Cloud Security in Reliable Blockchain Technology

Beena G Pillai, Madhurya J A

The Blockchain is a release and dispersed ledger. Latest communications and information can be added on to a blockchain but precedent information cannot be obliterated. The Blockchain operation connecting two or more parties is confirmable and everlasting verification of information. In present system A BaaS platform which grant blockchain tune-up over cloud computing system exploitation and method supervising, smart convention investigation with analysis. This research work nearby consistency of BaaS communications. Looking for more exhaustive and adaptable assessment technique for BaaS communications. Transaction through blockchain technology is more secure and reliable, and it collaborate with decentralized cloud computing will get more reliability. The proposed investigation exertion can affect merkle tree in the deliberated algorithm on smart convention presentation optimization and involuntary refurbish. In this system merkle tree allows competent and protected authentication of huge data structures. Our proposed system include a trusted authority or a cloud provider to become a distribute service provider. Each dealer sends their IoT data with communication integrity, authentication code to the cloud server. Every consumer gives to the proceedings they are concerned in on the cloud. Every supplier becomes authenticated data generator on the cloud. Like this, examination contributors otherwise the users know how to optimize applicable apparatus or obtain equivalent defensive procedures according to the evaluation results. The smart contracts deployments and function calls within that block get executed on the node that mines the block cloud based IoT ecosystem proposed by many companies. All IoT devices communicate to the cloud and get global state info from the cloud. Blockchain technology integrated with cloud avoids cyber attack on cloud.

Keywords: BaaS, Blockchain, Cloud security, elegant contracts, IoT, merkle tree.

I. INTRODUCTION

Blockchain Blockchain is most popular topics for current situation. Though, the majority of professionals still notice that Block chain tools seeing that element of Bitcoin, additional crypto-currencies or currency transport method. Blockchain equipments are worldwide and also used in other areas, such as IoT, WSN and mobile devices.

Blockchain technology, are intriguing the world by tempest largely due to the accomplishment of Bitcoin, has been used in different pasture with its quick improvement, consequential in the crack of dawn of a latest financial system. In recent times, a broad variety of blockchain functions and operations appeared. On the other hand, the majority of programmers still be deficient in a suitable and efficient method to organize, sustain and supervise their relevancies, and thus they cannot make sure the consistency and protection of the functions. There are lots of reasons for this, but the nearly everyone significant the complication of the blockchain technology itself.

Blockchain requisition are categorize in various fields such as i) Finance: the communication between investment and blockchain applications: (1) Enhanced contract dispensation, (2) sustainable banking and Finance, (3) Improve economic protection (4) confidentiality and computerized financial dealings. ii) Healthcare: (1) Easier access to medicinal information, and (2) smooth the progress of distributing of medicinal proceedings, and (3) association and regulation of medical proceedings. iii) Government: (1) eGovernment, (2) constructing accurate digital characteristics, (3) eVoting, (4) improving evaluating apparatus parameter.

Blockchain technology possesses positive individuality to facilitate precious instruments developed functions and probable basis distraction used for recognized business. These contains the unchallengeable of the ledger, decentralization of information, conservation of isolation, payment of trustless dealings, effectiveness and sustainability of procedure plus the capability towards computerize multi step procedure by elegant contracts. Cloud storage space agrees to user to store up their information online and therefore access it where at any time. Accumulate all information in digital system. Block chain cloud storage resolution take the user's information and rupture it up in to miniature portion. The further coatings of protection and allocated it during the system. Block chain features like hashing utility public/private key encryption, transaction ledgers.

If impostors attempt to hack it, they first acquire encrypted information, then they get only portion of information and not to the complete file. This protected credentials in block chain found in the cloud storage. Owner is concealed; node does not accumulate owner information. The miner only get portions of information, consequently all perceptive information is protected and secured. Data redundancy and consignment corresponding can be practical. On every occasion user attempts to get information,

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author

Beena G Pillai*, Dept. of CSE, Gitam University, Bangalore, India. Email: beenagpillai.pradeep@gmail.com
Madhurya J A, Dept. of CSE, Gitam University, Bangalore, India. Email: madhurya72@gmail.com

all portions of the information are first authorized and if any modification is establish on an information chunk, then the miner who distorted the information portion is detached from the system. Block chain is the latest and probably the cheapest way to get cloud storage space. A lot of small unit contribute in cloud storage by provided that their calculating power and liberty to store up the information. Cloud storage space cost less and all the units that contribute in the system.

