Blockchain as a Platform for Secure Cloud Computing Services

[1]Prof. Vishal Shinde, [2]Mr. Jas Verma, [3]Miss. Mayuri Pawar, [4]Miss. Ruchita Gaikwad
[1]Asst.Professor,[2,3]UG Student,[1,2,3]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharashtra, India. *[1]mailme.vishalshinde@gmail.com, [2]jazverma101@gmail.com,[3]pawar03.mayuri@gmail.com, [4]ruchigaikwad976@gmail.com*

Abstract - In recent years problems associated with cyber-attacks and privacy of data have increased which is resulting in the speedy growth of Cloud Computing. Secure cloud computing services gets connected on a blockchain platform with the support of this work, which is called cloud@blockchain, which enjoy the notoriety and unchangeable side of blockchain. Cloud@blockchain designs two functions- unidentified file sharing and evaluation to seek out illegally uploaded files. And all the data can be accessed by cloud users through smart contracts, and identify all users within the appliance layer with the support of cloud@blockchain. The three architectures- a pure and hybrid blockchain with cache and a standard database in accessing data is analysed. The residual show the generality of the hybrid blockchain with the hard over the pure blockchain and therefore the historical database, outperforms by 500% and 53.19%, respectively.

Keywords - Blockchain as a Platform, Secure Cloud Computing, Cyber-Attack, Privacy, Smart Contract.

I. INTRODUCTION

With the fastest growth of communication and computing technology, various cloud applications are developed. Most services like Google Drive, Dropbox or Mega are support centralized architecture, but the unreliability of centralized applications is clear. In one among foremost famous relevant cases, Facebook did not protect the privacy of its users, allowing country Cambridge Analysis company to get an outsized amount of user data, allegedly with the goal of influencing elections within the US. Two years ago, Taiwan's First Bank was the victim of an ATM heist after a Trojan was into the host within the bank's London branch. These two cases reveal that services that are controlled by one organization are at a risk of human error and bugs within the system, which might end in the loss of important data. To enhance data privacy, the EU passed The General Data Protection Regulation (GDPR), which is the most far-reaching bill on data privacy so far. How can vulnerability to attacks be reduced, the right to use data maintained, and the advantages of original services maintained? In this work, a secure cloud computing architecture that is based on blockchain technology,called cloud@blockchain, is designed. In cloud@blockchain, each node has a citizen business book. All transactions are recorded and anyone can confirm their integrity and legitimacy. A decentralized application on cloud@blockchain is designed to prevent file infringement, protecting privacy. The proposed cloud@blockchain can be used in many scenarios, including anonymous contest and digital certificate verification. In this study, two mechanisms that operate on cloud@blockchain are developed to improve upon existing cloud computing services.

II. AIMS AND OBJECTIVE

a) Aim:

Since 1991 Blockchain technology has been around. Its earliest discovery was confined to currency transactions but, it saw the latest developments and future in other financial and inter-organizational transaction areas back in 2014, studying the new opportunities. And now during some last few years, its adoption has increased across almost in every industry for different use cases and deployments.

b) Objective:

Blockchain technology is now getting plenty of attention. It can revolutionize, optimize the world infrastructure of technologies connected with one another through the web. The fields visiting to be influenced by it are:

●It creates a decentralized system, a totally transparent and hospitable database, which brings transparency to the elections and the governance and removes the satiation of central servers and provides interaction among counterparts.

It basically contains 4 elements.

1.Consensus: Gives the Proof Of Work (POW) also within the networks it also verifies the action.

 DOI : 10.35291/2454-9150.2022.0167

2.Ledger: Provides the entire details of transactions within networks.

3.Cryptography: It takes care of everyone networks and data in ledger also gets ciphered and only approved users can decipher the data.

4.Smart contract: It is accustomed to validate and verify the network's participants.

III. LITERATURE SURVEY

Paper 1: Quantifying Security & Privacy in Internet of Things Solutions:

There has been a large and rapid promotion of Internet of things solutions in many arenas as the Internet of things goes on maturing. Nevertheless, the safety and privacy of those solutions are often underrated. The shortage of protection and seclusion within the solutions can cause catastrophic results, especially in sensitive domains like healthcare. Therefore, the insuring the protection and uniqueness is crucial. And while evaluating the protection and seclusion of the solutions it is seen that many stakeholders often find themselves unguided. This study proposes a framework to compare the privacy and protection in Internet of things solutions and make quantitative analyses using Investigative Hierarchy Process.

