large volume of data to process, store and back up cloud computing platforms like Google, Amazon, and others. The database systems are used to store indexes of search engines, social network data and webmail attachments. The standard database framework avoids data loss information with the use of error resistant hardware and cloud storage systems. This method performs data replication and recovery on a vast number of often failing commodity servers.

The unparalleled size of these computing arrays in combination with hardware deficiencies on commodity servers. Cloud storage is one of the storage system components that allows the data volume demands to be addressed. In IT, information management and data retention expenses are raised. The storage management systems that serve vast quantities of data and various demands manage those obstacles. The storage system is referred to as a facility for a small company which has no capital budget for its own facilities and maintenance.

The cloud storage solution swung over the deployment of storage technologies [4]. Depending upon the mainframe, client or servers and personal computer, the supremacy of storage and control is shifted. The cloud is one of the new versions to store massive data and gives storage consumers extra flexibility.

The two convincing advantages of cloud computing are focused on two fields such as cloud storage and recovery cloud backup. Between cloud storage and backup, there are various operations. Storage is connected to the space needs to cope with the preservation and integrity of the memory requirements and backup is used to store the saved data on the local drives. Cloud computing is facing problems

- The cloud storage dependency does not exist on the single server that causes dependence on hardware.
- The potential growth of data will be provided with a virtually stored container with less disk capacity.
- Continuation of operation is dependent on the accident scene.
- Reduction in access from the single point and location across the entire storage pool is dependent on the pay model.

2.2 Blockchain Overview

Blockchain is revolutionary and somewhat distinct from databases in preserving transaction records. Satoshi Nakamoto first introduced the Blockchain technology in 2008 and then introduced it as a central part of Bitcoin in 2009. (a popular crypto currency). The blockchain is a distributed booklet that chronologically tracks transactions [5]. In contrast to a centralized directory where the ledger is held on a server and every node updates transactions on that server in Figure 1 the ledger is managed by all participating nodes on a blockchain networks.

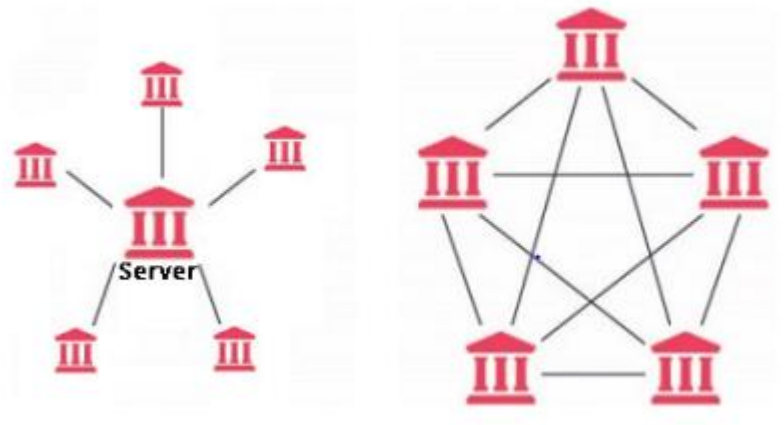

Figure 1: Centralized Ledger and Distributed Ledger

The following features make Blockchain a safer solution to company systems.

● Immutivity: Immutivity signifies no alteration after the completion of the transaction. Blockchain is focused on hacking that produces specific hash code for transaction blocking and any transaction changes resulting in hash code changes. Immutability is accomplished by cryptographic authentication and confirmation, meaning that attacks on blockchain data can be less feasible.

● Protected: the use of cryptography to ensure anonymity is safe for blockchain and transactions are mapped to user identity in a uniquely secure way [6]. The private key of users is used for this.

● Privacy: privacy concerns the protection of users' personal identities and ensures that encryption can be used via blockchain.

● Replicated: transactional data is distributed in blockchain and a copy of the entire data chain in every network node ensures that no single point of failure is secured. When a node initiates a transaction, the copy is transmitted to all nodes on the network.

● Transparency: all nodes in the transaction verification are guaranteed transparency and a full copy of the blockchain is provided for all participating nodes[7].

