International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Blockchain-Based Database to Ensure Data Integrity in Cloud Forensics

Chintha MadhumohanReddy[1], G Raghavendra[2]

[1]Department of MCA Sree Vidyanikethan Institute of Management, Sri Venkateswara University, Tirupati, Andhra Pradesh, India

[2]Assistant Professor, Department of MCA, Sree Vidyanikethan Institute of Management, A.Rangampeta, Tirupati, Andhra Pradesh, India

ABSTRACT

Alongside the expanding utilization of cloud services, security dangers are additionally expanding and assault techniques are winding up more differing. Be that as it may, there are as yet few measures and arrangements to manage security episodes in the cloud condition. Albeit numerous arrangements have been proposed through research on computerized criminology for reacting to security episodes, however it is as yet hard to demonstrate the uprightness of proof accumulation and capacity in the cloud condition. To take care of these issues, in this paper, we propose a blockchain based information logging and respectability service framework for cloud crime scene investigation. What's more, think about the performance of the proposed framework with the other blockchain based cryptographic money.

Keywords: Cloud Computing, Block chain, Cloud Forensics, Data Integrity

I. INTRODUCTION

Cloud computing is a technology that gives physical resources to clients through virtualization technology. Benefit of empowering system access to an adaptable and versatile pool of shareable physical or virtual resources with self-benefit provisioning and organization on-request benefit, cloud computing market is getting greater. Due to these attributes, the quantity of clients utilizing cloud computing is additionally expanded. Be that as it may, with the developing cloud computing market, security dangers started to develop. Numerous security answers for the cloud condition are being looked into; it is hard to apply the current advanced scientific techniques in view of virtualization technology. At the point when the cloud condition is characterized by the service show, access to some framework layers is constrained in Software-as-a-Service(SaaS) and Platform-as-a-Service(PaaS) situations, access to that layer is controlled by Cloud Service Provider(CSP). So the log information produced in the difficult to reach layer should be given to the CSP through agreements. In customary computerized crime scene investigation, agents have full control over the confirmation. Notwithstanding, in a cloud domain, the server farms are conveyed comprehensively, Cloud Service Customers(CSC) share physical resources, unstable information that vanishes when CSC close down the occasion, virtual system, stack adjusting and auto scaling for giving consistent service condition. In this manner, it is fundamental not exclusively to record information for cloud legal sciences previously a security episode for examination yet in addition to guarantee the uprightness of the log information since it is troublesome for the specialist to gather the information straightforwardly and gather the information from the remote site. There are a few techniques for guaranteeing the respectability of

information, one of which is a blockchain. A system called blockchain or appropriated record is being examined as a strategy for guaranteeing honesty since the past block influences the estimation of the following part. Since all parts are associated like chain, it is conceivable to check the uprightness of every past block just by confirming the hash estimation of the instantly going before part. In this paper, we depict the requirement for information logging framework for cloud legal sciences and propose a blockchain based information logging and service framework for cloud crime scene investigation.

II. RELATED WORK

2.1. Cloud Forensics

Cloud forensic is a branch of measurable science including the recuperation and examination of material found in cloud condition, frequently in connection to computer crime. As indicated by NIST, computer criminology comprises of four stages: Collection includes the procedure of physical securing of information. Examination is the way toward searching through the information for things of intrigue. Examination is the use of the fascinating things to the investigative inquiry. Detailing depicts the yield of examination. The contrast between cloud crime scene investigation and customary computerized legal sciences is the accumulation and ID steps. Since outsourcing resource is one of attributes in the cloud computing. For the more enhance legal examination strategy, for example, the capacity and transportation of information put away in the cloud server is included. Since this is have to ensure the unwavering quality of such information secrecy and respectability of information legal examination. The issue of applying the gathering and recognizable proof technique for advanced criminology to the cloud condition is that the cloud condition is an outsourcing resource to utilize the coveted service or resource from the CSP and it is hard to know the genuine area of the information in light of the virtualization technology connected. In this manner, there is a requirement for a solid recognizable proof and gathering strategy for information that considers the qualities of the earth.

