CET351 Research Paper

Assignment Cover sheet

(this page will be deleted before the paper is published)

Student name: Begang Godwin Nthubu

Student Registration Number: Bh77oe (Fcse17-012)

Students Degree: Computer Systems Engineering

Off Campus Centre or College:

**Research Paper title:** A Critical Analysis of Block Chain Technology Systems to Improve Cloud Computing Storage Data Loss and Security

Word count: 2538

Relevance of this research topic: block chain technology is a new concept in the world of information systems and internet of things, it was first implemented in cryptocurrency bitcoin to enhance security and it proved worthy to be adapted as a security feature. This research is very relevant to the course studied because it addresses the programming aspect learnt throughout the course, it also highlights and enhances research skills and writing skills which can be applied to other modules.

A Critical Analysis of Block Chain Technology Systems to Improve Cloud Computing Storage Data Loss and Security

Begang Godwin Nthubu

Abstract

Cloud computing is regarded as one of the most growing technology in the market of information technology and internet of things. However, the biggest problem is data loss and security problems caused by its structure of having a centralized administration. The purpose of this survey paper is to critically analyse how block chain technology decentralized or distributed system can be used to improve cloud computing, and to evaluate other systems proposed by different authors.

In this survey paper current knowledge aimed at improving cloud computing data loss and security will be discussed and analysed. It focuses on three different methods which use blockchain as a foundation to create a decentralized or distributed cloud computing system. The results and experiments conducted are assessed to determine the best solution for creating a decentralized cloud computing storage using block chain. In conclusion the author suggests ways of improving the experiments and results.

1 Introduction

According to Horsman (2020), Cloud computing is a well-adapted technology used by different people and organizations. This technology is used to send, store, and manage data online without having any infrastructure, hardware or local server put in place. Karumanchi et al (2019) explains that cloud computing provides three main services, software as a service (SaaS), this service is delivered over the internet and developed for the end users. Platform as a service (Paas) is a set of services and tools design to simplify coding and deployment of applications efficiently. Infrastructure as a service (Iaas), is the main infrastructure that powers the cloud, it contains hardware servers, software, storage and different networking operating systems. Sanghi et al(2018) continues to explain that the problem with the current system is that it is expensive and centralized making it vulnerable to security threats such as Denial of services(DDOS), data loss, data leakages and system crashes.

Hulwan and Chavan (2018) discussed that cloud computing has changed how different organizations do their business and their work in the market. The main problem is that data is being outsourced and centralized in the cloud. Cloud computing has brought a new challenge or threats towards centralized and outsourced data. Cearnău (2019) believes that the removal of central administration authority from the database is very important and it is the most powerful aspect that can be implemented in the cloud. With a decentralized cloud computing solution hardware cost can become cheaper. The risk of attacks or third parties interfering, or eavesdropping can be lowered or even eliminated. (Angséus et al. 2015.

Park and park (2017) propose that block chain can be applied to different concepts beyond the internet of things. it provides security through the use of peer to peer, encryption and generation of hash algorithms. If this technology is combined with cloud computing, “block chain can be upgraded to a convenient service that provides stronger security”.

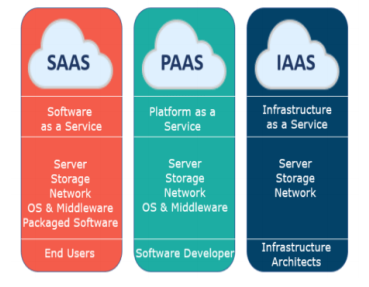


Fig. 1 Cloud computing services. (Karumanchi et. al. 2019)

****2 Previous works****

This section will introduce, discuss and analyse research papers aimed at improving cloud computing data loss and security

The method proposed by Angelus et.al., (2015) proved to be a better method to create a distributed cloud computing system because of its reliable network. Even though Angeus et al, 2015 discussed that the methods not yet ready to be used in a productive environment. They state that the method has security limitations that affect the production of business. Its main advantage is that the method is able to create a decentralized cloud computing environment through the use of proof of work.

