BULLET: Jurnal Multidisiplin Ilmu
Volume 1, No. 04, Augustus-September (2022)
ISSN 2829-2049 (media online)
Hal 736-748

Block chain-Based Solutions for Improved Cloud Data Integrity and Security

Md Tanvir Rahman Tarafder[1], Arafath Bin Mohiuddin[2], Nisher Ahmed[3], Md Abu Shihab[4], Md Farhad Kabir[5]
[1, 2] Faculty of Science and Technology, American International University-Bangladesh, Dhaka, Bangladesh.
[3]College of Technology & Engineering, Westcliff University, Irvine, California, USA.
[4]School of Information Technology, SEGi University, Selangor, Malaysia.
[5]Marshall School of Business, University of Southern California, Los Angeles, California, USA.
[1]tanviraditto90@gmail.com, [2]arafath2307@gmail.com, [3]n.ahmed.511@westcliff.edu ,
[4]abushihabhtc@gmail.com, [5]mkabir@marshall.usc.edu

Abstract

The evolution of cloud computing, however, has not been all smooth sailing, and it still struggles with data security and trusted computing to this day. Alternative solutions like data integrity tests and secure multi-party computation is often accompanied by computational complexity and scalability concerns. Block chain technology has been developed as an abstract setting of decentralized distributed computing, and applied to secure storage and computation in various cloud environments. In response, we propose a distributed virtual machine agent model that uses the mobile agent technology to create a cooperative and multi-tenant environment for the verification of trust in the data. This model assures the data are stored and monitored reliable way and provides a verification method that is the base of a Block chain based integrity protection mechanism. Using this model, we create a Block chain model that utilizes Merkle hash trees in order to create unique file hashes. Smart contracts monitor changes to this data and will notify users of any tampering. Additionally, in a block-and-response manner, it provides a strong cloud data integrity verification solution.

Keywords: Block chain, Cloud data, Integrity verification, Merkel hash tree

INTRODUCTION

Block chain is expected to be a key element in the information technology revolution 2.0. It becomes a valuable frontier field for its distinctive strengths, innovative ideas, and wide applications. Actually some technologists argue that the disruptive nature of the Block chain is only comparable to the steam engine, electricity and the actual internet. The problem Block chain solves is in theory, a trust issue [1]. Like a public ledger, it enables all too record, view, and maintain entries, each time-stamped and immutable. The modern economy suffers from trust issues, and unlike the traditional internet, Block chain solves this issue by decentralization. Block chain swaps need you to only trust the tech instead of each other [2].

In addition, Block chain can also make data authentic, and be able to circulate and share with each other, which also helps to converge data. We are now living in what I call the "Value Internet" age. The internet completely redefined the way that we interact with information — however, how to transfer value remained as it was before, inefficient [3]. Block chain is expected to be a value transfer network like the former information network, which would promote the establishment of a credit-based society in the future that is transparent, open and reliable.

Although we live in the era of big data but it has its own challenges, such as, collaborative data sharing, collaborative data transaction, and privacy protection [4]. Though there are solutions, Block chain presents a unique method of tackling these problems. Due to dependencies on trusted third-party organizations, current centralized data processing solutions come with various risks. Such organizations can cause a huge loss to the users as well as the data owners if they are compromised [5]. When coupled with big data, Block chain provides a decentralized solution that overcomes these vulnerabilities as well as some big data related challenges.

The World Economic Forum notes how the interest in Block chain has gone global, with it being seen as a fruitful avenue for investment across multiple countries and a substantial number of banks running Block chain projects [6]. There is a three-stage evolution of what Block chain applications will be (19):

Phase 1.0: Centers around digital currency, such as Bitcoin, allowing for secure, seamless transactions without the need for intermediaries [7].

Phase 2.0: Combination of digital currencies and smart contracts for efficient payments and automatic execution of contracts. Use cases have trading of assets, clearing of funds and intelligent agreements [8].

Phase 3.0: Expands out of finance into applications in social management (i.e. governance), healthcare, and culture and beyond and may fundamentally change society.

The Block chain has recently gained even more prominence. The research and development in this field is being done by major technology companies and financial institutions. For instance, Alibaba's donation platform based is on the Block chain and Tencent has recently entered Block chain banking [9]. Block chain is a promising technology for areas such as the Internet of Things (IoT), financial technology (fintech), and e-government, and should be further studied and developed to fully mature and enter the mainstream [10].

PROPOSED METHOD

Block chain: Block chain is a type of ledger that is distributed and immutable, that is used to record and verify transactions between different scattered computers. Key characteristics include:

Decentralization: The lack of a centralized authority in charge of the Block chain boosts security, and immunity against censorship.

Immutable: Once written, transactions cannot be changed or removed, which means data integrity [11].

Transparency: Participation of all stakeholders in transaction history to ensure accountability.

Security: The block chain is protected from tampering with the help of cryptographic hashing and consensus methods [12].

There are many kinds of chains such as public (permissionless) versus private (permissioned) and consortium chains. Only public Block chains such as Bit coin are open to everyone, private and consortium Block chains only allow access to select participants.

A Block chain is a series of blocks containing a timestamp, transaction data, and the hash of the previous block. This relation structure allows for the integrity and time order of the data [13]. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code and can be used on Block chains to automate processes and increase trust. The reason it holds the potential to transform countless industries are because of it can its ability to increase trust, security and transparency [14].