Blockchain enforces trust through the straightforward handling of the transaction and the hashing mechanism (Merkle tree) renders it unchanging. Blockchain reduces the possibility of a single failure point, since this is distributed in nature and a backup of transaction data is sent to all network nodes. A blockchain allows rapid transfers between parties without the need for an intermediary to protect the legitimacy of the transactions. Blockchain technology mostly has two categories, i.e., fewer permits than permitted.

Both users have an authorisation less blockchain that is also called a public blockchain. While it has enormous potential like Bitcoin, it might not be appropriate for owners of businesses who want control of the transaction management system. Business processes may have unique specifications and dynamic activities which require tailor-made solutions and limit external interference. Allowable blockchain also suffers from such problems such as scalability, governmental authorities and evolution regulation.

This has provided companies the opportunity to consider other options, including permitted blockchain, for which membership in the blockchain network can only be managed privately by trusted members. The blockchain permitted is also called the private blockchain.

2.3 Related Work

Many emerging tools and applications with the current keen interest in blockchain technology have been launched. Many reviews of blockchain's benefits to current apps have been released. Examples of those studies include company blockchain tech nology [8][9], electric management [10], safety [11-13],

sharding [16], cloud exchanges [17], cutting edge computing [18] and so on. Some reports have addressed obstructions, outlooks and future ambitions. For eg, references [14, 19, 20] deal with security issues and blockchain opportunities.

The study in [51] pro provides a concise analysis of cloud storage privacy and security issues that include emerging risks and blockchain-based identification techniques. Authors discuss blockchain technologies in the areas of health and medicine in references [12-13]. Reference[16] provides core ideas for different blockchain application sharding mechanisms. The authors discuss aspects of encryption, security and transaction management in relation to blockchain usage for cloud sharing in Reference [17].

Furthermore, the reference [18] concerns blockchains and their possible application for edge computing systems. Every previous study discusses the safety trend of cloud computing and plans to implement blockchain technologies in various environments.

In [21] authors suggested a DESCAST hybrid cloud data protection algorithm. This approach has ensured the safety of vast data transmitted by the media. The plaintext was encrypted with the hidden key in the DES algorithm, and this key was assigned to the DES input. For both encryption and decryption, the same hidden key was used. Both CAST and DES were used in the algorithm proposed. There are two encryption steps and two decryption phases of this algorithm.

In the encoding process, the single text was implemented with the CAST encryption algorithm and the encrypted texts with the DES encoding algorithm. The DES algorithm of decryption for the cipher text was used during the decryption stage and the CAST algorithm of decryption was added to the decrypted text. The combination of the DES and CAST algorithms guaranteed protection from attacks in plain text.

A hybrid symmetric encryption algorithm was suggested by authors in [22] to provide information protection and data security. By combining the substitution chip and the transposition chip, the proposed algorithm has been developed. Both methods used cipher text alphabets and translated the text to the ASCII code value in plain text. The traditional encryption technology has key ranges from 1 to 26, while the algorithm proposed has key values from 1 to 256. The two phases of encryption and decryption are listed in the proposed algorithm.

The encryption algorithm first computed the number of characters inside the plain text, then translated the number of characters into ASCII equivalent and constructed the matrix. The matrix was then divided into 3 parts: top, diagonal and bottom. The values of each matrix from right to left and the ASCII code have been translated into the value of the character. The cloud was able to recover encrypted data by means of the decryption algorithm.

The encryption and decryption used the key values to read the data. The proposed symmetric encryption algorithm has been efficient to handle large number of data in the cloud. The user does not have any control over the data after the session got expired or logged out. The administrator cannot access data and hence security has been enhanced.

The revokable Identity Based Encryption (IBE) scheme was introduced for enhancing security by researchers[23]. The new strategy for collusion resistance was proposed, providing each recipient with the hybrid private key. The user received a privately-owned key generator ID and default time variable (PKG). The customer asked to update the cloud service provider key on a periodic basis (KU-CSP). The KU-CSP was a third party public cloud which supplied PKG and reduced the costs of PKG calculations and storage.

In the proposed scheme, which worked in the two following regions, the private upgrade process has been implemented. Each consumer has a hybrid private key that has AND gates that bind the ID and Time Components (TK). In PKG key edition mode the IK was developed and in KUCSP key update mode, the TK was changed. The user ID and T-time T is considered the input for encryption. When the name and the amount of time matched the private key it is allowed to decrypt.

