ZKG INTERNATIONAL ISSN: 2366-1313

Cloud computing and Blockchain Multi-Factor Group Authentication

[1]RAYA PAVAN KUMAR, [2]G. SRIHARI, [3]YANNAM RAVI, [4]BADRI ASHOK REDDY, [5]T. LAKSHMAN NAIDU

[1]Assistant Professor, Dept. Of AI, ABR College of Engineering and Technology, Kanigiri

[2, 3, 4, 5,] BTech Student, Dept. Of AI, ABR College of Engineering and Technology, Kanigiri

Abstract: *Technological advances have resulted in organizations digitalizing many parts of their operations. The threat landscape of cyber-attacks is rapidly changing and the potential impact of such attacks is uncertain, because there is a lack of effective metrics, tools and frameworks to understand and assess the harm organizations face from cyber-attacks. Cyber-attacks are not new to IoT, but as IoT will be deeply interwoven in our lives and societies, it is becoming necessary to step up and take cyber defence seriously. Hence, there is a real need to secure IoT, which has consequently resulted in a need to comprehensively understand the threats and attacks on IoT infrastructure. The main objective of the paper is to analyse the effect of the cyber-attacks in the traditional cyber framework and study the block chain crypto-currency architecture to assess the shortcomings and safety performance. This paper briefly examines some characteristics of integration between blockchain and cloud computing. Contributions of this paper contain (i) a representation of two integrated retail cloud computing and blockchain circumstances; and (ii) some research possibilities on the use of both environments.*

Keywords: *Cloud computing, Blockchain, Internet of Things, Cyber-attacks, integrated environment*.

I. INTRODUCTION

The recent rapid development of the Internet of Things (IoT) [1] and its ability to offer different types of services have made it the fastest growing technology, with huge impact on social life and business environments. IoT has gradually permeated all aspects of modern human life, such as education, healthcare, and business, involving the storage of sensitive information about individuals and companies, financial data transactions, product development and marketing. The vast diffusion of connected devices in the IoT has created enormous demand for robust security in response to the growing

demand of millions or perhaps billions of connected devices and services worldwide [2]. The number of threats is rising daily, and attacks have been on the increase in both number and complexity. Not only is the number of potential attackersalong with the size of networks growing, but the tools available to potentialattackers are also becoming more sophisticated, efficient and effective [3]. Therefore, for IoT to achieve fullest potential, it needs protection against threats and vulnerabilities. Security has been defined as a process to protect an object against physical damage, unauthorized access, theft, or loss, by maintaining high confidentiality and integrity of information about the object and making information about that object available whenever needed.

Nowadays cryptocurrency has become a buzzword in both industry and academia. As one of the most successful cryptocurrencies, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016. With a specially designed data storage structure, transactions in Bitcoin network could happen without any third party and the core technology to build Bitcoin is blockchain, which was first proposed in 2008 and implemented in 2009. Blockchain could be regarded as a public ledger and all committed transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency.

Blockchain can be used in various financial services such as digital assets, remittance and online payment. Additionally, it can also be applied into other fields including smart contracts, public services, Internet of Things (IoT).

As for smart contracts, the contract could be executed by miners automatically once the contract has been deployed on the blockchain. Although the blockchain technology has great potential for the construction of the future Internet systems, it is facing a number of technical challenges. Firstly, scalability is a huge concern. Bitcoin block size is limited to 1 MB now while a block is mined about every ten minutes. Subsequently, the Bitcoin network is restricted to a rate of 7 transactions per second, which is incapable of dealing with high frequency trading.

ISSN: 2366-1313

However, larger blocks mean larger storage space and slower propagation in the network. This will lead to centralization gradually as less users would like to maintain such a large blockchain. Therefore, the trade-off between block size and security has been a tough challenge. Secondly, it has been proved that miners could achieve larger revenue than their fair share through selfish mining strategy. Miners hide their mined blocks for more revenue in the future. In that way, branches could take place frequently, which hinders blockchain development. Hence some solutions need to be put forward to fix this problem.

