



Article Title: Enhancing Data Security in Cloud Computing using Block chain

Enhancing Data Security in Cloud Computing using Block chain

Divya S¹, Gini R²

¹Student, Department of MCA, Narayanaguru College of Engineering, Anna University, Chennai.

²Assistant Professor, Department of MCA, Narayanaguru College of Engineering, Anna University.

ABSTRACT

Block chain (BC) and Software Defined Networking (SDN) are some of the most prominent emerging technologies in recent research. These technologies provide security, integrity, as well as confidentiality in their respective applications. Cloud computing has also been a popular comprehensive technology for several years. Confidential information is often shared with the cloud infrastructure to give customers access to remote resources, such as computation and storage operations. However, cloud computing also presents substantial security threats, issues, and challenges. Therefore, to overcome these difficulties, we propose integrating Block chain and SDN in the cloud computing platform. In this research, we introduce the “DistB-SD Cloud” architecture to better secure clouds. Moreover, we leverage a distributed Block chain approach to convey security, confidentiality, privacy, integrity, adaptability, and scalability in the proposed architecture. BC provides a distributed or decentralized and efficient environment for users. Also, we present an SDN approach to improving the reliability, stability, and load balancing capabilities of the cloud infrastructure. Finally, we provide an experimental evaluation of the performance of our SDN and BCbased implementation using different parameters, also monitoring some attacks in the system and proving its efficacy.

Keywords: Block chain, SDN, Security, Privacy, Open Flow, SDN-Controller, Data Security, Cloud Computing, and Cloud Management.

1 Introduction

In today's interconnected world, cloud technology is seen as a crucial enabler of IT industry innovation. It is a model that provides consumers with various on-demand services, and network access to shared databases of physical resources such as computation and storage. In this way, customers do not have to buy expensive hardware anymore, they can access these services using commodity hardware (such as a laptop) connected to the Internet, giving them the means to develop solutions to complex problems. Furthermore, cloud computing enables users to access resources from any location remotely, allowing for virtual collaboration. It enables users to improve resources relatively quickly; previously, this was time-demanding with traditional hardware-based computing systems. Proper resource usage aids in mitigating the over and under-utilization problem [1]. Cloud computing provides a range of services like Software as a Service, Platform as a Service, and Infrastructure as a Service, which are in



Article Title: Enhancing Data Security in Cloud Computing using Block chain

short known as SaaS, PaaS, IaaS respectively. Also, cloud services are scalable, flexible, and reliable on-demand for users [2], [3]. Another technology is Block chain, but it has a focus on security. For this reason, Block chain technology has attracted particular interest in the financial environment, and in general wherever data security is of topmost priority. Block chain with the addition of secret sharing security enhancement is possible in cloud services with the improvement of data security [4]. Further, Block chain technology helps detect malicious use by enforcing a distrustful provider to detect suspicious suppliers [5].

In this architecture, a hash value is generated to secure the information transmitted through the Block chain structure. Further, Block chain stores the information in a public ledger where any change can be noticed by others connected to the ledger. This is why no third party can disturb the transaction [6]. Furthermore, as cloud computing is interconnected with many security issues and financial transactions, Block chain can strengthen the reliability of the cloud computing functionalities [7]. Another emerging paradigm is SDN [8], which makes network management is straighter forward. It has found extensive application in cloud computing, where networks are challenging to manage and troubleshoot. As already stated, network performance is crucial to the quality of service of the final users, who access shared resources provided over the Internet. Another emerging technology is an SDN used to control a network employing some program. With the use of an SDN, it is easy to manage network issues, as cloud computing is full of network issues. Without the network, cloud computing is nothing since the resources will be shared and provided to the users over the Internet. Recent applications of SDN employ multiple controllers, adding a new dimension to the network of devices.

2 Related Works

[1] Enhancing security of cloud storage through block chain-based sdn in IoT network.

In 2020, A. Rahman, M. J. Islam, M. Saikat Islam Khan, S. Kabir, A. I. Pritom, and M. Razaul Karim, , demonstrated on a novel method software Defined Networking (SDN) and Block chain (BC) are the most recent research trends in emerging technology. These technologies have currently been used in the IoT networking environment for various purposes, such as protection, stability, scalability, confidentiality, and so on. Such techniques can be used in this regard to effectively provide security, privacy, and confidentiality to cloud storage. In this paper, the authors proposed Block-SDoTCloud architecture to significantly enhance security within the cloud storage network. In order to give the cloud storage environment the requisite facilities, two leading technologies, i.e., SDN and Block chain were applied. The centralized SDN controller provided the proposed model with tremendous reliability, versatility, and load balancing in one side while on the other hand, a distributed Block chain created a deep trust between the transaction levels resulting into effective protection for the presented scheme. The efficiency of the proposed architecture is justified through close observation of simulation with a careful selection of relevant parameters.