SetUp, KeyGen, Encrypt, Decrypt, Revoke and KeyUpdate are the measures included throughout the suggested system. By reconstructing private keys, the writers prohibited revoked users from colluding with other users. In this system, during main updates the user does not have to touch PKG and the revoke list is passed to KUCSP.

The new central patient system for safe personal health records was introduced by the researchers[24] (PHR). In order to achieve fine grained and scalable data, the technique for Atribute Based Encryption (ABE) was proposed. The data owner has updated the user data to the cloud data center of third parties. The dynamic modification of access policies also allows the same data values to be accessed by multiple data owner. The key management challenges were addressed by dividing the users into two types such as public and personal domain.

The suggested architecture concurrently processed the various forms of PHR applications. The Multi Authority ABE (MA-ABE) was used by the public domain to enhance stability. The owners assigned direct access rights and PHR encryption in their personal domain. The Key Generation Center (KGC) has randomly generated keys 66 and no control of the key. By generating their attributes the KCG decrypts all ciphertexts addressed by any device. The key generation system generated and supplied the user with the key. The application center accessed this key. Confidential data access by means of the provided key.

The Cloud Service Alliance (CSA) framework for cloud service protection was considered by researchers[25]. The trustworthy model was developed to calculate the strength of security and confidence. A methodology was developed to calculate the trust of many cloud service providers in the cloud world. Four feature models, including cloud service manager, trust model, service log, and site research, are provided in the system. The cloud service manager gathered the sort, number of registered users and the service provider information [26].

The confidence value of the cloud server was retained in order to improve security. Static and core confidence values were determined by the trust model. The service log contains the log record database such as service use, number of completed and unsuccessful transactions and response time.

3. A Framework for Secure Storage of Data in Cloud

A framework for secure storage of data in cloud is shown below in figure 2. In this framework, owner of data has all rights over data. Data owner sets smart contracts. Data owner stores hash of data in smart contracts. Ethereum performs encryption on data. It is also responsible for generating hash on data. User of data sends request to data owner. The owner of data updates details in smart contracts. Then user of data receives access rights and duration from smart contracts. After that user of data is capable of accessing data from the cloud storage.