Paper 2: Security and Privacy in Decentralized Energy Trading through Multi signatures, Blockchain & Anonymous Messaging Streams:

The complication of contingent proceedings security in localised smart framework energy trading without dependence on reliable third parties. Using Blockchain technology a proof-of-concept for dispersed energy trading system has been implemented, incognito encrypted messaging streams and multi signatures, authorizing peers to anonymously work out energy prices and securely perform trading transactions. We conducted case studies to perform security analysis and performance evaluation within the context of the elicited security and privacy requirements.

Paper 3: Sora Identity Secure, Digital Identity on the Blockchain:

Digital integrity is the foundation of a mainframe discretion. Although, proving identity vaguely is difficult to try. Now, to it complicate, identity is sometimes not a worldwide, total build, but the data differs according to the various parties it is shared with, supporting the connection to the user. Therefore, a practical answer for digital identity should enable users to own full power over their exclusive data and be able to share only the data that they want to share with each service.

IV. EXISTING SYSTEM

In the existing system services like Google Drive, Dropbox or Mega are supported by centralized architecture, but the unreliability of centralized applications is obvious. In one among the foremost famous relevant cases, Facebook did not protect the privacy of its users, allowing British Cambridge Analysis company to get an outsized amount of user data, allegedly with the goal of influencing elections within the US. Two years ago, Taiwan's First Bank was the victim of an ATM heist after a Trojan was into the host within the bank's London branch. These two cases reveal that services that are controlled by one organization are prone to human error and bugs within the system, which may lead to the loss of private property.

V. COMPARTIVE STUDY

Table 1. Comparative Analysis

SR NO.	PAPER TITLE	AUTHOR NAME	METHOD	ADVANTAGE	DISADVANTAGE
1.	Quantifying Security & Privacy in Internet of Things Solutions.	F. Alsubaei, A.Abuhussein and S. Shiva pp.1-6, Taiwan, April 2018	Based on M2M connection.	Minimizes the human work and effort.	Increased privacy concerns
2.	Security and Privacy in Decentralized Energy Trading through Multisignatures, Blockchain & Anonymous Messaging Streams..	N. Zhumabekuly Aitzhan and D. Svetinovic Vol.15, No.5, pp.840-852, 2016.	Based on transactions on dependable and secure computing .	Availability , Reliability, Safety and Integrity	Faults, Errors and Failures
3.	Sora Identity: Secure, Digital Identity on the Blockchain.	M. Takemiya and B. Vanieiev Pp.582-587, Japan, July 2018.	Based on 42nd annual computer software and applications conference.	Trust, Security, Simplicity and Privacy	Cyberattacks and Fraud
4.	Security Services Using Blockchains: A State of the Art Survey.	T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka Vol .21, No.1, pp.858-	Based on security services using blockchains.	Secure Transactions, Instant Transactions and No third party interference.	Difficulty of Development, Crime, Human Error.

 DOI : 10.35291/2454-9150.2022.0167

		880, 2019.			
5.	Blockchain as a Service (BaaS): Providers and Trust.	J. and J.D Michels Pp.67-74, UK, April 2018.	Based on blockchain as a service(BaaS).	Transparency, Time and Money, Focus on Features and Testing.	Lack of knowledge, Still new, Energy Use, Compliance issues.

VI. PROBLEM STATEMENT

Power Outages, menial or home computer crashes, cyberattack, universal calamity, and representative vandalize all present severe concern to the aspect of the field. And yes absolutely, cloud solutions cannot totally abolish all the hazard, but surely it can secure you from what you've got straight away. But there are some matters like cloud confrontation for design, management, security, availability of skill sets, consumers and more in the future. All these problems are directly associated with some of their features of concurrency, remoteness, abstraction, distribution, etc and there's nothing wrong. Anything has both pros and cons sides. you've got to either adjust with the limitations, or perhaps refuse to generate control of a selected product. And cloud computing isn't any exception. Let's observe their problems and claims existing now. The major problem is the transfer of existing applications to the "cloud". Firstly, this is often not always possible thanks to the planning of a specific application, its cording to various other systems, solutions or services that can hardly be moved to the "clouds" till today.

VII. PROPOSED SYSTEM

In the proposed system user data is protected against unauthorized access by account-based security procedures. The blockchain-based cloud computing differs from traditional computing in many application scenarios and aspects of data transactions. In the proposed architecture, which comprises Blockchain, Smart Contract, Cloud Storage and file owners. The overall system consists of the operating system, a fully functional application and a signal function unit, a flat design and all applications are based on the blockchain platforms, which are called "user". Smart Contract is the mediation layer that is used for communication. Smart Contract can process and store metadata uploaded by the owner. On the user side, any cryptographic algorithm, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), can be used to quickly confirm the identity of the owner.

