Combining Blockchain Multi Authority and Botnet to Create a Hybrid Adaptive Crypto Cloud Framework

Ravikumar Ch
Computer Science and Engineering
Lovely Professional University
Punjab, India.
chrk5814@gmail.com

Dr. Isha Batra
Computer Science and Engineering
Lovely Professional University
Punjab, India.
isha.17451@lpu.co.in

Dr Arun Malik
Computer Science and Engineering
Lovely Professional University
Punjab, India
arun.17442@lpu.co.in

2021 International Conference on Computing Sciences (ICCS) | 978-1-6654-9445-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCS54944.2021.00028

***Abstract*-Blockchain technology has now spread like wildfire across the internet. Blockchain has emerged as a game-changing technology for complex industrial processes as a result of its openness, availability, and security. In this study, we used a hybrid adaptive crypto cloud framework that combines blockchain technology with multiple authorities and a botnet framework to improve cloud security while reducing computation time. The proposed adaptive crypto cloud system divides the cloud security framework into stages to organize secure data communication and reduce communication latency while detecting internal and external threats. In order to compute authentication using hash mapping and deploy an authentication system to safeguard the various users' authentication information, the whole system placed a major emphasis on block chain technology. The technology not only improves security but also makes the role-based access control system and anonymous authentication system more user-friendly.**

Keywords: Cloud Cryptography, Blockchain, Multi authority Attributes, Botnet

I. Introduction

Machines can be seen as an artificial intelligence Now a day's Blockchain technology became a positive pandemic by holding the internet by storm. Thanks to its free accessibility and safety in nature where the technology of blockchain had emerged as a technology of revolution for the next coming waves of a buzz industrial profile. One is Stuff's Network which is sponsored by the company Cloud Infrastructure and Internet things (IoT).In just such a context, Blockchain technology offers transformative solutions in terms of centralization of power, anonymity, and network stability to tackle cloud problems, Though the Internet of Things offers elastic properties and flexible usability to optimize the Blockchain efficiency of operations. Therefore, Blockchain and the cloud with objects, called the BCoT prototype, are viewed as a promising enabling factor for only a post-set of specific conditions. Among these articles, we are bringing a state-of-the-art analysis of BCoT execution to provide a BCoT overview for strategic in specific facets such as sensor data, encouragement, and integration of technologies. In brief, we provide a concise description of BCoT deployments, providing a thorough review with use-case strategies and their reach within and outside 5 G systems.

The cryptocurrency is a Blockchain that is safe, open, and easy to use. The Blockchain concept is built on a peer-to-peer database network in which transactions are held by no centralized authority. All Blockchain network members have deep sub access to blockchain transactions. Blockchain uses encryption and encryption techniques to verify the authenticity of data transfers, ensuring security from changes and alterations in the linked chains.

Furthermore, the Blockchain improves the fascinating aspects of federalism, transparency, and protection, which frequently promote client engagement and significantly reduce operating costs. The adoption of architecturally based Blockchain technical advancements has risen as a result of their amazing features. Now might be an excellent time to respond to the field of hot analysis. From a technology aspect, Blockchain is a shared service that was first employed in commercial activity as the nucleotide lead of the Bitcoin cryptocurrency.

The transformation in connectivity and networking, on the other hand, has opened up a slew of new possibilities for digital technology, including the Internet of Things (IoT) and storage systems. Growth, business procedures, and structures are all aided by new building technology. Many communications operations, such as tiny towns, major buildings, animals, and hospitals, employ the Internet of Things. However, due to a lack of resources, energy, and technological capital on IoT computers, they frequently delegate IoT device functions to cloud computing, adhering to the Cloud of Things philosophy (CoT). The Cloud of Things network, which is supported by IoT networks, provides unrestricted computing and analytical capabilities.

This also includes a flexible, elastic online storage system that allows for the deployment of a large network of IoT applications, displaying a massive potential for improving user interface quality, device performance, and service delivery capabilities. However, because to the aforementioned problems, current CoT infrastructures appear to be unsuccessful. Second, traditional CoT systems rely primarily on remote networking technologies, in which IoT devices are connected, controlled, and maintained by remote cloud servers.

In light of the growing ubiquity of IoT networks, this proposal is unlikely to gain traction. Such a set-up is not only constrained by critical component issues and failure rates that lead to the destruction of the CoT network. Second, greater integrated CoT capabilities will necessitate the management of IoT devices by a third party, such as a cloud provider, raising worries about data security.

