Leveraging BlockChain for Security and Authentication of IoT Devices

Sheeba DM
Department of Computer Science
New Prince Shri Bhavani Arts And Science College
Chennai, India
sheebadm@gmail.com

Dr.S. Jayalakshmi
Department of Computer Applications
School of computing sciences
VISTAS , Chennai,India
jai.scs@velsuniv.ac.in

Abstract—**Authentication in IoT architecture is depends on third party institutions, Certificate Authority, Identity Management; these could be vulnerable since it is prone to single-point-failure attacks. When Authentication method is intruded, it is difficult to identify data theft and other security vulnerabilities. To mitigate these and provide enhanced security against attacks, BlockChain is a foolproof methodology Secure, immutable, distributed ledger for IoT. Each IoT node to be assigned with the DeviceID in the BlockChain , such a way each other can authenticate securely. Hash of the firmware data is stored securely in the blocks and state change triggered when any attacks against the firmware. Finally proposed solution demonstrated using HyperLedger.**

Keywords—IoT blockchain; identity authentication; security; data protection;

I. INTRODUCTION

Internet of things (IoT) brought a revolution in devices connected to network and growth is ever slowing, there are reports which define connected devices will be more than human population in near future. Whereas a small issue in all the connected devices may cause a disaster effects in daily life. Enterprises are utilizing the power of IoT in all spheres starting from procurement till delivery of services to end customers. Mirai malware accounts for 39% of attacks and causes minor damages until it activates itself. Authentication plays a key role in enabling entire architecture of IoT systems since it follows conventional point of authentication in CA or through username password; it is prone to fail when central authority goes down. Also primary and public key based infrastructures are vulnerable in IoT

Central Authentication mechanism can be removed completely and enabled with BlockChain which follows distributed Ledger to create a nodes and blocks. This allows each of the nodes to check and verify adjacent nodes are valid or otherwise never allowed in system to take part in transactions. Since there is no central validator, every node ensures at all times BlockChain remains with only authenticated nodes through hash rates [1]. Immutability of the block ensures even the internal node cannot alter the content of already completed transactions.

For Security and Authentication, BlockChain brings a proven methodology where each node is securely can be validated with feasible solution over BlockChain. Irrespective of low computing resources or high, deploying BlockChain is possible, since it requires less computing power. Centralized authentication is changed to multi-centered or decentralized through BlockChain implementation and allows devices to improve security. IoT networks are vulnerable since it always has a two-way communication with critical data payload and it makes prime target of hackers.

So Ensuring security in IoT is inevitable and need of the hour. System stores DeviceId, its public Key and critical data hash so that device authentication is allowed based on request [2]. Hash provides immutability and it can validate any change made to data. IoT security mechanisms are yet to be standardized as a International practice and requires lot of attention from researchers on the Security Frameworks. BlockChain for IoT devices brings proven Immutability and Data Security in the form of Blocks and Transactions. Even insider attacks are eliminated since distributed ledger with peer to peer validation in place, before making change to written data Node to ensure it is having 51% of whole Block capacity [4]. So Blockchain basic features provide best in class security to IoT Devices.

II. RELATED WORKS

Although BlockChain (BC) is mostly used for Bitcoin and Crypto currency, Applications of BC reached over to all other industry like Accounting, Retail, Agriculture, Management and Government Organizations [15]. Also it is evaluated for most of the Authorization and Identity management problems in Computer Networks.

A BlockChain oriented identity management protocol is proposed to achieve a framework, architecture to bring the transparent identity validation. Also introduced FairAccess as a fully decentralized pseudonymous and privacy preserving authorization management framework [3]. Decentralized trust verification for eliminating Denial of Service attacks and Docker image verification is mentioned along with trustless signature verification [4]. Elimination of Distributed denial of service attacks through secure BlockChain of existing fraudulent IP addresses [5]. A decentralized data management of personal information is proposed through BlockChain and it limits the central authority for authorization; also provides mechanism for secure personal information management through BC. Security and privacy ensured when BC handles the data storage, access and retrieval [6].

Elliptic curve cryptography and smart contracts architecture proposed to mitigate the DDoS attacks by automated validation of IP protocols and application layer security [7]. Validation of firm-ware version and its integrity is ensured using BC approach. Node can initiate the firmware request to peers and validate its version against the latest one, latest version downloaded if old is used and updated [8]. An enhanced version of security authentication proposed using BC and password authentication done at end of network transactions life cycle in [9].

Use of BlockChain proposed to store the financial transactions to ensure credibility of audit records in [10]. An approach to validate anti-quantum entries is proposed using BlockChain in the paper [11].

An user authentication approach is proposed where identities are stores and encrypted using the BlockChain. Smart contracts are enabled with permission to each application or site for read or write access [12]. An authentication in cross domain applications proposed in the paper and Certificate Authority to enable authentication used to ensure the security and data privacy [13]. Large data verification and validation proposed using BlockChain in distributed environments [14].

All of the studies performed shows that it concentrates on trust management, data protection. Proposed mechanism brings the simple way of bringing peer to peer authentication and immutability of authentication ledger, identity management through firmware data storage in block structure.

III. Problem Definition

A. *Node Integrity Validation*

In IoT Architecture to ensure data privacy and security, ensuring the node authorization plays a critical role. Without authentication control mechanism, data is at risk and also be exposed to outer Networks. The node attached to IoT network is authenticated using username and password, proof validation, Authorization token from certifying authority.