BLOCKCHAIN ARCHITECTURE

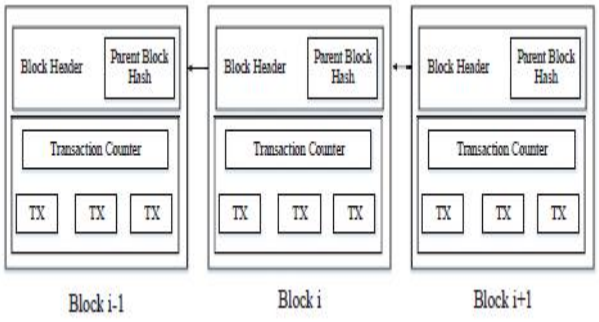

Fig.1 An example of blockchain which consists of a continuous sequence of blocks.

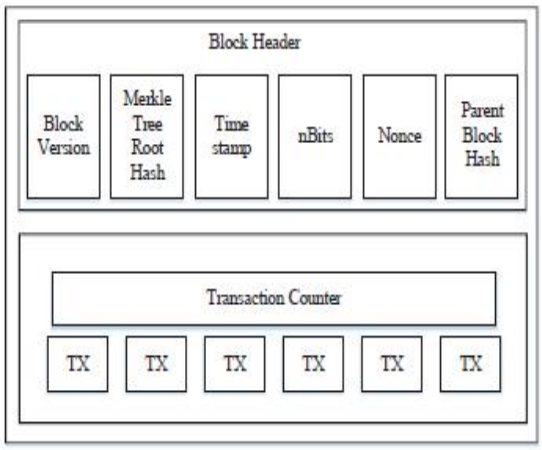

Fig.2 Block structure

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. Figure 1 illustrates an example of a blockchain. With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks (children of the block's ancestors) hashes would also be stored in ethereum blockchain. The first block of a blockchainis called genesis block which has no parent block. We then explain the internals of blockchain in details.

II. LITERATURE SURVEY

Cloud storage is a kind of internet technology for sharing resources with IT-related capabilities, which is important to either enterprises or individual users. Traditional cloud storage security strategies mainly focus on information encryption, access control and etc. Recently, the Software Defined Storage

(SDS) integrates a number of distributed cloud storage services to deal with problem that separate clouds cannot meet the demands of users.

Nguyen et al. [2020] Blockchain technology was taking the world by storm. Blockchain has emerged as a disruptive technology for the next generation of numerous industrial applications. In this paper, a novel paradigm of blockchain and Cloud of Things integration, called BCoT, has been widely regarded as a promising enabler for various application scenarios. This article presented a state-of-the-art review on the BCoT integration to provide general readers with an overview of the BCoT in various aspects, including background knowledge, motivation, and integrated architecture. They also provided an in-depth survey of BCoT applications in different use-case domains such as smart healthcare, smart city, smart transportation and smart industry.

WissamZaki et al. [2020] Cloud computing was a very useful technology in our daily life, this computing uses the Internet to provide applications and also to transfer and maintain data, it was imperative to provide an environment that protects applications and data within this cloud, networks have to be protocols that used strong algorithms to protect them. This paper discussed some of them and compared them with others, data security and encryption was considered one of the most important discoveries, despite its development in the old days completely separatelythat reality showed a close connection between them.

Mohamed MounirMoussa et al.[2020] analysed the implementation and organizational approaches related to Dew Computing, where the processing was brought even closer to the user compared to other IoT computing paradigms. This paper aimed to present a threat analysis of the IoT and to use a deep learning approach to counter cyber anomalies, then validate it by analyzing its metrics. They evaluated the case of transferring data between the cloud and the enduser dew devices integrated into the connected vehicle. They used a modified version of the Stacked Autoencoder that improved the accuracy of detecting the defined attacks, using the loss over the training data as a threshold.

Aditi Patel et al. [2020] were suggestedan emerging technology that delivers computing services such as online business applications and data storage over the Internet. And Implemented cloud enables a distributed working environment where that reduced expenditure of the

organization, provided data, information security and so on. As many organizations were adopting cloud computing, attackers exploit the cloud to obtain unauthorized control on the valuable data stored in it. Evolution of traditional computing to cloud has led to many security challenges for both customers and service providers. Different types of services were provided by trusted cloud providers over the Internet by using many technologies, which ariseddifferent security threats.

Tonglai Liu et al. [2019]suggesteda double-chain scheme to improve the security of the blockchain network. The problem of storage unbalance was formalized. A heuristic algorithm named FMA was proposed, followed by a customized genetic algorithm (GA), together with a tabu search algorithm (TSA), to deal with non-local data storage. Numerical results show that the proposed FMA can obtain the same storage fitness compared with GA and TSA for the small number of nodes. GA was able to outperform the other two algorithms in terms of storage fitness, and the qualities of FMA and GA bind the solution quality of TSA.

