IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125182

SURVEY ON AN INTEGRATED ARCHITECTURE FOR MAINTAINING SECURITY IN CLOUD COMPUTING BASED ON BLOCKCHAIN

Prof Megha V, Chandana BR, M Vivek Mahanthesh, Surya Prathap S, Vaishnavi B

Dept. of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysore

Abstract: By enabling on-demand access to computer resources and services through the internet, cloud computing has completely transformed the IT sector. Yet, because of the centralised architecture of cloud services, the security and privacy of data have grown to be significant issues. Blockchain technology has been suggested as a potential remedy to address these problems by offering a secure and decentralised foundation for cloud computing. This review article overviews current work on a blockchain-based integrated architecture for preserving security in cloud computing. This study examines the many elements of the integrated architecture, such as security standards, blockchain technology, and cloud computing. The survey also examines the various methods for integrating permissioned and permissionless blockchains, smart contracts, and consensus mechanisms into cloud computing. The study research also covers the benefits and difficulties of incorporating blockchain technology into cloud computing, including interoperability, scalability, and data protection. The report also provides a comparative review of the current methods for cloud computing integration of blockchain technology based on several factors including security, performance, and cost-effectiveness. The survey paper's conclusions discuss the directions that research in this area should take going forward, emphasising the need for more investigation into how blockchain and cloud computing technologies can work together to improve the security, privacy, and effectiveness of cloud computing services.

Keywords — Blockchain, Cloud Computing, Decentralized, Smart Contracts, Data Privacy, Security, Scalability, Permissioned Blockchain

1. INTRODUCTION

By enabling online, on-demand access to computer resources and services, cloud computing has completely changed the IT sector. It is a desirable alternative for both enterprises and people because of a number of advantages it provides, including cost savings, scalability, and flexibility. However, the centralised architecture of cloud systems poses significant issues with regard to data security and privacy. The complex security concerns in the cloud environment cannot be fully addressed by conventional security techniques like firewalls and encryption.

Cloud computing is a popular choice for both organisations and people because it offers on-demand access to computer resources and services. It provides a number of advantages, including cost savings, scalability, and flexibility. However, the centralised design of cloud systems has led to significant worries regarding data security and privacy. Sensitive information, including financial transactions, private information, and proprietary corporate information, is stored in cloud systems. Because of its centralised architecture, cloud systems are susceptible to cyberattacks, data breaches, and other security risks since there is only one point of failure. The complex security concerns in the cloud environment cannot be fully addressed by conventional security techniques like firewalls and encryption.

A distributed ledger made possible by blockchain technology can securely record transactions and shield them from manipulation. It provides a decentralised, open, and unchangeable structure that can improve the security, privacy, and effectiveness of cloud computing services. Distributed consensus, smart contracts, and cryptographic algorithms are some of the salient characteristics of blockchain technology. Distributed consensus makes ensuring that all users of the network concur that a transaction is legitimate. Smart contracts streamline transaction negotiation and execution by acting as self-executing contracts. Data security and privacy are ensured by cryptographic techniques through data encryption and safe authentication.

Blockchain technology has been suggested as a potential remedy to address these problems by offering a secure and

DOI: 10.17148/IJARCCE.2023.125182

decentralised foundation for cloud computing.

The distributed, transparent, and immutable ledger that blockchain technology offers can securely store transaction data and guard against manipulation. The security, privacy, and effectiveness of cloud computing services can be improved by using blockchain technology. This survey article overviews current work on a blockchain-based integrated architecture for preserving security in cloud computing. We examine the many elements of the integrated architecture, such as blockchain, cloud computing, and security protocols. We examine the various methods employed to incorporate permissioned and permissionless blockchains, smart contracts, and consensus mechanisms into cloud computing.
Also covered are the benefits and difficulties of incorporating blockchain technology into cloud computing, including interoperability, scalability, and data privacy. Based on different factors including security, performance, and cost-effectiveness, we give a comparative review of the current methods for integrating blockchain technology into cloud computing.

2. BACKGROUND AND RELATED WORK

In this article [1], they suggest a taxonomy for blockchains and systems built on them. The taxonomy may be used to compare blockchains and to help with the creation and assessment of blockchain-based software systems. Our taxonomy covers the key blockchain architectural traits as well as the effects of various choices. This taxonomy is meant to aid in crucial architectural deliberations on the performance and quality aspects (such as availability, security, and performance) ofblockchain-based systems. Patterns are another method for categorising and organising the current solutions in addition to taxonomy. A new technology called blockchain enables the decentralized, transactional exchange of data across vast networks of untrusted users. This enables new distributed software architectures that enable shared state agreement without relying on a centralintegration point. Decentralization transfers power and authority from a central location. Bitcoin is a digital currency and its underlying technology is called the blockchain. Many banks are participating in blockchain technology experiments. The first use case explored is related to financial transactions, but there are others.

