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

Security Preservation in Blockchain IoT

Ajay[1], Ravi Kumar[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, 8221917551, 9416430134*

DOI: https://doi.org/10.26438/ijcse/v7i10.168173 | Available online at: www.ijcseonline.org

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

Abstract- With rapid development of Internet of Things (IoT), it is evident that users get convenience in different fields such as smart homes,transportation,supply chain, smart contracts etc.Blockchain Mechanisms play a vital role in securing many IoT oriented applications.Blockchain and IoT are both intended to be world changing technologies. Merging these technologies could result in something more than the sum of its parts.IoT security using Blockchain is aimed at providing better security mechanisms so that authentication, confidentiality and integrity constraints are preserved. Based on component interaction in IoTenvironment , the security measures that are depicted in the existing work ensures that no alien commodity is allowed to tamper the data and other devices in IoT environment. However IoT devices are surprisingly insecure.Hence security issue is one of the most challenging task for utilizing Blockchain.

Keywords- IoT, Blockchain, firewalls, DDOS, Availability, Decentralized, Crypto currency, Privacy preservation etc.

I. INTRODUCTION

Blockchain is a distributed technology that provides very hard to temper ledger record. It permits storage of all exchanges/transactions into permanent records and each record conveyed crosswise over numerous member hubs. The security originates from utilization of strong public key cryptography, strong cryptographic hash and complete decentralization. Blocks are the key components of this innovation; they are little arrangements of exchange that include occurred inside the framework. Each new block stores the reference of past exchange by including a SHA-256 hash of the past exchange. This way it creates a „chain‟ of blocks and hence the name "Blockchain". Blocks are computationally hard to make and takes various specific processors and huge measure of time to be created.

Miners are the individuals who run amazing PCs to make squares. Blockchain can be utilized to verify the work arranges in the IOT condition with the goal that associated gadgets are verified from any risk. Each IOT hub can be enlisted in the blockchain and will have a blockchain ID and will uniquely identify a device in the universal namespace.

For a gadget to associate with another device, one will utilize the blockchain ID as URL and will his nearby blockchain wallet to raise a personality request. The wallet will make a carefully marked solicitation and send to the focused on gadget that will utilize the blockchain administrations to approve the mark utilizing the open key of the sender [1].While there is numerous security proposals for IOT, for example, biometrics and two- factor approval yet blockchain is viewed as progressively secure of them all.

Blockchain contains solid insurance against information treating, locking access to IOT and permitting bargained gadgets in an IOT n/w to be closed down [1].

Figure 1 represents the various real life applications of blockchain with IoT:

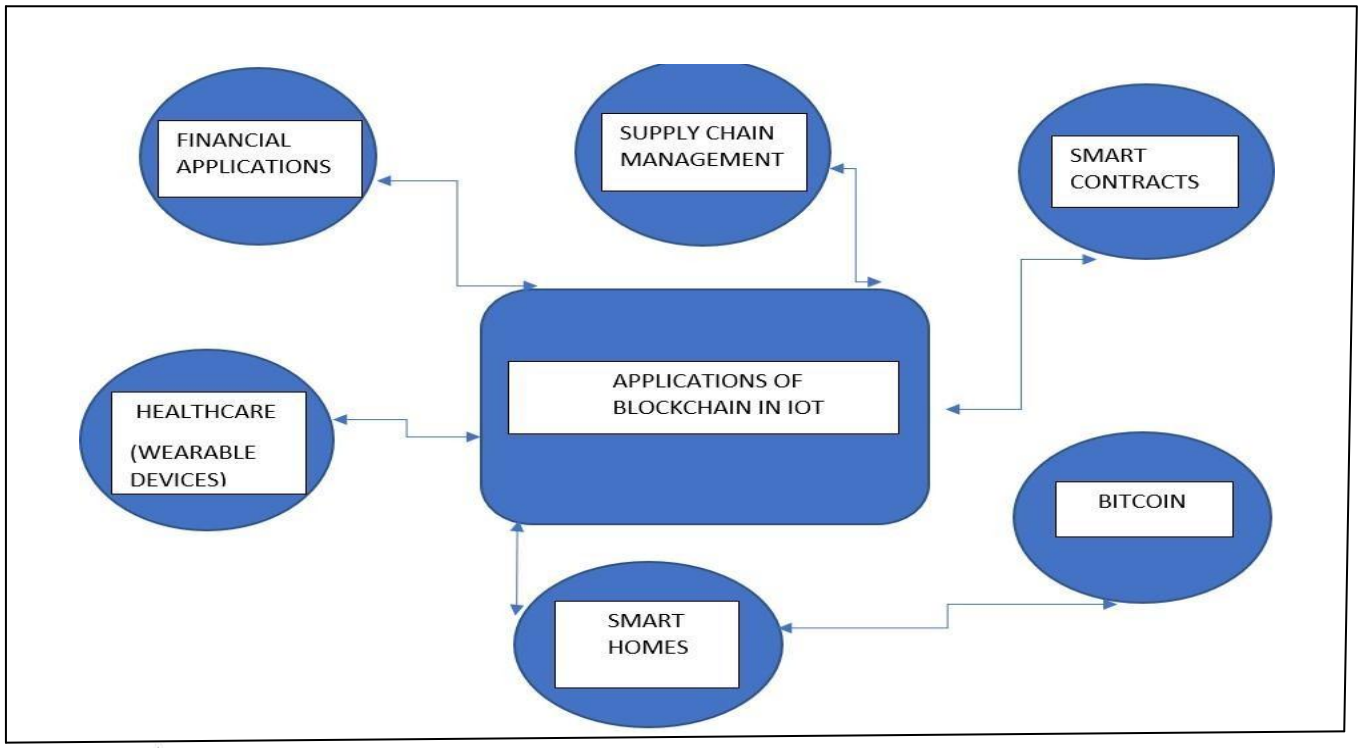

Fig : 1 Applications of blockchain

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

In traditional IoT systems, collected data is stored in certain centralized server for future use. Therefore, IoT users have to develop trust for the centralized servers to ensure their sensitive and private data is safe in these servers [2].
This paper presents the existing work in area of IoT security that is being expained in next section.

II. EXISTING WORK

2.1Blockchaintechnologyforsecurityissuesandchallengesin IOT

Manojkumar et.al [3] examined the different sorts of issues and moves identified with IOT security, for example, interopera- bility, absence of models, legitimate difficulties, administrati- ve issues, right issues, economy issues, etc. Blockchain innovation has following favourable circumstances:

1. Tamper evidence information
2. Trust-less and P2P informing ability.
3. Robustness, reliability and protection.
4. Distributed document sharing.
5. Elimination of single control authority.
6. Built in trust and quick exchanges.

Blockchain allows a peer-to-peer messaging in a faster way with the help of distributed ledger. In IoT with blockchain the data flow is from sensor-network-router-distributed blockchai- ns analytic user. Appropriated record doesn't permit any misinterpretations, wrong verifications in information. Difficulties in blockchain incorporate the constraint of record storeroom, restricted advancements in innovation, absence of legitimate lawful codes and models, absence of talented workforce, varietyes in appropriate speed and time such are some of basic issues tended to by IoT security. This work distinguishes the job of blockchain in IoT security and difficulties looked by this amalgamation of two wideadvancements/technologies.

2.2 A blockchain future for IoT security

Mandrita Banerjee et.al [4] studied the various types of Intrusion Detection procedures and their therapeutic technique- es in this specific paper. Most of the Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are intended to recognize unapproved access endeavours and DDoS(Distribut- ed Denial of Service).

Predictive security procedures focus on the quantitative secure- ty measurements which are helpful to evaluate the overall security of the framework, given that the splendidly secure framework doesn't exist.

As data inIoT environment is exchanges very frequently so the integrity of data must be ensured and preserved so as to guarantee the sense of reliability to the end-user. For maintaining the integrity of data Reference Integrity Metric (RIM) has been maintained using blockchain in the distributed ledger.