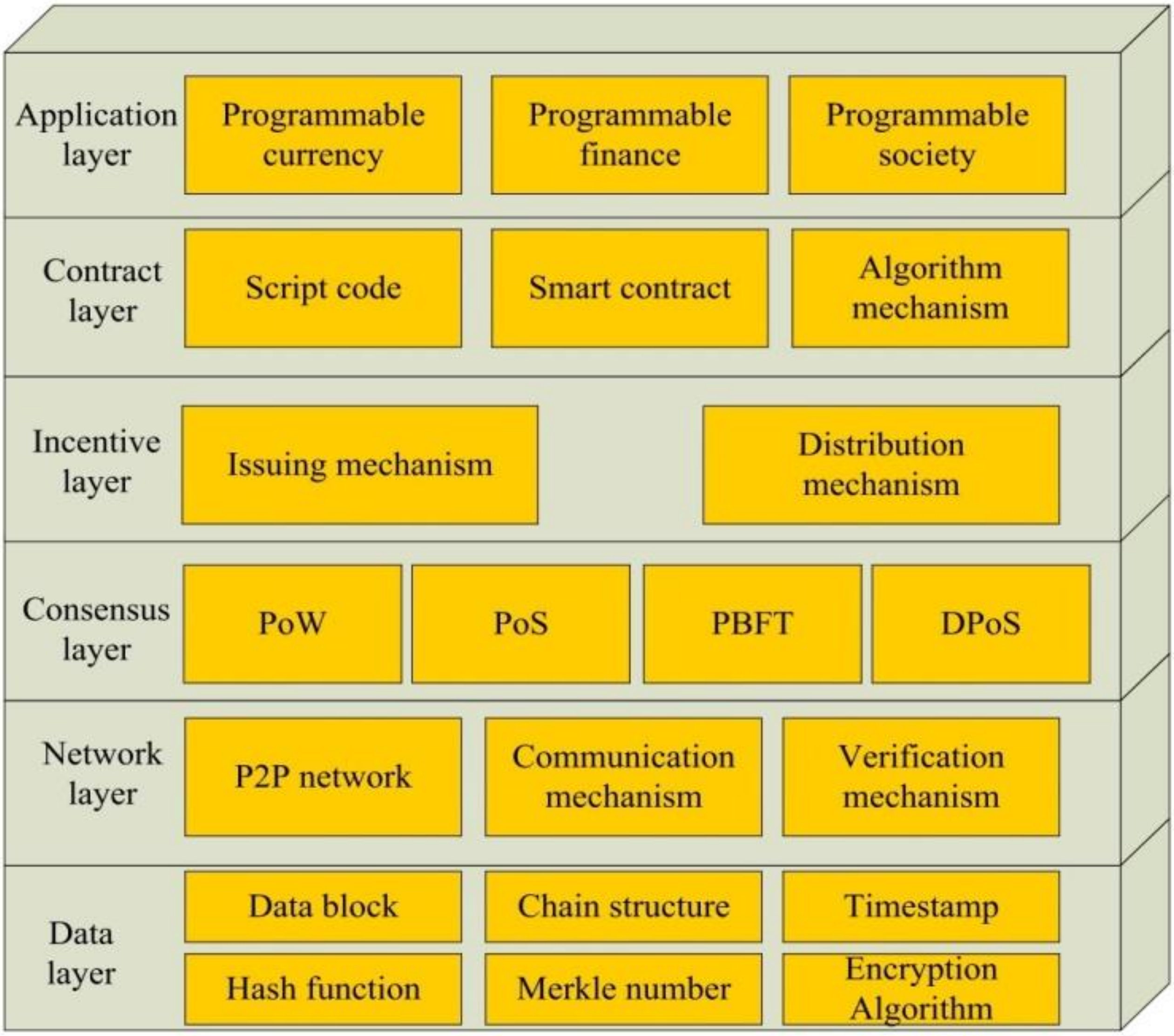


Fig. 1. Block chain infrastructure

TECHNOLOGY RELATED TO SECURITY OF CLOUD DATA STORAGE

It consists of a set of technologies that underpin the security of data at rest and data in transit, assuring data confidentiality, integrity, and availability in cloud data storage. Key focus areas and specific technologies in this space include:

Encryption: Used to keep data consistent by not understanding it in the first place. Here are some common types of encryption:

Symmetric-key encryption: The same key is used for encrypting and decrypting [15].

Asymmetric-key encryption: Uses different keys for encrypting and decrypting.

Holomorphic encryption: Theoretically, this enables computation of encrypted data without needing access to unencrypted data [16].

Access Control: It limits access to data as per the policies and functionality defined according to user roles. Related technologies include:

Role-Based Access Control: this is another way of assigning permissions based on roles.

Access Control Based on Attributes: where access is based on the attributes of users, data, and the surrounding environment Cloud Safe: Protecting sensitive data processing from sensitive information exposure risk in vulnerable cloud virtualization stacks [17].

Integrity: Verifies that the data has not been modified Techniques include:

Hashing: Creates unique fingerprints from data to identify changes.

Digital Signatures: Sign data with cryptography to assure its authenticity and integrity. (Improved for a secure, efficient data deduplication scheme with dynamic ownership management in cloud computing [18].

General Authentication Codes: Allows it to check the integrity and authenticity.

Intrusion detection and prevention: Monitors network traffic and system activity for malicious activity. Privacy Preserving and Access Control to Intrusion Detection in Cloud System, Technologies include:

IDS: Identify suspicious patterns [19].

Intrusion Prevention Systems: These help in blocking the traffic that seems malicious.

Data Loss Prevention: Blocks any unauthorized transfer of sensitive data out of an organization. Note Techniques include.

Encrypting data: At rest and in transit.

Control of access: Prevents access to confidential data.

Data Masking- Masks sensitive data elements.

SIEM (Security Information and Event Management): Collects and analyzes security logs to identify threats and vulnerabilities [20].

Backup and Restore Functionality: Revives data in case of a failure or disaster. Hosted Security: Focuses on host-based specialization for virtual environments [21].