This study [2] provided an empirical analysis of a spam-based "stress test" DoS attack against Bitcoin. Our cluster-based methodology shows that 385,256 (23.41%) of a total of 1,645,667 bitcoin transactions were spam during the 10 days at the peak of the spam campaign. The attack also showed a 51% increase in average cost (from 45 to 68 satoshi/byte) and a 7x increase in processing latency for non-spam transactions (from 0.33 hours to 2.67 hours). It warns that changing Bitcoin's floor may reduce some of the spam patterns they've seen so far. Our results demonstrate the need for additional research into Bitcoin transaction spam filtering methods and other Bitcoin DoS mitigation solutions. This shows that a malicious party can perform a Bitcoin DoS if they are willing to distribute a small amount of Bitcoin (minimum$49,000). Other techniques such as “money drop” and transaction malleability they're used in his subsequent DoS attacks against Bitcoin resulting in poor performance. In contrast to other research looking for patterns in Bitcoin, our clustering method removesidentifying data and groups transaction attributes in order to detect patterns, as opposed to connecting transactions tode-anonymize individuals.

A homomorphic encryption scheme based on elliptic curve cryptography (HES-ECC) is proposed in this work [3] for secure data transmission and storage. This plan encrypts your data before storing it in the cloud. When you perform operations such as addition and multiplication on encrypted data stored in the cloud, the result is returned to the original data without being decrypted beforehand. This allows the cloud server to access only encrypted data, perform the necessary calculations, and perform the actions required by the user. This ensures the security of data storage and transmission.A modified Weil pairing is used in the proposedHES-ECC public key construction to provide additional homomorphic properties and encryption. Bilinear pairing is also used in HES-ECC for multiplicative homomorphic properties. The HES-ECC that has been presented is a system that merely makes use of the algebraic structure ofelliptic curves and pairings. Apart from those, no further computations, such as xor operations, hash functions, secure key distributors, trustworthy third parties, etc., are required. There is no way to see open messages in transit or in the public cloud. Safe communication is offered since plaintext is not utilised at any point throughout the process. The complexity of the ECDLP and the WDHP is the basis for the security of the encryption approach that they suggest to WDHP. As ensuring the security of cloud storage is our main objective, our encryption strategy makes use of homomorphic encryption techniques. The study also uses modified Weil pairing and bilinear pairing for the homomorphic property. Hence, ECDPL, WDHP, and the BDHP are the foundations for the security of homomorphic property BDHP.

This study [4] emphasises the OP RETURN special programming language instruction allows the Bitcoin protocol to save any data on the blockchain. A rising number of protocols take advantage of this functionality to expand the scope of uses for the Bitcoin network beyond money transfers. This essay is an empirical examination of OP RETURN's historical use. Based on OP RETURN, we distinguish a number of protocols, which we then categorise according to their

DOI: 10.17148/IJARCCE.2023.125182

application domain. We track the changes in utilisation over time, the distribution of OP RETURN transactions across application domains, and their space usage. Finally, they calculate the amount of OP RETURN information and theratio of OP RETURN transaction size to the total block chain transaction size. To the best of our knowledge, it is our duty to most thoroughly test OP RETURN usage. A tool that we have created serves as the basis for all of our analysis.

This study [5] emphasises symmetric algorithms with the goal of determining which one should be used for cloud-based applications and services that need link data and encryption. The paper provides a brief comparative

analysis and overview of cryptographic algorithms, focusing on the symmetric approach that should be used for cloud-based applications and services that require link data and encryption. The capacity to protect data from attacks and the speed and efficiency with which it does so are the two key characteristics that set one encryption method apart from another. Equally effective at safeguarding the transferred data across any communication medium are symmetric and asymmetric key methods. They weighed the advantages and disadvantages of the suggested and standard algorithms in relation to symmetric and asymmetric key cryptography. They have also examined the importance of these two cryptography methods. It has been determined thatBlowfish, AES, RSA, and DES are the finest security algorithms to use in cloud computing so that data is safe and not vulnerable to hackers. The issue of data disclosureis reduced by a method that was proposed, in which encryption is used to offer security while data is being transmitted. This system employed the idea of the RSA algorithm, Hash function, and only encoded data was communicated across the channel.