2.2 Cloud Forensic Challenges Unlike heritage frameworks that claim the greater part of the computing resources, in the cloud computing condition, the CSP gives foundation, stage, and application. The CSC uses the services gave. This basic distinction causes numerous issues in cloud measurable, for example, the capacity of information and capacity areas, and access the information. The principal motivation behind why hard to apply criminological technology in cloud computing is that information handling is scattered in huge size of computing resources. Second, in customary PC legal sciences, examiners have full control over the proof. Be that as it may, it is hard in cloud condition. Third, there is an absence of dependable proof as it is hard to gather prove due to the multi-inhabitant highlights. Fourth, when VM close down, it is hard to protect unstable information. Fifth, chains of care may plainly delineate how the proof was gathered, examined, and saved. 6th, agents are totally reliant on CSPs for getting evidence. Keeping in mind the end goal to tackle the issue, it may be put something aside for avert loss of unstable information (e.g. preview). In addition, gathered proof may be guaranteed that the honesty has not been controlled amid the procedure.

2.3 Previous Research on Data Management Methods in a Cloud Computing Environment In the cloud condition, server farms are scattered around every nation, so there is a probability that clients feel that one information however it is dispersed among a few physical machines really. Chun, Byung-Gon et al, propose a technique to oversee information through a copy set that imitates all information keeping in mind the end goal to avoid information misfortune in a disseminated hub condition and to limit harm. Despite the fact that this strategy has the benefit of taking care of the information misfortune issue, there

is an impediment that the information is overseen through the reproduction, which causes an extensive upkeep cost. Additionally, since the cloud condition has a service show that compensation as-you-go, it is hard to apply the strategy as it may be. Nepal, Surya et al. propose a service that ensures the uprightness of information in cloud storage service. The framework gives an approach to avert information altering in a cloud domain by including a respectability specialist organization in a situation where a cloud benefit client utilizes a capacity service to transfer/download information to/from the cloud, called Data uprightness as a Service (DIaaS). This service comprises of a Key Management Service (KMS) that oversees key esteems, a Trust Management Service (TMS) that guarantees trust, and an Integrity Management Service (IMS) that oversees respectability of information. What's more, they propose a model that can ensure the respectability of information by arranging the CSP and IMS into four cases, which are trust and untrust individually. Edorado Gaetani et al. propose a part chain based information service strategy for cloud organization condition in view of the European SUNFISH venture, to tackle security issues, for example, information service technique and information respectability in the cloud league condition. Characteristic objective of cloud organization is sharing services among individuals by making managed, secured between cloud collaborations. With a specific end goal to characterize conceivable dangers in the cloud organization condition and take care of the issue of performance debasement because of the utilization of part chain technology, they concocted a two-layer blockchain based database structure. To begin with layer guarantees satisfactory performance by lightweight dispersed accord convention, second layer guarantees solid honesty ensures by PoW based blockchain strategies.

2.4. Block Chains A part chain is a disseminated record procedure in which a majority of companions oversee and store information by commonly concurred rules. The hubs (peers) that need to deal with the information take an interest in the P2P arrange and every hub can check the trustworthiness of the part. Each companion can make a block, where the part of the primary effective associate engenders to all companions, and if every one of the companions concur that the block is supported, the part is added to all companions. On the off chance that the new block is appropriately made, it implies that the check of the past part is additionally finished. In this manner, the more extended the block length, the higher the dependability of the whole part. Confirmation of the trustworthiness of a block can likewise check that every single past part are right by looking at the hash esteem. Notwithstanding, this does not ensure that the block is totally reliable, and that it has been recognized that it has completed a considerable measure of work sealing. In this way, the more companions taking part, the more secure it is. New blocks are made utilizing the Proof of Work (PoW) or Proof of Stake (PoS) strategy. The PoW technique is an errand to discover a hash esteem that fulfills a specific condition, and it is worked by altering the level of trouble for a normal of 10 minutes if there should be an occurrence of Bitcoin. The PoS strategy is a technique for sparing the cost and support cost of equipment gear and is an idea to take care of the issue of PoW strategy in the field of crypto currency. As of late, digital currency has been created that consolidates the two strategies appropriately because of framework support cost and security issues. Likewise, explore is in progress to apply digital currency as well as the fields that need to ensure the uprightness of information. For instance, the blockchain based advanced substance appropriation system, utilizing blockchain for restorative information get to management, a structure for averting twofold financing, blockchains and savvy contracts for the Internet of Things are looked into.

III. LOGGING SYSTEM FOR CLOUD FORENSICS BASED ON BLOCK CHAIN

In cloud computing condition, CSP need to gather and store their own information, in which case there is a plausibility of information control and misfortune, with the goal that the trustworthiness of the information needs to be ensured. Along these lines, in this segment, we propose a framework structure that can ensure the trustworthiness by blockchain technology while CSP gather information itself.

