|| Volume 5 || Issue 12 || April 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH & ENGINEERING TRENDS
Multidisciplinary Journal
Double-Blind Peer Reviewed Refereed Open Access International Journal

SIMULATION DESIGN AND IMPLEMENTATION OF BLOCKCHAIN IN REAL WORLD APPLICATION

Urvashi Ganesh Patkar[1], Prof V.D Dhore[2]

M. Tech Student: Department of Computer Engineering & Information Technology, VJTI, Mumbai[1]

Professor: Department of Computer Engineering & Information Technology, VJTI, Mumbai[2]

Abstract: ***A lot of studies have been done over the last few years to cope with this issue. A comparative and analytical review of the state-of-the-art blockchain consensus algorithms is presented in this paper to illuminate the strengths and constraints of each algorithm. Based on their inherent specifications, each algorithm has a different applicability domain that yields several performance criteria to be proposed for evaluating these algorithms. In order to provide an overview and a basis for comparison for further work in the field, a set of incommensurable and conflicting performance assessment criteria is identified and weighted by the pair comparison method. These criteria are classified into four categories including algorithms' throughput, the profitability of mining, degree of decentralization and consensus algorithms vulnerabilities and security issues.***

Keywords: *Blockchain, consensus algorithms, performance evaluation criteria, security vulnerability, trust and permission models*

I INTRODUCTION

The expression "blockchain technology" ordinarily alludes to the straightforward, trustless, openly available record that enables us to safely move the responsibility for of worth utilizing open key encryption and verification of work methods. The technology utilizes decentralized agreement to keep up the system, which implies it isn't midway constrained by a bank, organization, or government. Truth be told, the bigger the system develops and turns out to be progressively decentralized, the more secure it becomes. The potential for blockchain innovation isn't restricted to bitcoin. In that capacity, it has increased a great deal of consideration in an assortment of ventures including: budgetary administrations, philanthropies and not-for-profits, expressions of the human experience, and internet business. Nowadays in both industry and academia, cryptocurrency has become a buzzword. Bitcoin has witnessed huge success as one of the most profitable cryptocurrencies with its capital market exceeding 30 billion in 2018. The basis of the block chain is the Peer-to-Peer distributed network, hash algorithm and consensus mechanism. Consensus mechanism largely determines the trust degree among the nodes of the entire block chain system. It is the task of getting all processes in a group to agree on some specific value based on the votes of each processes. In the proposed system we deploy (n) data nodes network with proposed blockchain, and define all functionality which perform all consensus algorithms. Each algorithm performs the activities according to requirements. The custom smart contract as well as mining policy written by us which will take time as well as provides security accordingly. We will do following configuration changes. This paper we evaluate the various consensus algorithm performance evaluation using blockchain technology.

Block

The definition of the block header is given in the above figure 1.1. the block header and the frame are the contents of block

1. version: indicates which set of rules to follow for block validation

2. root hash: All blocks hash value

3. nBits: goal block hash threshold.

4. Nonce:: a 4-byte field that usually starts at 0 and increases the calculation for each hash

5. Parent hash key: a hash value of 256-bit pointing to the previous block.

6. Timestamp: present standard time as seconds

Key Characteristics of Blockchain

Decentralization Payment must be checked through the central trusted entity (e.g. the central bank) in traditional hierarchical transaction structures, ultimately resulting the cost and performance bottlenecks on the central servers. In comparison to the hierarchical mode, blockchain no longer requires third parties. Consensus algorithms in blockchain are used in the distributed network to preserve data integrity.

Persistency Transactions can be easily checked and honest miners would not accept fraudulent transactions. Once they are included in the blockchain, it is almost impossible to delete or rollback transactions. Blocks containing invalid transactions could be automatically discovered

Anonymity Each user must communicate with a created address with the blockchain, which does not disclose the user's real identity. Because of the inherent constraint, blockchain can not guarantee total security.