Together, these technologies offer a complete cloud data security posture. The actual technologies used are based on the data sensitivity, compliance requirements, and the organizations willingness to take risk [22].

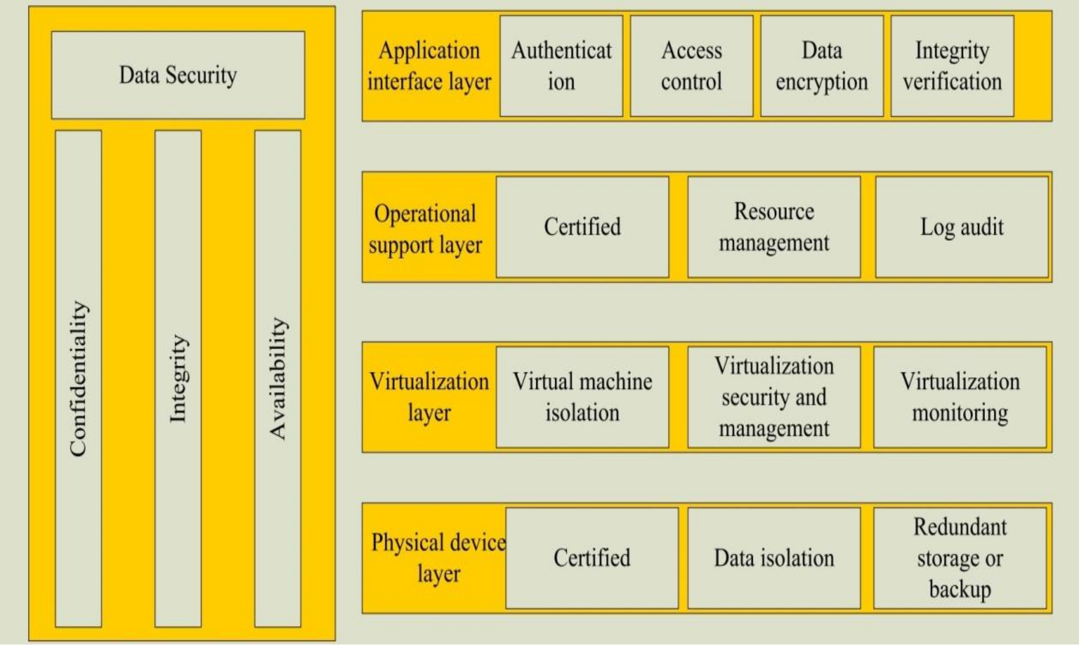


Fig. 2. Cloud storage service security model.

VERIFICATION PROCESS CORRECTNESS

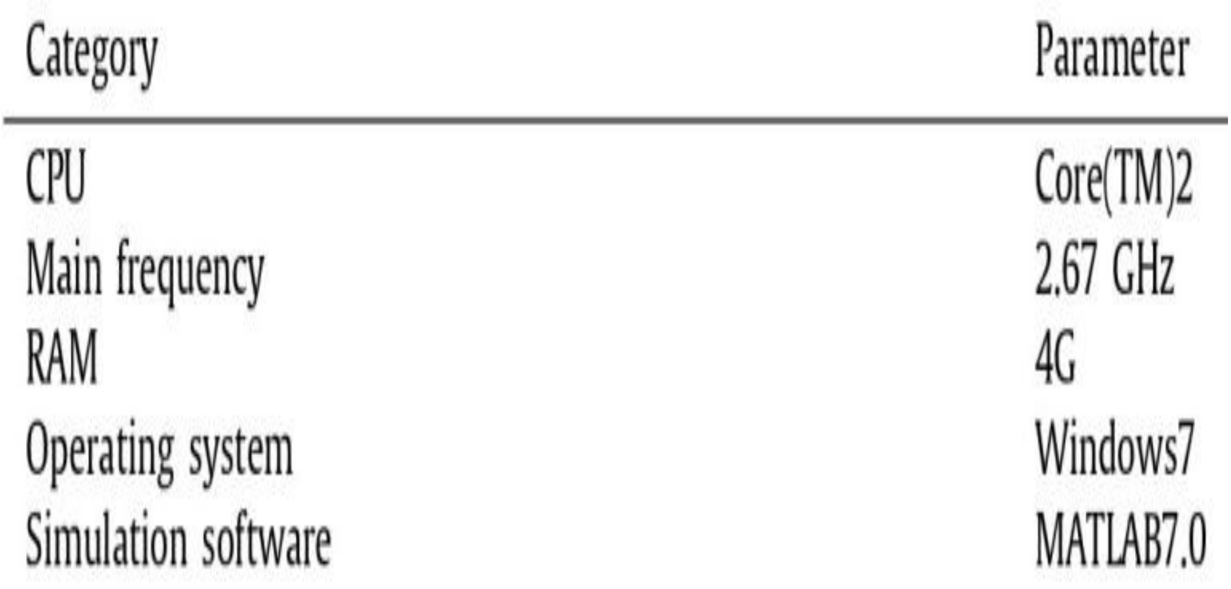
In single-user verification, the user gets a proof from the storage service. The user computes a verification equation using their public key and a set of predefined parameters to confirm whether data has been changed [23]. If this equation stands true, you can verify that the data was not altered in any way. Failure of the equation indicates possible corruption of data or illegal modification [24].

Cost Calculation: All these k query attributes are customized and in return built the storage cost which is the summation of the storage costs of the verification tree storage done by tenant on the query attributes. This leads to (k − 1) • N • |k| + k • |s| − (N • 2 • |k| + N−1 f −1 (|h| − |p|)), which can be derived by taking the difference of (11)–(12) from the equation above [25]. Given that the digital signature and hash settles in excess of the inquiry watchword and pointer size, it infers that it is not the same as every others query quality. For the pivot table and the universal table respectively, the data the m-MHT method is constructed of. Third, the MTAS (Algorithm 4) decreases the system storage cost, as the MTAS saves the (k − 1) • N/f hash value on the leaf node and decreases the k • |s| root node signature storage on the root node [26].

