IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-10, Oct 2019 E-ISSN: 2347-2693

Privacy Preservation in Blockchain IoT

Sapna Bhardwaj[1*], Sagun Sharma[2], Anuradha[3]

[1,2,3]Dept. of Computer Science and Engineering, JC Bose University of Science and Technology, Faridabad, India

[*]*Corresponding Author: anuangra@yahoo.com Tel.: 9810646641 , 7834884506, 7838839808*

DOI: https://doi.org/10.26438/ijcse/v7i10.185190 | Available online at: www.ijcseonline.org

Accepted: 10/Oct/2019, Published: 31/Oct/2019

***Abstract*—**Blockchain, as a decentralized and appropriated open record innovation in shared system, has received impressive consideration as of late. It uses a connected block structure to confirm and store information, and a linked block structure to verify and store data, and applies the trusted mechanism to synchronize changes in data, which makes it possible to create a tamper-proof digital platform for storing and sharing data.
In this paper, the privacy issues caused due to incorporation of blockchain in IoT applications by centering over the utilizations of our everyday use has been discussed. Besides, examining of usage of five security protection methodologies in blockchain-based IoT frameworks namely anonymization, encryption, private contract, mixing, and differential protection has been done. Different architectures for blockchain based IoT applications arediscussed that helps in ensuring privacy while performing a number of operations andtransactions.

***Keywords*--** IoT, Blockchain, Anonymization, Smart Contract, Trusted data access, Mixing, Bitcoin, Decentralized, Crypto currency, Privacy preservation etc.

I. INTRODUCTION

Previously, every one of the applications that can run distinctly through a confided/trusted in middle person (intermediary), presently with the creation of blockchain can work in a decentralized way, with no requirement for a central power or authority and can accomplish a similar usefulness with same assurance. Blockchain advances were a consequence of online digital money named as Bitcoin in 2008[1]. Bitcoin is acryptographic money, it is a decentralized computerized cash without a central director that can be sent from peer-to- peer on the distributed bitcoin network, and the explanation for such fast spread of Bitcoin was its nonattendance of control from any concentrated budgetary/financial element or authority.

A blockchain is an appropriated information structure that is duplicated and shared among the individuals from a system. To take care of the twofold spending issue, bitcoin was presented. The working of blockchain relies upon a decentralized dispersed record structure that is shared among each blockchain center point. The information on record is open and direct; hence every trade even from the earliest starting point of system can be analyzed using this clear nature[2].

As shown in figure 1 each square in the chain conveys a rundown of an exchanges and a hash to the past block.
The special case to this is the principal block of the chain called beginning, which is basic to all customers in a blockchain network and has no parent.

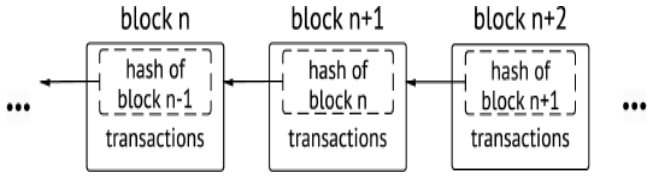


Fig 1: Structure of a Blockchain

1.1. Contribution of this article

While few researchers highlighted and surveyed concept of privacy preservation in blockchain technology, there is no article discussing the importance, application, and protection techniques of blockchain technology from IoT perspective, to the best of our knowledge. In this paper, we present state-of-the-art literature on privacy protection in blockchain-based IoT systems. In summary, the key contributions made in this article are asfollows:

- We outline various open issues, challenges, and certain future direction for research in privacy protection of blockchain-based IoTsystems.
- We highlight the importance of privacy protection in blockchain-based IoTsystems.
- We focus more over presenting the practical issues caused due to privacy leakage in IoT systems operating on blockchaintechnology.
- We provide an analysis about implementation of privacy protection techniques of blockchain-based IoTsystems.
- We focus on integration of privacy preservation technologies in practical applications of IoT systems working overblockchain.