II LITERATURE SURVEY

Describe how to ensure the quality and validity of this forensic data by using distributed ledger-based solutions to safely store audit trails and log files in immutable databases. An intruder cannot delete or alter past trails or logs due to this method, but simply stop generating new data in log files. The role described here is novel and sufficiently light for practical use. Use distributed ledger-based solutions for cloud storage of audit trails and, more precisely, micro-service deployments. The distributed ledger's security features maintain audit trail integrity which is necessary for trustable cloud forensics.[1]

Incorporation of all three systems or fields, such as Big Data Analytics, the Block Chain and the IoT. We concluded that all three Big Data Analytics, Block Chain and the Internet of Things (IoT) technologies will play a vital role in overcoming each other's restrictions. It will support for future research work based on our study and case studies. Big data analytics is very important and can be easily integrated with Internet of Things (IoT) powered applications and block chain database technology and the block chain database domain can address two of the unsolved problems of big data, such as how to trust or data privacy, and how to create a global data exchange[2].

A platform for blockchain-based validation of data integrity in P2P cloud storage to make verification more accessible, transparent and auditable. In this context, we present Merkle tree for verification of data integrity, and analyze system performance under different structures of Merkle trees. In addition, we are developing logical sampling strategies to make verification of samples more effective. In addition, we address the optimum sample size for dealing with the conflict between overhead verification and verification precision, and propose two effective verification order algorithms. Mainstream cloud storage systems like Google's GFS (Google File System), Amazon's elastic cloud, and open source HDFS (Hadoop Distributed File System) have adopted a similar distributed architecture, with a huge risk of single point failure [3].

Learned lessons and insights learned from a series of experimental blockchain projects, focusing on off-chain: How to transfer off-chain computing and data, without losing the implemented properties and benefits obtained by using blockchains in the first place. After deriving key challenges from the implementation of several blockchain-based applications based on our observations, we presented five off-chain patterns for moving computation and data off the blockchain without sacrificing essential blockchain properties, in particular the trust lessens property [4].

A thorough examination of the often exaggerated advantages of blockchain technology found in the literature and their consequences for government organizations and processes; They are arguing for a move from a technology-driven to need driven approach in which blockchain technologies are tailored to suit the administrative process requirements and the administrative processes are modified to benefit from the technology. It is found that having sound governance models is a prerequisite for achieving benefits. On the one side, the BC governance viewpoint, in which public entities implement BCT for their own systems, such as service provisioning, and in which BCT is used for transaction governance. The other viewpoint is called BC Governance, which defines how BC will look, how to adapt to change, and how to ensure that public ideals and societal needs are met. These require a thorough understanding of the BC technology and the situation at hand [5].

An innovative approach to governance maintaining centralized and democratic control within cloud federations. Beginning with FaaS, a recent proposal for a cloud federation, we are proposing a federation registry blockchain platform incorporating the proposed governance

approach. Therefore, there is no single point-of-failure and it supports the democratic control and implementation of the business contract of the federation, thereby preventing conspiracy attacks against members of the federation. This is realized through the manipulation of a ledger based on blockchain. Blockchain framework for cloud federation registry deployment and realization of creative cloud federation governance [6].

Blockchain-based ICT-based conceptualisation. In addition, a model ICT e-farming program with a blockchain network is being developed for use at local and regional level. An assessment tool is provided to assess specific technical and social background criteria of the blockchain technology for ICT e-agricultural systems. The framework and technology proposed can be tested and extended to further growth of e-agricultural systems. The contribution of ICT to digital democratization has gone from trusted closed and centralized networks to open access to centralized cloud computing and now to blockchain distributed networks that do not require public faith in a centralized authority. E-farming will improve economic efficiency, food safety and reduce risk of uncertainty while achieving sustainable agricultural development [7]

A licensed blockchain system between the various elements involved in managing the data collected about the vehicle. Specifically, to provide membership establishment and privacy, we first incorporate Vehicular Public Key Management (VPKI) into the proposed blockchains. First, we develop a fragmented ledger that will store comprehensive vehicle-related data such as maintenance / history records, car diagnostic reports, etc. The proposed forensic architecture allows post-accident analysis that is trust less, traceable and privacy-aware with limited overhead storage and processing. VPKI in permitted blockchain and fragmented ledger which allows the hashed data to be stored in the shared ledger while the details are stored as non-hashed data in fragmented ledgers. Additionally, the use of identity pseudonyms helps preserve user privacy [8].

