International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

Implementation of Dynamic Replication Integrated Blockchain for Security in Cloud Environment

Kapil Aggarwal, S. K. Yadav

Abstract*— Cloud Computing is one of the key domains with the specific focus towards the security and integrity. For enforce the security and integrity, a number of approaches can be implemented but the integration of Blockchain Technology is quite novel and effectual. The information replication is one of the key errands during the database security and accessibility and for this there is have to incorporate the blockchain innovation with the security viewpoints. In current situation, the blockchain innovation is increasingly engaged towards digital forms of money in which the appropriated record is kept up for the exchanges. The dispersed record alludes to the recreated, synchronized and shared computerized resource for various areas and gadgets with the goal that the outsider control can't be conceivable. For instance, if a bank pursues the disseminated database record with blockchain innovation can uphold higher level of security. In the event that that bank is having one million clients, at that point the records of the exchanges will be put away on those one million gadgets. It alludes to the way that the programmer should hack one million gadgets continuously as opposed to a solitary server. This is the real preferred position of utilizing the decentralized blockchain technology. In instance of incorporated application, in the event that programmer enters the server of a bank, at that point every one of the subtleties and records of the considerable number of clients can be replicated. That is the principle reason on account of which the administration organizations should concentrate on decentralizing their electronic applications. In this research manuscript, the security parts of cloud databases are proposed to be advanced utilizing the blockchain innovations towards the specific scenarios integrated with the cloud applications.

Keywords : Blockchains; Cloud Security; Cryptocurrency; Cryptography; Data Replication.

I. INTRODUCTION

The Cloud Applications are now days in huge prominence and widely used with the assorted key points but there is need to enforce the security in assorted dimensions [1, 2]. This domain is the key domain of research in the related aspects. These cryptographic types of cash join BitCoin, Ethereum, LiteCoin, Zcash, PeerCoin and various others [3, 4]. These blockchain based advanced monetary forms don't have any most of the way bank or portion entryway to record the log of the trades. That is the standard reason due to which various countries are not allowing the computerized types of cash as real money trade.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Kapil Aggarwal*, Research Scholar, Department of Computer Science & Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India. Email: kapil594@gmail.com
S. K. Yadav, Vice President & Director Research, Department of Computer Science & Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India. Email: drskyadav@hotmail.com

Everything considered, these blockchain based advanced monetary forms are commended and used because of enormous security features [5, 6, 7]. Following are the key aspects associated with the domain and the segments with this area.

Fig. 1. Dimensions of Cloud Security

The blockchain sort out is having a huge number of replicated records with the secured algorithms in which each and every record is connected with the dynamic cryptography so all of the trades can be encoded with no probability of sniffing or hacking attempts [8, 9].

II. NEED OF SECURITY IN CLOUD

A. E-Governance Applications

The applications of blockchain applications are not limited for corporate but also for the government applications including e-governance and e-citizen applications.

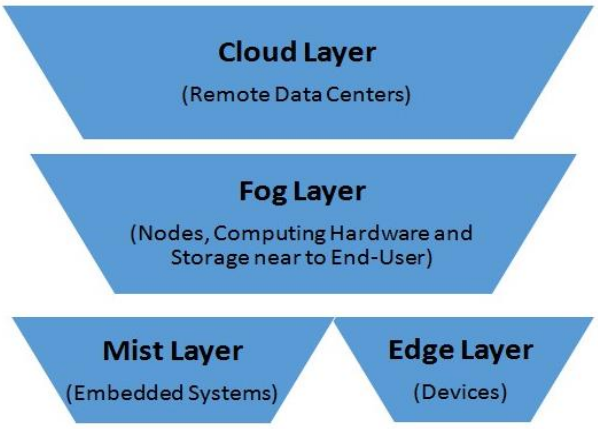

Fig. 2. Layered Approach with Cloud Environment

B. Decentralized Applications

The key base of secured blockchain applications is the decentralized applications or dApp in which the blockchain deployment is done on enormous systems to ensure the security and integrity. According to the examination investigation and reports from Statista.com, the size of BitCoin blockchain from year 2010 to current year 2019 and that is having tremendous use all through the globe.