© 2019, IJCSE All Rights Reserved

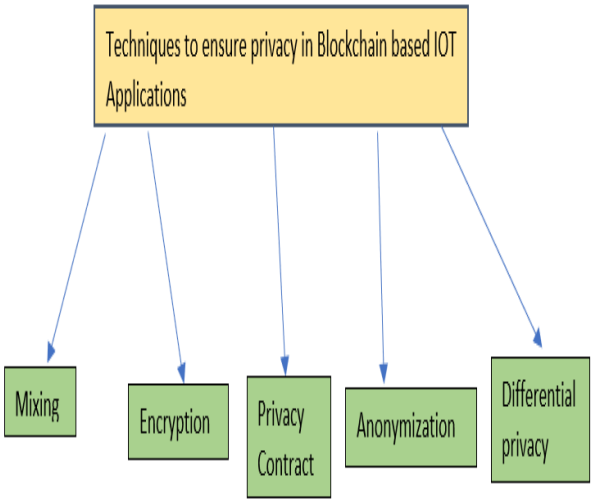


Fig 2 : Privacy preservation strategies in blockchain based IoT systems

The above figure 2 depicts the five privacy preservation strategies in blockchain based IoT systems: These strategies will help in preserving privacy in block chain IoT based applications i.e. different privacy attacks can be overcome by them.

In , this paper Section I contains the introduction of Blockchain , IoT and contribution of this work, Section II contain the related work of privacy preservation in blockchain IoT based applications , Section III contain the different methodologies used in this research work, Section IV describes results and discussion, Section V concludes research work with future directions.

II. RELATED WORK

2.1 Implementation of Smart Contracts Using Hybrid Architectures in blockchain IoT: Carlos Molina-Jimenez et al. [3] discussed about how smart contracts can be implemented to preserve the privacy in blockchain. In this paper the implementation of smart contracts on hybrid architectures have been discussed. As a proof of concept, it has been shown how a smart contract can be split and executed. A smart contract is an executable program that is deployed to mediate contractual interactions between two or more parties. Its task is to detect deviations from the agreed upon behavior[4].

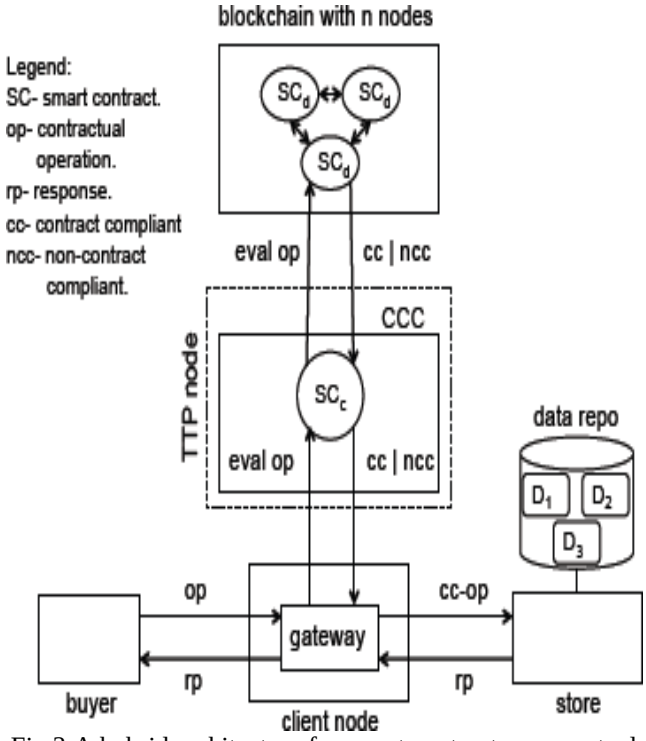


Fig.3:A hybrid architecture for smart contracts: conceptual view

The central idea of the hybrid approach is to divide the contractual operations into off-blockchain operations and on-blockchain operations as shown in figure 3. Off-blockchain operations are evaluated for contract compliance by a centralized smart contract deployed on a trusted third party. In contrast, on-blockchain operations are evaluated by a decentralized smart contract deployed on a blockchain.

2.2 Blockchain for IoT Privacy: The Case Study of a Smart Home: Salil S. Kanhere et al.[5] proposed a smart home engineering that is a blockchain based IoT application that safeguard protection and defeat the diverse attacks on privacy. Each smart home is outfitted with a ,constantly on the web, high asset gadget, known as "miners" that is answerable for dealing with all correspondence inside and outside to the home. The miner additionally saves a private and secure BC, utilized for controlling and examining interchanges[6].

In this paper it is being proposed that BC-based smart home system is secure by altogether breaking down its security as for the key security objectives of secrecy, honesty, and accessibility.