VIII. ALGORITHM

The general idea of working of proposed system algorithms is given as follows:

Consensus Algorithm:
Step 1: Start
Step 2: Validator stakes some amount of money
Step 3: Validator is chosen
Step 4: Validator creates a block
Step 5: Is Block valid?
Step 6: If no then, reward and stakes amount
Step 7: If yes then, Block is combined to the blockchain
Step 8: Validator recieves reward and staked amount
Step 9: End

Consensus Classification:
Step 1: Start
Step 2: Miners group the transactions mass that need to be verified
Step 3: Server generates Mathematical puzzle
Step 4: Miners compete to solve the problem
Step 5: First one to solve the solution sends the block to the network
Step 6: Validator stakes some amount of money
Step 7: Validator is randomly chosen
Step 8: Mined block is assigned to a group of validators to verify
Step 9: Is Block valid?
Step 10: If no then, reward and stakes amount
Step 11: If yes then, Block is combined to the blockchain
Step 12: Miners and Validators recieves reward and staked amount
Step 13: End

IX. MATHEMATICAL MODEL

Consensus Algorithm:

A consensus algorithm may be a process in engineering want to achieve agreement on one data value among distributed processes or systems.

In order to perform the mathematical analysis of the consensus algorithms and to spot the foremost priority algorithm for implementation within the financial sphere, an algorithm efficiency parameter was introduced, which is determined based on proportion of the common time of generation of the transaction, the confirmation delay, and also the numeral executions per second:

$$F = C * TPS/ V$$

where V is that the average transaction generation time, which determines the time for which the new block is combined to the ledger (registry); TPS is that the numeral executions per second; and C is that the transaction confirmation delay. The average time for the creation of the new block V determines the time for which this new block are going to be added to the registry and shows the block processing speed.

 DOI : 10.35291/2454-9150.2022.0167

Consensus Classification:

The common consensus algorithm is classified as follows: PoW, PoW + PoS, DPoS, PoS, BF, DAG and other.

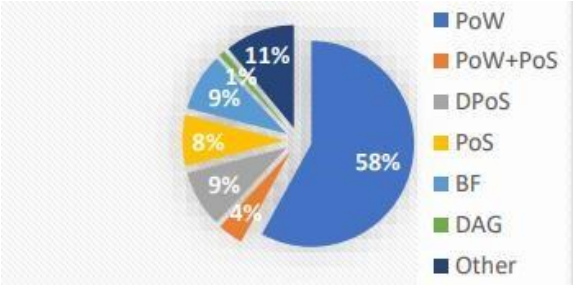

Figure 1: Percentage distribution of the uttermost leading consensus algorithms.

X. SYSTEM ARCHITECTURE

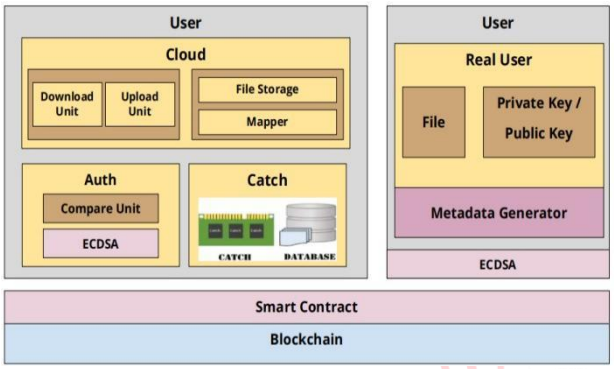

Figure2: Proposed cloud@blockchain architecture

Description:

It represents proposed cloud@blockchain architecture, including Blockchain, Smart Contract, Cloud Storage and file owner. The system consists of the operating system, a fully functional application and a signal function unit. It has a flat design and all applications are based on the blockchain platform, which are called "user". Smart Contract is the mediation layer used for communication. It can process and store metadata uploaded by the owner. On the user side, any cryptographic algorithm, like the Elliptic Curve Digital Signature Algorithm (ECDSA), is used to confirm the identity of the data owner quickly. Users (cloud side) can provide online storage services, having received an upload request from the owner (user side). The cloud storage facility can verify the owner's permission through the authentication unit, the upload unit, the file storage unit and the mapper. The blockchain preserves the anonymity of owners while remaining accessible for open consultation by public. Although nothing is totally secure, tampering with blockchain is almost impossible.

