PalArch's Journal of Archaeology of Egypt / Egyptology

CYBER RISK MITIGATION IN CLOUD COMPUTING ENVIRONMENTS USING BLOCKCHAIN TECHNOLOGY

Harsh Sengar[1], *Sujata Joshi*[2]

Symbiosis Institute of Digital and Telecom Management,

Symbiosis International (Deemed University), Pune, India

Email: sjoshi@sidtm.edu.in

Harsh Sengar, Sujata Joshi: Cyber Risk Mitigation in Cloud Computing Environments using Blockchain Technology -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(6). ISSN 1567-214x

Keywords: Barriers, e-learning, Blackboard system.

ABSTRACT

Cloud Computing has gained widespread use over the past few years. However, in recent times, there is an alarming rise in the cyber-crimes across the globe which has made it a major concern. IT systems and the information generated is being target of the advanced cyber-attacks therefore threats to data integrity are of foremost pertinence. Blockchain technology is providing convincing properties about data integrity.

In academic research, very few studies have focused on how Blockchain Technology can be used in cloud computing environments for data integrity.

The objective of this paper is to comprehend how Blockchain can be used to mitigate the data integrity threats caused due to various cyber-attacks in the cloud computing environment.

Case study approach has been adopted for this study wherein the use cases of Blockchain Technology in cloud computing environments are briefly discussed along-with future applications which will help create customized solutions for the clients.

1. Introduction

Cloud Computing has introduced a shift in the way how the technology is used and managed nowadays. Organizations are provided with the ability to reconfigure computing environments quickly as per changing business

requirements to optimize spending. As mentioned in the article by Louis Columbus [1], 83% of workload of various enterprises will be shifted to cloud by the year 2020. Data is a key asset nowadays. According to World Economic Forum [2], around 463 exabyte of data will be generated daily in the world by the year 2025. Data assists in driving various business decisions in different fields, ranging from public administration to healthcare, finance, education, insurance, finance, and developing new marketing strategies. The critical role possessed by of data has therefore made it an appealing target for cyber-attacks, which undermines the Confidentiality, Integrity and Availability (CIA) properties which the data should show so as to be trusted. Data tampering by altering particular sections of the data or deleting specific entries causes impairments on data trust as it can go undetected and maliciously drive operations. As mentioned in the article by Fran Howarth [3], Kaspersky uncovered massive cyber-attack that was targeting the financial/banking industry, attackers got into the accounting systems using spear phishing attack and siphoned off around $ 1 billion by inflating the account balances of over 100 financial institutions. Once the data integrity is lost the original data cannot be restored. Therefore, in this paper main focus is on the integrity of the data rather than availability and confidentiality.

Private and public organizations are doing cloud-based data outsourcing as it alleviates them of overhead cost of storing the data locally as well as maintenance cost. According to IDC [4], it is estimated that from 2016 to 2022, cloud computing usage will be going to add $ 859 billion in revenue – around $ 140 per year – to progressing revenue streams of Salesforce clients.

Data owners are not able to control where the data is stored and who is accessing the data in the cloud making data integrity issues more severe. Therefore, maintaining proper data integrity has become very important. Data integrity is provided by the means of asymmetric keys and by appropriate data replication strategies in the cloud, a successful attack would require the infringement of the keys to bypass integrity checks. These cyber-attacks are hard to implement, but once done successfully they have a huge impact on the organizations. This paper portrays how blockchain technology can be utilized to overcome such cyber-attacks.

Earlier, blockchain has been used as a public ledger to carry out the bitcoin transactions successfully. Blockchain uses a distributed consensus mechanism which is designed to withstand tampering. Using a rule, transaction records are encrypted and are operated in the frameworks that run blockchain software. Because of the qualities such as open attribute and intrinsic replication, implementing blockchain in areas such as cloud can be done to mitigate the cybersecurity risks and data integrity issues.

Objective of the study:

Hence the objective of this research paper is to comprehend the effect of blockchain technology in cloud computing environments.