Paula Fraga-Lamas et al. [2019]Industry 4.0 was a concept devised to improve the way modern factories operate by using some of the latest technologies. One such technology was blockchain, adding trust, security, and decentralization to different industrial fields. This article was focused on analyzing the benefits and challenges of using blockchain and smart contracts to develop Industry 4.0 applications. In addition, this paper presented a thorough review of the most relevant blockchain-based applications for Industry 4.0 technologies. Thus, it aims to provide a detailed guide for the future Industry 4.0 developers that allows for determining how the blockchain can enhance the next generation of cyber-secure industrial applications.

Xuelian Liu et al. [2019] proposed a mechanism based on a combinatorial double auction to offload the mining process of miners to the edge servers. The mechanism was formulated as a resource allocation problem. The corresponding allocation algorithms and payment schemes were proposed to allocate resources and calculate trade prices, respectively. Also, this paper proved that the proposed mechanism was efficient in terms of computation. It satisfies three properties of the economic auction: budget balance, individual rationality, and truthfulness.

Chengpeng Xia et al. [2018] provided incentive to encourage edge servers to serve mobile users for the mobile blockchain application. They formulated the problem as a resource allocation problem, then they proposed a three-stage auction to implement resource allocation specially designed for mobile blockchain, and introduced the group-buying mechanism to motivate mobile users. Also proved that their auction scheme was truthful, individual rationality, and computational efficiency. They were compared proposed scheme with TACD and HAF mechanisms, and simulation results showed that the social welfare achieved by their scheme was higher than that of TACD and HAF mechanisms.

III. BLOCKCHAIN TECHNOLOGY

A blockchain can be called a dispensed ledger, where a third party does not control data and transactions [2]. Any transaction on the blockchain is recorded on a completely public ledger permanently and verifiable. Examples of blockchain solutions are Ethereum and Hyperledger. All of them have some common elements, such as the following: (i) Replicated Ledger – All nodes of the blockchain network store transactions securely logged. Everyday transactions are packed into a block, which is then added immutably. All transactions within blocks are assigned and replicated between all nodes, being part of the community. (ii) Peer-to-peer community: All nodes share a public ledger without a central controlling actor. All nodes are connected through a peer-to-peer community, and transactions and blocks are synchronized. (iii) Consensus: Before inserting blocks into the chain, all nodes in the network want to reach a consensus on the correctness and order of the transactions in the blocks. The most representative consensus algorithm in the public chain is proof of work, which is used in Bitcoin. and (iv) Cryptography: Security in the blockchain is entirely based on knowledge of cryptography. In a blockchain community, transaction integrity supports digital signatures and proprietary fact structures (e.g., Merkel Tree in Bitcoin, Merkel Patricia Tree in Ethereum). Additionally, digital signatures support transaction authenticity, and an asymmetric cryptographic system supports transaction confidentiality.

IV. EXAMPLES OF INTEGRATED CLOUD COMPUTING AND BLOCKCHAIN ENVIRONMENTS

Amazon has a blockchain service called AWS Blockchain. AWS Blockchain is

ISSN: 2366-1313

templated at its core, providing a realistic way to easily build and deploy blockchain networks using an open-source framework. These templates allow the person to learn how to build blockchain applications. AWS Blockchain Models configures your chosen blockchain format into boxes, such as an Amazon Elastic Container Service cluster or a live EC2 instance running Docker. The blockchain network is built on your private network, which allows you to use your subnet and access it to manipulate lists.

Additionally, the user can assign permissions to limit what sources can be accessed. The templates can also be applied to blockchain-only infrastructure, with models available: AWS Blockchain for Ethereum and AWS Blockchain for Hyperledger Fabric. The AWS Blockchain for Ethereum template uses Ethereum, an open-source blockchain framework from the Ethereum Foundation that allows you to interpret blockchain applications that run on an exact schedule without timing, censorship, fraud, or interference. Goes on. of 1/3 parts. It is used when a user needs to perform peer-to-peer transactions in the Ethereum public community, create a new public community, or use Ethereum's Solidity smart contract language.