A new contract formed, an innovative block is repeatedly produce situation timestamp when documentation goes through in the block. Every time a new business deal verified or presented operation simplified, additional new blocks get produced. Every time new block is produced it is transmitted in actual time to all internet associated computers called nodes. When developers are manipulating production code, they are unacquainted of the force from the intricate fundamental method, so they cannot take safety measures to deal with upcoming mistakes. As well as, due to need of specialized awareness, general developers or squads frequently not succeed to observe the administration situation of their methods and cannot consequently categorize and take suitable procedures to stick the coordination fault in time. In regulate to resolve these troubles; developers repeatedly require devoting lots of power to knows the essential tools of the blockchain, slightly point lying on the intend of production system. Conversely, efforts concerning this fundamental equipment are complicated on behalf of developers or teams.

This is very complicated along with expensive designed for general developers and panels to install retain and observe a blockchain system. BaaS projected during current days. As a result of implanted the blockchain structure interested in the cloud computing domains, a BaaS domain preserve influence to the installation and administration returns of cloud service communications in the direction of developers through suitable, high presentation blockchain network along with associated services. This research present consistency of BaaS transportation. In search of additional and adaptable assessment techniques for BaaS communications. During the service contributors or the service consumers be capable of optimize the appropriate mechanism otherwise acquire consequent precautionary procedures according to the assessment outcomes. The proposed research work can be relevant t merkle tree in the deliberate algorithm on elegant contracts presentation optimization.

II. SPECIFIC OBJECTIVES

A. Provide Cloud Security.

To develop the protection of blockchain technology using Cloud environment. To progress the consistency of blockchain technology.

B. Contributing to the society in proposing a practically implementable solution to overcome the problem of existing system by blockchain technology.

C. To improve the transparency of blockchain deployment and runtime

III. RELATED WORK

The Thorough lessons look at the key protection regarding. There a worldwide indication of the Bitcoin rules and its main apparatus, specify the offered pressure and weakness of the Bitcoin method in addition to its major tools together with the blockchain procedure, present protection studies with explanation and review unlock research confront and developments in support of upcoming investigation in Bitcoin security. A taxonomic categorization in addition to exact conversation of presented clarification also applications to facilitate use machine learning (ML) methods to work out general precautions and inconsistent behaviors in Bitcoin systems and blockchain.

Distinctive characteristics to the blockchain, for instance privacy, protection ambiguity, transference, and immutability, endow with important profits to different areas and subject. Moreover come across to investigation functions of blockchain have barely begin among several restricted learning into regions, for instance the IoT, power, funding, healthcare, and administration, to furthermore situate towards profits inexplicably commencing its accomplishment. Recognize the subsequently wave of investigation to core approximately cryptocurrencies along with correlated customer-centered recognition and implementation research with the intention of generate boundary and production representations skilled in reformation of blockchain combination into the different fields.

The accomplishment of Blockchain technology into sensor networks like component of IoT. The perception of Continuing Blockchain be projected, which is utilized to construct WSN by the contribution of stylish Cars. The regulation of block arrangement and construction during the sequence is planned along with arithmetical replica is formed it.

Approximation the most favorable quantity of WSN nodes, the amount of associations linking nodes, in support of particular system consistency ethics, was executed. The problem of defense investigation and security in opposition to chopping of the anticipated technique. Also, the concerns make use of the Merkle tree designed for this category of system and procession missing to release.

A blockchain supported IoT forensic structure for forensic investigation into the IoT background is projected, which afforded complete information derivation construction along with declaration of assessment procedure. For the time being, it can also afford protection solitude and accessibility with the transparency, traceability, expectation linking proof/ thing and investigators, and uninterrupted veracity of all substantiation things.