Yes, IoT (internet of things) is a serious threat to the cloud, but until then, sensitive information can be triggered without user consent due to large identity disclosure and channel security issues.

Third, IoT users of modern CoT processors are experiencing poor results. IoT owners have no control over

978-1-6654-9445-8/21/$31.00 ©2021 IEEE
DOI 10.1109/ICCS54944.2021.00028

their customers' data in modern CoT designs, and they find it difficult to manage data access through cloud IoT universes. Inevitably, centralized communication network research leads to strong moving image as well as power utilization for IoT applications, resulting in significant data transfer, which limits broad-scale CoT development in severe circumstances.

Crypto has evolved as a dynamic, secure, but transparent avenue to address basic concerns with present central service providers and to push the next generation of solutions for CoT technology. The combination of Blockchain and Comet, in particular, makes a substantial contribution to a revolutionary paradigm we call the BCoT framework. Integrating this new technology provides enormous benefits to all civilizations, piquing the interest of academics and industry alike. The adoption of Blockchain will provide major benefits to emerging CoT networks.

II. IMPLEMENTATION BENEFITS OF BLOCK-CHAIN

As one of the first cryptographic keys, RSA (Rivest-Shamir-Adleman) is widely used to store records. In a very cryptographic algorithm, there is the key to encryption that is distinct from either the private secret decryption key. Inside RSA this asymmetry centered on either the difficulty of computer technology to take into account two of the slightly positive product quality integers, the "factoring issue"[1].

Configurable assistance to cryptocurrencies with Blockchain: For broad Blockchain networks the amount of information in the different blockchains may be massive. Therefore, it would be very important to include powerful statistical services to increase the speed procedure of making so that scalable Blockchain services can be made available. The Blockchain, along with its dielectric and scalability capabilities, would provide on-demand computing resources for Blockchain organizational culture in the maximum context. For instance, the public clouds offer a broader footprint in a federated cloud scenario for Blockchain network operators. Besides capturing blockchains across the mesh network and using the urgent virtual machine skills and strategies within each cloud, cloud programs help in these contexts. And cloud computing and Blockchain integration make the deployed application highly scalable. Some the benefits which are related to blockchain are listed:

1. Decentralization
2. Security measures
3. Data privacy
4. Corporation
5. Safety Blockchain
6. Fault tolerance

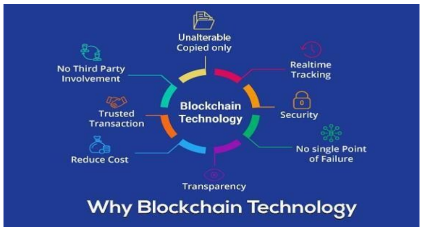

Fig 1: Importance of BlockChain [2]

On the (in) sustainability of contemporary authentication protocols based on PKI, all available community methodology This is based on a public key infrastructure (PKI) where user licenses are provided by a reasonably authority trustworthy and the auditor will have to handle customer certificates to locate the appropriate strong authentication key. However, Authentication Company including granting, transportation, distribution, or authorization is quite expensive and tedious. Removing the credentials management problem can also be competitive and, in fact, advantageous [2].

EoS is a Block One-built open Blockchain network. EoS aims to build a Blockchain network that facilitates features and operating system-like applications. EoS uses an efficient feature block with DPoS contract to facilitate a stronger Blockchain especially compared to the drawbacks of low availability and lack of traditional Blockchain performance. The DPoS nodes must participate in the witness voting, as opposed to PoW and PoS compromise schemes. Only those nodes winning the general poll (minimum 21 votes) qualify for block generation [3].

Although employees hereinafter generally referred to by senders and receivers as "customers" benefit tremendously from cloud power plants, protective issues related to confidential data purchases are already vastly posed. One of the major security concerns is data protection. From the user's point of view, privatized application fabric is very vulnerable that could not be publicly revealed for privacy security purposes. This can be achieved by regular encryption, but checking keywords paired with antique brass encrypted-texts is challenging. The public key encryption test (PEKS) is basic cryptography which response to the above question [4].

A more effective way of proving a file's existence is to cryptographically encrypt text queries with a time- stamp. The symbol uses a trusted provider (TSP) to assist users in trying to stamp their information at night, where a file is sent to TSP after it has been created, and TSP delays it and posts it to the ownerof the file with the time- stamp. Incorporate a time- stamp in cloud storage systems to easily outsource results. Yet with such a system, there are two issues [5].