This study [6] suggests, a modular residue-based verification technique to validate homomorphic cryptographic computations. over the whole finite body. Depending on the underlying cryptosystems used, the performance of the proposed method has varied. However,according to the cryptosystems evaluated, this technique has a storage cost of 1.5% and a configurable computationcost of 1%. Such a cost is a reasonable compromise for cloud verification, which is very important for cloud computing. The modular residuals of the extrinsic computation are evaluated in this research in order to propose an effective DIV method for HE on Zp. The number of modules that may be employed is only constrained by the client's word count in the flexible and extendable architecture of the proposed approach. It is technically conceivable to have 264 modules on a 64-bit computer. The storage need on the client's computer is thus, based on 64-bit computers, less than 1.5% of thedata size saved on the CSP. If a check is applied to the homomorphic math, the worst computation cost incurred by the client on any of the tested cryptosystems is less than 3% of the actual homomorphic computation incurred by the CSP.

In this [7] study, the status of the UTXO sets is far from perfect right now, according to a review of the amount of unspent coins in three of the most well-known cryptocurrencies in the world. A subset of transaction outputs that have not yet been spent is known as an unspent transaction output (UTXO) set. According to a fee-per-byte rate f, the Bitcoin Core client treats a certain UTXO out as dust. According to their definition, an unprofitable output is one that, after just accounting for the amount of the input that would be required, has less value than the charge that must be paid. They provide twoindicators for determining if an output is worthwhile investing in. They provide two indicators to determine if amanufacturing operation is worth the investment. Following these measurements, Pérez-Solà and his colleagues analyze three sets of UTXOs of the three currencies listed above. More than 50% of the UTXOs in the collection can be considered dust for low charge-per-byte values of 116 satoshi/byte or more. The researchers argue that the discovery represents a first step in solving the problem of UTXO not being worth it. The researchers plan to create both tactics to encourage dust accumulation and discourage UTXO production.

Ben'msik University research team [8] led by Mouhib Ibtihal proposed a secure design to address the privacy issue of photos stored on his cloud servers. Create a private/public cloud infrastructure using an open-source project called OpenStack. They propose a hybrid architecture consisting of two clouds. The first is a privatecloud used only for encryption and decryption and the second is a public cloud used for storing encrypted images. Mobile cloud computing has emerged as a new technology that enhances the capabilities of mobile computing. MCC provides wireless customers with enhanced access to storage and reliability. In mobile cloudcomputing settings, an architecture is suggested in this research for safeguarding offloaded pictures. This architecture is built on the idea of encryption as a service, where encryption and decryption are handled exclusively by a private cloud. To demonstrate the scheme's functioning, they constructed the water treatment technique (DWT) and the Pailier cryptosystem, an additively homomorphic encryption scheme. As the encryption and decryption processes were quick, they discovered that they might be applied as a data security/privacy solution in such a setting.

3. LITERATURE REVIEW

Table 1 Relevant studies on advantages and disadvantages of various security methods in cloud computing

Related Studies	Advantages	Disadvantages	Description
	• Classification is	To publish a collection of design	

DOI: 10.17148/IJARCCE.2023.125182

[1]	informed by existing academic literature, technical forums, industry products, and our experience in blockchain usage and prototype development.	patterns for blockchain-based application development. We also intend to examine the models currently in use for distributed systems, peer-to-peer systems, and software in general, and determine if these models	A classification that encapsulatesthe most architecturally important characteristics of different blockchains has been proposed. It also indicates the quality categories supported byeach blockchain.
	● This is meant to serveas a foundation for designing blockchain-basedsolutions.	can be used for applicationsbased on blockchain or not.	
[2]	● A clustering-based technique was utilised to find spam transactions. ● Verified the clusteringdata and came up with a cautious estimate that during the campaign's peak 10-day period, 385,256 transactionswere spam.	They indicated that additional research into Bitcoin transaction spam filtering methods and other Bitcoin DoS mitigation solutionsis necessary.	An empirical analysis of a recent spam campaign that resulted in a denial-of-service assault on Bitcoin in this paper. Our investigation's goal is to comprehend spammers' tactics and how they affect Bitcoin users.
[3]	● The plan encrypts the data before storing it in the cloud. ● The cloud server can only access theencrypted data in order to run the necessary calculations and carry out the user's desired actions.	Although the hash function has drawbacks, safe hashing is necessary to prevent collisions since, without it, the encryption method is weak.	For safe data transit and storage, HES-ECC is suggested.
[4]	The special programming language instruction OPRETURN allows the Bitcoin protocol to store all data on the blockchain.	--	This article is an empirical examination of OP RETURN's historical use.
[5]	In this work, ways to use encryption to address severalissues with cloud computing security from the client and provider viewpoints were described.	--	Provides a review of 12 papers' literature.