Article Title: Enhancing Data Security in Cloud Computing using Block chain

[2] Block chain security in cloud computing Use cases, challenges, and solutions. In 2017 J. H. Park and J. H. Park, demonstrated on a novel method block chain has drawn attention as the next-generation financial technology due to its security that suits the informatization era. In particular, it provides security through the authentication of peers that share virtual cash, encryption, and the generation of hash value. According to the global financial industry, the market for security-based block chain technology is expected to grow to about USD 20 billion by 2020. In addition, block chain can be applied beyond the Internet of Things (IoT) environment; its applications are expected to expand. Cloud computing has been dramatically adopted in all IT environments for its efficiency and availability. In this paper, we discuss the concept of block chain technology and its hot research trends. In addition, we will study how to adapt block chain security to cloud computing and its secure solutions in detail.

[3] Cloud based secure service providing for IoT's using block chain. In 2019 M. Rehman, N. Javaid, M. Awais, M. Imran, and N. Naseer demonstrated on a novel method internet of Things (IoTs) is widely growing domain of the modern era. With the advancement in technologies, the use of IoTs devices also increases. However, security risks regarding service provisioning and data sharing also increases. There are many existing security approaches. However, these approaches are not suitable for IoTs devices due to their limited storage and computation resources. These secure approaches also require a specific hardware. With the invention of block chain technologies, many security risks are eliminated. Block chain also supports data sharing mechanism. In this paper, we proposed a secure service providing mechanism for IoTs using block chain. We introduced cloud nodes for maintaining the validity states of edge service providers. The edge node reputation is considered as a service rating given by end users. Incentive is given to edge servers after validation of service codes. Incentive is in the form of crypto currency. Incentive and edge node reputation values are stored in cloud node and are updated with respect to time. Smart contract is proposed to check the validity state of the edge servers. Smart contract is also used for the comparison and verification of the service codes provided by edge servers. In our proposed system, we perform service authentication at both cloud and edge server layer. Moreover, Proof of Authority (PoA) is used as a consensus mechanism. PoA enhanced overall performance of our proposed system. By experimental analysis, it is shown that our proposed model is suitable for resource constrained devices.

[4] Block chain data-based cloud data integrity protection mechanism. In 2020, P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, demonstrated on a novel method despite the rapid development of cloud computing for many years, data security and trusted computing are still the main challenges in current cloud computing applications. In order to solve this problem, many scholars have carried out a lot of research on this, and proposed many models including data integrity test and secure multi-party calculation. However, most of these solutions face problems such as excessive computational complexity or lack of scalability. This paper studies the use of block chain techniques to improve this situation. Block chain is a decentralized new distributed computing paradigm.



Article Title: Enhancing Data Security in Cloud Computing using Block chain

Applying blockchain technology to cloud computing, using the security mechanism of the former to improve the performance of the latter's secure storage and secure computing is a promising research topic. In this paper, the distributed virtual machine agent model is deployed in the cloud by using mobile agent technology. The virtual machine agent enables multi-tenants to cooperate with each other to ensure data trust verification. The tasks of reliable data storage, monitoring and verification are completed by virtual machine agent mechanism. This is also a necessary condition for building a block chain integrity protection mechanism. The block chain-based integrity protection framework is built by the virtual machine proxy model, and the unique hash value corresponding to the file generated by the Merkel hash tree is used to monitor the data change by means of the smart contract on the block chain, and the data is owned in time. The user issues a warning message for data tampering; in addition, a "block-and-response" mode is used to construct a block chain-based cloud data integrity verification scheme.

[5] A distributed secure block chain based online certificate verification system from Bangladesh perspective. In 2020, M. Hasan, A. Rahman, and M. J. Islam, "Distb-cvs, demonstrated on a novel method during the academic career, students achieve numerous academic credentials. These educational credentials are offered by the student while applying for a job or scholarship. Therefore, the goal of this paper is to propose a theoretical block chain-based certificate verification system on the cloud that can offer a potential solution for academic certificate issuing and verification where crypto currencies are banned. By this regarding in this research, we address the Block chain (BC) technology for solving these problems. This BC can be capable of providing immutability and publicly verifiable transactions. Moreover, these properties of BC are used to generate the digital academic credential, which is anti-counterfeited can be verified easily in a little time. In addition, the proposed "DistB-CVS" showed that crypto currencies banned country could leverage the BC technology. It satisfies all the requirements necessary for a modern academic certificate verification system. Furthermore, it tries to close the holes and difficulties in the existing systems to verify academic certificate authenticity.