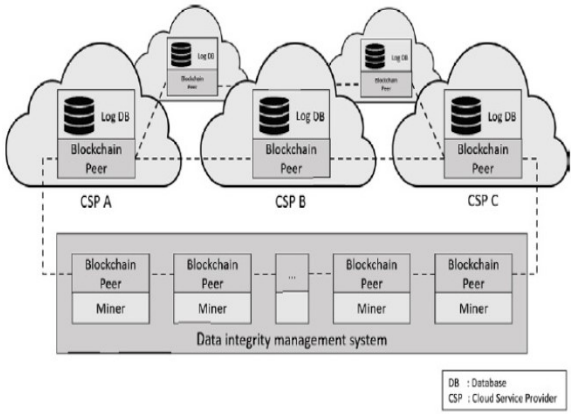

Figure 1. Blockchain based data integrity management system

Figure 1 demonstrates the structure of the blockchain based information trustworthiness service framework. In this paper, the information of CSP is put away without anyone else's input, yet the methodology for checking the honesty of the information is performed through blockchain. Information that requires stockpiling for cloud crime scene investigation is resolved through understanding amongst CSP and CSC. Right now, the CSC ought to consider the extra cost acquired to store the information in the cloud condition. The gathered log information is changed over into a hash an incentive through a hash work. This information is utilized to make a hash tree and build a block. On account of consent less blockchain, for example, Bitcoin, all associates partaking in the system can perform mining to make new blocks. Be that as it may, this isn't appropriate for proposed system because not all CSP associates can be trusted. Additionally, if all CSPs take part in mining by PoW technique, the proposed framework is exceptionally wasteful on the grounds that it needs to expend all the more computing control than mining energy of CSPs. Hence, just the information respectability service framework performs making block and the each part comprises of the hash estimation of the CSP information. One part can contain information of one CSP and the information of CSP taking part in the framework is put away all together. The age time of the block is dictated by the assention of the CSPs taking an interest in the framework, and it is resolved with regards to the handling performance.

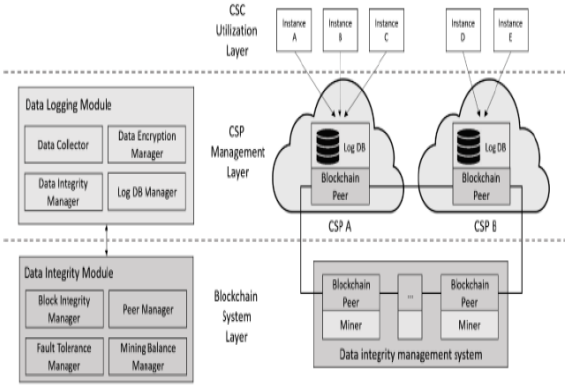

Figure 2. Overview and detailed functions of the proposed system

Figure 2 demonstrates the general stream and point by point elements of the proposed framework. In CSC Utilization Layer, the information of case utilized by CSC is put away in the CSP Management Layer and the Blockchain System Layer deals with the uprightness of put away information. The Data Integrity Module comprise of four capacities: Block Integrity Manager, Peer Manager, Fault Tolerance Manager, and Mining Balance Manager. Subtle elements of each capacity are as per the following.

3.1 Block Integrity Manger The Block Integrity Manger performs uprightness beware of information got from CSP when new block is made. Honesty confirmation is the way toward checking the hash an incentive to check whether the scrambled information has not changed and confirming that the information is being sent by that CSP.

3.2 Peer Manger The Peer Manager screens the quantity of CSPs taking an interest in the system and changes the quantity of associates with the goal that the Byzantine Generals Problem does not happen. At the point when a part is made and proliferated, it plays out an errand of keeping up a base number of 3n + 1 peers so n pernicious CSP hubs don't meddle with the block age process. Likewise, the measure of the part is acclimated to get the ideal performance thinking about the quantity of companions. It additionally deals with the companions of the CSPs that need to join or leave the system.

3.3 Fault Tolerance Manger The Fault Tolerance Manger performs undertakings, for example, constructing a block by settling a blame circumstance, for example, expanding or agreement falling into a gridlock while stacking parts.

3.4 Mining Balance Manager The Mining Balance Manager plays out the errand of altering the cycle of creating block time. In the event that the period isn't steady, size of the information in each block might be lopsided, which may entangle the uprightness confirmation of the information while doing cloud crime scene investigation. In this manner, by modifying the base time and greatest time extend in which another block is made, it is conceivable to stack information of a legitimate size into one part. The Data Logging module in CSP Management Layer comprise of four capacities: Data Collector, Data Encryption Manager, Data Integrity Manager, Log DB Manager Details of each capacity are as per the following.