Here, in figure 4 the smart home architecture based on blockchain based IoT has been shown. This architecture comprises of smart devices, local storage, overlay network, local BC where all transaction are done with preserving the whole privacy.

© 2019, IJCSE All Rights Reserved

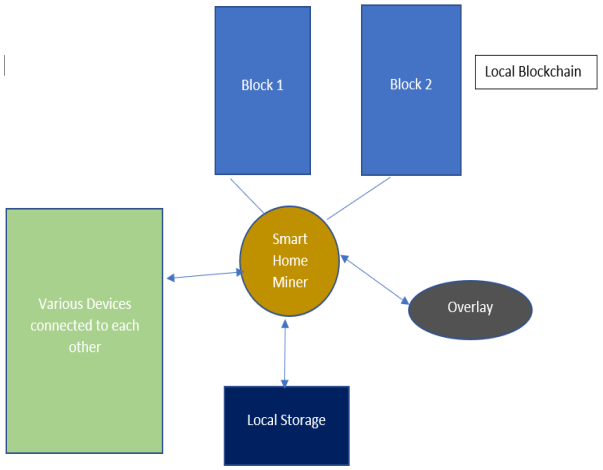


Fig.4: Overview of proposed smart home based on blockchain IoT

2.3: Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions: Muneeb et al. [7] discussed about the implementation of five privacy preservation strategies in blockchain-based IoT systems named as anonymization, encryption, private contract, mixing, and differential privacy. In this paper, challenges and future directions for research in privacy preservation of blockchain-based IoT systems has been discussed. This work can fill in as a premise of advancement of future security safeguarding procedures to address a few protection issues of IoT frameworks working over blockchain.

2.4: A Decentralized Solution for IoT Data Trusted Exchange Based-onBlockchain: Zhiqing Huanget al.[8] focused on the following layers with respect to blockchain based IoT data exchange platforms as shown in figure 5:

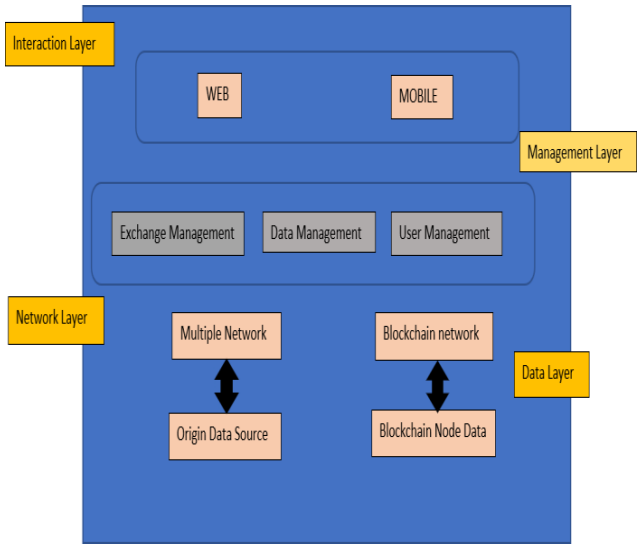


Fig 5 : Architecture of Blockchain based Iot data exchange platform

This paper deeply analyses current trusted requirements in IoT data exchange and divide them into three categories - trusted trading, trusted data access and trusted privacy preserve.

Trusted trading: This means the entire transaction process is recorded and cannot be modified by either party if onceconfirmed.

Trusted data access: This states that the dataowner can hold their ownership.

Trusted privacy preserve: This states that the data owner can protect their personal information during dataexchange. Besides, this paper provides architecture of above solution and detailed design of its main trust component. Finally, it realizes a prototype by using Ethereum blockchain and smart contracts and presents its auditable, transparent, decentralized features visually.

2.5: Privacy in Blockchain-Enabled IoT Devices
Privacy is always at stake when common resources are shared. The resource being shared being controlled by its current owner cannot be the ultimate solution to the problem. Arman Pouraghily et al. [9] discussed a solution to this challenge by introducing a trusted third party between the resource and the requester (of the resource), although finding such a trusted third party is a major task initself.

In this paper, a smart contract is being used as a third party between a device (the resource) and the buyer. The contract is created by the manufacturer of the camera once it is produced. The buyer needs to fill out the required details in the contract – public key, duration of feed which is requested etc. This is a design paper; the researchers plan to implement this design on Raspberry Pi in their next paper.