On the other hand, the AWS blockchain version for Hyperledger Fabric uses Hyperledger Fabric, an open-source blockchain framework from the Linux Foundation that allows you to write blockchain programs and manipulate data from the blockchain. Provides access to permissions. It is used when users want to create a private blockchain network or limit transactions that character parties can view.

V. DISCUSSION AND RESEARCH OPPORTUNITIES

1) Integration Aspects

Cloud computing environments certainly have various tools and offerings, whether optimizing software or infrastructure. And there is also a combination of these sacrifices. With blockchain underpinning, the ability to mix environments and applications becomes more common once the blessings of the age are considered. However, because the amount of technology is so large, there is a risk of integration problems. An example is a PaaS service that offers some programming language for rapidly developing a utility that uses blockchain functions.

ISSN: 2366-1313

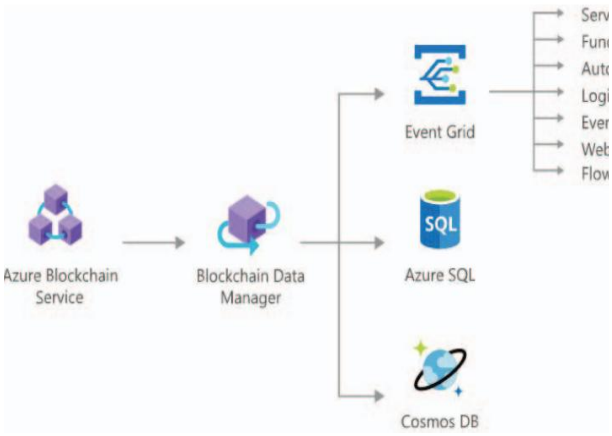

Fig.1 Flow for publishing data in Azure Blockchain

2) Modeling

Just as the number of services is vast in cloud computing environments, and blockchain applicability in many areas also grows, the way in which applications are modeled must be handled with care. Business services often have tools for modelling and deploying services, from infrastructure to end application. This may contribute to the speed of development, but it is still necessary to mature in these tools to make it easier for the user to create their own applications. The use of blockchain design patterns can help in modelling systems. The notation to be used should also provide mechanisms for modelling static and dynamic aspects of the proposed applications.

3) Smart Contracts and Cloud Computing

Smart contracts and blockchain are revolutionizing business by removing intermediaries. Farther, they have the potential to change the current cloud/fog markets, by enabling the creation of a blockchain-based decentralized cloud solutions to face these problems. The development of blockchain-based solutions for cloud computing has only recently started and focuses on commercial targets. In this context, several challenges arise, such as: performance analysis of environments, security of access, data management, and cost effectiveness of applications running inside the blockchain and outside the blockchain.

VI. CONCLUSION

Cloud computing and blockchain packages are starting to be used together. Each appears beneficial for many sectors, including healthcare, training and logistics. Both have several technologies for full use, and include prerequisites, mainly architectures that consider both environments and register exchanges between them. Observing the better of the two environments working together is an interesting situation to research. Functional and non-functional requirements must be correct to benefit from both technologies. This promotes further testing to varying degrees. As target paintings, we intend

model prototypes to explore Amazon and Azure blockchain environments, understand their structure and components, and analyze the applications' performance in such environments.

REFERENCES

1. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
2. J. S. Kumar and D. R. Patel, "Asurvey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, pp. 20–26, March 2014, published by Foundation of Computer Science, New York, USA.
3. B. Schneier, Secrets and lies: digital security in a networked world. John Wiley & Sons, 2011.
4. "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/ state-of-blockchain-q1-2016/
5. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
6. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.
7. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: https://ssrn.com/abstract=2394738
8. Nguyen, Pubudu N. Pathirana, Ming Ding, ArunaSeneviratne, "Integration of Blockchain and Cloud of Things: Architecture Applications and Challenges", Communications Surveys & Tutorials IEEE, vol. 22, no. 4, pp. 2521-2549, 2020.
9. Tonglai Liu, Jigang Wu, Jiaxing Li, Jingyi Li, "Secure and Balanced Scheme for Non-Local Data Storage in Blockchain Network",2019 IEEE 21st International Conference on, pp. 2424-2427.
10. Paula Fraga-Lamas and Fernández-Caramés, "A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories", Access IEEE, vol. 7, pp. 45201-45218, 2019
11. Prasadu Peddi (2015) "A machine learning method intended to predict a student's academic achievement", ISSN: 2366-1313, Vol 1, issue 2, pp:23-37.