Blockchains as the foundation of the cryptocurrencies, e.g. bitcoin, have gained broad attention. Cryptocurrencies may or may not be money's future but blockchains are another matter. Blockchains are considered to be a new form of IT that could revolutionize technology, business, and commerce. In this article we are discussing the winds of change that are currently blowing on the thriving global consumer electronics (CE) market, which is multibillion dollar. This addresses the ground breaking effect of blockchain technology on supply chain management as well as future CE use cases [9]

Reliable Big Data Sharing Model based on Blockchain Technology and Smart Contract to secure data resource circulation. Such regulations encourage the standardization of the big data industry which to some degree protects the dissemination of data. Nevertheless, since every person's actions cannot be regulated completely only from legal and moral perspectives, this issue is not fundamentally solved. A secure data sharing network for data producers and demand parties through the development of a decentralized blockchain and smart contract-based data circulation security system. Blockchain guarantees traceability of data, and the automated execution of the smart contract offers data security sharing protection [10].

III RESEARCH METHODOLOGY

The verification process, the security of the network, validation time and the cost of processing all depend on the consensus mechanism followed by a cryptocurrency. Comparative evaluation of consensus mechanisms is presented in Table 1. Most of the cryptocurrencies place the greatest emphasis on security and decentralization. As a result, more cryptocurrencies use Proof of Work as a consensus protocol. Because of its validation process, the next most popular consensus mechanism is Proof of Stake. Based on their techniques and characteristics, different consensus mechanisms can be divided into five major groups: Proof of Work; Proof of Stake; a hybrid or combination of both PoW and PoS; Byzantine Fault Tolerance with different versions; and Tangle. Proof of Work, which is an established decentralized and secure protocol, requires a significant amount of computational energy in order to create a block. Also, all cryptocurrencies that follow PoW algorithm are facing scalability issues.

As a solution, PoS came into play with an easier validation process and with lower energy consumption. However, the PoS mechanism faces centralization issues. It is assumed that only a few investors in the future will control the cryptocurrencies under the PoS mechanism. As a result, the hybrid or combined mechanisms of PoW and PoS were created. These hybrid mechanisms differ from one another.

The PoW emphasizes the decentralization and security of the network while the PoS emphasizes scalability and energy consumption. Thus, the combined mechanisms consist of both the pros and cons of the PoW and PoS. However, both mechanisms face storage issues since, due to centralization, all peers need to save the continuous public ledger. The Byzantine Fault Tolerance related mechanism solves most of the drawbacks of both the PoS and PoW. However, it is centralized. As a consequence, this mechanism is mostly used in private or permissioned blockchains rather than in a public Blockchain. The major difference between Tangle and other mechanisms is that Tangle does not use a Blockchain network but uses DAG to grow the network. Thus, the validation process in Tangle is different from others.

According to Zyskind, Guy et.al[11] A unified framework for the management of personal data ensuring that users own and access data. Our introduce a protocol that converts a blockchain into an automated access-control manager that needs no third party trust. Unlike Bitcoin, our system's transactions are not purely financial–they're used to hold instructions like storing, querying, and sharing data.

According to [12] MedRec: A new, decentralized record management system used by blockchain technology to handle EMRs. Our system provides patients with thorough, unchanging monitoring and easy access to their medical information through facilities and treatment sites. Using special blockchain properties, MedRec handles security, confidentiality, transparency, and data sharing–crucial considerations when managing sensitive data. It gives them access to aggregate, anonymize data as mining incentives, in exchange for maintaining and protecting the network through Proof of Work. MedRec thus enables the emergence of data economics, supplying big data to empower researchers while engaging patients and providers in the choice to release metadata.

According to [13] Creating an identity-based (ID-based) RDIC protocol using key-homomorphic cryptographic primitive to reduce the complexity of the system and the expense of defining and maintaining the public key authentication process in PKI-based RDIC systems. They formalize RDIC and its protection model based on ID including security against a malicious cloud server and verifies zero information privacy against a third party. During the RDIC method the proposed ID-based RDIC protocol leaks no information about the stored data to the checked.

According to [14] A novel proxy-oriented data upload and remote data integrity check model in identity-based public key cryptography: identity-based proxy-oriented data upload and remote data integrity test in a public cloud (ID-PUIC) environment. They provide formal definition, model of a system, and model of protection. Instead, using the bilinear pairings a concrete ID-PUIC protocol is developed. The proposed ID-PUIC protocol is demonstrably safe based on the hardness of the Diffie–Hellman computational problem. The protocol to ID-PUIC is powerful and versatile, too.