A BaaS proposal described NutBaaS, offers blockchain services more than cloud computing settings, for example system installation, system supervising, smart contracts investigation and testing. Depends on services, programmers preserve on the industry code to survey how be relevant to the blockchain technology further properly in the direction of their business situations, without inconvenience to sustain and observe the system.

IV. PROPOSED SOLUTION

BaaS infrastructure be the innovative type deliberation it happens in support of service, would increase the security, decentralization and trustless method of blockchain. Existing system it is very complex with expensive to sustain & supervise a blockchain. Incapable to make certain consistency along with safety of Baas Platform. The proposed system used as an Identity chain technology and smart contracts susceptibility recognition. The proposed system used to find reliability of Baas infrastructure. The main objective of the proposed system is transparency of block deployment and runtime. In proposed systems use merkle tree to find the smart contract performance optimization and automatic repair. To progress the security of blockchain equipment using Cloud background. To improve the reliability of blockchain technology. Contributing to the society in proposing a practically implementable solution to overcome the problem of existing system by blockchain technology. The proposed research work is to design a decentralized cloud server using Baas platform. The major concern in this work is not only transaction but also to protect the data in a secured manner. Merkle Tree can be used for raising the constancy and power utilization of knob is cost-effective in support of using long blockchains.

The existing methods are examined to discover their executing metrics. In the proposed system an improved conduct will be tried to accomplish it, so that it can be pragmatically deployable. To present a stretchy structural design for organizing cloud- blockchain technology and the simplicity of block chain adaptability. To afford privacy for the information stored in the sub servers and an proficient approach to retrieve information stored in the sub servers. To give security of smart contracts.

Bitcoin is a crypto currency that use consent network algorithm called Proof of work. 1) verify signature 2) authenticate balance 3) Decide the chunk is valid 4) Determine how miners validate a block 5) construct the method to move a chunk 6) construct the method for creating new coins 7) Tell the system how to determine consensus.

Merkle tree algorithm is best suited for distributed systems, where identical information should be present in several places. Merkle tree can also be used to verify inconsistencies. Apache Cassandra uses Merkle tree to identify inconsistencies between replicas of complete record. It is liberated and unlocks, circulated large features, NoSQL record administration is planned to hold huge amount of information transversely lots of servers. Cassandra provides strong support for clusters straddling several data centers; by means of asynchronous master fewer duplication allow short latency process in favor of the entire customers. It is a java based system, wide column store. It introduces Cassandra Query Language (CQL) alternative is SQL.

Merkle tree is an essential element of block chain technology. It is the composition that consent to proficient and protected confirmation of satisfied in a huge amount of data.

A merkle tree provides a synopsis of all transactions in a chunk thus produce digital finger print for the complete group of dealings, thereby enabling a customer to authenticate whether a contract is integrated in a chunk or not. Merkle trees are formed by recurring hashing couple of nodes until here is simply single hash present.

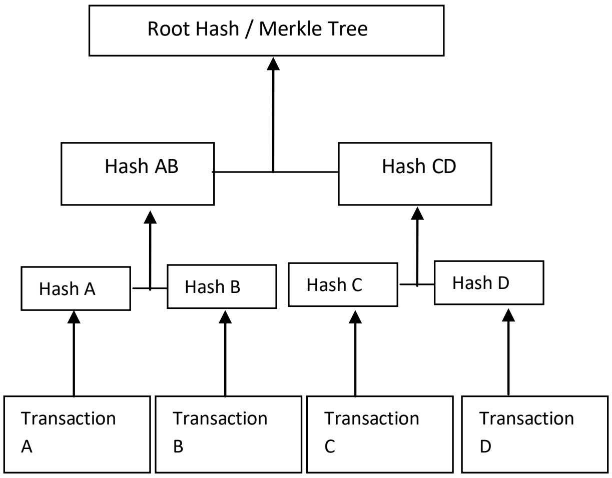
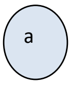


Fig 1: Merkle Tree Algorithm

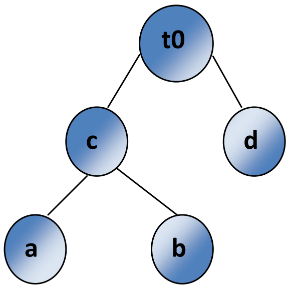
Merkle tree can be extensively reducing the quantity of information that a trusted authorization has to uphold for confirmation purpose. Digital currency require digital wallet. Wallet is an address in the block chain. Wallet is a public key. A transaction is placed in a block by users, who are individual nodes,