2. Literature Review

2.1 Cyber risk in cloud computing

According to PWC [5], cyber risk is the risk resulting in the interruption, financial loss or harm of the notoriety of an organization due to the failure or unapproved utilization of its data frameworks. When the cloud services are compromised due to a cyber-attack, hackers can interrupt the services or can gain access to the sensitive data and manipulate it. As mentioned in the article by Phil Muncaster [6], a significant DDOS (Distributed Denial of Services) attack which lasted for approximately eight hours took out AWS S3 (Simple Storage Service) and other services including Relational Database Service (RDS), Elastic Cloud Compute (EC2) those required public Domain Name System (DNS) resolution.

2.2 Definition of blockchain

According to Zheng et al. [7] Blockchain is the public ledger where the carried out transactions are stored in the list in the form of blocks. The list grows continuously with the addition of the new blocks. In blockchain, asymmetric encryption and distributed consensus have been actualized for client security and record consistency. According to Abdelrahman & Farah [8], Blockchain is an appropriated database of records which can be either public ledger of advanced issues or transactions that are achieved among the participating parties over a huge system of untrusted participants.

2.3 Blockchain Technology application in various fields.

Various studies have been conducted on the application of blockchain in the different fields, for example, voting, internet of things (IoT), healthcare, international trade, logistics, insurance, copyright protection, advertising, supply chain management, business and information systems, etc. H. S. Chen et al. [9] have studied the application of blockchain in healthcare industry in which they used Ethereum service to provide security to the patient's records. Hjálmarsson & Hreiðarsson, n.d. [10] in their study discussed the use of blockchain in the e-voting system. DHL [11] discussed blockchain technology application in tourism. Blossey et al. [12] discussed blockchain technology application in supply chain management. Beck et al. [13] discussed blockchain technology application in different industries.

The report by Cloud Security Alliance [14] discusses how the organizations which are implementing IoT solutions are experiencing various challenges identifying the security technologies and the approaches that are sufficient to mitigate the threats to IoT. It is showing how blockchain is playing a major role in overcoming these challenges. Belu [15] discussed the application of blockchain in international trade. The study by W. Chen et al. [16] shows that how blockchain can be used in various areas such as insurance, copyright protection, and advertising.

The study by Malviya [17] discusses in particular about the blockchain cloud for data storage purposes. Abinaya et al. [18] investigated the blockchain-based cloud storage model and identified the various advantages it has over traditional cloud storage for data integrity.

3. Research Methodology

Case study approach is adopted for this research where various cases of Blockchain adoption in the area of cloud computing have been referred and the

benefits accrued for the same are discussed. Various whitepapers, reports, articles and online databases have been collected and studied for the data required. For relevance to the topic, collected literature was then analysed.
The questions that were addressed through this study are as follows:

- For data integrity purposes, is Blockchain technology playing a significant role in cloud computing environments?
- Are there any specific use cases where Blockchain technology application has been adopted in the cloud computing environment for data integrity?

4. Blockchain Technology In Cloud Computing: Use Cases

4.1 Use Case 1: Alibaba Cloud

Alibaba Cloud BaaS (Blockchain as a Service) which is using the capabilities of Alibaba Cloud in maintenance, computing, databases, and security is built on Alibaba Cloud Container Service for Kubernetes clusters. It is an enterprise-level PaaS (Platform as a Service) that is based on blockchain technologies such as Enterprise Ethereum - Quorum and Hyperledger Fabric helping to focus on business innovation [19].

Benefits Accrued

Alibaba Cloud BaaS provides advanced security protection, high stability, openness, and sharing and also supports quick deployment of the production level blockchain environment. Alibaba Cloud BaaS simplifies development and reduces the time with the help of pre-configured infrastructure and networks by adding enterprises and businesses dynamically in the blockchain network [19].

4.2 Use Case 2: IBM Blockchain

IBM Blockchain Platform for IBM Cloud is based on Hyperledger Fabric, which provides total control over the deployment, private keys, and certificates. IBM Blockchain helps the customers in deploying applications and data securely and quickly by providing a highly reliable and scalable platform. Some of the biggest banking and commercial industries are using IBM Blockchain.

Benefits Accrued

IBM Blockchain platform helps in building integrated developer experience allowing users to easily code smart contracts in JavaScript, Golang, Node.js, or Java. The Hyperledger Fabric v1.4.6 feature private data collection provides data privacy by making sure that the data is shared only amongst the authorized peers. Also, the unified codebase feature of the IBM Blockchain platform console allows the users to run the components anywhere on the environment supported by IBM Cloud [20].