2.6:Blockchain's roles in strengthening cybersecurity and protecting privacy: According to Nir Kshetri [10], the need for blockchain arose from the fact that this technology can provide a robust and strong cybersecurity solution and better privacy as it is secured by design itself. The idea is that if an intruder manages to penetrate a network and tries to misfunction, the multiple redundant copies of the original prevents him from doing so[11]. Practically, about 50 % of the systems in the network need to be hacked in order to successfully alter the original contents.

The researcher also focuses on the fact that blockchain has not been used and adopted widely enough to be used at its maximum benefit. Most organizations in the networks tend to use the same piece of code with minor modifications only. The paper also draws a comparison between a centralized cloud model versus a decentralized blockchain model as solutions to enhance security and privacy. A major part of the paper focuses primarily on IoT security.

© 2019, IJCSE All Rights Reserved

III. METHODOLOGY

Internet of Things (IOT)
We can state IOT as a network of devices which can sense, accumulate and transfer data over the internet without human intervention. IOT is an ecosystem of connected physical objects that are accessible through theinternet.

The adoption of IoT-based technologies emerges with so many new opportunities in various aspects of our daily lives, Many researchers conclude that blockchain technology is the missing link to settle scalability, privacy and reliability concerns in the Internet of Things. Blockchain technology can be used in tracking billions of connected devices and enable the processing of transactions and coordination between devices. In context of IoT, blockchain permits two devices to communicate and exchange, resources, information, and data in a decentralized peer-to-peer (P2P) network.
There are different types of blockchain available:

Public blockchain: A permission less or public blockchain is essentially an open source decentralized stage in which each individual autonomous of its association or foundation can join, and can perform mining or exchange operations[12]. Every node participating in blockchain has full authority to perform operation of reading, writing, auditing, or reviewing of blockchain at any instance of time.

Private blockchain: A permissioned or private blockchain system is a decentralized network which is designed to assist private exchange and sharing of volume/data within an organization or specified group ofpeople.

Consortium blockchain: Consortium blockchain framework is commonly considered as a merger of public and private blockchain. A multi signature plan is utilized to mine the block in the system, in which the mined block is as it were considered as a legitimate block if the controlling hubs affirm and sign it up.

Integration of block chain with IoT
The interconnection of IoT hubs requires security, consistent validation, heartiness and simple support administrations. The decentralized nature of blockchain has resolved many security, maintenance, and authentication issues of IoT systems [13].The following figure 3 represents the various real life applications of blockchain with IoT:

such as home automation, intelligent transportation and manufacturing.

Blockchain
Blockchain is a new approach towards decentralized storage and data management, as it actually works over the concept of a shared, secured, and distributed ledger that stores and keeps records without any centralized authority or trusted third-party.

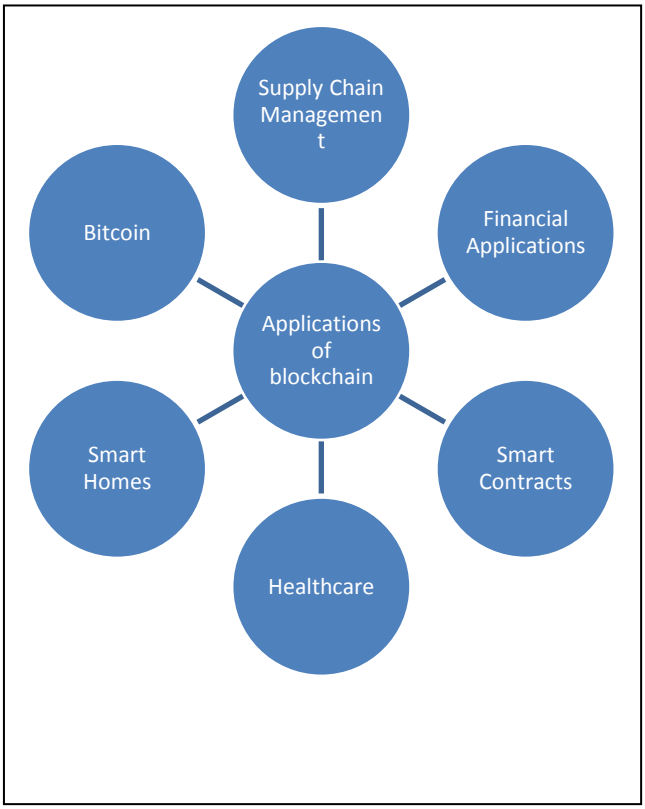


Fig 6: Applications of blockchain with IoT

The exponential growth of devices using Internet of Things (IoT) technology has attracted attention of both academia and industrial sector [14].