Fig. 3. Associated Aspects with Cloud

The decentralized application (dApp) alludes to the product application that executes on the appropriated channels with the goal that the hacking of use will be close to incomprehensible. In conventional incorporated application, the application is sent on a solitary server [10, 11]. The fundamental constraint with incorporated methodology is that on the off chance that that brought together server is hacked; at that point everything can be harmed or duplicated from that server [12, 13, 14, 15, 16].

Fig. 4. IBM Bluemix Based Cloud

In the situation of decentralized application, the programmer should break every gadget which belongs to that application and that will be exceptionally troublesome continuously utilizing shrewd contracts.

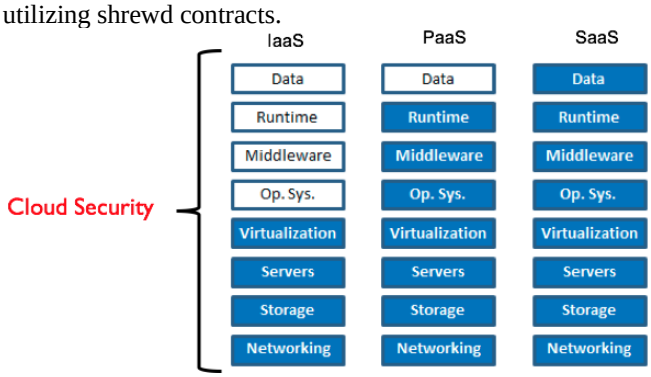

Fig. 5. Cloud Security

In shrewd contracts based dApp, the dynamic token sharing is actualized with the goal that the exchanges will have greatest safety efforts.

III. DYNAMIC BLOCKCHAINS FOR SECURITY IN CLOUD ENVIRONMENT

The cloud platforms using the blockchains make use of the smart contract programming in which every transaction is getting recorded and validated. The smart contract writing computer programs is required for the globalization based exchanges. It implies that the exchanges should be possible over the general population who can't impart on account of various landmasses, dialects and customs. Smart Contracts consequently approve the exchanges and business dealings between the general populations who can't comprehend the language of one another.

Robustness is one of the amazing and elite programming languages for composing smart contracts. It pursues item situated programming worldview with higher level of security and execution which can be incorporated with arranged blockchain stages. The code of robustness is gathered and changed to bytecode which is executed on Ethereum Virtual Machine (EVM) [19, 20]. Robustness Programming is having the key base of numerous programming dialects and contents including Python, JavaScript, C++ so it tends to be incorporated to various conditions and stages for joining with blockchains. To work with Solidity Programming, there are many Integrated Development Environments (IDEs) and Editors which can be utilized including Remix, EthFiddle, JetBrains and numerous others [21, 22].

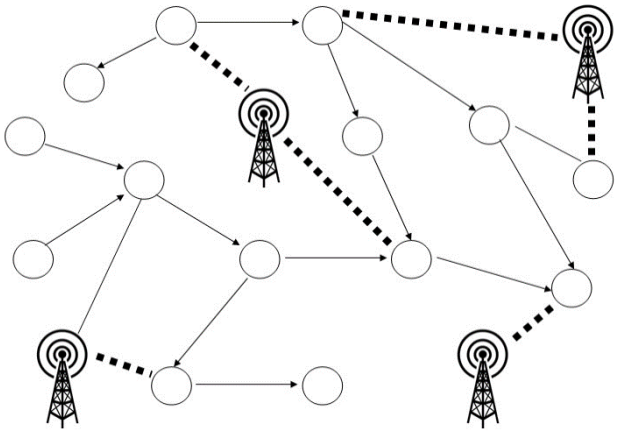

Fig. 6. Cloud Aspects with Network Applications

To begin with Solidity Programming, Remix is one of the ground-breaking IDEs that is open source and furthermore gives the electronic interface. The electronic interface of Remix IDE is simple for the engineers to make the Smart Contracts with Blockchain Programming [23, 24, 25].