XI. ADVANATGES

- Helps solve complex real-world problems with several constraints.
- Manage problems like, having little oral most no labeled data availability.
- Ease of transferring knowledge from one model to another based on domains and tasks.
- Without any human intelligence, it detects the important feature on its own.
- In less quantity of data, we can achieve more accuracy.

XII. DESIGN DETAILS

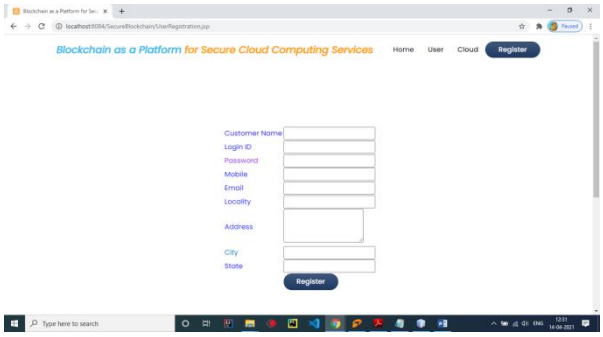

Figure3 : Cloud User Registration

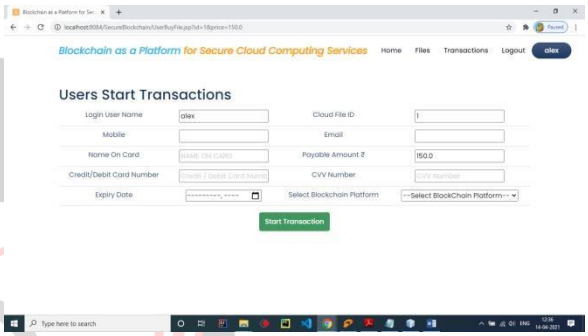

Figure4: User Buy File

XIII. CONCLUSION

Thus, we have tried to implement the paper,Wang-You Tsai, Tzu-Chuan Chou, Jiann-Liang Chen, Yi-Wei Ma, Chen-Jui Huang,"Blockchain as a platform for secure cloud computing services", ICACT 2020 and according to the implementation, this work develops a cloud@blockchain platform making two main contributions:

(1) An anonymous file sharing mechanism which provides privacy, data sharing.

(2) A mechanism for inspecting files identifying illegal uploads. These both are combined, and file sharing is performed to achieve real power dispersion and data sharing. An analysis reveals The proposed cloud@blockchain is feasible. Although it performs 0.88 times with the traditional database solution, the user experience is as expected.

REFERENCES

[1] Wang-You Tsai, Tzu-Chuan Chou, Jiann-Liang Chen, Yi-Wei Ma, Chen-Jui Huang,"Blockchain as a platform for secure cloud computing services", ICACT 2020

[2] F. Alsubaei, A. Abuhussein and S. Shiva, "Quantifying Security and Privacy in Internet of Things Solutions,"

 DOI : 10.35291/2454-9150.2022.0167

Proceedings of the IEEE/IFIP Network Operations and Management Symposium, pp.1-6, Taiwan, April 2018.

[3] M. Takemiya and B. Vanieiev, "Sora Identity: Secure, Digital Identity on the Blockchain," Proceedings of the IEEE 42nd Annual Computer Software and Applications Conference, pp.582-587, Japan, July 2018.

[4] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda and V. Santamaria, “To Blockchain or Not to Blockchain: That is the Question,” IT Professional, pp.62-74, March/April 2018.

[5]Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Bitcoin Organization, 2008.

[6] R. Henry, A. Herzberg and A. Kate, Blockchain Access Privacy: Challenges and Directions, IEEE Security & Privacy, Vol.16, No.4, pp.33-45, July/August 2018.

[7] N. Kshetri and J. Voas, “Blockchain-enabled E-voting,” IEEE Software, pp.95-99, July/August 2018.

[8] V. Sharma, “An Energy-Efficient Transaction Model for the Blockchain-Enabled Internet of Vehicles (IoV),” IEEE Communications Letters, Vol.23, No.2, pp.246~249, February 2019.

[9] M.P. Andersen, J. Kolb, K. Chen, G. Fierro, D.E. Culler and R.A. Popa, WAVE: A Decentralized Authorization System for IoT via Blockchain Smart Contracts, EECS

Department, University of California, Berkeley, 2017.

[10] T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, “Security Services using Blockchains: A State of the Art Survey,” IEEE Communications Surveys & Tutorials, Vo.21, No.1, pp.858-880, 2019.

 DOI : 10.35291/2454-9150.2022.0167