In the RIM approach for IoT security there is a focal centre point that keeps up references of part archives where the datasets are really put away and conveyed. The participation capacity is recorded and shared by every one of the individuals including the centre. There is another chain of obstructs that keeps up the RIM of datasets.

Blockchain compromised firmware detection and self-healing for compromised devices is another approach followed in this paper. The blockchain is an appropriated database that keeps record of the considerable number of exchanges. Since all participating devices maintain same record, unless an adversary manages to compromise the majority of devices, the integrity of records will be assured. Redundancy is regularly used to recuperate the defiled programming where the equivalent or comparable code replaces the ruined code. By utilizing the blockchain the historical backdrop of firmware can be followed, thus when compromised firmware is detected, it will be compelled to move back to its past form.

2.3 Blockchain mechanism for IoT security

Daniel Minoliet.al[5] reflected upon the different uses of blockchain in IoT security and certain security requirements in IoT in general and e-health and Intelligent Transportation Systems (ITS). Blockchains as clarified in this paper offer a component for individuals who don't have a clue or trust each other to make a common record of benefit possession. The blockchain is a period stepped database that holds the total logged history of exchanges on the framework, every exchange processor on the framework holds their neighbourhood duplicate of this database and agreement development calculations enable each duplicate to stay synchronized.

Interruption identification Systems Firewalls, availability , confidentiality , integrity and link encryption and decryption, these are some factors that are overcome by blockchain architecture. The functionality of blockchain has been shown in figure 2.

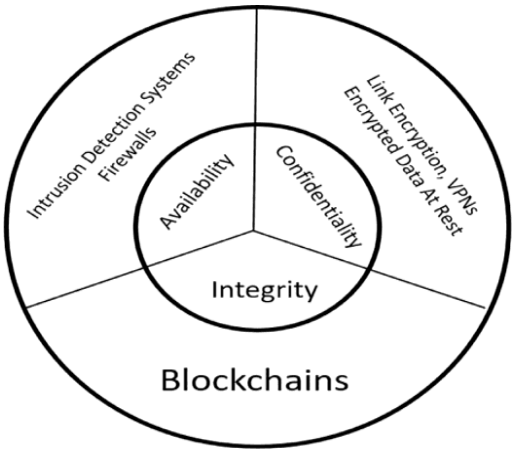

Fig:2 Functionality of blockchain

In a blockchain, the hash of a previous block in a sequence is a temper-proof sequence because as a function of the design, a hash is very sensitive. So, to change any variable of any one of the hashes in a given block would cause a domino effect, altering all of the previous transactions in the block. Form of Hash function used in blockchain has been shown in figure 3.

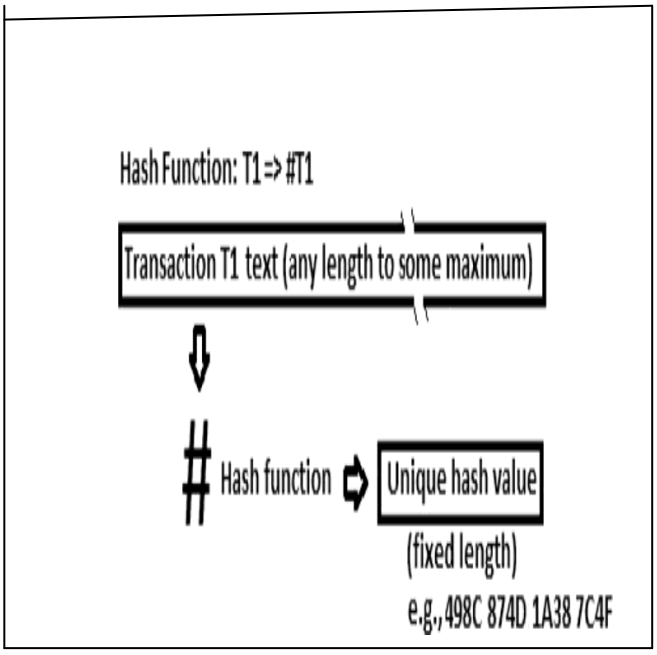

Fig:3 Hash function used in Blockchain

This paper focuses on the layer-wise appropriation of security instruments for IoT biological system. Various layers are independent in their functionality but they pass the information to upper layers in the architecture, in the IoT ecosystem the prime focus is on the integrity and the encryption of variety of IOT devices as shown in figure 4.