Product marketing habits are changed by the introduction of TSP by cloud storage devices: Because TSP is a legitimate cloud-independent company; it allows subscribers to connect both to TSP including cloud storage to protect their data against details. Consumers already experience not only a high contact risk but the cost that use TSP as well.

All the Chain SDI structure and the APIs will rectify many critical and urgent statistically significant research issues. Such concerns arise health threats will recognize, thus facilitating successful rehabilitation would lead to timely response, thereby engaging care practitioners and stakeholders. We understand the importance of regulatory use of the Chain SDI system, as well as the simplicity and agility of managing the Chain SDI APIs. [6].

For eg, a customer (say Alice) will produce two independent orders at the same time; use two separate receivers (say, Bob, and Carol) of the same coin set. This type of risky consumer behavior is known as double-spending. Blockchain is an incoherent state where the receiver executes the contract independently depending on their local Blockchain understanding, as long as the validity of the contract is a good one. It overwrites the economic command required to escape the aforementioned issue [7][8].

We conclude that the registration of unauthorized Bitcoin handles is an immediate prerequisite by evaluating a sequence of transactions. For some other deceptive practices that could live together following Bitcoin which is known as the biggest disappointment that crooks have used produce company in achieving high-interest costs,– for example, 1-2 percent cent of the sum per day. [9].

The Internet of Things (IoT) in our daily operations can become truly worthy of worship and that also gets confused about general security. Detection of infringement is crucial for the safety and security and wellbeing of a transmitted IoT network [10].

Crypto- economics' demand over the past 5 years was primarily due to the rise in blindness virtual currencies but instead digital tokens, implementing strong encryption to a new and exciting layer. If a security researcher is likely to follow the method "this method is destined to be uncertain as long as these appropriate statistical problems exist confusing," the location of temple economic principles has to address fuzzy quantitative imperatives such as the randomness of plot assaults, the contrasting amount of altruism, profit-seekingand bashing-altruistic collectives and the increasing emphasis [11][12][13].

In modern cryptography, protection standards tend to look like this:

1. No-one would do more than 279 moves ofestimation
2. Factoring is hard (i.e. super polynomial)
3. It's hard to take nth roots modulocomposites

The dilemma with the elliptic curve with a specific probability distribution cannot be addressed more effectively than in $2^{n/2}$.

In crypt economics, but on the other side, the basic safety assumptions that we depend on are approximately the following in contrast to the mathematical premises:

1. No community of people who control greater than 25percent of all computerresources will work together.
2. Any group of people who own 25 percent of all resources can be colluding The estimated total of some of these career evidence that can be done with some kind of amount of income is not superliner below the lowest point.
3. There is an enormous number of sociopaths and an apparent number of the system'scrazy people or political adversaries and most people can be regarded as relatively commercially acceptable.

The creation of public users is strong, but even users can look likely or vanish at any moment, and if at least some uses are widespread repression of free speech is unlikely and any sensor devices can send relatively brief messaging with one another. Other protection theories can still arise and are special to such issues. However, it definitely won't be able to accurately say the method is safe or dangerous, or whether the problem solved. Solution generation and refinement designed for specific social and scientific complexities will be extremely important [11], [12], [13].

2. Related Work

In this paper [14] Lin Zhong, Qianhong expanding participates, severe network bandwidth and lower entry speeds hinder their widespread use of existing blockchain networks. And to alleviate that illness, heindicated a reliable, ergonomic Light Payment System (SVLP). Billing and offering refunds approaches are versatile. This is because the division within our arrangement lacks computational complexity, so users don't have to find each week for pre-images mostly in the long chain.

In this paper [15] DorianePerard, Lucas Gicquel, et.al, defined the use of blockchains to build a new, decentralized computer network that has been deemed. The methodology of Blockhouses focuses on a method that contains three components: initialization of the storage device, day-audits, and conclusion of the device. It focuses on proofs of retrievability for authenticated messages, allowing contracts to check the data is securely preserved by the server. The main problem that happens in the network may be that the scale of the block-chain is too drastically it is impossible to store.

In this paper [16] Jin Ho Park, Jong Hyuk Park, presented the transaction of P2P Network technology. Basic measures such as production proof but stack proof were introduced to strengthen the credibility of the blockchains. The 51 percent state of attack that includes problems just of infringed credibility and transaction lack of availability after a violation that concerns 51 percent of the transaction ledger.