Merkel Hash Tree: A Merkle hash tree (or Merkle tree) is a well-known data structure in cryptography and computer science for the secure checking of very large datasets. It accomplishes this recursively building data blocks, where only a single hash is produced, and the root hash. File storage in the cloud using a Merkel hash tree of file integrity checks in OCaml (GitHub - coders-creed/FileZeus: cloud file storage system with Merkel hash tree integrity checks [27].

EXPERIMENTS

Experimental environment: It seems like you are preparing a document for experiments along with their setup. I need some context to give you the most relevant information to describe your experimental environment. What do you experiment with? I'll be able to advise you more specifically if I know the domain [28].



Category	Parameter
CPU	Core(TM)2
Main frequency	2.67 GHz
RAM	4G
Operating system	Windows7
Simulation software	MATLAB7.0

Table 1 Experimental environment parameters.

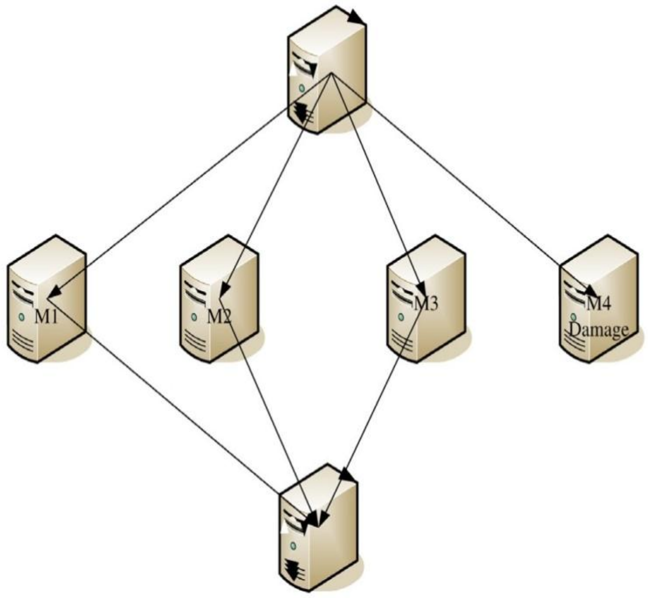


Fig. 3. Simulation experiment topology.

CALCULATION IN THE PROGRAM

Distributing agents of virtual machine in the cloud and leveraging the cloud multi-tenancy to build out a Block chain network, this paper. Background Process Data Pre-processing (BPDP) Integrity Verification Scheme Cloud Data- It has five algorithms:

(1) Create a private–public key pair;

KeyGen (1k) → (pk.sk)

Let us create an output label in digital form,

TagBlock(pk, sk, m) −→ Tm

We create information about the challenge,

GenChal (c, r) → chal

Create evidence according to

V (20) → Gen Pr oof (pk, F, chal, Σ)