Merkle tree signific

```
func(self*CompactMerklrTree)Root()common.Uint256{
if len(self.hashes)==0{
return hash_empty()
}
hashes = self.hashes
1: = len(hashes)
accum : =      hashes[l=1]
for i:=1-2;i>=0;i—
{
accum = hash_children(hashes[i],accum)
}
return accum
}
```



File Storage: Tree Size : 1, Hashes[a]



File Storage: [a,b,c,d], Tree Size : 3, Hashes[c,d]

Merkle tree can considerably progress the execution and storage capability of consensus node. So by using this method, we can revise the Merkle tree by using read and write operation on LevelDB. The time complexity is reduced to O(log(n)).

Key generation

Primary certification Nodes designed for every one iє{0,1,…..H-1}: Compute

```
Authi = $\Phi$(ni,1)
Intial first Nodes used for every I $\epsilon$ {0,1,…….H-1} :
Setup Stackk among the particular node assessment
Authi = $\Phi$(ni,1)
Public Key: Determine and distribute tree root, $\Phi$(root)
Typical Merkle Tree Traversal
1.  Locate flag = 0.
2.  Output:
      Calculate and result $\Phi$(flag) among FLAGCALC(flag).
      for every h$\epsilon$[0,H-1] output {Authh}
3.  Restore Auth Nodes:
      For all h such that 2h divides flag+1:
      Locate Authh be the single node cost in Stackh.
      Locate startnode = (leaf+1+2h)  ○h
      Stackk.initialize(startnode,h).
4.  Construct Stacks:
          For all h$\epsilon$[0,H-1]:
          Stackh.update(2).
5.  Loop:
          Set flag = flag+1.
          If flag<2H go to Step 2.
```

Blockchain as a service (BaaS), the consortium of cloud computing and blockchain, to facilitate clients to support cloud based resolution to construct, swarm along with handle their possess blockchain application, elegant conventions and functions on the blockchain. The BaaS provider supervises every part of the required responsibilities and events to maintain the transportation responsive, operational and simply reachable. It is a fascinating improvement in the blockchain network so as to most of the enterprises for business purposes adopting blockchain technology indirectly, which reduces business transaction process and investment cost. Thus it mechanism related on the way to the perception of Platform as a Service representation.

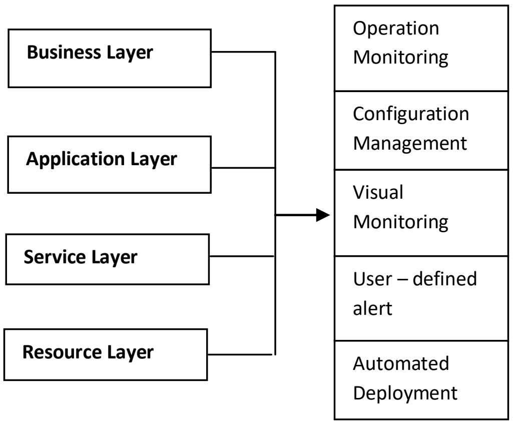


Fig2: Baas Architecture

The main goal of the BaaS architecture design is to make available a complete and detailed operation monitoring method for the blockchain technology. The above mentioned are the four main layers intended for this objective. The above specified method covers up four features of blockchain procedure: relationship management, visual supervision, consumer distinct attentive and computerized exploitation. Computerized exploitation objective is to provide an incorporated service like installing assessment systems, scripting and checking elegant dealings, modifying relevancies, distribution of applications. The major role of Configuration management is the upholding of the network, primary installation of network and network relationship renew at runtime. The use visual supervision and consumer distinct attentive is to supply visual data to the consumer, and to send data in the alert form to the client, i.e. done according to the alarm entry assessment set by the client, so that the client instantaneously find out the coordination difficulties and resolve it.