[6] An energy-efficient sdn controller architecture for IoT networks with block chain-based security. In 2020 Abbas Yazdinejad, Reza M Parizi, Ali Dehghantanha, Qi Zhang, and Kim-Kwang Raymond Choo, demonstrated on a novel method Internet of Things (IoT) is a disruptive technology in many aspects of our society, ranging from communications to financial transactions to national security (e.g., Internet of Battlefield / Military Things), and so on. There are long-standing challenges in IoT, such as security, comparability, energy consumption, and heterogeneity of devices. Security and energy aspects play important roles in data transmission across IoT and edge networks, due to limited energy and computing (e.g., processing and storage) resources of networked devices. Whether malicious or accidental, interference with data in an IoT network potentially has real-world consequences. In this article, we explore the potential of integrating block chain and software-defined networking (SDN) in mitigating some of the challenges. Specifically, we propose a secure



Article Title: Enhancing Data Security in Cloud Computing using Block chain

and energy-efficient block chain-enabled architecture of SDN controllers for IoT networks using a cluster structure with a new routing protocol. The architecture uses public and private block chains for Peer to Peer (P2P) communication between IoT devices and SDN controllers, which eliminates Proof-of-Work (POW), as well as using an efficient authentication method with the distributed trust, making the block chain suitable for resource-constrained IoT devices. The experimental results indicate that the routing protocol based on the cluster structure has higher throughput, lower delay, and lower energy consumption than EESCFD, SMSN, AODV, AOMDV, and DSDV routing protocols. In other words, our proposed architecture is demonstrated to outperform classic block chain.

3 Conclusion

Recently, the demand for cloud computing services has been rising rapidly, with the number of customers increasing dramatically. However, cloud computing is faces several threats and challenges, like security, privacy, compliance, compatibility, control, and reliability. To address these threats, researchers have proposed several tips and techniques; however, the security of these services still faces several challenges that remain an open research question. In this work, we propose the “DistB-SD Cloud” architecture to enhance the security and confidentiality of cloud computing systems. We have leveraged a distributed Blockchain approach integrated into an SDN architecture to increase the security, privacy, stability, reliability, successful accessibility, and the confidentiality of the cloud computing services for users. As part of future research, we intend to effectively implement this architectural approach in diverse applications such as the fog and edge computing domains. The proposed system paradigm will then be more reliant to by SDN and Blockchain technologies.

References

1. A. Rahman; M. J. Islam; M. Saikat Islam Khan; S. Kabir; A. I. Pritom; M. Razaul Karim, Year: 2020, “Block-sdot cloud: Enhancing security of cloud storage through block chain-based sdn in iot network,” in 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), pp. 1–6.
2. J. H. Park; J. H. Park, Year: 2017, “Block chain security in cloud computing: Use cases, challenges, and solutions,” Symmetry, Vol: 9, no: 8, pp. 164.
3. M. Rehman; N. Javaid; M. Awais; M. Imran; N. Naseer, Year: 2019, “Cloud based secure service providing for IoT’s using blockchain,” in 2019 IEEE Global Communications Conference (GLOBECOM) IEEE, pp. 1–7.
4. P. Wei; D. Wang; Y. Zhao; S. K. S. Tyagi; N. Kumar, Year: 2020, “Blockchain data-based cloud data integrity protection mechanism,” Future Generation Computer Systems, Vol: 102, pp. 902–911.
5. M. Hasan; A. Rahman; M. J. Islam, Year: 2020, “Distb-cvs: A distributed secure blockchain based



Article Title: Enhancing Data Security in Cloud Computing using Block chain

online certificate verification system from Bangladesh perspective,” in 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT), pp. 460–465.

6. Abbas Yazdinejad; Reza M Parizi; Ali Dehghantanha; Qi Zhang; Kim-Kwang Raymond Choo, Year: 2020, “An energy-efficient sdn controller architecture for IoT networks with blockchain-based security”, IEEE Transactions on Services Computing, Vol: 13, no: 4, pp. 625–638.

7. M. J. Islam; A. Rahman; S. Kabir; A. Khatun; A. Pritom; M. Chowdhury, Year: 2021, “Sdot-nfv: A distributed sdn based security system with IoT for smart city environments,” GUB Journal of Science and Engineering, Vol: 7, pp. 27–35.

8. X. Liang; S. Shetty; D. Tosh; C. Kamhoua; K. Kwiat; L. Njilla, Year: 2017, “Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,” in 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID) IEEE, pp. 468–477.

