International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 05 | May 2021 www.irjet.net p-ISSN: 2395-0072

CREATING SECURE CLOUDS BY CONTINUOUS AUDITING AND PROVIDING CERTIFICATES

Arun S A [1], Aravindh M[2], Gokulvassan E A[3], Mohanaprakash T A[4]

[1-3]UG Student, Dept. of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, India.
4Associate Professor, Dept. of Computer Science and Engineer

Abstract - *The activity of cloud storage services has necessary edges in managing information for users. However, it additionally causes several security issues, and one amongst them is information integrity. Public verification techniques will modification a user to use a third-party auditor to verify the knowledge integrity on behalf of her/him, whereas existing public verification schemes are vulnerable to procrastinating auditors World Health Organization won't perform verification's on time. what's extra, most of public verification schemes ar created on the overall public key infrastructure (PKI), and thereby suffer from certificate management recoil. throughout this paper, we've got a bent to tend to propose the primary certificate-less public verification theme against procrastinating auditors (CPVPA) by pattern block-chain technology. The key prepare is to would really like auditors to record every verification result into a block-chain as a gaggle action. Since transactions on the block-chain are time-sensitive, the verification is time-stamped once the corresponding act is recorded into the block-chain, that permits users to check whether or not or not or not auditors perform the verification's at the prescribed time. Moreover, CPVPA is formed on certificate-less cryptography, and is free from the certificate management recoil. we've got a bent to tend to gift rigorous security proofs to demonstrate the protection of CPVPA, and conduct a comprehensive performance analysis to suggests that CPVPA is economical.*

Key Words: Secure Cloud , Auditing, block-chain technology, CPVPA, Time efficiency.

1. BLOCKCHAIN

With the emergence of Digital Currency (aka Crypto currency), several enterprises or financial institutions are experimenting with the Distributed Ledger system as a trusted way to track the ownership of the assets without any central authority. The core system behind the new currency system isBlockchain technology[1]. A walkthrough of the basic building blocks of the Blockchain technology is described below.A Blockchain is basically a chain of Blocks. Blocks are hashed using SHA-256 hashing algorithm to generate the signature of the data associated with it. Imagine a Blockchain as a linked-list whose node contains below attributes Block number – a sequence number (monotonically increasing) assigned tothe block Nonce – a random number which is used to generate Hash (as in #5) value which starts with 4 zeroes (0000). The process of generating thisNonce is called Mining .

Data – the actual userdata associated with the block
Prev – contains the Hash of the previous block
Hash – current block's Hash value (generated using SHA - 256).

All of the above attributes excluding Hash e.g. Block#, N once, data, Prev are used to calculate the Hash of this block.

[#=1,Nonce=3409,Data=x,Prev=00..0,Hash=0000ffgr5rg67j] <- [#=2, Nonce=4986,Data=x,Prev=0000ffgr5rg67j, Hash=000045tggr5rg..77yh] <-……and thechain goes on

e.g. in above block #1, the value for Hash=0000ffgr5rg67j is generated using the values 1,3409,x,00..0. In case value for any of these 4 attributes changes, it will change the Hash value of this block.Once the Hash value of this Block changes (e.g. from 0000ffgr5rg67jto 34sdffgr5rg67j), it will break the next Block (#2) as its Prev field will point to invalid Hash (0000ffgr5rg67j doesn't exist anymore). This leads to a ripple effect and turns whole chain as invalid/tampered.

One way to fix it is to run mining and recalculate the Hash value of Block #1 which basically will generate new value for Nonce and hence leading to a valid Hash value which startswith 4 zeroes. Copying this to next Block #2's Prev field will fix these 2 Blocks[2][3]. However in order to fix the whole Blockchain, we need to continue with this process for all the Blocks in the chain so that all Blocks point to new & valid Hash codes of their previous blocks.The cost of fixing the tampered Blockchain as described in above process is very high. Because we have to go and fix the Chain from the starting Block to the last one. In case the Chain is large, it becomes costly operation[4]. In case of Distributed Blockchain where several Peers are involved in the processand keeping the copy of the Blockchain, the repairing the Blocks becomes even more costlyoperation.The other and more efficient process isto come up with the compensating data and add this Block at the end of the Chain.There is a Fig below of creating Secure Cloud by Continuous Auditing and Providiting Certificates[5][6].