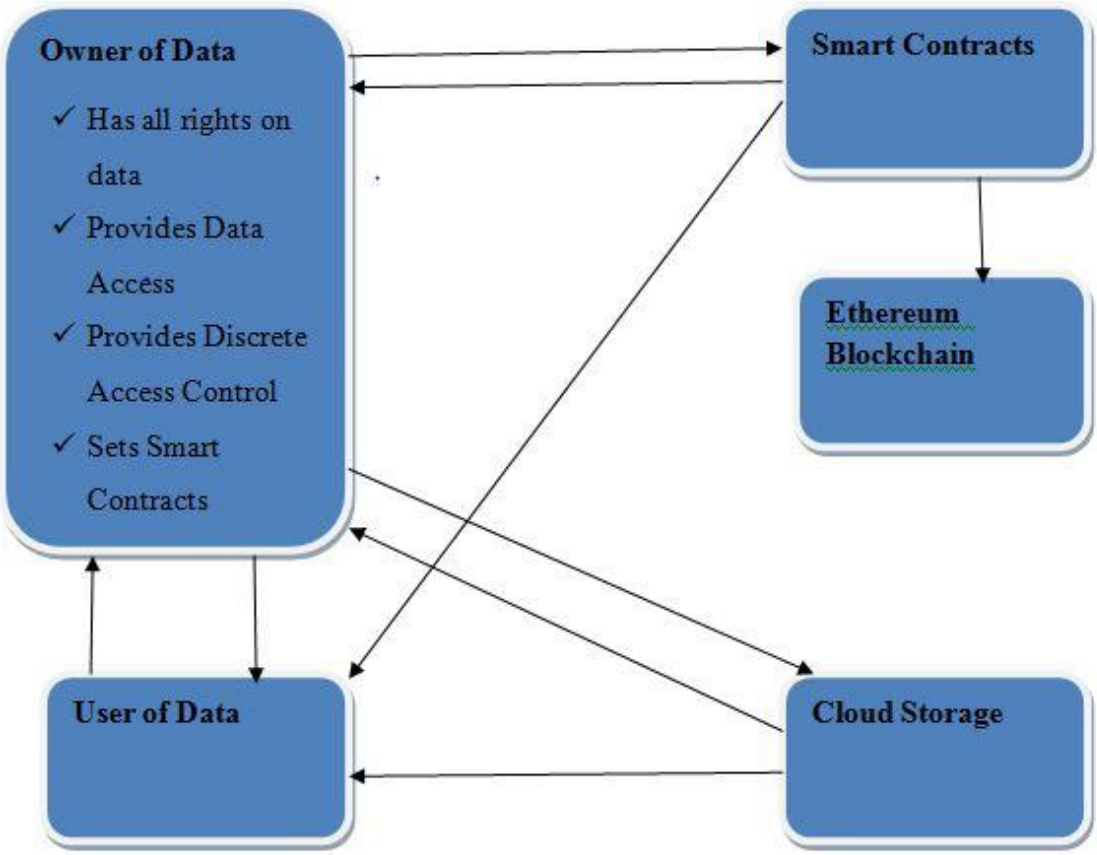

Figure 2: Blockchain based framework for secure cloud storage

The benefit of deploying the Smart Contract on the blockchain is that it is impossible to change the contract and that the cost of delivery, authentication, and fraud detection is reduced. Another value is that distributed ledgers execute seamlessly and in an unbreakable manner. Each transaction can be tracked and is permanent. The Smart Contract's bytecode was implemented in the blockchain, and the action occurred under if-then conditions. When opposed to a conventional contract, the Smart Contract offers greater stability. It also lowers processing costs.

4. Conclusion

In a number of theoretical and functional fields, ongoing research has been fuelled by the need and the relevance of Blockhain development. Even as it is still in its early stages of growth, the blockchain is seen as a forward-looking solution to contemporary technology concerns like decentralization, identification and trust. The revolutionary blockchain provides important input if the optimum approach to storage and access cloud data is sought. This paper explores the use of cloud computing protected by blockchain technology. In this study, a system for safe data management in the cloud computing setting is also provided. Smart contracts and permission lists are used in this application to ensure data protection.

References

[1] Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren. 2016. A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. IEEE Trans. Info. Forensics Secur. 11, 11 (2016), 2594–2608. https://doi.org/10.1109/TIFS.2016.2590944

[2] Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. 2017. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing. 468–477. https://doi.org/10.1109/CCGRID.2017.8

[3] Pol, Rohit, Thakur, Vishwajeet, Bhise, Ruturaj, and Kate, Akash, " Data leakage Detection," International Journal of Engineering 180 Research and Applications (IJERA) ISSN: 2248-9622 ,Vol. 2, Issue 3, May-Jun 2012, pp. 404-410.

[4] Tang, J, Cui, Y, Li, Q, Ren, K, Liu, J & Buyya, R 2016, „Ensuring security and privacy preservation for cloud data services", ACM Computing Surveys, vol. 49, no. 1, pp. 1-39.

[5] Cachin, C. (2016), Architecture of the Hyperledger Blockchain Fabric, in 'Workshop on distributed cryptocurrencies and consensus ledgers'. IBM, pp.1–4. https://www.zurich. ibm.com/dccl/papers/cachin_dccl.pdf.

[6] S. Velliangiri and P. Karthikeyan, "Blockchain Technology: Challenges and Security issues in Consensus algorithm," 2020 International Conference on Computer Communication and Informatics (ICCCI), 2020, pp. 1-8, doi: 10.1109/ICCCI48352.2020.9104132.

[7] L. Madaan, A. Kumar and B. Bhushan, "Working principle, Application areas and Challenges for Blockchain Technology," 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), 2020, pp. 254-259, doi: 10.1109/CSNT48778.2020.9115794.