In this paper [17] Huaqun Wang et.al, suggested a private PDP program focused on Blockchain. The method may even recognize the security of the Customer according to a discussion on anonymity. There is also a need to remove the certificate authentication mechanism to further boost efficiency. Hence the blockchain-based PDP scheme focused on identification is essential for research. Analyzing the keys-evolving blockchain- based PDP system is essential if more strengthening of the private key is necessary.

In this paper [18] Yuan Zhang, Chunxiang Xu, et.al, proposed against the napping auditor in this article a credential less public authentication system, called CPVPA. CPVPA uses on-chain currencies where the on-chain blockchain currency integrates through auditor-led authentication into a transaction. The security analysis shows that CPVPA provides the best defense against current schemes. This should investigate options to turn the CPVPA into other blockchain technologies for future research. Because energy use is the biggest disadvantage of job facts (PoW) that build CPVPA on other resource-saving blockchain frameworks.

In this paper [19] ZehuiXiong, Jiawen Kang, et.al, In this article, used a theoretical paradigm for tri- leader multi-follower game play to analyze relationships in public blockchain verifiable evidence-of among cloud-edge suppliers and miners- working systems.

In this paper [20] Mona Taghavi, Jamal Bentahar, et.al, Proposed a blockchain-based, multi-agent data analytics framework to address the conventional cloud vendor federations problem and impacted QoS. In this current proposal, a multi-strategy has been implemented in which an oracle takes on the role of a verifier agent in evaluating the level of service whenever it is called by the matching engine agents built on the developed architecture has been seen as cost-effective and helpful in terms of cloud app transparency, especially in avoiding SLA breaches.

PROBLEM IDENTIFICATION

The fast expansion of the Blockchain as just radical technologies is setting the stage in the next generation of industrial and financial service industries:

1. Here are all the issues we find with various sources relevant to the investigation of Blockchain and cloud technology.
2. The authorization case does not have clarityas it has the problem of revealing the keys to assault the Blockchain by splitting the private keys; it does not include security for actively supported, as it does not verify the full removal of the digital signature. The cases of information security do not provide compatibility either owing to malicious interference the system is inaccessible it does not provide leftover data security because it does not guarantee that the digital wallet will be removed.
3. As per the Block-chain, cloud-based frameworks have problems with both the violated credibility and lack of availability of digital currency after an attack that alters the transaction ledger.
4. The improved Block-chain scenario neither ensures confidentiality nor offers accessibility. Subsequently, it doesn't offer the security of residual details as it does not verify that perhaps the digital asset is completely removed.

III.RESEARCH OBJECTIVES

1. To build a cloud Blockchain multi-authoritybotnet with the credited dependent crypto method for recognizing the attack functionality and identify the traffic on a network or application data to maintain a protected data control system.
2. To perform the experimental template to evaluate the device output for different quality situations such as processing time, capacity, detecting rate, consumption rate.

IV. PROPOSED METHODOLOGY

To tackle the drawbacks and future research that were identified throughout the section-2, we propose a modified cloud cryptography blockchain system by integrating the consumer and cloud framework attributes visual techniques. The adaptive architecture integrates the design of Blockchain technology functionality while implementing the security system at user areas to ensure stronger security and guarantees the access protection to model to evaluate the threat functionality.

To determine the efficiency of the proposed methodology, will employ a network and data attack features to determine the proposed methodology efficiency in-terms of network latency, detection rate, processing time and prevent the security breaches. In contrast, adaptive architecture incorporates the botnet functionality to identify the data and network threats by assessing the attacker's functionality.

The botnet function coordinates at the Blockchain technology stage to evaluate the identifiers and blocking the fraud. To evaluate the assault functionality, we merge the attacker signature by integrating the identification mechanism. Within this method, we utilize the machine learning access control rate levels by comparing it with existing secured and data sharing models.

Block-Chain Multi Authority Botnet Framework (BCMAB) is fundamental to evaluate trust communication and privacy protection on over cloud services.

The proposed framework divides into the following stages:

1. System Initialization
2. Block-Chain Authentication Server
3. Multiple Attribute-Based Authentication
4. Attack Detection and Attribute Revocation
5. Privacy Data prevention

4.1. SYSTEM INITIALIZATION

This process determines the blockchain network and botnet setup. The blockchain is a decentralized network that composes a series of the data block and all the blocks are linked together to maintain the user's pseudonyms and authentication information. The block-chain database intern connected with the botnet system and cloud system. The blockchain authentication mechanism is composed of four participants; including the multiple attribute-basedAuthority (MAA), User Access Control list, Botnet system, and Cloud Server. The blockchain network among all user's access list information is located on the cloud server, which stores the authentication information of users.