4.3 Use Case 3: Huawei Cloud

Huawei Cloud for enterprises and developers provides a blockchain-based platform known as Blockchain service (BCS). It is based on Hyerledger Fabric helping the users to quickly deploy, manage, and maintain networks on Huawei Cloud. Huawei Cloud's Blockchain Service platform is used in various industries, such as healthcare, e-government, and supply chain logistics for ensuring data security and reliability [21].

Benefits Accrued

Blockchain Service (BCS) helps the enterprises in the easy deployment of the blockchain network within a few minutes thereby reducing development and deployment costs. It provides robust security by using multi-layer encryption, management, and isolation of keys, users, and permissions. Also, it overcomes the data tampering issues with the help of certificate management and by the blockchain structure of the data [21].

4.4 Use Case 4: Oracle Blockchain

Blockcahin as a Service (BaaS) on Oracle Cloud is based on Hyperledger Fabric. It is an enterprise-grade platform consisting of many validating nodes that by executing smart contract node updates the ledger and provides the response to the queries [22]. Oracle Blockchain platform assists the businesses to provide agility in transactions and increasing trust across the whole business network. It can connect seamlessly with several Oracle solutions such as Oracle ERP Cloud and Oracle SCM Cloud.

Benefits Accrued

Oracle Blockchain platform provides a dependable and adaptable network security infrastructure to additionally control how administrators, clients, and other cloud services access the service instances and their applications [22]. It allows us to conduct private transactions by using confidentiality domains and by controlling member access privileges [23].

5. Future Applications

The cloud computing industry has encountered a critical upheaval over the past decade, and it is progressing rapidly. It is believed that the future is distributed i.e. blockchain technology will be the key to overcome the existing security challenges due to the cyber-attacks in storage, networks, and data in transmission areas.

Most of the organizations are trying to get the maximum benefits of vast data storage, computational resources, and networking services offered by cloud services providers such as Amazon AWS, IBM Cloud, Google Cloud Platform and Microsoft Azure. However, the data stored in centrally controlled facilities makes it difficult to analyse it in real-time and take appropriate actions. With the Internet of Things (IoT) advancing quickly, edge computing is gaining momentum as it creates new ways for enterprises to improve performance and maximize operational efficiency. This shows the trend of the transition of networks to decentralized cloud computing.

Blockchain-based cloud computing is progressively revealing itself as the optimal medium to accomplish the grand objectives of IoT. Additionally, Blockchain-based cloud computing means that there will be increased data security as compared to data stored at a central location. This will help in reducing the risk due to the increased number of attacks. Therefore, blockchain technology in cloud computing environments can be viewed as the next step to supplement the growth of the IoT industry.

6. Conclusion and Future Research Direction

Blockchain technology is continuously evolving and finding a lot of applications in the modern world. One such application where blockchain has been studied and applied is cybersecurity. The blockchain technology usage in cloud computing environments is the need of the hour for mitigating the cyber risk.

We can conclude from various studies that the main benefits of the shift from traditional cloud storage to blockchain-based cloud storage are increased data integrity, enhanced security, improved transparency, and data accountability.

For future researchers, it is recommended to use single blockchain technology for developing security solutions since the greater part of the current solutions uses different blockchain technologies resulting in difficulties while integration.

References

Columbus, Louis, "83% of Enterprise Workloads Will Be in the Cloud by 2020". Forbes, January 2018 [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#1f5f428c6261 [Accessed May 26, 2020]

Desjardins, Jeff, "How much data is generated each day?". World Economic Forum, April 2019 [Online]. Available: https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/ [Accessed May 27, 2020]

Howarth, Fran, "Sabotage: The Latest Threat to the Financial/Banking Industry". Security Intelligence, August 2016 [Online]. Available: https://securityintelligence.com/sabotage-the-latest-threat-to-the-financialbanking-industry/ [Accessed May 27, 2020]

Gantz, John. F., "The Salesforce Economy Forecast: 3.3 Million New Jobs and $859 Billion New Business Revenue to Be Created from 2016 to 2022". IDC Whitepaper, October, 2017 [Online] Available: https://www.salesforce.com/content/dam/web/en_us/www/documents/white-papers/idc-study-salesforce-economy.pdf [Accessed May 28, 2020]