Test Evidence

We pass from Pr oof (sk, V) → result

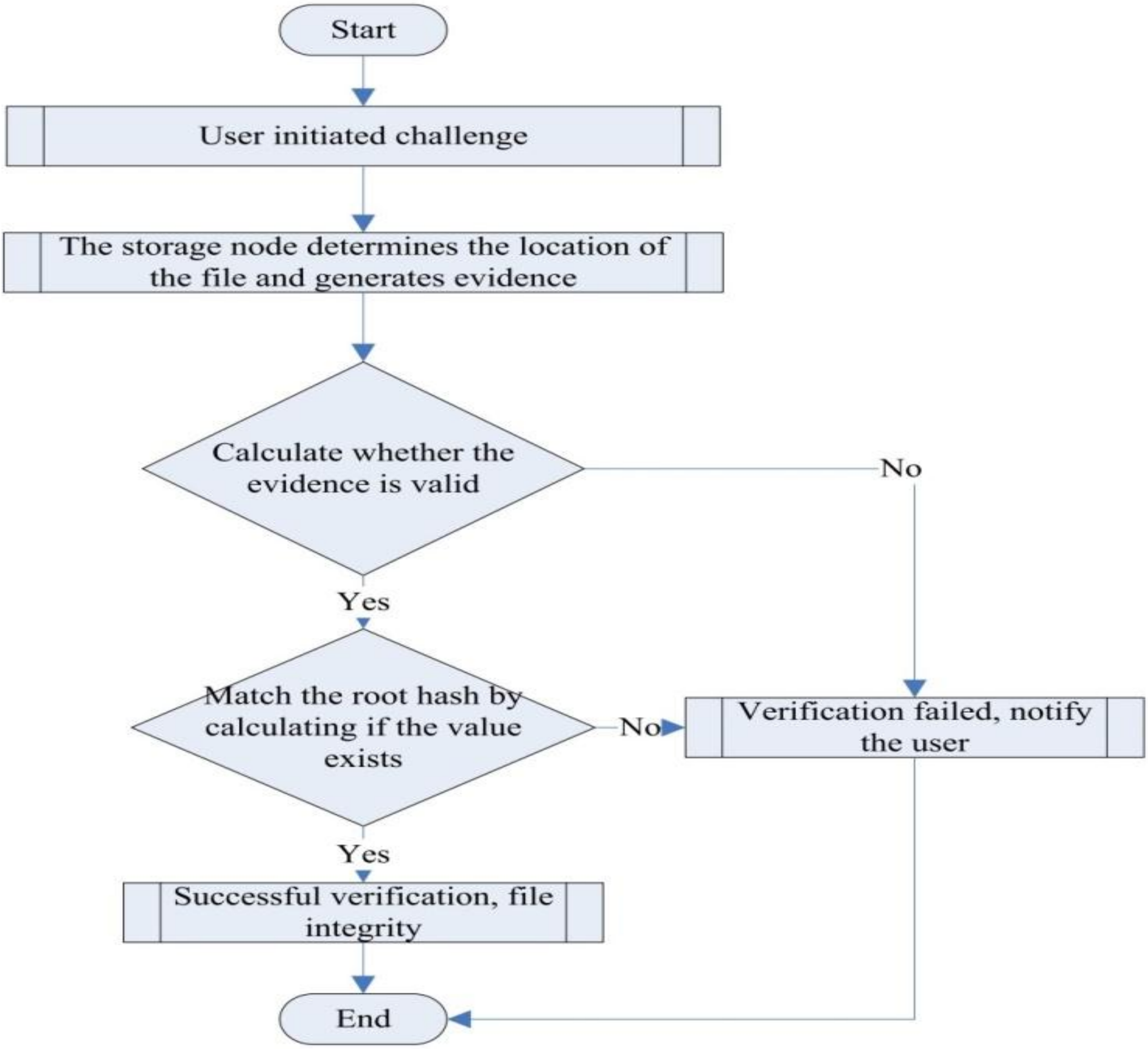

Start
User initiated challenge
The storage node determines the location of the file and generates evidence
Calculate whether the evidence is valid
No
Yes
Match the root hash by calculating if the value exists
No
Verification failed, notify the user
Yes
Successful verification, file integrity
End

Fig. 4. Integrity verification flow chart.

Method for checking integrity

As you can see in Fig, it is the integrity verification phase. 4. The user picks a data block at random, and calls up the storage node of CSP via VMA node, gets file location by proves the challenge block in the IPFS cluster and sends proof back it to the VMA [29]. The verification is passing through the VMA to determine the evidence. If it is valid (and it is, if so), the next step is verified [30].

DISCUSSION

Block chain based cloud data integrity analysis: The accuracy of a sampling-based integrity verification protocol for cloud data in this paper. Let n be the number of whole data blocks and e be the number of corrumpted blocks therefor the corrupt ratio is pb = e/n. P: Probability of detecting tampering for t challenged blocks per verification This probability P is most likely some as-of yet undefined function of the above terms t, n, and e [31]. Some elaboration on how 'P' is measured and what it means for integrity assessment for Block chained behaviour would be helpful.

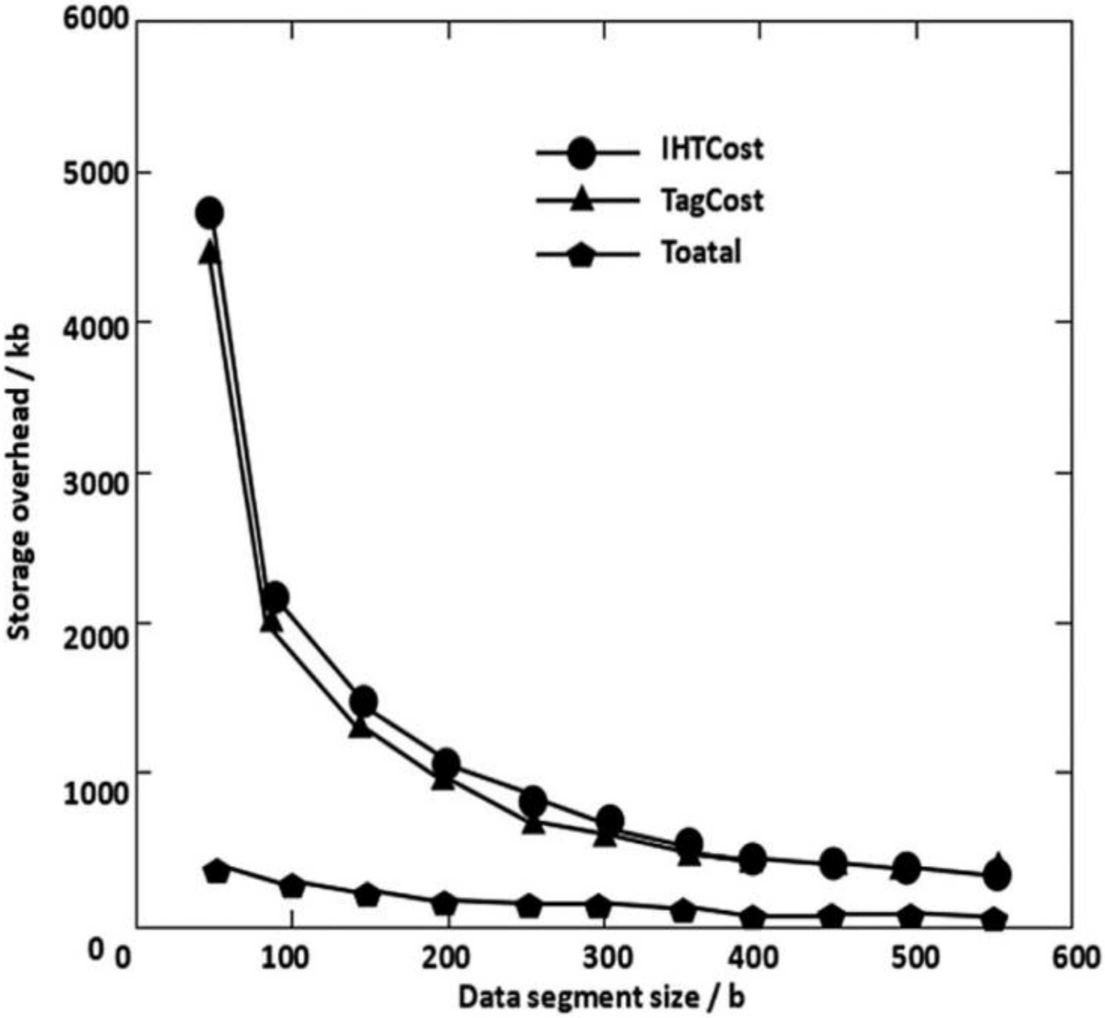


Fig. 5. Storage overhead map.