The research conducted by Hulwan and Chavan (2018), uses a critical algorithm that uses three major keys. These keys allow for a distributed cloud computing system that function to improve security. The advantage of this system is that it works better at sharing data, it can be used as a secure data sharing protocol.

Gaetani et.al., (2020), proposed a new method which uses Federation-as-a-Service (FaaS). This method is a new and innovative service that allows users to create a secure and managed cloud computing system. This method uses advanced data security services and design principles that allows the system to be a distributed or decentralized. FaaS provides users with an assurance that their data will be kept private and that their integrity of contacts will not be tampered with.

Gaetani et.al., (2020), continues to explain that this method was made possible through the use

of block chain technology which uses per to peer instead of having a centralized authority. This method addresses security threats to data loss and integrity. This method uses a two-layer block chain system. The first layer provides users with adequate and better performance while the second layer provides a strong integrity of data.

In conclusion, Gaetani et.al.,(2020), explains that their proposed method uses two layer blockchain system in which the first layer has a very weak point when it comes to data integrity thus needing the second layer to improve its weaknesses. All in all, the system proves to be a good method to address data loss and security issues found on the cloud computing services.

Critical analysis shows that all the three methods are highly effective in developing a distributed cloud computing storage system and improve data loss and security. Even though further research is required to fully develop and solve all the drawbacks that the methods have.

****3**** A Critical Analysis of Block Chain Technology Systems

This section of this survey paper is to critically analyse how block chain technology decentralized or distributed system can be used to improve cloud computing data loss and security.

The research analysed throughout this paper focused at improving data loss and security in the cloud computing environment through the use of block chain technology. All the methods proposed have their advantages and disadvantages. The methods discussed all aimed at producing a reliable and accurate system that will work in the cloud and also work in different technology sectors.

3.1 Ethereum general-purpose blockchain

Angséus et.al., (2015) conducted research and a test experiment was selected and set up to test the implementation of a decentralized cloud computing platform with multiple actors. A few tools where selected to provide a more efficient development process and planning strategy. Pivotal tracker tool was used to add story boards to a virtual planning board which follows the agile development methodology. A second tool was used called eleuthero which is a graphical client used for Ethereum. It is used to develop Ethereum based decentralized applications with access to block chain and the devp2p network. It also allows one to debug and make transactions. Angséus et.al., (2015) explains that to fully test the project computers with a lot of processing power where required for hosting. a simple and a small block chain as well as a web server was required. The author chose the raspberry pi 2 model b computer because it is cheap and viable.

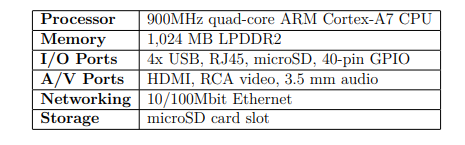


Fig. 1 Raspberry pi 2 model b specifications. (Angséus et. al. 2015)

Angséus et.al., (2015) states that during the development stage, a local network was made for testing and research purpose. which consisted of three raspberry pi 2 computers. This network was the backbone for the distributed development of the private block chain, local Ethereum and the test network nodes. This network allows anyone with a computer to register and become a worker. It connects clients with workers which will be paid to perform work.

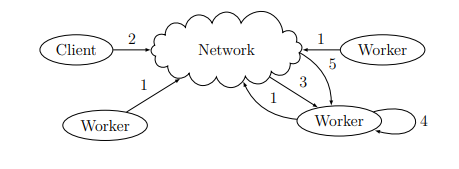


Fig. 2 proposed network state diagram. (Angséus et. al. 2015)

In conclusion, Angséus et.al., (2015) created a robust and reliable network for a decentralized cloud computing. The network only handles the problem of distributing work in the network, the proposed protocol should be seen as a generalized attempt at solving all three problems (centralization, data loss and security).