The URL of Web Based Remix IDE is remix.ethereum.org that can be gotten to legitimately on the internet browsers for composing, ordering and executing the smart contracts.

```
Cpragma strength ^0.4.18;
contract MyCloud {
string open name = 'GCloud';
/Name of the New Cloud
string open CloudName = 'Cloud1.0';
/Select Cloud
map (dc => uint) VMs;
/Key-Value Pair for Dc-Account
occasion Transfer(dc _sender, dc _receiver, uint256 _value);
/Log Recording
constructor() open {
/Constructor on Creating the Contract
VMs[msg.sender] = 100000;
/VM Confirmation
}
```

work sendCloudlet(dc _receiver, uint _Cloudlet) open returns(bool adequate) {
in the event that (VMs[msg.sender] < _Cloudlet) return false;
/Authentication of the Transfer
VMs[msg.sender] - = _Cloudlet;
VMs[_receiver] += _Cloudlet;
emanate Transfer(msg.sender, _receiver, _Cloudlet);
/Commit of Payment Transfer with Transaction Recording
return genuine;
}
work getVM(dc _addr) general visibility returns(uint) {
/Checking the VM
return VMs[_addr];
}
}

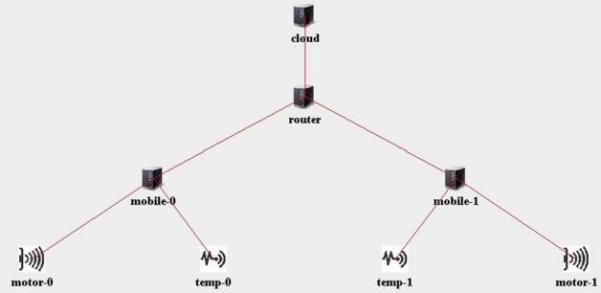

Fig. 7. Cloud Integrated Transmission

IV. SIMULATION RESULTS

The presented approach is making use of NodeJS is the key library and framework for the integration patterns. NodeJS is a cross-stage open source stage for JavaScript based programming. It tends to be utilized for the improvement of various applications including Blockchain Development, Smartphone Applications, Distributed Web Applications, NoSQL Processing, Big Data Analytics, Machine Learning, Internet of Things (IoT) and numerous others identified with cutting edge registering [26, 27].

For blockchain programming, NodeJS is coordinated with Web3JS. Web3JS alludes to the arrangement of libraries and instruments for cooperation with blockchain based associations [32].

The Web3JS Platform for blockchains and dApp can be coordinated with adhering to directions npm: npm introduce Block3 unadulterated js: interface the dist/Block3.min.js meteor: meteor include ethereum:Block3

After establishment, the code in JavaScript and Server Side Scripts is composed with the smart contracts and organization for the verified applications.

Truffle is another programming suite for the advancement of blockchain based smart gets that can be introduced with NodeJS and can be executed on Ethereum Virtual Machine (EVM) [28].

With the execution of adhering to guidance, the Truffle Suite is related with NPM

npm introduce - g truffle

After establishment of Truffle, the adaptations of introduced rendition can be checked in the terminal

truffle rendition

The new task Cloudblockchain in Truffle can be mapped as

mkdir Cloudblockchain
album Cloudblockchain
truffle Cloudblockchain

In Truffle, the accompanying catalog structure is pursued to code the application

- migrations/: Migration System and Handlers for the Smart Contracts
- truffle.js: Configuration File for Truffle
- contracts/: Source Code for the Smart Contracts
- test/: Tests and JavaScript Code
- Cloudblockchain: Additional Folders and Files required for coding the blockchain

Another document <filename.sol> is made in contracts/registry for the base coding of smart contracts in the accompanying arrangement

Cpragma strength ^0.5.0;
contract Mysmartcontract {
}
Sending Signals
work adopt(uint MyVar) open returns (uint) {
require(MyVar >= 0 && MyVar <= 15);
adopters[MyVar] = msg.sender;
return MyVar;
}

The gathering of Truffle Code is done as pursues

truffle aggregate

The structure of Embark gives the apparatuses and libraries to advancement of decentralized applications so that blockchain based usage should be possible [29, 30, 31]. Leave can be utilized as another to Truffle. To work with Embark, there is have to incorporate Node Version Manager (NVM) having different renditions of NodeJS.