PWC, "Cyber Risk- Enlightenment through information risk management", 2017 [Online] Available:https://www.pwc.com.au/consulting/assets/cyber-risk-paper-july2017.pdf [Accessed June 01, 2020]

Muncaster, Phil, "AWS left Reeling After Eight-Hour DDoS". Info Security Group, October 2019 [Online]. Available: https://www.infosecurity-magazine.com/news/aws-customers-hit-by-eighthour-ddos/ [Accessed June 01, 2020]

Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE International Congress on Big Data (Big Data Congress), Honolulu, HI, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85 https://doi.org/10.1109/BigDataCongress.2017.85, 2017

Abdelrahman, N., & Farah, A. Blockchain Technology : Classification , Opportunities , and Challenges. International Research Journal of Engineering and Technology (IRJET), 5(5), 3423-3426, 2018

Chen, H. S., Jarrell, J. T., Carpenter, K. A., Cohen, D. S., Huang, X., Carpenter, K. A., & David, S. Blockchain in Healthcare: A Patient-Centred Model. Biomedical Journal of Scientific & Technical Research, 20 (3), pp 15017-15022 https://doi.org/10.26717/BJSTR.2019.20.003448, 2019

Hjálmarsson, F. Þ., & Hreiðarsson, G. K. Blockchain-Based E-Voting System. IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151, 2018

DHL. Blockchain in logistics. DHL Customer Solutions & Innovation, 1–28, 2018 [Online]. Available: https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf [Accessed June 06, 2020]

Blossey, G., Eisenhardt, J., & Hahn, G. Blockchain Technology in Supply Chain Management: An Application Perspective. Proceedings of the 52nd Hawaii International Conference on System Sciences, 6, 6885–6893. https://doi.org/10.24251/hicss.2019.824, 2019

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. Blockchain Technology in Business, and Information Systems Research. Business and Information Systems Engineering, 59(6), 381–384. https://doi.org/10.1007/s12599-017-0505-1, 2017

Cloud Security Alliance, "Using Blockchain Technology to secure the Internet of Things", 2018 [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/blockchain/Using_BlockChain_Technology_to_Secure_the_Internet_of_Things.pdf [Accessed May 29,2020]

Belu, M. Application of Blockchain in International Trade: An Overview. Romanian Economic Journal, XXII (71), 2–16, 2019

Chen, W., Xu, Z., Shi, S., Zhao, Y., & Zhao, J. A survey of blockchain applications in different domains. ACM International Conference Proceeding Series, 17–21. https://doi.org/10.1145/3301403.3301407, 2018

Malviya, H. Reinventing Cloud with Blockchain. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2885274, 2016

Abinaya, G., Kothari, P., Alex Pavithran, K. P., Biswas, M., & Khan, F. Block chain based decentralized cloud storage. International Journal of Engineering and Advanced Technology, 8(4), 643–684, 2019

Alibaba Cloud, "Blockchain as a Service – Product Information", [Online]. Available: http://docs-aliyun.cn-hangzhou.oss.aliyun-inc.com/pdf/baas-product_intro-intl-en-2020-04-28.pdf?spm=a2c63.p38356.879954.4.a1ddec9dt1UVuS&file=baas-product_intro-intl-en-2020-04-28.pdf [Accessed June 11, 2020]

IBM Cloud, "About IBM Blockchain Platform for IBM Cloud", [Online] Available: https://cloud.ibm.com/docs/blockchain?topic=blockchain-ibp-console-overview [Accessed June 11, 2020]

Huawei (2019, July 30), "Blockchain Service – Service Overview", Huawei Cloud, July 2019 [Online]. Available: https://support.huaweicloud.com/intl/en-us/productdesc-bcs/bcs-productdesc.pdf [Accessed June 11, 2020]

Oracle, "Administering Oracle Blockchain Platform", Oracle Cloud, September 2019 [Online]. Available: https://docs.oracle.com/en/cloud/paas/blockchain-cloud/administer/administering-oracle-blockchain-platform.pdf [Accessed June 11, 2020]

Oracle Cloud, "Product Features", [Online]. Available: https://www.oracle.com/in/application-development/cloud-services/blockchain-platform/ [Accessed June 11,2020]