According to [15] By incorporating fuzzy identity-based auditing-the first in such an approach, to the best of our knowledge, seek to address the dynamic key management problem of cloud data integrity checking. In particular, they present the fundamental of Fuzzy Identity-based data auditing, where the identity of a user can be interpreted as a set of descriptive attributes. For this new primitive they formalize the machine model and the protection model. Instead, by using biometrics as the fuzzy identity, they present a concrete specification of a fuzzy identity-based auditing Protocol.

IV PROPOSED SYSTE DESIGN

The below figure 1 illustrates proposed system execution which carried out custom blockchain implementation. This research basically describes the data security approach in blockchain environment with various consensus algorithms. The first phase system deals with a graphical user interface (GUI) where end-user uploads some data or information. Each uploading event considered as a transaction for each block, we carried open Smart contract for custom blockchain. SHA-256 hash generation algorithm and use to generate a hash of transactional data. Mining policy validates the transaction with the combination of current has as well as previous hash. For the first transaction system considered this block as a Genesis block and defined threshold value considered as the previous hash. ones the mining policy has fulfill system commit the transaction with an entire number of data nodes. P2P network executive various consensus algorithms to validate respect to the transaction in entire data nodes. we propose

PoS, PoS, LPoS and PoET consensus algorithm during the execution.

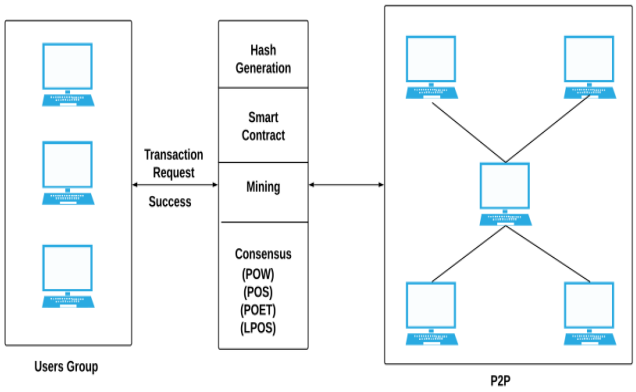

Figure 1 : Basic blockchain architecture in cloud

The majority voting technique has been used by respective consensus algorithms to validate the data consistency when sometimes majority cooking violates any policy system automatically recover respective date node with other blockchains. The basic benefit of this system data should be immutable or whenever any third party attacked generated automatically recover search data node when the next conjunction has performed an the entire framework.

Algorithm Design

Algorithm 1 : Hash Generation

Input : initial genesis block Gb, Previous hash Ph, Data data[],

Output : Hash generation using SHA256 algorithm on data

Step 1 : Input data data[]

Step 2 : Perform SHA 256 from SHA suitable algorithms

Step 3 : New Hash= SHA256(data[])

Step 4 : Retrun String(**New**Hash)

Algorithm 2 : Protocol for peer to Peer node verification

Input : User Transaction query, Current Node Chain CNode[chain], Additional Outstanding Nodes blockchain NodesChain[Nodeid] [chain],

Output : Recover if any chain is invalid else execute current query

Step 1 : Transactional data or any event data for input to blockchain

Step 2 : Extract current server blockchain of time[t]

Cchain ← Cnode[Chain]

Step 3 : For'each

$$NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$$

End for

Step 4 : Foreach (read I into NodeChain)

If (!.equals NodeChain[i] with (Cchain))

Flag 1

Else Continue Commit query

Step 5 : if (Flag == 1)

CCount = SimilaryNodesBlockchian()

Step 6 : Determine the majority of server

Recover inacceptable blockchin from precise node

Step 7: End if

End for

End for

Mining Algorithm for valid hash creation

Input : Hash Validation Policy smart_contract[], Current Hash Values hash_Val

Output : Valid hash generation according to smart contract

Step 1 : System generate the hash_Value for ith transaction using Algorithm no. 1

Step 2 : if (hash_Value.valid with smart_contract [])

Valid hash

Flag =1

Else

Flag=0

Mine the current hash again randomly

Step 3 : Return valid_hash when flag=1

V RESULTS AND DISCUSSION

For the system performance evaluation, the system calculates the matrices for accuracy. The system is executed on java 3-

tier architecture framework with INTEL 2.8 GHz i3 processor and 4 GB RAM with a distributed environment. The below figure (b) shows the time required for a consensus algorithm to validate the blockchain in 4 nodes. The x-axis shows the size of blockchain and Y shows the time required in milliseconds for validation.