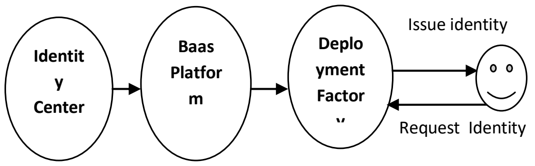


Fig3: Identity Chain Architecture

The Identity-Chain technology explained above, a general client of an organization can register an account in identity chain and instigate a procedure on the system as a split unit. The confidentiality of the separate client data and the protection for operations are provided by client's private key. Any operation that has to be executed successfully means it has to exit throughout the consent procedure. Identity Chain a tool reduces the description registration of hyper ledger basics, by tolerate the clients of the element peers to interrelate with the blockchain system. As cloud computing rising while the majority proficient, general in addition to squashed proposal, the SDP (Software Defined Perimeter) resolve emigrated in the direction of the cloud atmosphere. This determination communally enhances the production, methodological with client repayment. Executing SDP in the cloud will transform the environment designed for homeland safety. The SDP is an integrated stage to effortlessly incorporated element, services, whether they are executed through cloud equipment. It creates probable matching of centralized and decentralized services along with the exploitation of presented support networks on behalf of general purposes. By revealing normal service interfaces in the system, facilitate intermediators to put together their services. Rapidly to construct original services depends on the service mechanisms endow with the Baas. This covers the method for quick commerce replica through supreme selling opportunity.

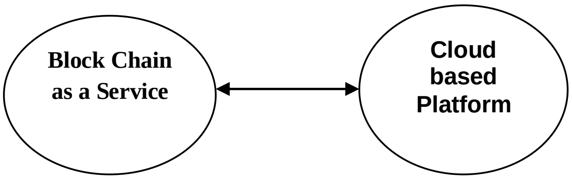


Fig4: Cloud Based Platform with Block Chain as a Service

Dissimilar safety measures preserve effortlessly and insightfully assist with one another sequentially to rapid recognition and expressive preparing protection and evolution by synchronized. Suitable opposition a procedure contains measured by means of all the clearness and assurance to several kinds of precautions pressure by the promising phase itself. Real time alert contains be dispersed to establishment throughout the cloud based announcement method. The safety aptitude acquire an enhance through the entire the safety information receiving since different resources and pointed a diversity of exhaustive analysis to expose hazard prototypes.

This assists regarding behavior and resources of removing any kind of adversity for people and properties.

V. RESULT & DISCUSSIONS

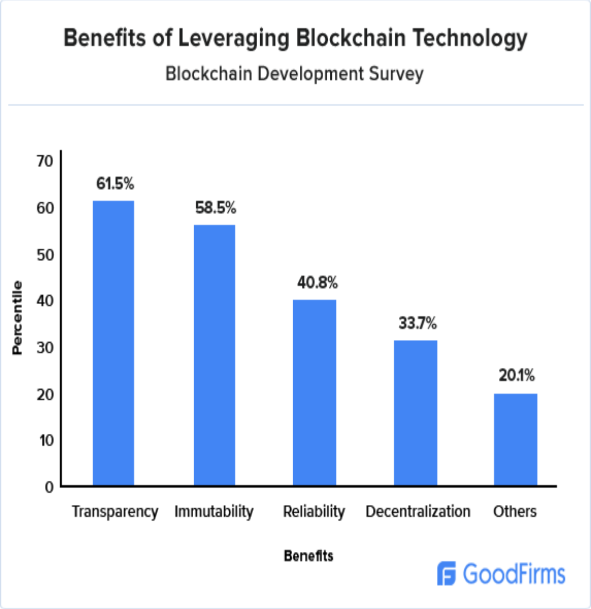


Fig5: Benefits of Blockchain Technology

Transparency and immutability twisted away designate winner produce the confirmation of 61.5% and 58.5% of these blockchain review applicants correspondingly. Reliability and continues a great deal beyond fixed up with logical hold up of 40.8% the survey. The purpose of blockchain improvement is in the direction of be secure and stable, through a condition of complicated fault tolerance. The next blockchain advantage in the peak for to be decentralization as preferred by 33.7% of the blockchain consultant.