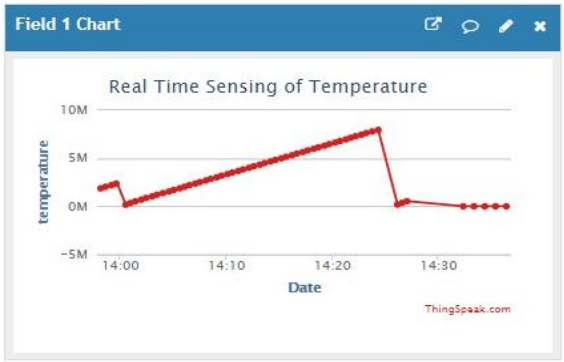

Fig. 8. ThingSpeak Based Secured Cloud

Utilizing "set out run", the dashboard of Embark is conjured
The token age can be additionally written in code
Cpragma solidityversion;
import "openzeppe-solidit/contract/tkn/ERZC20.sol";
contracts CryptoBaseToken EZRC20 {
constructor() open {
}
}

Table- I: Simulation vs. Performance

Simulation Attempt	Accuracy Factor	Cumulative Performance
1	99	98
2	99	98
3	96	99
4	98	98
5	97	99
6	99	99

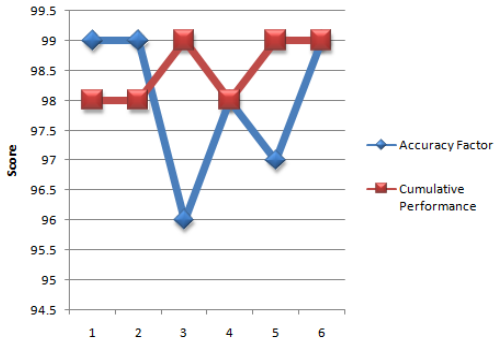

Fig. 9. Blockchain Integrated Performance

As in the model with the blockchain integrated the overall performance and accuracy can be elevated to higher levels so that the cumulative performance shall be effectual. It very well may be anything according to the necessities of the smart contract related with the blockchain in the cloud environment.

V. CONCLUSION

The domain of cloud security and integrity with the cryptography is quite novel and needs huge elevation in the performance. The integration of approaches and algorithms of blockchain technology can provide the higher degree of accuracy with this approach. The presented work is depicting the usage patterns of blockchain based approach for the higher degree of accuracy and cumulative performance.