3.5 Data Collector The Data Collector plays out the undertaking of gathering the service information or log that the CSC asked for to be gathered. It is suggested that you utilize a public device that can be utilized for cloud crime scene investigation when gathering, for instance grunt to store arrange bundle information.

3.6 Data Encryption Manger Because information in the cloud condition might be identified with the security of the CSC, the Data Encryption Manager performs encryption of the information gathered by the information authority. Encoded information is prescribed to be scrambled utilizing the CSC's public key.

3.7 Data Integrity Manager The Data Integrity Manager deals with the honesty of information gathering and capacity. It is hard to believe CSP's uprightness of information in a domain gave by CSP itself. This implies CSP deals with the information that is put away before it can be utilized as proof for the cloud measurable agent by this method.

3.8 Log DB Manager The Log DB Manager plays out the undertaking of putting away the gathered information. The put away information is transmitted to the Data Integrity Management System in the wake of playing out a hash task.

IV. PERFORMANCE ALGORITHM

In this area, we think about exchanges per second (tps) with the other digital currency instrument with our proposed framework. One reason why mining-based authorization less digital money is not utilized as a part of other region is that the quantity of exchanges every second is too little. The tps recipe of digital money is as per the following.

$$tps = \frac{Blocksize}{Blocktime \times Size\ of\ the\ Transaction} \qquad (1)$$

VISA, a credit card company, handles 100,000 transactions per minute in 2016. Compared to that, the tps of the crypto currency is too low. For example, 6.41tps for Bitcoin, 15.65tps for Ethereum, 26.67tps for Zcash (unshielded), and 6.67tps for Zcash (shielded). The contents are shown in Table 1.

Table 1. Comparison of TPS of the proposed system with other crypto currency

	Blocksize (MB)	Blocktime (sec)	Transaction size (bytes)	tps
Bitcoin	1	600	260	6.41
Ethereum	4.7	14.3	21000	15.65
Zcash(unshielded)	2	150	500	26.67
Zcash(shielded)	2	150	2000	6.67
Proposed System (tps ; per CSP)	3.2	600	32	166.67

The proposed framework, expecting that uses an authorization blockchain, for example, Hyperledger, the chief can reconsider the chain code to set the run the show. In the proposed framework, when the information of one CSP is put away in a cycle of 10 minutes, the exchange of the blockchain framework in 10 CSP condition can be thought to happen once per minute. To expect the span of the log information, past research about security information logging framework for cloud crime scene investigation proposed by Zawoad et al. each log utilizes SHA-256 hash work. In this manner, it is expected that our proposed framework additionally utilizes that technique. Accepting that the log is produced once every second, around 600 logs are made in light of the fact that one part is put away at regular intervals in one CSP. The hash estimation of each log can be characterized as exchange. In the event that the span of scrambled log is 100byte, size of one part can be 3.2MB incorporating Hyperledger's block header with a specific end goal to spare this sign in hash tree. In view of this circumstance, we ascertain around 1667 tps of the proposed technique and around 167 tps per CSP on the grounds that there are 10 CSPs. The chart contrasting TPS and other digital money is appeared in Figure 3.