Typical Blockchain Environment in IoT

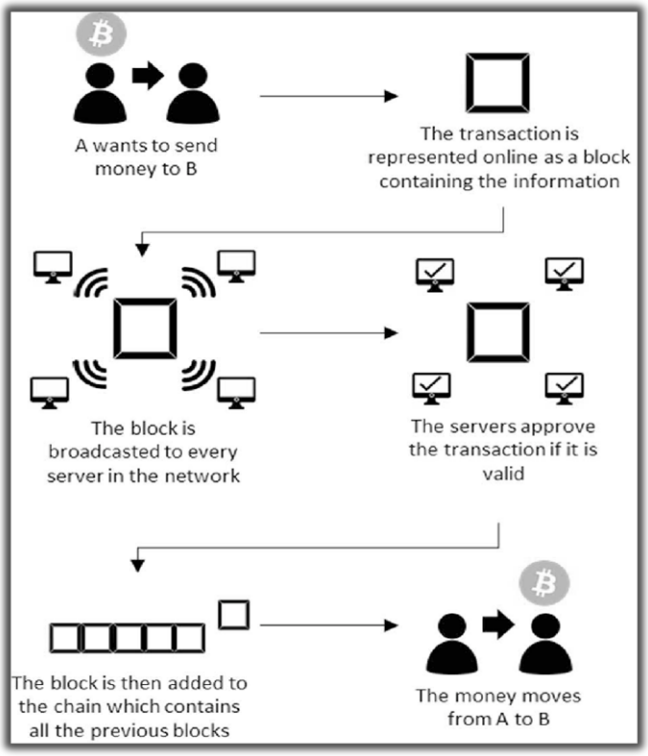

Fig 4. Typical Blockchain environment in IoT

Alongside giving security answers for IoT, blockchains should be joined with other security components including firewalling, encryption , confided in execution condition and other verification, approval and bookkeeping systems[6]. The upside of utilizing blockchains is that they can work at the lower layer of correspondence models just as at the application layer , along these lines empowering the synergetic utilization of mechanisms crosswise over layers and areas of the IoT biological system. Start to finish blockchains, examination/stockpiling level , door level , site level and gadget level area portion of the practical necessities of blockchain usage[7]. Every one of these necessities are mapped to the different layers of the security i.e in particular seven layers of the security which starts from gadgets and stacks upto the applicationlevel.

2.4 TowardsdecentralizedIOTsecurity,a blockchain approach

Yongfeng Qian et.al [8] proposed the combination of blockchain in the discernibility of IOT gadgets, which includes cooper ation between IoT gadget and the system transmission, IOT gadgets and the cloud. For the IoT devices and the network transmission the problems include the identify ication of malicious hotspots, malicious terminal access, abnormal traffic monitoring etc [9]. With the utilization of bloc kchain innovation, it can understand the validation without outsiders, spare/save the client time and henceforth bring QOE to the clients.