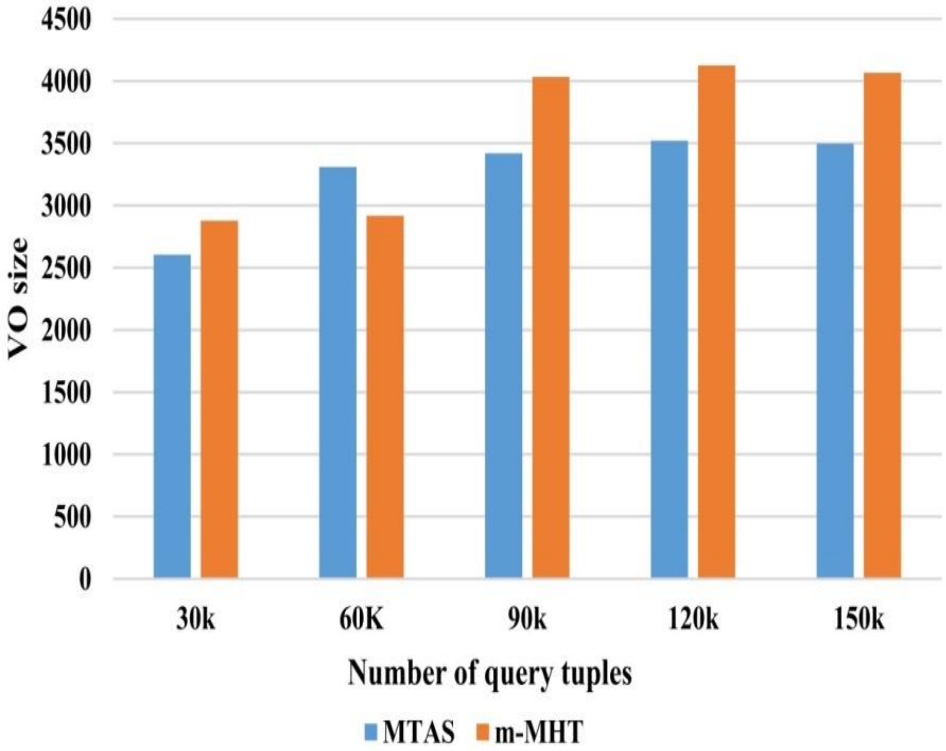
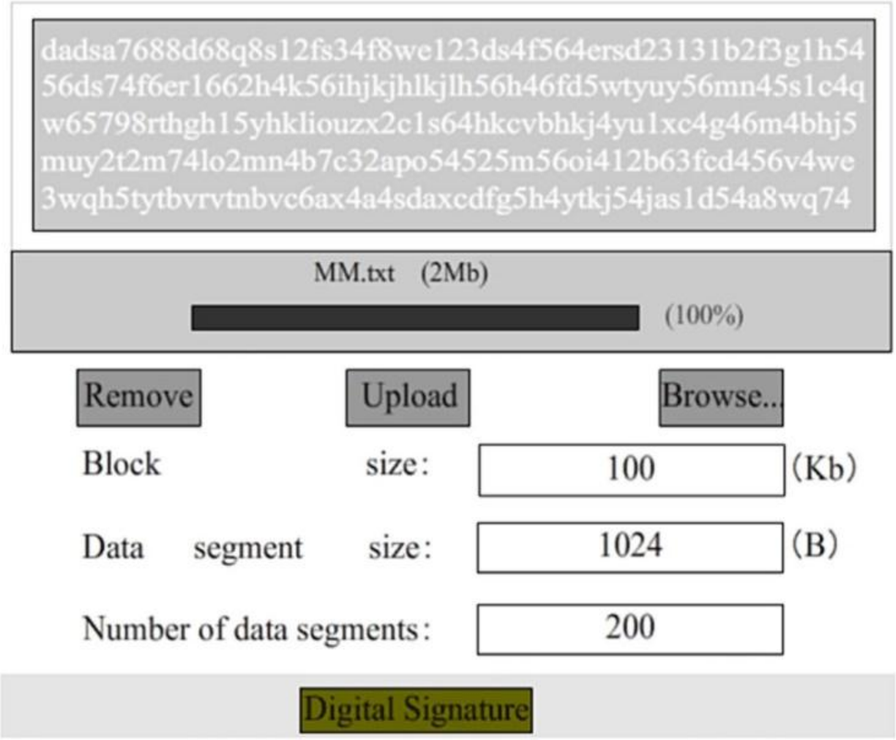


Fig. 6. Comparison of V0 size in m-MHT and MTAS



dadsa7688d68q8s12fs34f8we123ds4f564ersd23131b2f3g1h54
56ds74f6er1662h4k56ihjkjhlkjlh56h46fd5wtyuy56mn45s1c4q
w65798rthgh15yhkliouzx2c1s64hkcvbhkj4yu1xc4g46m4bhj5
muy2t2m74lo2mn4b7c32apo54525m56oi412b63fcd456v4we
3wqh5tytbvrvtnbvc6ax4a4sdaxcdfg5h4ytkj54jas1d54a8wq74

MM.txt (2Mb)

(100%)

Block size: 100 (Kb)

Data segment size: 1024 (B)

Number of data segments: 200

Fig. 7. Preprocessing function.