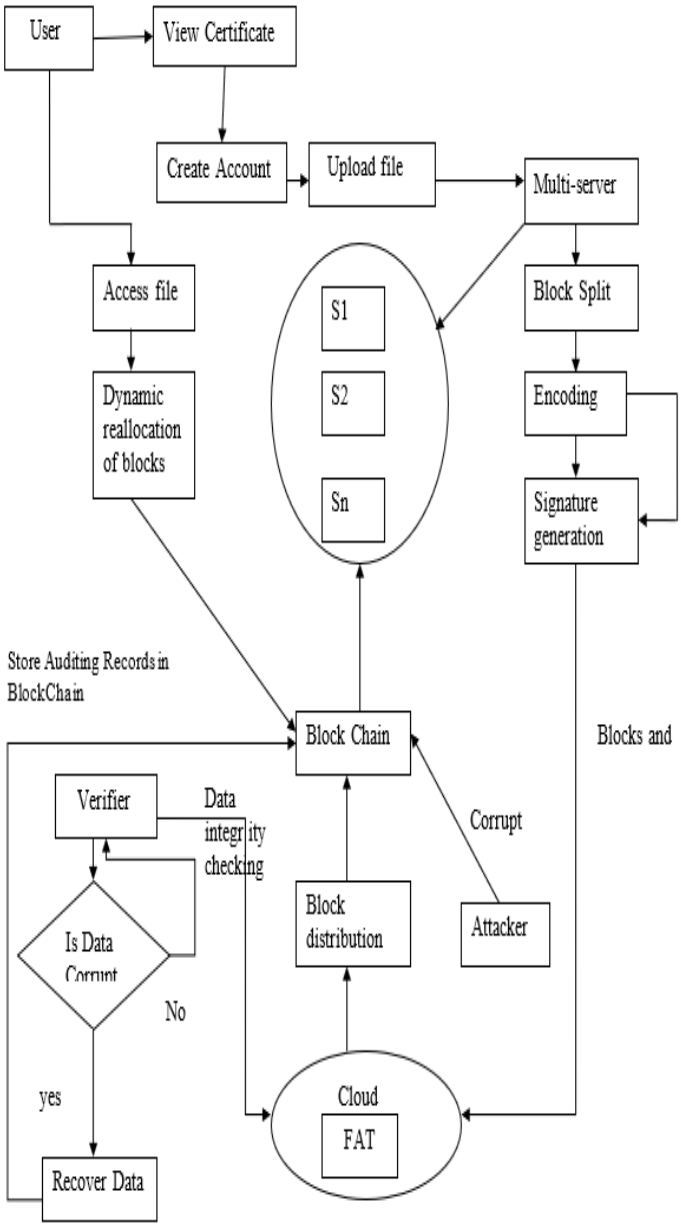
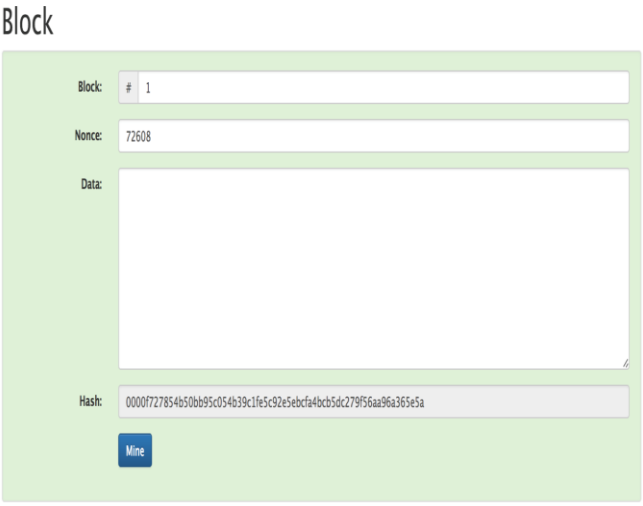
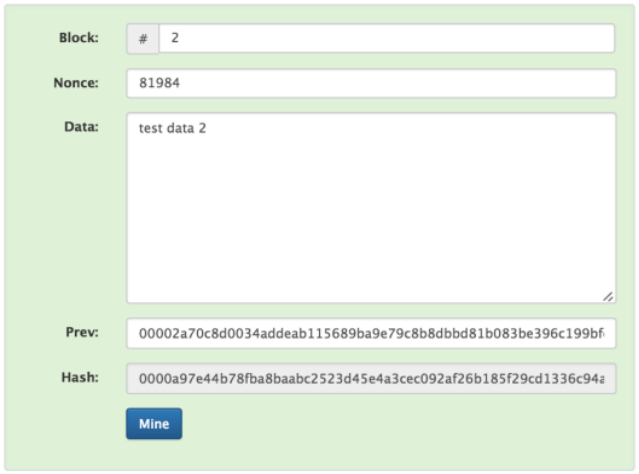