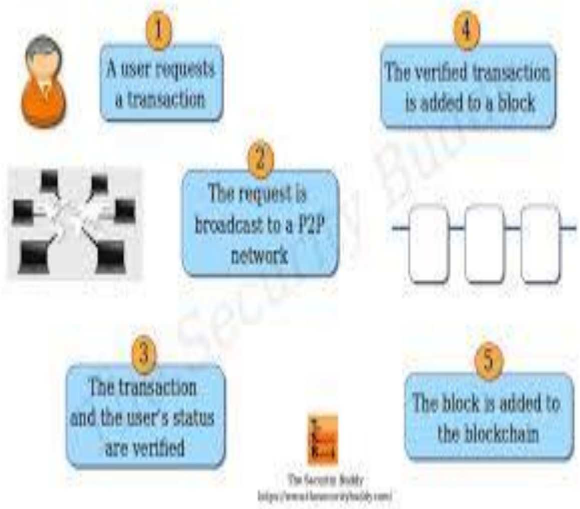

1
A user requests a transaction
2
The request is broadcast to a P2P network
3
The transaction and the user's status are verified
4
The verified transaction is added to a block
5
The block is added to the blockchain
The Security Buddy
https://www.thesecuritybuddy.com/

Fig6: Blockchain working diagram

A user request a transaction using network through the cloud server, the request is broadcasted to a peer to peer network and made any changes in the both network side. The transaction and the user's status are verified. The verified transaction is added to a block and these types of number of blocks are added to the blockchain. These block chains are added to the cloud. Security is done through this cloud made more potential and reliable.

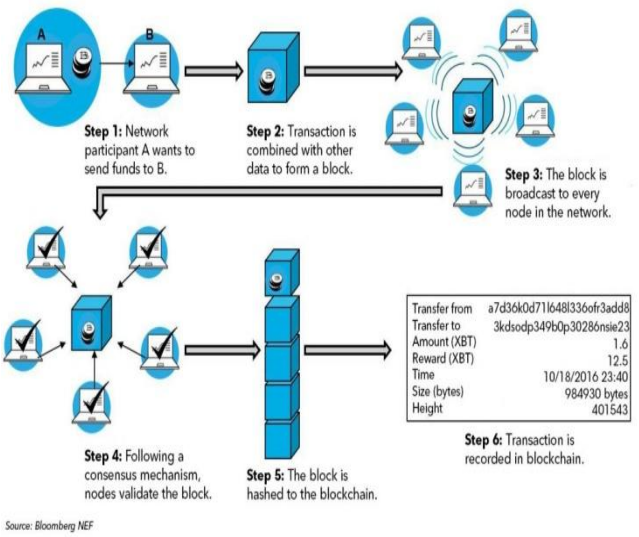

A
B
Step 1: Network participant A wants to send funds to B.
Step 2: Transaction is combined with other data to form a block.
Step 3: The block is broadcast to every node in the network.
Step 4: Following a consensus mechanism, nodes validate the block.
Step 5: The block is hashed to the blockchain.
Transfer from a7d36k0d71l648l336ofr3add8
Transfer to 3kdsodp349b0p30286nsie23
Amount (XBT) 1.6
Reward (XBT) 12.5
Time 10/18/2016 23:40
Size (bytes) 984930 bytes
Height 401543
Step 6: Transaction is recorded in blockchain.
Source: Bloomberg NEF

Fig7: Blockchain in cloud security

Clients are additional anxious with reference to information safety forever, and, particular the decentralized environment of blockchain, it might be how corporate and customers obtain relaxed among allocation their confidential facts designed for make use of in big algorithm progression.

VI. CONCLUSION

(1) Simplicity of blockchain installation and runtime: Pertain an innovative service prototype to BaaS. Raising the simplicity of blockchain installation along with runtime during the innovative relevance patterns on the way to decrease the harmful of BaaS proposal since an intermediation to the decentralization of blockchain. **(2) Consistency of BaaS communications:** Looking in support of an additional and adaptable assessment technique for BaaS infrastructure. Like this, the service sources otherwise the utility customers preserve improve the applicable mechanism or acquire equivalent defensive actions allows the valuation consequences. **(3) Protection of elegant agreements:** refinement of the current machine learning representation as well as carry out exploration on elegant agreements presentation development and involuntary renovation.