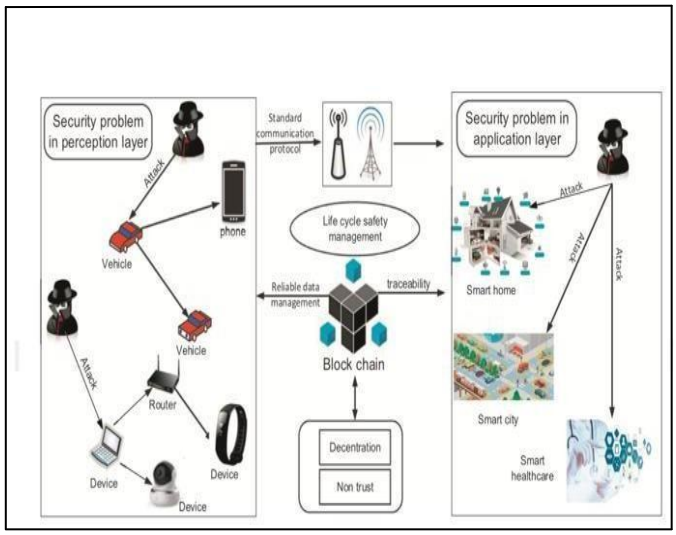

Fig 5: Blockchain enhanced IOT security architecture

With thought to IOT as help and blockchain innovation as the primary strategy, IOT resource database that faces enormous gadgets in full life cycle the executives is incorporated with the stage layer [10]. Terminal layer, security layer and application layer security issues are portrayed in this paper as shown in figure 5.

Blockchain record structure is utilized to confirm gadgets that interface with the system and cloud based administrations. Block chain maintains ledger for IOT devices which keeps track of all the related transactions that are executed and then consensus is made based on the entries of the ledger, that's why this blockchain architecture is called time- stamped database storage system.

The blockchain ledger structure for IoT devices has been shown in figure 6. Administration solicitations are made by the gadgets when associating with the system and information solicitations are adjusted through cloud based usefulness.

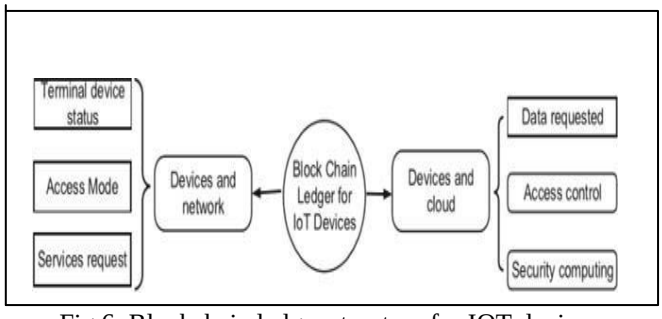

Fig 6: Blockchain ledger structure for IOT devices

This paper puts forward a distributed storage models on IOT based on blockchain and device ledger, where related production and application of IOT devices is analysed. In any case, with the expansion of IOT gadgets, there are huge IOT terminals [11]. Consequently, a lot of registering

power at terminals would fundamentally be expended dependent on conventional blockchain innovation. With respect to IOT, issues, for example, computational efficiency, security insurance, and supervision for circulated hub information the executives in blockchain must be understood. Along these lines, the foundation of blockchain based cloud stage for IOT gadgets [12] the executives in the full life cycle can be considered, contingent upon the disseminated cloud calculation.

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 the internet.

The adoption of IoT-based technologies emerges with so many new opportunities in various aspects of our daily lives, such as home automation, intelligent transportation and manufacturing.

Blockchain

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.

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.The exponential growth of devices using Internet of Things (IoT) technology has attracted attention of both academia and industrial sector.In traditional IoT systems, collected data is stored in certain centralized server for future use. 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 methodologies that can be used to overcome securities issues and attacks:

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.

IV. RESULTS AND DISCUSSIONS

Comparison Table

	Author's Name	Motive/Major Contribution	Security Attacks	Security Requirements
1.	Manojkumar et.al [3]	The scope for Block chain integration with IOT is explained in this paper along with advantages and limitations.	Legal issues, DOS, Variation in Computing capabilities, Processing time, Scalability.	Reliability, availability, distributed file sharing, Decentralized computing.
2.	Mandrita Banerjee et.al [4]	Collaborative security techniques, Access control mechanisms, protocols, Predictive security techniques	Transaction attacks, firewall attacks firmware, compromising security	Hybrid encryption techniques, Game theory, Intrusion Detection systems, Firewall.
3.	Daniel Minoli et.al [5]	Functioning of cyber-physical systems, public key management, base station/gateway security.	Encryption security attacks, attacks on operating systems, password attacks, device keys.	Block chains for sensor data, end to end requirements, strong applications, strong user interface, secure key storage.
4.	Yongfeng Qian et.al [6]	Potential security risks are identified in this pap problems of layers are introduced.	DOS attacks, DDOS attacks, attacks smart home, attacks on smart cities, attacks on smart healthcare, and Security problems in perception layer.	Authentication, interaction between IOT device and remote cloud, high-security management mechanism to archive overall Security management