9. D. C. Nguyen; P. N. Pathirana; M. Ding; A. Seneviratne, Year: 2020, “Integration of blockchain and cloud of things: Architecture, applications and challenges,” IEEE Communications Surveys & Tutorials.

10. P. K. Sharma; M.-Y. Chen; J. H. Park, Year: 2017, “A software defined fog node based distributed blockchain cloud architecture for IoT,” IEEE Access, Vol: 6, pp. 115–124.

11. C. Yang; L. Tan; N. Shi; B. Xu; Y. Cao; K. Yu, Year: 2020, “Authprivacychain: A block chain-based access control framework with privacy protection in cloud,” IEEE Access, Vol: 8, pp. 70 604–70 615.

12. S. Singh, I.-H. Ra; W. Meng; M. Kaur; G. H. Cho, Year: 2019, “Sh-blockcc: A secure and efficient internet of things smart home architecture based on cloud computing and blockchain technology,” International Journal of Distributed Sensor Networks, Vol: 15, no: 4, pp. 1550147719844159.

13. E. Gaetani; L. Aniello; R. Baldoni; F. Lombardi; A. Margheri; V. Sassone, Year: 2017, “Blockchain-based database to ensure data integrity in cloud computing environments.”

14. Z. Li; A. V. Barenji; G. Q. Huang, Year: 2018, “Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform,” Robotics and Computer-Integrated Manufacturing, Vol: 54, pp. 133–144.

15. S. Tuli, R. Mahmud; S. Tuli; R. Buyya, Year: 2019, “Fogbus: A blockchain-based lightweight framework for edge and fog computing,” Journal of Systems and Software, Vol: 154, pp. 22–36.

16. A. Rahman; U. Sara; D. Kundu; S. Islam; M. J. Islam; M. Hasan; Z. Rahman; M. K. Nasir, Year: 2020, “Distb-sdoindustry: Enhancing security in industry 4.0 services based on distributed blockchain



Article Title: Enhancing Data Security in Cloud Computing using Block chain

through software defined networking-IoT enabled architecture,” International Journal of Advanced Computer Science and Applications, Vol: 11, no: 9.

17. T. Dillon; C. Wu; E. Chang, Year: 2010, “Cloud computing: issues and challenges,” in 2010 24th IEEE conference on advanced information networking and applications, pp. 27–33.

18. Jeonghun Cha; Sushil Kumar Singh; Tae Woo Kim; Jong Hyuk Park, Year: 2021, “Blockchain-empowered cloud architecture based on secret sharing for smart city,” Journal of Information Security and Applications, Vol: 57, pp. 102686.

19. H. Wang; Y. Song, Year: 2018, “Secure cloud-based ehr system using attributebased cryptosystem and blockchain,” Journal of medical systems, Vol: 42, no: 8, pp. 152.

20. Mohammad Riyaz Belgaum; Zainab Alansari; Shahrulniza Musa; Muhammad Mansoor Alam; MS Mazliham, Year: 2021, “Role of artificial intelligence in cloud computing, IoT and sdn: Reliability and scalability issues,” International Journal of Electrical and Computer Engineering (IJECE), Vol: 11, no: 5, pp. 4458–4470.

21. Yogesh Sharma; B Balamurugan; Nidhi Snegar; A Ilavendhan, Year: 2021, “How IoT, and blockchain will revolutionize business,” In Blockchain, Internet of Things, and Artificial Intelligence, pp. 235–255.

22. H. L. Cech; M. Großmann; U. R. Krieger, Year: 2019, “A fog computing architecture to share sensor data by means of blockchain functionality,” in 2019 IEEE International Conference on Fog Computing (ICFC), pp. 31–40.

23. J. Q. Navid Rajabi, Year: 2019, “Sdiobot: A software-defined internet of blockchain of things model, international journal of internet of things,” International Journal of Internet of Things, Vol: 8, pp. 17–26.

24. Rajat Chaudhary; Anish Jindal; Gagangeet Singh Aujla; Shubhani Aggarwal; Neeraj Kumar; Kim-Kwang Raymond Choo, Year: 2019, “Best: Blockchain based secure energy trading in sdn-enabled intelligent transportation system,” Comput. Secur, Vol: 85, pp. 288–299.

25. A. Rahman; M. K. Nasir; Z. Rahman; A. Mosavi; S. Shahab; B. Minaei-Bidgoli, Year: 2020, “Distblock building: A distributed blockchain-based sdn-IoT network for smart building management,” IEEE Access, Vol: 8, pp. 140 008–140 018.