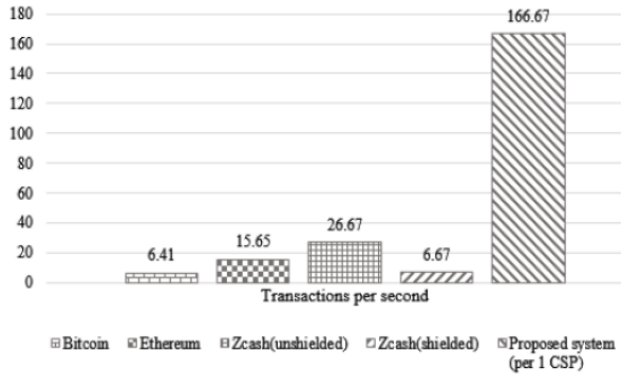

Figure 3. Compare transaction per second with other crypto currency

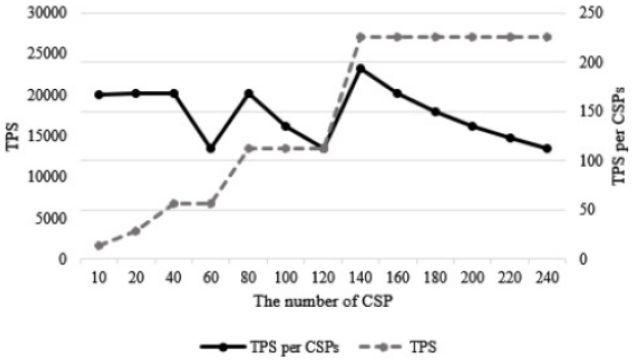

Figure 4. Comparison of tps according to the number of CSP

In Figure 4, we check tps as indicated by the quantity of CSP taking part in the proposed framework. The flat pivot speaks to the quantity of CSP. In the proposed framework, the blocktime and the exchange size of the block bind are thought to be the same, so the general TPS demonstrates an expanding prpublicsity. The tps per CSP demonstrates a specific range contingent upon the quantity of CSP. This is on account of the hash tree is sorted out in a paired tree. In the event that the quantity of logs is not as much as the accessible number of hash tree, the stature of the hash tree is extended. It can be seen that the tps per CSP diminishes as the quantity of logs and the measure of the hash tree end up level with. Permission blockchain, for example, Hyperledger can't ensure the precision of the tps in light of the fact that the client can discretionarily control the measure of the block and the part age period, and the performance may shift contingent upon how the earth is arranged. What's more, the proposed framework does not consider the time required for agreement and the time required to

process every exchange, so genuine performance is relied upon to be lower. Be that as it may, the current PoW-based consent less blockchain organize has a low preparing speed in light of the fact that untrusted people are permitted to take part in the system while looking after dependability. In this way, the preparing pace of a consent block anchor can be relied upon to be speedier.

V. CONCLUSION

In this paper, we explore the explanation behind signing in cloud condition for cloud crime scene investigation and propose the authorization blockchain based information uprightness service framework. The proposed framework can ensure the trustworthiness of information while handling a greater number of exchanges than existing consent less based blockchains. In any case, there is an impediment that the performance assessment of the present framework cannot play out the genuine assessment only by contrasting the ascertained outcome esteems by computing the normal information estimate. The proposed framework can be utilized as one of the philosophies for adapting to security episodes in the cloud condition. As future work we gather arrange information with grunt and perform reproduction to compute exact tps by utilizing Hyperledger. The purpose behind picking system information is that cloud condition has a mind boggling system condition because of the virtual system arrangement, and there are numerous occurrences that adventure its vulnerabilities. We will likewise play out a performance assessment looking at the time required for different accord algorithms for correlation between authorization blockchains.

VI. REFERENCES

[1]. Nepal, Surya, et al. "DIaaS: Data integrity as a service in the cloud." Cloud Computing (CLOUD), 2011 IEEE International Conference on. IEEE, 2011.

[2]. Gaetani, Edoardo, et al. "Blockchain-Based Database to Ensure Data Integrity in Cloud Computing Environments." ITASEC. 2017.

[3]. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.

[4]. K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," NIST Special Publication, pp. 80-86, 2006.

[5]. Josiah Dykstra, Alan T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques", Digital Investigation 9, 2012

[6]. J. Dykstra and A. T. Sherman, "Understanding issues in cloud forensics: two hypothetical case studies," in Proceedings of the Conference on Digital Forensics, Security and Law, 2011, p. 45.

[7]. K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," NIST Special Publication, pp. 80-86, 2006.

[8]. S. Zawoad and R. Hasan, "Digital forensics in the cloud," DTIC Document, 2013.

[9]. Giuseppe Ateniese, Randal Burns. Provable Data Possession at Untrusted Stores. 14th ACM Conference on Computer and Communications Security(CCS 2007)

[10]. Tsirlov, L. Bases of information security of the automated systems.Short course.Phoenix (2008)

[11]. Wilkinson, S., Lowry J. Metadisk: Blockchain-Based Decentralized File Storage. Application (2014)

[12]. Sompolinsky, Y., Zohar, A. Secure High-Rate Transaction Processing in Bitcoin (2015)

[13]. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)

[14]. Zyskind, G., Nathan, O., Pentland, A. Decentralizing privacy: Using blockchain to protect personal data (2015)

[15]. Andy Majot and Roman Yampolskiy, 2015. Global catastrophic risk and security implications of quantum computers. Futures, vol. 72 (September), pages 17-26.

About Authors:

Mr. Chintha MadhumohanReddy is currently pursuing his Master Of Computer Applications, Sree Vidyanikethan Institute of Management, Tirupati, A.P. He received his Master of Computer Applications from Sri Venkateswara University, Tirupati.

Mr. G Raghavendra is currently working as an Assistant Professor in Master of Computer Applications Department, Sree Vidyanikethan Institute of Management, Tirupati, A.P.