REFERENCES

1. Liiang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L., "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing, IEEE Press, May 2017, pp. 468-477.
2. Xiia, Q. I., Siffah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M., "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol.5, 2017, pp. 14757-14767.
3. Sharma, P. K., Chenn, M. Y., & Park, J. H., "A software defined fog node based distributed blockchain cloud architecture for IoT," IEEE Access, vol. 6, 2017, pp. 115-124.
4. Yuee, X., Wang, H., Jin, D., Li, M., & Jiang, W., "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, vol. 40, no. 10, 2016, pp. 218.
5. Xia, Q., Siffah, E., Smahi, A., Amofa, S., & Zhang, X., "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," Information, vol. 8, no. 2, 2017, pp. 44.
6. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R., "Blockchain: A panacea for healthcare cloud-based data security and privacy," IEEE Cloud Computing, vol. 5, no. 1, 2018, pp. 31-37.
7. Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V., "Blockchain-based database to ensure data integrity in cloud computing environments," 2017.
8. Samaniego, M., & Deter, R., "Blockchain as a Service for IoT," in IEEE International Conference on Internet of Things (iThings), IEEE, Dec. 2016, pp. 433-436.
9. Toosh, D. K., Shetty, S., Liang, X., Kamhoua, C. A., Kwiat, K. A., & Njilla, L., "Security implications of blockchain cloud with analysis of block withholding attack," in Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, IEEE Press, May 2017, pp. 458-467.
10. Kshetrii, N., "Can blockchain strengthen the internet of things?," IT Professional, vol. 19, no. 4, 2017, pp. 68-72.
11. Yaang, C., Chen, X., & Xiiang, Y., "Blockchain-based publicly verifiable data deletion scheme for cloud storage," Journal of Network and Computer Applications, vol. 103, 2018, pp. 185-193.
12. Lii, Z., Barenji, A. V., & Huang, G. Q., "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform," Robotics and Computer-Integrated Manufacturing, vol. 54, 2018, pp. 133-144.
13. Stanciu, A., "Blockchain based distributed control system for edge computing," in 21st International Conference on Control Systems and Computer Science, IEEE, May 2017, pp. 667-671.
14. Anjumm, A., Sporny, M., & Sill, A., "Blockchain standards for compliance and trust," IEEE Cloud Computing, vol. 4, no. 4, 2017, pp. 84-90.
15. Liiang, X., Zhao, J., Shetty, S., Liiu, J., & Li, D., " Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, IEEE, Oct. 2017, pp. 1-5.
16. Hu, S., Cai, C., Wang, Q., Wang, C., Luo, X., & Ren, K., "Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization," in IEEE INFOCOM 2018-IEEE Conference on Computer Communications, IEEE, Apr. 2018, pp. 792-800.
17. Waang, H., & Song, Y., "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," Journal of medical systems, 2018, vol. 42, no. 8, pp. 152.
18. Shaffagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S., "Towards blockchain-based auditable storage and sharing of IoT data," in Proceedings of Cloud Computing Security Workshop, ACM, Nov. 2017, pp. 45-50.
19. Kaur, H., Alaam, M. A., Jameel, R., Mourya, A. K., & Chang, V., "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. Journal of medical systems,", vol. 42, no. 8, 2018, pp. 156.
20. Singh, I., & Le, S. W., "Comparative requirement analysis for the feasibility of blockchain for secure cloud," in Asia Pacific Requirements Engeneering Conference, Springer, Nov. 2017, pp. 57-72.
21. Zikratov, I., Kuzzmin, A., Akimenko, V., Niculichev, V., & Yalansky, L., "Ensuring data integrity using blockchain technology," in 20th Conference of Open Innovations Association (FRUCT), IEEE, Apr. 2017, pp. 534-539.
22. Li, J., Wu, J., & Chen, L., "Block-secure: Blockchain based scheme for secure P2P cloud storage," Information Sciences, vol. 465, 2018, pp. 219-231.
23. Swan, M., "Blockchain: Blueprint for a new economy.," O'Reilly Media, Inc., 2015.
24. Xiong, Z., Feng, S., Waang, W., Niyato, D., Wang, P., & Han, Z., "Cloud/fog computing resource management and pricing for blockchain networks," IEEE Internet of Things Journal, 2018.
25. Woodside, J. M., Augstine Jr, F. K., & Giberson, W., "Blockchain technology adoption status and strategies," Journal of International Technology and Information Management, vol. 26, no. 2, 2017, pp. 65-93.
26. Kuo, T. T., Kiim, H. E., & Ohno-Machado, L., "Blockchain distributed ledger technologies for biomedical and health care applications," Journal of the American Medical Informatics Association, vol. 24, no. 6, 2017, pp. 1211-1220.
27. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P., "Blockchain for IoT security and privacy: The case study of a smart home," in IEEE international conference on pervasive computing and communications workshops (PerCom workshops), IEEE, Mar. 2017, pp. 618-623.

AUTHORS PROFILE

Kapil Aggarwal is pursuing Ph.D. Computer Science and Engineering from Shri JagdishPrasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India. He is a renowned researcher and obtained B.E. from Nagpur. His key domains of research includes Wireless Networks, Cloud Computing, Internet of Things (IoT) and related aspects.

Dr. S. K. Yadav is one of the key academicians and researchers in the domain of computer science and engineering. He is the working as Director Research in Shri JJT University, Rajasthan, India. He is having the experience of more than 20 years in research and development with the membership of IETE and AIMA.