REFERENCES

1. Mohamed Rahouti, Kaiqi Xiong, And Nasir Ghani "Bitcoin Concepts, Threats, and Machine-Learning Security Solutions", Digital Object Identifier 10.1109/ACCESS.2018.2874539 VOLUME 6, 2018
2. Joe Abou Jaoude And Raafat George Saade, "Blockchain Applications - Usage in Different Domains", Digital Object Identifier 10.1109/ACCESS.2019.2902501 VOLUME 7, 2019
3. Sergii Kushch, Francisco Prieto-Castrillo "Blockchain for Dynamic Nodes in a Smart City" , 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) 978-1-5386-4980-0/19/$31.00 ©2019 IEEE
4. Shancang Li , Senior Member, IEEE, Tao Qin, and Geyong Min "Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems", IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS, 2329-924X © 2019 IEEE
5. Weilin Zheng, Zibin Zheng, Xiangping Chen, Kemian Dai, Peishan Li, And Renfei Chen "NutBaaS: A Blockchain-as-a-Service Platform" IEEE Access, Digital Object Identifier 10.1109/ACCESS.2019.2941905 VOLUME 7, 2019
6. M. Swan, Blockchain: Blueprint for a New Economy. Newton, MA, USA:O'Reilly Media, 2015.

7. E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, andY. Manevich, ``Hyperledger fabric: A distributed operating system for permissioned blockchains," in Proc. 13th EuroSys Conf., 2018, p. 30.
8. P. Hunt, M. Konar, F. P. Junqueira, and B. Reed, ``ZooKeeper: Wait-free coordination for Internet-scale systems," in Proc. USENIX Annu. Tech. Conf., vol. 8, no. 9, Boston, MA, USA, 2010.
9. J. Kreps, N. Narkhede, and J. Rao, ``Kafka:Adistributed messaging system for log processing," in Proc. NetDB, 2011, pp. 17.
10. (2017). Microsoft Azure Blockchain Solutions. [Online]. Available: https://azure.microsoft.com/en-in/solutions/blockchain/
11. (2018). Ethereum Blockchain as a Service on Azure. [Online]. Available: https://azure.microsoft.com/en-us/blog/ethereum-blockchain-as-aservice- now-on-azure/
12. Sergi Kushch, Francisco Prieto – Castrillo, “ Blco chain for Dynamic Nodes in Smart City” in 2019 IEEE 5th world Forum on Internet of things (WF-IoT)
13. Juntao Chen, Student Member, IEEE, and Quanyan Zhu, Member, IEEE “Security as a Service for Cloud-Enabled Internet of Controlled Things Under Advanced Persistent Threats: A Contract Design Approach” IEEE Transactions On Information Forensics And Security, Vol. 12, No. 11, November 2017.
14. [1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, and G. Lee et al. "A view of cloud computing.", Communications of the ACM 53, no. 4 (2010): 50-58.
15. Q. Zhang, L. Cheng, and R. Boutaba. "Cloud computing: state-of the-art and research challenges."□Journal of Internet services and applications□1, no. 1 (2010): 7-18.
16. M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and A. Vakali. "Cloud computing: Distributed internet computing for IT and scientific research." IEEE Internet computing 13, no. 5 (2009).

AUTHORS PROFILE

Beena G Pillai received the B.Tech degree in Computer Science & Engineering from Acharya Nagrajuna University, Guntur, in 2012, the M.Tech degree in computer science and Engineering from Jawaharlal Nehru Technological University, Anantapur, in 2015. She is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Gitam University, Bangalore. Her current research focuses on the security in Block chain technology, Cloud Computing and Cyber Security

Madhurya J A received the B.E degree in Information Science & Engineering from Visvesvaraya Technological University, Belgaum in 2011, the M.Tech degree in computer science and Engineering from Visvesvaraya Technological University, Belgaum, in 2017. She is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Gitam University, Bangalore. Her current research focuses on the security in Cloud Computing, Cyber Security, IoT.