In traditional IoT systems, collected data is stored in certain centralized server for future use [15]. Therefore, IoT users have to develop trust for the centralized servers to ensure their sensitive and private data is safe in these servers.
There are some strategies / methodologies that are used to preserve privacy in blockchain IoT has been discussed:

ENCRYPTION
Encryption strategy is widely used in almost every blockchain network for secure transactions and data transmissions. Every user in blockchain network do receive different keys, one type of key is public key that is to be used by the other blockchain users in order to send the

© 2019, IJCSE All Rights Reserved

message to this specific node, and one private key to decrypt and read only the desired messages. This encryption and decryption phenomenon protects individual message and transaction privacy of blockchain transactions.

SMART CONTRACTS

In smart contracts based blockchain, the transaction details are not stored over blocks, instead a smart contract is written that contains all data and information related to transaction. Smart contract is like a programmable code operating over blockchain that IoT nodes can write according to the requirement of transaction, and then they can execute the contract into blockchain network. Once the contract gets deployed in the blockchain, it start execution and then no IoT user can stop this execution,not even the creator of code.

ANONYMIZATION

Anonymization is a famous method to preserve privacy in IoT based systems. Many researchers have applied anonymization techniques to protect privacy of blockchain-based IoT applications. In anonymization, personal identifiable information (PII) is identified in the data and these PIIs are then protected using various anonymization strategies.

MIXING

In transactions of mixing phenomenon, every blockchain IoT user transmits its encrypted fresh address to the mixer (third-party), which afterwards decrypts and shuffles the addresses randomly and sends it back to transmitter nodes. However, recent mixing strategies do not require involvement of third-party for mixing.

DIFFERENTIAL MIXING

Differential privacy is an efficient privacy preservation strategy to maintain the confidentiality of data without risking its leakage. C. Dwork first introduced the concept of differential privacy by presenting a mechanism that effectively protect database privacy by adding noise during query evaluation.

Now, further the privacy requirements and how different strategies can be used as a safeguard [16] to prevent privacy in blockchain has been discussed in table 1.

Table 1: Privacy requirements

Requirements	**Employed Safeguards**
Confidentiality	Achieved using symmetric encryption(Encryption)
Integrity	Hashing is employed to achieve integrity(Smart contracts)
Availability	Achieved by limiting acceptable transactions by devices and the miner
User control	Achieved by logging transactions in local BC.
Authorization	Achieved by using a policy header and shared keys

IV. RESULTS AND DISCUSSION

COMPARISON TABLE: Table 2 describes different methodologies, privacy trusted requirements and different strategies to preserve privacy in different papers.

Table 2: Comparison Study of different papers on the basis of different parameters.

Sr No.	**Major Contribution**	**Methodology discussed**	**Privacy / Trusted Requirements**	**Privacy Preservation Strategies (Yes / No)**
1	Implementation of Smart Contracts Using Hybrid Architectures in blockchain IoT [2018]	Smart contracts	Hybrid Architecture for smart contracts	Yes
2	Blockchain for IoT Privacy: The Case Study of a Smart Home[2017]	Encryption and Local BC	Smart home architecture to preserve confidentiality and integrity.	Yes
3	Privacy preservation in blockchain based Iot systems [2019]	1. AddressReuse 2. Wallet privacy leakage 3. Sybilattacks 4. Deanonymization analysis usinggraphs 5. Message Spoofing	1. Identity Privacy 2. Transaction Privacy	Yes
4	A decentralized solution for Iot data trusted exchange based on blockchain [2017]	1. Exchange management contracts 2. Data management contracts 3. User management contracts.	1. Trustedtrading 2. Trusted Data Access 3. Trustedprivacy Preserve	No

© 2019, IJCSE All Rights Reserved

5	Privacy in blockchain- enabled Iot Devices [2018]	Example of CCTV camera to explain the concept.	1. Privacy inshared Resources	Yes
6	Blockchains' s roles in strengthening cybersecurity and protecting privacy [2017]	-	None	Yes