Fig : Creating Secure Clouds by Continuous Auditing and providing certificates Architecture diagram

E.g. In case your Chain contains the financial transaction (money movement) in Data field of the Block. Then instead of fixing each of the Block's Data with corrected financial transaction, come up with the adjusted financial transaction (aka compensating transaction) and create a Block (with Data=adjusted transaction record) and add this Block to the Blockchain (adds to the end of the Chain).[7][8]





3. LITERATURE SURVEY

Project Title	Author Name	Year of Publish	Abstract
An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computiang	Kan Yang	2012	In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud.
Providing Task Allocation and Secure Deduplication for Mobile Crowd sensing via Fog Computing	Jianbing Ni, Kuan Zhang,Yong Yu,Xiaodong Lin,Xuemin (Sherman) Shen	2017	Mobile crowd sensing enables a crowd of individuals to cooperatively collect data for special interest customers using their mobile devices. The success of mobile crowd sensing largely depends on the participating mobile users. The broader participation, the more sensing data are collected; nevertheless, the more replicate data may be generated, thereby bringing unnecessary heavy communication overhead.
Provable Data Possession at Untrusted Stores	Giuseppe Ateniese Randal	2017	We introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs.
Privacy-Preserving Public Auditing for Secure Cloud Storage	Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, Wenjing Lou	2016	Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources.
Bit coin and Beyond: A Technical Survey on Decentralized Digital Currencies	Florian Tschorsch Björn Scheuermann	2013	Besides attracting a billion dollar economy, Bit coin revolutionized the field of digital currencies and inuenced many adjacent areas. This also induced significant scientific interest. In this survey, we unroll and structure the many fold results and research directions.
Bit coin: A Peer-to-Peer Electronic Cash System	Satoshi Nakamoto	2014	A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

4. SYSTEM DESIGN AND IMPLEMENTATION

An increasing number of organizations outsource their data, applications and business processes to the cloud, empowering them to achieve financial and technical benefits due to on-demand provisioning and pay-per-use pricing. However, organizations are still hesitant to adopt cloud services because of security, privacy, and reliability concerns regarding provisioned cloud services as well as doubts about trustworthiness of their cloud service provider[9][10][11]. Cloud service certifications (CSC) are good means to address these concerns by establishing trust, and increasing transparency of the cloud market.

Working Models

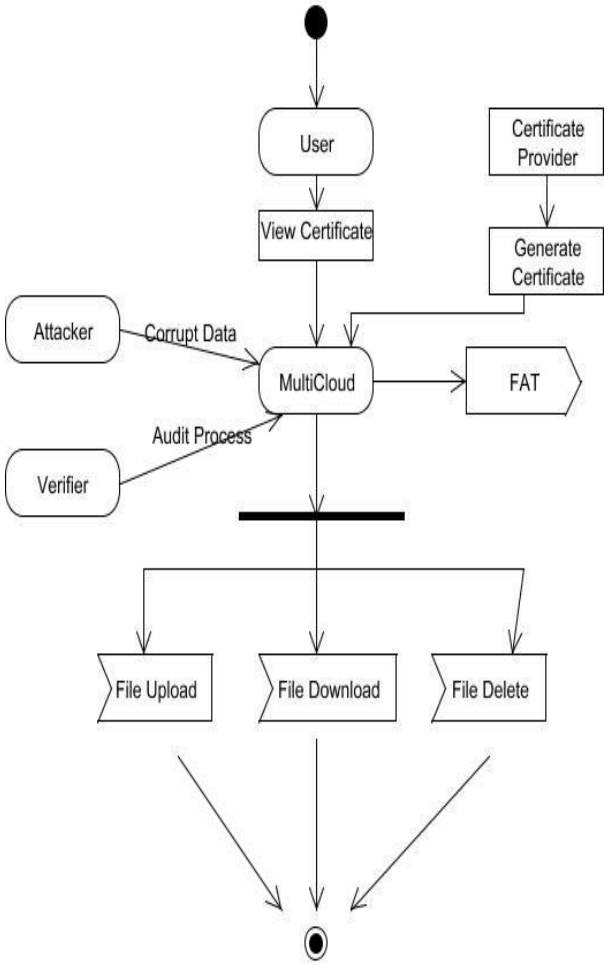


Fig. System flow on the Blockchain-BasedPublic Integrity Verification

Cloud servicecertifications attempt to assure a high level of security and compliance. However, consideringthat cloud services are part of an ever changing environment, multi-year validity periods may put in doubt reliability of such certifications. We argue that continuous auditing (CA) of selected certification criteria is required to assure continuously reliable and secure cloud services, and thereby increase trustworthiness of certifications. CA of cloud services is still inits infancy and we reveal that most of existing methodologies are not applicable for third party auditing purposes[12][13][14]. Therefore, we propose a conceptual CA architecture, and highlight important components and processes that have to be implemented.