V. CONCLUSION

The pattern of joining of Internet of Things (IoT) frameworks in our day by day life is expanding exponentially, and it has profited our lives from multiple points of view. This progression has raised certain security and validation difficulties, for example, mining, hacking, and administration refusal assaults as a result of incorporated nature, however blockchain innovation came up as an ideal method to beat these difficulties. Nonetheless, blockchain-based IoT frameworks are likewise helpless against different protection dangers that should be settled before their handy usage.

IoT security using blockchain has been studied extensively in the four scenarios. These scenarios have been examining the data being attacked and DDoS in IoT environment. Security measures for IoT integration in blockchain is duly enhanced by certain advantages as being offered by blockchain mechanisms. Variety of encryption attacks and masquerades are prime form of attacks and their impact is studied extensively in this paper.

REFERENCES

[1]S. Ølnes and A. Jansen, ``Blockchain technology as infrastructurein public sector: An analytical framework," in *Proc. 19thAnnu. Int. Conf. Digit. Government Res., Governance Data Age*,New York, NY, USA, 2018, pp. 77:1_77:10. [Online]. Available: http://doi.acm.org/10.1145/3209281.3209293

[2]R. Beck and C. Muller-Bloch, ``Blockchain as radical innovation: Aframework for engaging with distributed ledgers," in *Proc. 50th HawaiiInt. Conf. Syst. Sci.*, 2017, pp. 5390_5399.

[3]NallapaneniManoj Kumar, Pradeep Kumar Mallick,"The Internet of Things: Insights into the building blocks, component interactions, and architecture layers", 2018,www.keaipublishing.com/en/journals/digital- communications-and-networks.

[4]Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo,2018, ScienceDirect.

[5]Daniel Minoli, Benedict Occhiogrosso DVI Communications,2018, Elsevier

[6]YongfengQian,YingyingJiang,JingChenetal.,MatevžPustišekSchoolofComputerScience,ChinaUniversityofGeosciences,Wuhan,China,SchoolofComputerScienceandTechnology,HuazhongUniversity ofScienceandTechnology,Wuhan430074.

[7]ABassi,MBauer,MFiedler,TKramp,RvanKranenburg,SLange,SMeissner(Eds.),EnablingtheInternetofThings,Springer,2013.

[8] A.K. Pathan (Ed.), "Securing Cyber Physical Systems", CRC,2015.

[9]A.M. Rahmani, P. Liljeberg, J.-S. Preden, A. Jantsch, "Fog Computing in the Internet Of Things" , Springer,2017.

[10]Q.Hassan,A.R.Khan,S.A.Madani(Eds.),"InternetofThings:Challenges,AdvancesandApplications",CRCPress, 2017 ISBN9781498778510.

[11]A. Pal, B. Purushothaman, "IoT Technical Challenges and Solutions," ArtechHouse ISBN: 978-1-63081-111-2,Norwood,Mass,2016.

[12]A.Rayes,S.Salam,"Internet of Things From Hype to Reality",Springer,2016.

Author's Profile

Mr.Ajay pursued Bachelor of Technology in Computer Science& Engineering from GJUS &T Hisar Haryana in 2017. He is currently pursuing Master of Technology in Computer Engineering From JC Bose YMCA University Faridabad, India. His main research work focusses on the Blokchain, IoT.

Mr. Ravi kumar pursued Bachelor of Technology in Computer Science& Engineering from NGFCET, MDURohtak Haryana in 2016.
He is currently pursuing Master of Technology in Computer Engineering From JC Bose YMCA University Faridabad ,India.His main research work focusses on the Blokchain,IoT.

Dr. Anuradha Ph.D,Assistant Professor
Department of Compter Engineering JC Bose YMCA University, Faridabad, Haryana, India