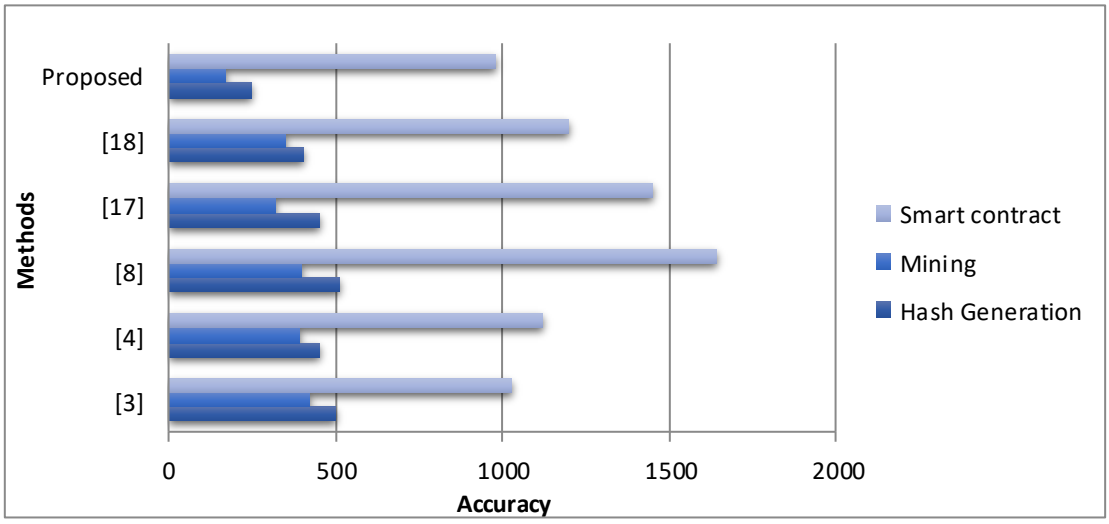

Figure 2 : Execution cost of each algorithm

In another test case we evaluate the proposed system with smart contract validation by consensus algorithm in different number of peer to peer node.

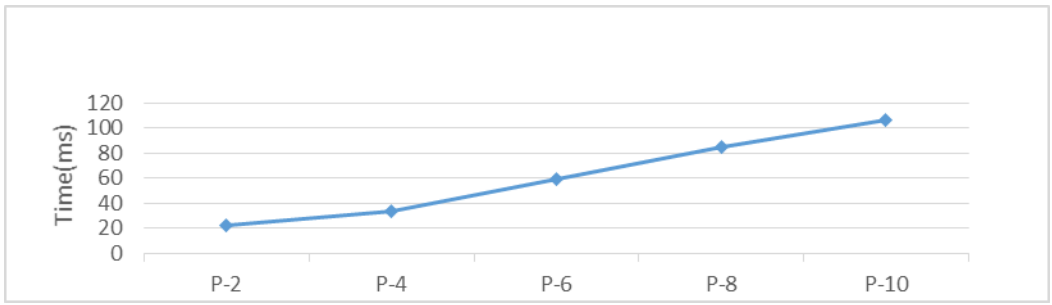

Figure 3: Time required for smart contract validation with different no. of P2P network in blockchain.

The number of variation taken by algorithm from propose SHA value are evaluated in the third test case. Basically this has been done to evaluate the propose hash string is valid or not according to given mining policy. In many times when system generates SHA code for given transactional data its never fulfill the mining policy. To fulfill the propose mining policy according to given scenario mining to generate the multiple variation on given string. The below figure (d) shows the time required to generate the valid SHA string for specific transaction.