V. CONCLUSION

The integration of Internet of Things (IoT) systems in our daily life is the need of the hour, and it is benefiting our lives in multiple ways- from smart appliances to smart assistants. This increased advancement has raised certain security and authentication challenges such as mining, hacking, and service denial attacks because of the centralized nature, but blockchain technology came up as an optimal way to overcome these challenges. IoT devices are capable of collecting, transmitting, and sharing highly sensitive information. This makes blockchain-based IoT systems vulnerable to various privacy threats that need to be resolved. Here, five major privacy preservation strategies being used in blockchain-based IoT systems such as anonymization, encryption, mixing, private contract, and differential privacy has been extensively covered in the paper. Within these privacy preservation strategies, we briefly surveyed the applications of IoT being used in our daily lives such as healthcare, finances, energy systems, vehicular networks, and wearable devices. In this context, this survey reviews the existing privacy issues associated with the blockchain network. Then, we present a comprehensive analysis of cryptographic protection mechanisms in terms of both anonymity and transaction privacy. Based on the review and discussions for these mechanisms that achieve privacy protection in the blockchain, we identify future research directions for blockchain's privacy protection.

REFERENCES

[1] S. Nakamoto, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions",Elsevier,2014.

[2] A.M. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies",O'Reilly Media,2014.

[3] N. Szabo, "Smart contracts: Formalizing and securing relationships on public networks," First Monday, vol. 2, no. 9, Sep. 1997.

[4] Carlos Molina-Jimenez,"Implementation of Smart Contracts Using Hybrid Architect- ures in blockchain IoT", arxiv,2018.

[5] Salil S. Kanhere, "Blockchain for IoT Privacy: The Case Study of a Smart Home" , CSIRO,2017.

[6] S. Sicari, A. Rizzardi, " L. A. Grieco,and A. Coen- Porisini, "Security, privacy and trust in internet of things: The road ahead", Computer Networks, vol. 76,pp. 146– 2015.

[7] Muneeb et al., "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions", IEEE, 2019.

[8] Zhiqing Huang et al., "A Decentralized Solution for IoT Data Trusted Exchange Based-on Blockchain",IEEE, 2017.

[9] Arman Pouraghily et al., "Privacy in Blockchain-Enabled Iot Devices", IEEE,2018.

[10] Nir Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy", IEEE,2017.

[11] A.Rayes,S.Salam, "Internet of Things", FromHypeto Reality, Springer, 2016.

[12] F. Tschorsch, B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies",IEEE,2016.

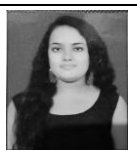
[13] A. Al-Fuqaha, M. Guizani, M. Mohammadi,"Internet of things: A survey on enabling technologies, protocols, and applications", IEEE,2015.

[14] A. Ericsson, "Mobility report: On the pulse of the networked society", Tech. Rep. EAB-14, 61078,2015.

[15] L. Zhou, L. Wang, Y. Sun, P. Lv, BeeKeeper,"A blockchain-based IoT system with secure storage and homomorphiccomputation", IEEE Access, 2018.

[16] A. Pal,B. Purushothaman, "IoT Technical Challenges and Solutions", Artech HouseI SBN: 978-1-63081-111-2, Norwood, Mass, 2016.

Authors Profile



Miss Sapna Bhardwaj pursued her Bachelor of Technology from BSAITM, MDU, Faridabad, Haryana, India. She received Gold Medal in Bachelor degree for being topper of Computer Engineering Department. She is currently pursuing Masters of technology in computer engineering from J C Bose University of Science and Technology, YMCA, Faridabad, India. Her main research work focuses on Blockchain , IoT, and Big data analytics based education.

Miss Sagun Sharma has done her Bachelor of Technology from BSAITM, MDU, Faridabad, Haryana, India. She has worked in a big data Analytics firm. She is currently pursuing her Masters from JC Bose university of Science and Technolgy, YMCA, Faridabad, India Her main research work focuses on Blockchain , IoT, and Big data analytics based education.

Dr.Anuradha Ph.D,Assistant Professor Department of Compter Engineering JC Bose YMCA University, Faridabad, Haryana ,India.Her main research work focuses on Database, IoT.

© 2019, IJCSE All Rights Reserved