CLOUD DATA INTEGRITY SOLUTION USING BLOCK CHAIN

The Block chain capability for immutability, transparency, and decentralization can be used to analyze cloud data integrity and improve trust and verifiability. This analysis entails several important factors:

Data Integrity Verification: Block chain provides a way to verify integrity of data into the blocks as they get modified in separate tamper-proof chain by storing their hashes [32]. If any change is made to the data, the hash would be changed, so it would be easy to spot the change. This allows one to abandon relying on the integrity of a cloud provider [33].

Origin Tracking: The entire history of data can be tracked, including where it came from, how it has been processed, and every time it has been accessed using the Block chain. Block chain creates a transparent and verifiable log of data provenance which ultimately improves accountability and trust [34].

This means that using Block chain, there is no need for a single central authority to ge a confirmation on the integrity of the data. Block chain offers a number of benefits over traditional databases, including decentralization and higher trust and attack resistance by allowing multiple parties to participate in the verification process [35].

Improved Security: As a cryptographic technology, Block chain incorporates multiple security layers that help protect data from being tampered with or accessed dynamically. This authenticity and integrity of data is ensured using digital signatures and hash functions.

Auditing and Compliance: The transparent and immutable nature of Block chain enables easier audits and compliance with regulatory standards [36]. A Block chain-based Flight Data Recorder for Cloud Accountability 2018 all data operations are transparently accessible for audit purposes.

The Effect of Block chain on IT Research – Accountability and Responsibility Block chain enables accountability by having clear responsibility about the specific parties involved in using the data [37]. A Block chain based Flight Data Recorder for cloud accountability 2018 this is a significant aspect in environments that involve multiple parties accessing data on a cloud.

Challenges and considerations: While Block chain has great potential for cloud data integrity analysis, there are also challenges to consider including scalability and performance, as well as integrating Block chain with the current cloud infrastructure [38]. The consensus mechanism that is used & the handling of the Block chain keys matters too. Secure Consistency Verification for Public Block chains over Untrusted Cloud Storage

With that in mind, considering these factors will tremendously enhance the cloud data integrity analysis using Block chain, setting up the basis for trust, transparency, and accountability for data in cloud-stored environments. The code snippet shared by you details about Block chain-based integrity verification system and explains overall flow from data submission to generate evidence of integrity all the way to data verification. It also points out the use of IPFS for file storage and Block chain for redundant storage and easy retrieval of data.

CONCLUSIONS

Enhancing Security and Data Integrity in Cloud Computing Environments using Block chain Technology: A Multi-Party Computation Approach These contributions can be summarized as follows: A secure data trust verification framework, based on mobile agent technology and a distributed virtual machine proxy model that allows an encrypted data to be verified, monitored and checked for its integrity, The framework leverages virtual machine agents to foster multi-tenant collaboration in the cloud. A new secure multi-party computation scheme is proposed by integrating both the advantages of typical Block chain and cloud computing. This helps to maintain data security and integrity as well as facilitate the data management process related to the data stored in the cloud. The heart of the proposed data integrity verification scheme is a block-and-response model by integrating smart contracts and Merkle hash trees. This method enables continuous data monitoring, timely update of data ownership and instant identification tampering. With the Merkle hash tree, we create a hash for every file and allow for data integrity to be checked efficiently. This paper proposes a real-world application of Block chain for securing and integrity-proving cloud-based multi-party computation. This scheme uses the decentralized and immutable characteristic of Block chain to trust, transparent and accountable cloud data management.

REFERENCES

1. Abler, R., Owen, H., & Riley, G F. (2003, May 1). University methodology for internetworking principles and design projects. IEEE Education Society, 46(2), 218-225. https://doi.org/10.1109/te.2002.808239
2. AWS Cost Calculator | EC2, S3, Lambda and Data Transfer Cost. (2020, July 1). https://www.cloudysave.com/aws/cost-calculator/
3. Becher, B. (2022, September 1). Block chain: What It Is, How It Works, and Why It Matters. https://builtin.com/Blockchain
4. Beck, R., Müller-Bloch, C., & King, J L. (2018, January 1). Governance in the Block chain Economy: A Framework and Research Agenda. Association for Information Systems, 1020-1034
5. Beck, R., Müller-Bloch, C., & King, J L. (2018, January 1). Governance in the Block chain Economy: A Framework and Research Agenda. Association for Information Systems, 1020-1034. https://doi.org/10.17705/1jais.00518
6. Celo Wallet Verification | Celo Documentation. (2022, January 1). https://docs.celo.org/wallet/celo-wallet/verification
7. Cohen, T S., Boland, M L., Boland, B B., Takahashi, V., Tovchigrechko, A., Lee, Y., Wilde, A D., Mazaitis, M J., Jones-Nelson, O., Tkaczyk, C., Raja, R., Stover, C K., & Sellman, B R. (2018, February 1). S. aureus Evades Macrophage Killing through NLRP3-Dependent Effects on Mitochondrial Trafficking. Cell Press, 22(9), 2431-2441. https://doi.org/10.1016/j.celrep.2018.02.027
8. CostStorage.com | Quickly estimate the cost of storing your data on S3, Azure, Google Cloud, and more.. (2016, January 22). https://coststorage.com/
9. Fekih, R B., & Lahami, M. (2020, January 1). Application of Block chain Technology in Healthcare: A Comprehensive Study. Springer Science+Business Media, 268-276. https://doi.org/10.1007/978-3-030-51517-1_23
10. Fisher, C. (2018, January 1). Cloud versus On-Premise Computing. Scientific Research Publishing, 08(09), 1991-2006. https://doi.org/10.4236/ajibm.2018.89133
11. Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2017, January 1). Block chain-Based Database to Ensure Data Integrity in Cloud Computing Environments.. , 146-155
12. Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2017, January 1). Block chain-Based Database to Ensure Data Integrity in Cloud Computing Environments.. , 146-155. http://ceur-ws.org/Vol-1816/paper-15.pdf
13. Gejibo, S., Grasso, D., Mancini, F., & Mughal, K A. (2013, September 2). Secure cloud storage for remote mobile data collection. https://doi.org/10.1145/2513534.2513538