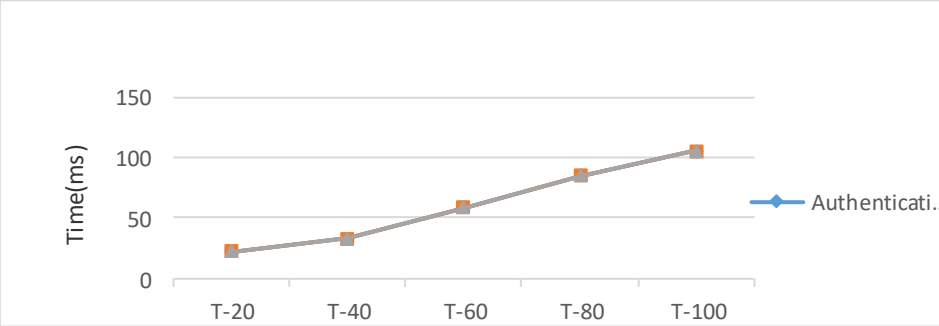

Figure 4: Time required for mining for number of transactions in milliseconds

CONCLUSION AND FUTURE WORK

Based on the proposed framework, the pros and cons of consensus algorithms are systematically analysed and compared in order to provide a deep understanding of the existing research challenges and clarify the future study directions. The system evaluate the performance of four consensus algorithm in sequential manner and demonstrates each algorithms effectives and utilization according to requirements.

REFERENCES

[1] Neovius M, Karlsson J, Westerlund M, Pulkkis G. Providing Tamper-Resistant Audit Trails for Cloud Forensics with Distributed Ledger based Solutions. CLOUD COMPUTING 2018. 2018 Feb 18:29.

[2] Liu B, Yu XL, Chen S, Xu X, Zhu L. Blockchain based data integrity service framework for IoT data. In2017 IEEE International Conference on Web Services (ICWS) 2017 Jun 25 (pp. 468-475). IEEE.

[3] Yue D, Li R, Zhang Y, Tian W, Peng C. Blockchain based data integrity verification in P2P cloud storage. In2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS) 2018 Dec 11 (pp. 561-568). IEEE.

[4] Delmolino K, Arnett M, Kosba A, Miller A, Shi E. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. InInternational conference on financial cryptography and data security 2016 Feb 22 (pp. 79-94). Springer, Berlin, Heidelberg.

[5] Olnes S, Ubacht J, Janssen M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing.

[6] Margheri A, Ferdous MS, Yang M, Sassone V. A distributed infrastructure for democratic cloud federations. In2017 IEEE 10th International Conference on Cloud Computing (CLOUD) 2017 Jun 25 (pp. 688-691). IEEE.

[7] Lin YP, Petway JR, Anthony J, Mukhtar H, Liao SW, Chou CF, Ho YF. Blockchain: The evolutionary next step for ICT e-agriculture. Environments. 2017 Sep;4(3):50.

[8] Cebe M, Erdin E, Akkaya K, Aksu H, Uluagac S. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Communications Magazine. 2018 Oct 16;56(10):50-7.

[9] Pilkington M, Lee JH. How the Blockchain Revolution Will Reshape the Consumer Electronics Industry. forthcoming (provisional draft, do not cite). 2017.

[10] Yue L, Junqin H, Shengzhi Q, Ruijin W. Big data model of security sharing based on blockchain. In2017 3rd International Conference on Big Data Computing and Communications (BIGCOM) 2017 Aug 10 (pp. 117-121). IEEE.

[11] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data. In2015 IEEE Security and Privacy Workshops 2015 May 21 (pp. 180-184). IEEE.

[12] Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In2016 2nd International Conference on Open and Big Data (OBD) 2016 Aug 22 (pp. 25-30). IEEE.

[13] Yu Y, Au MH, Ateniese G, Huang X, Susilo W, Dai Y, Min G. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security. 2016 Oct 7;12(4):767-78.

[14] Wang H, He D, Tang S. Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud. IEEE Transactions on Information Forensics and Security. 2016 Jan 21;11(6):1165-76.

[15]Li Y, Yu Y, Min G, Susilo W, Ni J, Choo KK. Fuzzy identity-based data integrity auditing for reliable cloud storage systems. IEEE Transactions on Dependable and Secure Computing. 2017 Feb 1;16(1):72-83.