A hierarchical structuring of relations may result in more classes and a more complicated structure to implement. Therefore it is advisable to transform the hierarchical relation structure to a simpler structure such as a classical flat one. It is rather straightforward to transform the developed hierarchical model into a bipartite, flat model, consisting of classes on the one handand flat relations on the other. Flat relations are preferred at the design level for reasons of simplicity and implementation ease. There is no identity or functionality associated with a flat relation. A flat relation corresponds with the relation concept of entity-relationship modeling and many object oriented methods[15][16][17]. and lightweight solution works on Windows, Linux, and Mac – hence the“cross-platform” part.

5. CONCLUSIONS

In this paper, we have proposed a certificate-less public verification scheme against the procrastinating auditor, namely CPVPA. CPVPA utilizes the on-chain currencies, where each verification performed by the auditor is integrated into a transaction onthe blockchain of on-chain currencies. Furthermore, CPVPA is free from thecertificate management problem. The security analysis demonstrates that CPVPA provides the strongest security guarantee compared with existing schemes. We have also conducted a comprehensive performance analysis, which demonstrates that CPVPA has constant communication overhead and is efficient in terms of computation overhead.

REFERENCES

[1] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, “Privacy-preserving data aggregation computing in cyber-physical social systems,” ACM Transactions on Cyber-Physical Systems, vol. 3, no. 1, p. 8, 2018.

[2] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, “Querying in internet of things with privacy preserving: Challenges, solutions and opportunities,” IEEE Network, vol. 32, no. 6, pp. 144–151, 2018.

[3] J. Li, H. Ye,W.Wang,W. Lou, Y. T. Hou, J. Liu, and R. Lu, “Efficient and secure outsourcing of differentially private data publication,” in Proc. ESORICS, 2018, pp. 187–206.

[4] L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, “A secure versatile light payment system based on blockchain,” Future Generation Computer Systems, vol. 93, pp. 327–337, 2019.

[5] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, “Enabling efficient and geometric range query with access control over encrypted spatial data,” IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870–885, 2019.

[6] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, "Privacypreserving attribute-keyword based data publish-subscribe service on cloud platforms," Information Sciences, vol. 387, pp. 116– 131, 2017.

[7] W. Shen, B. Yin, X. Cao, Y. Cheng, and X. Shen, "A distributed secure outsourcing scheme for solving linear algebraic equations in ad hoc clouds," IEEE Trans. Cloud Computing, to appear, doi: 10.1109/TCC.2016.2647718.

[8] H. Yang, X. Wang, C. Yang, X. Cong, and Y. Zhang, "Securing -centric networks with content-based encryption," Journal of Network and Computer Applications, vol. 128, pp. 21–32, 2019.

[9] Q. Wang, C. Wang, J. Li, K. Ren, and W.
Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS, 2009, pp. 355–370.

[10] X. Zhang, H. Wang, and C. Xu, "Identity-based key-exposure resilient cloud storage public auditing scheme from lattices," Information Sciences, vol. 472, pp. 223–234, 2018.

[11] K.Wang, J. Yu, X. Liu, and S. Guo, "A pre-authentication approach to proxy re-encryption in big data context," IEEE Transactions on Big Data, 2017, to appear, doi. 10.1109/TBDATA.2017.2702176.

[12] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Providing task allocation and secure deduplication for mobile crowdsensing via fog computing," IEEE Transactions on Dependable and Secure Computing, to appear, doi. 10.1109/TDSC.2018.2791432.

[13] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation," IEEE Trans. Information Forensics and Security, vol. 12, no. 3, pp. 676–688, 2017.

[14] H. Shacham and B. Waters, "Compact proofs of retrievability," of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.

[15] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2013.

[16] T. A. Mohanaprakash and J. Andrews, "Novel privacy preserving system for Cloud Data security using Signature Hashing Algorithm," 2019 International Carnahan Conference on Security Technology (ICCST), CHENNAI, India, 2019, pp. 1-6, doi: 10.1109/CCST.2019.8888420.

[17] G.Senthil kumar, Dr.M.P.Chitra, "Finite horizon markov decision process based fuzzy optimization for resource allocation in sdn enabled virtual networks in iaas cloud environment", Journal of Theoretical and Applied Information Technology 15th July 2020. Vol.98. No 13.