Angséus et.al., (2015) claims that the current proposed network is unstable for use in a production environment due to security concerns. This network is still capable of proof of work which is running in a decentralized block chain. In the future a reference implementation could be refined and extended to create a fully working networking using an advancement of the Ethereum decentralized application.

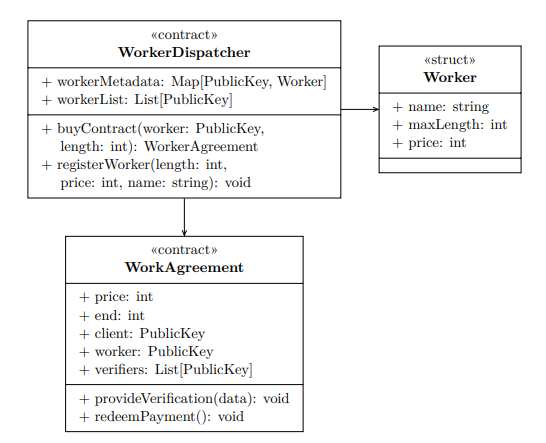


Fig. 3 Uml diagram showing the proposed smart contracts. (Angséus et. al. 2015)

3.2 Advance Encryption Standard Algorithm (Aes)

Shah et.al., (2020) proposed and developed a new system for creating a decentralized cloud computing storage, this system works in four modules. The first module allows users to register and create accounts on the system. Then a JavaScript framework called web3.js will fetch the users account address and wallet balance.

Shah et.al,.(2020) continues to explain that after the user has received their address and balance there will then select the file through a file picker, then the system will check the number of peers available. The system will then use the wallet balance and address as a key to encrypt and secure the file. The user will be required to pay for the service, after payment the users file will be stored across different available peers using a protocol called ifps (interplanetary file system) protocol. Shah, et al.,(2020) states that this protocol will return a hash value consisting of the file path, this path will then be mapped with the users account address using a smart contract and it will be stored securely in a block chain.

Shah et.al., (2020) claims that to fully achieve high availability of the data, the data uploaded to the system will then be replicated or created across three more peers. The transactions or files stored in this peer to peer network or infrastructure are tamperproof, there cannot be modified by any attacker or third party and that the identity of all the parties involved in the process is secured. Proof of work also makes it difficult for an attacker to gain access since it records all the history of all transactions and the attacker must gain a majority of the CPU(central processing unit) power to fully control the system.

In conclusion, shah et.al., (2015) enunciates that their proposed system improves security of data by providing a decentralized system which also allows data to be encrypted and distributed across different peers in the system.

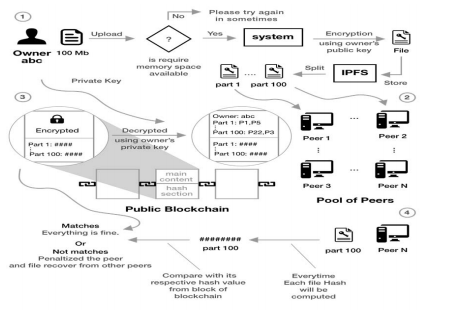


Fig. 1.Aes system design and flow for a distributed cloud computing. (Shah et. al. 2020)

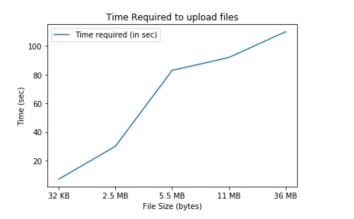


Fig. 2 total amount of time required to upload files. (Shah et. al. 2020)

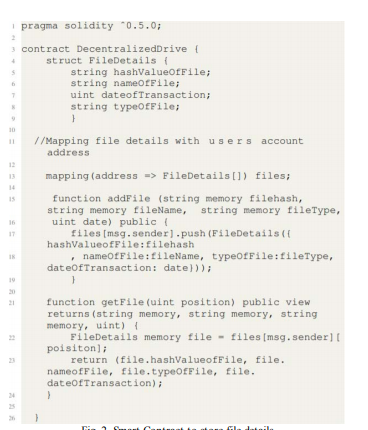


Fig. 3 a smart contact used to store user details.