4.2. USER AUTHENTICATION GENERATION

Originally, each agency produces a pair with encryption keys. User A utilizes the block-chain module to send attribute-based Authorization Information as well as its initial offering keys or resources to demonstrate its legal status once accessing the cloud infrastructure. Secure authentication Authorities must submit a registered warrant to the Block-chain server if the access control details are correct. Next, Botnet Program must issue the initial authorization signature to the user. Notice that perhaps the user-provided authentication data includes the user's private details.

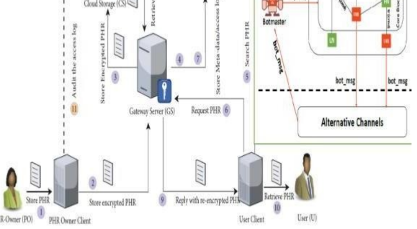

Fig 2: System architecture [21]

4.2.1. AUTHENTICATION UPDATE

User A will sends a request to the Botnet Multi-Attribute-Authority Network system for an authentication update in the following Criteria's:

1. Before the new authorization expired.
2. If the confidentiality of its encryption key ischallenged.
3. If it asks to delete its public key of security considerations.
4. If the user's attributes signature features tomatch with BOT signature features

4.3. MULTIPLE ATTRIBUTE BASEDAUTHENTICATION

Step 1 Users: receives user ID from of the authenticated user, and maintains a protected connection between both the Attributes server and Botnet network, then transfers user real ID as well as other user attribute information to an authenticated user.

Step 2 Block-chain Authorization Server (BAS): BAS verifies and validates the presence of true identity regarding the registered user, if the user existed, generates the authorization signatures that involves pseudonym PIDi, a pair of attribute key.

Step 3 Hash: The Authentication server determines 2 hash code by distributing user attribute keys to the blockchain network, the hashing mechanism produces hashing information which is H0 D (PIDi) and H1 D (UIDi).

Step 4 Cloud Server: Saves hash function H0 which are shared by the Authentication server.

Step 5 Attribute Information: Gets a Pseudo ID, authentication signature, H1, and a set of Public-Private key from the authentication server, and savesit here in the block-chain file.

4.4. ATTACK DETECTION AND ATTRIBUTEREVOCATION

User A utilizes its secret key to create user-shared data authentication signatures while Blockchain Authorities Database may use User A's key pair to validate the authentication signatures. The offender while Attach its username and signatures to theaddress to control user data to forward attacker request. Whenever the suspicious with a fake page is detected, the botnet device will track the malicious activity and then get the actual identity of a malicious attacker with support of the Block-chain authenticated user. To trade-off the attack the botnet database employee a neural network functions to assess the assault level and attack type.

4.5. PRIVACY DATA PREVENTION

Cloud infrastructure A utilizes its very own PID issued username via authorization processing to arrange a secure information exchange between both the client as well as the private cloud while reveling its real identity. Within authenticated users, pairs with identifiers and fake identities are processed in a higher degree of protection for exchange-off between privacy and security. This ensures that AS reveals the actual identities of every given username by each user as only AS does have the power to monitor the malicious activity while performing fake communications misbehaviors. Besides, only at the authentication point, the map of true identity and pseudonym is also documented on Blockchain, and Botnet Framework mapping threat details to detect suspicious functionality, improving data security, and the hashing data is created by the blockchain service to ensure data protection.

V. POSSIBLE OUTCOMES

For hybrid cloud service models, a trusted and reputable cloud system that uses block-chain and botnet mechanisms will reduce communication overhead by decreasing security computation characteristics and maximizing system efficiency when processing huge amounts of data. Furthermore, the suggested approach protects cloud privacy and enhances cloud applications by aiding various cloud services. More importantly, the cloud system uses attribute revocation to reduce latency and prevent data leakage.

VI. CONCLUSION

This study effort proved the necessity of cloud security; security is a key part of cloud usage and demand, and this research work defined and implemented blockchain technology into the cloud based on the cloud security problem. To identify andneutralize cloud internal threats, the suggested adaptive crypto cloud is organized using block chain and botnet technologies. The block chain authentication system defines accessibility by taking into account attribute-based feature sets and mapping the attribute sets using hashing techniques to ensure a safe access control system and avoid access control problems. Furthermore the botnet system defines the various attacks based mostly on layout of the attack function. The overall model combined with the mechanism of blockchain-botnet framework.