[8] Ioannis Konstantinidis, Georgious Siaminos, Christos Timplalexis, Panagiotis Zervas, Vassilios Peristeras, and Stefan Decker. 2018. Blockchain for business applications: A systematic literature review. In Proceedings of the International Conference on Business Information Systems. Springer, Cham, 384–399. https://doi.org/10.1007/978-3-319-939315_28

[9] Qalab E. Abbas, and Jang S. Bong. 2019. A survey of blockchain and its applications. In Proceedings of the International Conference on Artificial Intelligence in Information and Communication (ICAIIC'19).1–3.https://doi.org/10. 1109/ICAIIC.2019.8669067

[10] F. Rizal Batubara, Jolien Ubacht, and Marijn Janssen. 2018. Challenges of blockchain technology adoption for egovernment: A systematic literature review. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age.1–9.https://doi.org/10.1145/3209281.3209317

[11] Cornelius C. Agbo, Qusay H. Mahmoud, and J. Mikael Eklund. 2019. Blockchain technology in healthcare: A systematic review. Healthcare Multidisc. Digital Publish. Inst. 7, 2 (2019), 56. https://doi.org/10.3390/healthcare7020056

[12] Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine, and Rachid Benlamri. 2019. Blockchain technology in healthcare: A comprehensive review and directions for future research. Appl. Sci. 1–28. https://doi.org/10.3390/ app9091736

[13] Asad A. Siyal, Aisha Z. Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil, and Georgia Soursou. 2019. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography 3, 1 (2019), 1–16. https://doi.org/10.3390/cryptography3010003

[14] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and privacy issues on blockchain. ACM Comput. Surveys 52, 3 (2019), 1–35. https://doi.org/10.1145/3316481

[15] Joanna Kolodziej, Andrezej Wilczynski, Damian F. Cerero, and Alejandro F. Montes. 2018. Blockchain secure cloud: A new generation integrated cloud and blockchain platforms-general concepts and challenges. Eur. Cybersecur. J. 28–34.
[16] Guangsheng Yu, Xu Wang, Kan Yu, Wei Ni, J. Andrew Zhang, and Ren P. Liu. 2019. Survey: Sharding in blockchains. IEEE Access 8 (2019), 14155–14181. https://doi.org/10.1109/ACCESS.2020.2965147
[17] Shaoan Xie, Zibin Zheng, Weili Chen, Jiajing Wu, Hong N. Dai, and Muhammad Imran. 2019. Blockchain for cloud exchange: A survey. Comput. Electric. Engineer. 81 (2019), 1–20. https://doi.org/10.1016/j.compeleceng.2019.106526
[18] Ruizhe Yang, F. Richard Yu, Pengbo Si, Zhaoxin Yang, and Yanhua Zhang. 2018. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Commun. Surveys Tutor. 21, 2 (2018), 1–22. https://doi.org/10.1109/COMST.2019.2894727
[19] Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka. 2019. A security services using blockchains: A state of the art survey. IEEE Commun. Surveys Tutor. 21, 1 (2019), 858–879. https://doi.org/10.1109/ COMST.2018.2863956
[20] Bhabendu K. Mohanta, Debasish Jena, Soumyashree S. Panda, and Srichandan Sobhanayak. 2019. Blockchain technology: A survey on applications and security privacy challenges. Internet Things 8 (2019), 1–19. https://doi.org/10. 1016/j.iot.2019.100107

[21] Kumar, KV, Reddy, NCS & Reddy, BS 2015, „Preserving data privacy, security models and cryptographic algorithms in cloud computing", International Journal of Computer Engineering and Applications, vol. 7, no. 1, pp. 59-67.

[22] Arockiam, L & Monikandan, S 2013, „Data security and privacy in cloud storage using hybrid symmetric encryption algorithm", International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 8, pp. 3064-3070.

[23] Jung, T, Li, XY, Wan, Z & Wan, M 2013, „Privacy preserving cloud data access with multi-authorities", IEEE INFOCOM, Proceedings, pp. 2625- 2633.
[24] Ramesh, C, Krishna, D & Deepthi, G 2015, „Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption", International Journal of Advanced Technology and Innovative Research, vol. 7, no. 5, pp. 702-707.
[25] Shaikh, R & Sasikumar, M 2015, „Trust model for measuring security strength of cloud computing service", Procedia Computer Science, vol. 45, pp. 380-389.
[26] Mustafa, M., & Alzubi, S. (2020). Factors Affecting the Success of Internet of Things for Enhancing Quality and Efficiency Implementation in Hospitals Sector in Jordan During the Crises of Covid-19. In Internet of Medical Things for Smart Healthcare (pp. 107-140). Springer, Singapore.