3.3 Meta-Key Mechanism

Hulwan and Chavan (2018) proposed a system that allows for a distributed cloud computing infrastructure. This system is used to protect user data from third parties and cloud providers. It also secures transactions made between different servers to protect against untrusted parties.

Hulwan and Chavan (2018) explains that the system uses a critical algorithm to generate three major keys. public key (pk) which is made visible to users, this key can be used to encrypt the data and decrypted using a private key. A master key (me) is used by the owner of the data, this key can be used to modify and share data in the cloud. And a secret key (sk) is generated for data modification.

Hulwan and Chavan (2018) states that this system uses four methods to develop a distributed cloud computation, the first method is known as key generation. This method allows a user to generate a key using a random input, which produces two keys being the private key and public key. Hulwan and Chavan (2018) explains that after both keys have been generated a resigning key is generated only for users that are in the same group of the cloud. Then proof of verification by the administrator is checked by the verifier, the last method is known as regeneration of sign, it allows users to use the original data to compute a block for each signature.

In conclusion, Hulwan and Chavan (2018) explains that their proposed system introduces a secure data-sharing protocol that will be implemented using block chain-based cloud storage through the use of encryption keys. This system will be highly efficient in enhancing security.

Conclusion

This paper has critically analysed and evaluated three research papers aimed at improving cloud computing data loss and security through block chain technology systems. All research papers show that block chain is the answer to all the security threats and limitation of cloud computing. The methods where tested against speed to encrypt data, accuracy of encryption and the success rate against hackers and third parties. The method proposed by Hulwan and Chavan proved to be more accurate and more efficient to be used to improve cloud computing data loss and security.

Angséus et.al., (2015) need to do more research and experiments to fully improve their network which could be the next big thing in the development of distributed systems using blockchain technology

Prior to all the methods discussed a lot of work needs to be done to improve the accuracy, speed and performance of all the methods to fully improve data and security in the cloud.

References

*Horsman, G. (2020). What's In The Cloud? - An Examination Of The Impact Of Cloud Computing Usage On The Browser Cache. The Journal Of Digital Forensics, Security And Law: Jdfsl, 15(1), 1-16.*

*N. Sanghi, R. Bhatnagar, G. Kaur And V. Jain, "Blockcloud: Blockchain With Cloud Computing,” India, 2018, Pp. 430-434*

*M. Shah, M. Shaikh, V. Mishra And G. Tuscano, "Decentralized Cloud Storage Using Blockchain," Tirunelveli, India, 2020, Pp. 384-389.*

*I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev And L. Yalansky, "Ensuring Data Integrity Using Blockchain Technology,"2017, Pp. 534-539*

*CEARNĂU, D.-C., 2019. Block-Cloud: The New Paradigm Of Cloud Computing. Economy Informatics, 19(1/2019).*

*Nishant.G.Hulwan & Chavan, P. S., 2018. BLOCKCHAIN-BASED SECURITY ARCHITECTURE FOR DISTRIBUTED CLOUD STORAGE. International Journal Of Advanced Research In Computer Science, 9(6).*

*Ravishankar, D., Kulkarni, P. & V. M. V., 2020. Blockchain-Based Database To Ensure Data Integrity.*

*Sari, A., 2018. Use Of Blockchain In Strengthening Cybersecurity And Protecting Privacy. International Journal Of Engineering And Information Systems (IJEAIS), 2(12), Pp. 59-66.*

*Sarmah, S. S., 2019. Application Of Blockchain In Cloud Computing. 8(12).*

*ANGSÉUS, J. Et Al., 2015. Decentralized Cloud Computing Platforms. Building A Global Marketplace For Computing Power.*

*Gaetani, E. Et Al., 2020. Blockchain-Based Database To Ensure Data Integrity In Cloud Computing Environments.*

*Park, J. H. & Park, J. H., 2017. Blockchain Security In Cloud Computing: Use Cases, Challenges, And Solutions. 9(164).*