REFERENCES

[1]. Jia Yu, Huaqun Wang. "Strong Key-ExposureResilient Auditing for Secure Cloud Storage", *IEEE Transactions on Information Forensics andSecurity*, 12(8), pp. 1931-1940, 2017.

[2]. S. F. Sun, M. H. Au, J. K. Liu, T. H. Yuen,"RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Scheme for Blockchain Cryptocurrency Monero", *ESORICS 2017*, pp. 456-474, 2017

[3]. L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system based on blockchain," Future Generation Computer Systems, vol. 93, pp. 327–337, 2019.

[4]. J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo,"Privacy-preserving data aggregation computing in cyber-physical social systems," ACM Transactions on Cyber-Physical Systems, vol. 3, no. 1, p. 8, 2018.

[5]. X. Zhang, H. Wang, and C. Xu, "Identity- basedkey-exposure resilient cloud storage public auditing scheme from lattices," Information Sciences, vol.472, pp. 223–234, 2018.

[6]. Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: a survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[7]. M. Taghavi, J. Bentahar, H. Otrok, and K.Bakhtiyari,"Cloudchain: A blockchain-based coopetition differential game model for cloud computing," in International Conference on Service- Oriented Computing. Springer, 2018, pp. 146–161. [8].J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource- limited users in cloud computing," *Computers & Security*,vol. 72, pp. 1–12, 2018

[8]. Z. Li, Z. Yang and S. Xie, "Computing resource trading for edge cloud-assisted internet of things," IEEE Transactions on Industrial Informatics, Early Access, 2019.

[9]. Ziegeldorf, J.H.; Matzutt, R.; Henze, M.; Grossmann, F.;Wehrle, K. Secure and anonymous decentralized Bitcoin mixing. Future Gener. Comput. Syst. 2016

[10]. P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, "A detailed and real-time performance monitoring framework for blockchain systems," in Proceedings of the 40th InternationalConference on Software

Engineering: Software Engineering in Practice. ACM, 2018, pp. 134-143.

[11]. Yang, J. Xu, J. Weng, J. Zhou, and D. S. Wong, “Lightweight and privacy-preserving delegatable proofs of storage with data dynamics in cloud storage,” IEEE Trans. Cloud Computing, accepted 2018, to appear, doi: 10.1109/TCC.2018.2851256.

[12]. X. Zhang, C. Xu, H. Wang, Y. Zhang, and S. Wang, “FS-PEKS: Lattice-based forward secure public-key encryption with a keyword search forthe cloud-assisted industrial internet of things," IEEE Trans. Dependable and Secure Computing,accepted 2019, to appear, doi: 10.1109/TDSC.2019.2914117.

[13]. L Zhong, Q Wu, H Xie, and J Li, "A secure versatile light payment system based on blockchain",in *IEEE Systems Journal*,2020

[14]. D Perard, L Gicquel and J. Lacan, "BlockHouse: Blockchain-based Distributed Storehouse System ", from 'https://www.researchgate.net/publication/338737 884_BlockHouse_Blockchainbased_Distributed_ Storehouse_System’,2020

[15]. H. Wang, Q. Wang and D. He, "Blockchain- Based Private Provable Data Possession," *in IEEE Transactions on Dependable and Secure Computing*, DOI 10.1109/TDSC.2019

[16]. Y. Zhang, C. Xu, X. Lin and X. S. Shen, "Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors," *in IEEE Transactions on Cloud Computing*, DOI 10.1109/TCC.2019.

[17]. Z. Xiong, J. Kang, D. Niyato, P. Wang, and V. Poor, "Cloud/Edge Computing Service Management in Blockchain Networks: Multi-leader Multi- follower Game-based ADMM for Pricing," in *IEEE Transactions on Services Computing*, DOI 10.1109/TSC.2019 .

[18]. M. Taghavi, J. Bentahar, H. Otrok, and K. Bakhtiyari, "A Blockchain-based Model for CloudService Quality Monitoring," in *IEEE Transactionson Services Computing*, DOI 10.1109/TSC.2019.

[19]. M. Taghavi, J. Bentahar, H. Otrok, and K. Bakhtiyari, "A Blockchain-based Model for CloudService Quality Monitoring," in *IEEE Transactionson Services Computing*, DOI 10.1109/TSC.2019.

[20]. Thwin, Thein & Vasupongayya, Sangsuree. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. Security and Communication Networks. 2019. 1-15. 10.1155/2019/8315614.