DOI: 10.17148/IJARCCE.2023.125182

[6]	• Depending on theunderlying cryptosystems employed, the performance of thesuggested methodchanged. • Yet, according to the evaluated cryptosystems, thetechnique has a 1.5% storage overhead and a configurable 1% computing cost. Suchcost is a reasonabletrade-off for cloudcomputation verification, which is crucial for cloudcomputing.	Despite the fact that the scheme resolves the issue of ensuring the accuracy of the data calculations, the client may be required to supply storage space and additional labour to complete the verification step. Hence, in future work, we intendto move the verification process to distributed fog nodes that converse via consensus.	In order to enforce data confidentiality, privacy, andintegrity during an outsourced computation, this study suggests a verification technique based on the modular residue to authenticate homomorphic encryption computation over integer finite field.
[7]	The way each cryptocurrency is used differs somewhat and has various outcomes.	The issue of UTXOs that are not worthwhile spending. In this sense, we imagine designing both techniques to discourage the production of dust UTXOs and to reward dust consolidation.	The major three UTXO-based cryptocurrencies, Litecoin, Bitcoin Cash, and Bitcoin, have all had their UTXO sets thoroughly examined in this research. Our investigation reveals that the UTXO sets of the three cryptocurrencies exhibit both similarities and differences.
[8]	• RSA and IDEA are solely safe for the user, but AES and homomorphic are secure for the supplier as well. • AES is used to encrypt enormous amounts of data, is the best authenticity supplier, requires less Memory, and is faster than other methods.	To determine the best security algorithm, comparisons have been done.	The comparison is made using survey papers as a basis.

4. CONCLUSION

The topic of predicting flight delays using big data from the aviation industry and machine learning is active and expanding quickly. The way airlines and the aviation industry approach flight delay prediction may be revolutionised by the use of big data and machine learningtechniques. Regression analysis and ensemble approaches,among other classic statistical and machine learning algorithms, have all been recognised in the study as being utilised for predicting flight delays. The primary causes of flight delays have also been identified by the survey, including weather, airport operations, air traffic congestion, aircraft maintenance, staff scheduling, and passenger behaviour. Airlines can increase operational effectiveness, cut expenses, and offer a better customer experience by taking into account these elements and evaluating aviation big data.

Future advancements in machine learning algorithms and the incorporation of other data sources, including social media and real-time air traffic data, are key to improving the ability to anticipate flight delays. The trust and transparency of

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125182

flight delay prediction algorithms can also be improved by the application of interpretability and explainable AI approaches. Also, the inclusion of uncertainty and probabilistic modelling can produceforecasts that are more trustworthy and accurate.In conclusion, this analysis offers a thorough overview of the state of the art for machine learning and big data in aviation for predicting flight delays. The potential advantages of employing big data and machine learning approaches for flight delay prediction are substantial, evenif there are still difficulties and restrictions to be solved. As a result, ongoing research and development in this areawill unquestionably be essential to enhancing the effectiveness, dependability, and passenger experience of air transport.

REFERENCES

[1] Xu, Xiwei, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. "A taxonomy of blockchain-based systems for architecturedesign." In 2017 IEEE international conference on software architecture (ICSA), pp. 243-252. IEEE, 2017.

[2] Baqer, Khaled, Danny Yuxing Huang, Damon McCoy,and Nicholas Weaver. "Stressing out: Bitcoin “stress testing”." In Financial Cryptography and Data Security:FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers 20, pp. 3-18. Springer Berlin Heidelberg, 2016.

[3] Dogan, Demet Cidem, and Huseyin Altindis. "Storage and communication security in cloud computing using a homomorphic encryption scheme based Weil pairing." Elektronika ir Elektrotechnika 26, no. 1 (2020): 78-83.

[1] Bartoletti, Massimo, and Livio Pompianu. "An analysis of Bitcoin OP_RETURN metadata." In Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers 21, pp. 218-230. Springer International Publishing, 2017.

[2] Zaineldeen, Samar, and Abdelrahim Ate. "Review of cryptography in cloud computing." Int. J. Comput. Sci. Mobile Comput. 9, no. 3 (2020): 211-220.

[3] Awadallah, Ruba, Azman Samsudin, and Mishal Almazrooie. "Verifiable Homomorphic Encrypted Computations for Cloud Computing." International Journal of Advanced Computer Science and Applications 12, no. 10 (2021).

[4] Pérez-Solà, Cristina, Sergi Delgado-Segura, Guillermo Navarro-Arribas, and Jordi Herrera-Joancomartí. "Another coin bites the dust: an analysis of dust in UTXO-based cryptocurrencies." Royal Society open science 6, no. 1 (2019): 180817.

[5] Ibtihal, Mouhib, and Naanani Hassan. "Homomorphic encryption as a service for outsourced images in mobile cloud computing environment." In Cryptography: Breakthroughs in Research and Practice, pp. 316-330. IGI Global, 2020.