14. Goldman, A D., Uluagac, A S., & Copeland, J A. (2014, September 1). Cryptographically-Curated File System (CCFS): Secure, inter-operable, and easily implementable Information-Centric Networking. https://doi.org/10.1109/lcn.2014.6925766
15. Gunasinghe, H., Kundu, A., Bertino, E., Krawczyk, H., Chari, S T., Singh, K., & Su, D. (2019, May 13). PrivIdEx: Privacy Preserving and Secure Exchange of Digital Identity Assets.. https://doi.org/10.1145/3308558.3313574
16. Hanumanthakari, S., & Banik, B G. (2020, January 1). A Comprehensive Study of Block chain Services: Future of Cryptography. Science and Information Organization, 11(10). https://doi.org/10.14569/ijacsa.2020.0111037
17. Hook, M D., & Mayer, M. (2017, March 1). Miniature environmental chambers for temperature humidity bias testing of microelectronics. American Institute of Physics, 88(3). https://doi.org/10.1063/1.4978916
18. Jianliang, L K T Y K B H X. (2019, April 14). Secure Consistency Verification for Untrusted Cloud Storage by Public Block chains. https://arxiv.org/abs/1904.06626
19. Kalis, R., & Belloum, A. (2018, December 1). Validating Data Integrity with Block chain
20. Kalis, R., & Belloum, A. (2018, December 1). Validating Data Integrity with Block chain. https://doi.org/10.1109/cloudcom2018.2018.00060
21. Kouhizadeh, M., Saberi, S., & Sarkis, J. (2020, June 20). Block chain technology and the sustainable supply chain: Theoretically exploring adoption barriers. Elsevier BV, 231, 107831-107831. https://doi.org/10.1016/j.ijpe.2020.107831
22. Kumar, Y., Sharma, G., Sakpal, K., & Umbare, A. (2020, March 11). EKYC Mobile Application using Optical Character Recognition. International Research Publication House, V9(02). https://doi.org/10.17577/ijertv9is020418
23. Lansade, M T F C C P L C R N L. (2019, November 24). Horses Categorize Human Emotions Cross-Modally Based on Facial Expression and Non-Verbal Vocalizations. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6912773/figure/animals-09-00862-f001/
24. Lee, L., & Mautz, R D. (2012, February 21). Using cloud computing to manage costs. Wiley, 23(3), 11-15. https://doi.org/10.1002/jcaf.21748
25. Liu, B., Yu, X L., Chen, S., Xu, X., & Zhu, L. (2017, June 1). Block chain Based Data Integrity Service Framework for IoT Data
26. Liu, B., Yu, X L., Chen, S., Xu, X., & Zhu, L. (2017, June 1). Block chain Based Data Integrity Service Framework for IoT Data. https://doi.org/10.1109/icws.2017.54
27. Meena, S., Daniel, E., & Vasanthi, N A. (2013, March 1). Survey on various data integrity attacks in cloud environment and the solutions. https://doi.org/10.1109/iccpct.2013.6528889
28. Moreno, D G F S M. (2018, June 12). A Block chain-based Flight Data Recorder for Cloud Accountability. https://arxiv.org/abs/1806.04544
29. Naik, H., Bastien, R., Navab, N., & Couzin, I D. (2020, February 13). Animals in Virtual Environments. Institute of Electrical and Electronics Engineers, 26(5), 2073-2083. https://doi.org/10.1109/tvcg.2020.2973063
30. NY, S S O D U N V S V R A F R L R N C K A F R L R N K K A F R L R N L N A F R L R. (2017, April 5). Data provenance assurance in the cloud using Block chain. https://www.spiedigitallibrary.org/redirect/proceedings/proceeding?doi=10.1117/12.2266994

31. Pearson, S. (2012, June 27). Privacy, Security and Trust in Cloud Computing. , 3-42. https://doi.org/10.1007/978-1-4471-4189-1_1

32. Rivera-Valdes, J S R D G C. (2012, January 1). MulStiple Exemplar Instruction and the Emergence of Generative Production of Suffixes as Autoclitic Frames. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3363397/table/anvb-28-01-05-t03/

33. Sale, O S., Ghazali, O., & Al-Maatouk, Q. (2019, January 1). Graduation Certificate Verification Model: A Preliminary Study. Science and Information Organization, 10(7). https://doi.org/10.14569/ijacsa.2019.0100777

34. Sanghera, P. (2019, January 1). PMP® IN DEPTH PROJECT MANAGEMENT PROFESSIONAL CERTIFICATION STUDY GUIDE FOR THE PMP® EXAM

35. Staffa, D D N AN F S R M. (2014, January 1). The role of intrinsic motivations in attention allocation and shifting. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3978295/figure/F3/

36. Wermter, J Z A C S. (2014, January 1). Toward a self-organizing pre-symbolic neural model representing sensorimotor primitives. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3912404/figure/F3/

37. Zhiqiang, M X Y W Z Y B. (2022, August 18). A Secure and Efficient Data Deduplication Scheme with Dynamic Ownership Management in Cloud Computing

38. Zhiqiang, M X Y W Z Y B. (2022, August 18). A Secure and Efficient Data Deduplication Scheme with Dynamic Ownership Management in Cloud Computing. https://arxiv.org/abs/2208.09030