Public key based cryptography is used to authorize the nodes in IoT network and also a peer to peer authentication without any third party authorization members using BlockChain followed to provide high security and data integrity between nodes.

B. *Node Security Mechanism*

To ensure every node in IoT network is secure and protected against the attacks of external entities, It is essential to introduce a security Authentication along with multiple layer of authorization. Malicious node may get access to the IoT layer first time and may modify the configuration files to get access in future attempts. This will cause damage to entire network of devices exposing the data to external entities.

Given the scenario every IoT network has to have mechanism to address the real time security measure and also each node to be monitored by peers so that attacks can be eliminated.

Real time scanning or authorization provides additional layer of protection and also ensures all nodes are trustworthy to share any protected data among the entities.

C. *Security Mechanisms*

1) *Device Additions Control*

Every node or physical device in the IoT network is controlled through registration in BlockChain using DeviceID, Physical entities and configurations. Each device is allowed to perform certain activities using the controlled flags, Example. Node A allowed to read a certain data only but whereas Node B is allowed to read data from the Chain also modify the data created by it in the past. This ensures that data requests always flow through Node B since it owns.

No device can have access to read or write unless it gets the signature through device additions and configurations from the chain should match with the physical device entries, unless it is verified and validated device will not have access to data, this ensures devices are controlled and data is protected at all times.

2) *Secure Communication Channel*

Secured channels are established between nodes to share the data, validate the identity, verify the data request etc. This ensures no third party has access to messages between nodes and cannot modify the messages active or passive attacks. Data integrity is high since it is communicated only to relevant parties.

Only authenticated nodes and which has hash of previous transactions is allowed to intercept the message and decrypt, unless node with correct hash others will not be able to read or understand.

3) *Fast Node Synchronization*

Device control information, secure channel messages are relayed to all nodes in chain effectively so that no delay expected in Verification and Secure Authentication by peer nodes. Each node is performing these transactions with higher priority than other write data operations. This provides the nodes an ability to ensure no attacker gains the access due to delay in authorization.

IV. Proposed Model

BlockChain is a well established mechanism in Financial Area; similarly it can provide enhanced Security, Audit Mechanism and distributed validation through Ledgers. BC can be adopted in any of the nodes in a given network systems. In our proposed model BC ensures that authentication is done even though few of the nodes are failed during the operation. Distributed peer to peer authentication ensures no central authority in between nodes to ensure all the requests are valid. Malicious node cannot have access unless half of the network signatures match with device information shared by malicious node.

IoT nodes are authenticated and added to BlockChain Ledger in network with DeviceID, Physical Identity, configurations on firmware etc. This information is stored and replicated to all other nodes in the multi layered IoT network. Whenever communication between nodes are established, first this public ledger is used to validate node is not tampered by physical attack or through malicious code by validating configuration against the shared ledger values. Public key cryptographic method can be established to validate the nodes.

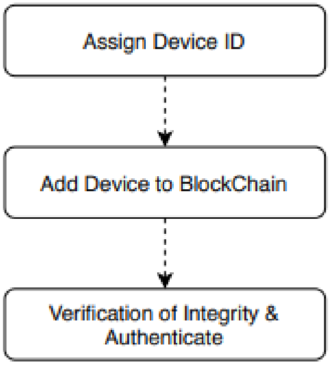

Figure 1. Device Addition Control

System is designed using three entities as below

1. Device Enrolment control ensures that each device go through formal addition to the network by the system administrator. First step should communicate node information to all other nodes in network as defined in III. C. 1.

2. Now device is enabled to access the network, it can notify the rest of the chain for read, write and modify requests. At this juncture rest of the nodes will ensure it is authenticated device through the verifications against its ledger. Verification includes DeviceID, Physical id and configurations defined during enrolment.

3. Verify that 50% of the nodes also have agreed that new device credentials are valid and it can be allowed to perform the transactions. Now the data level validation takes place to verify only intended operation is performed against dataset.

Figure 1. Shows the device enrolment and Figure 2 provides details about the system process.

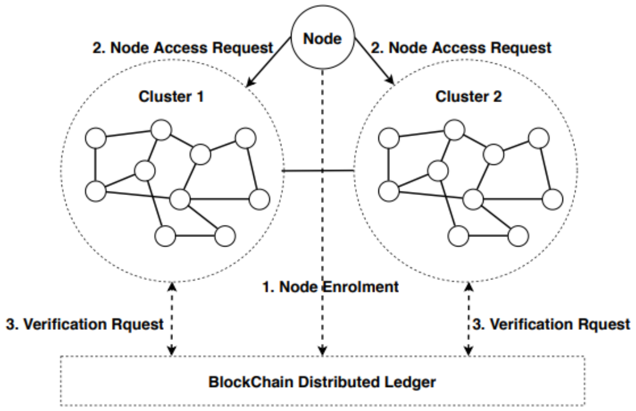

Figure 2. Authentication Mechanism

A. Types of Nodes in IoT

Two types of nodes present in IoT network as per their roles defined, first one is to provide consensus between nodes and enable to authorize other nodes requesting for access. Also communicates to other nodes about the authorization token and mode in which node should perform i.e. read, write and modify. Functions of nodes illustrated in Table 1.

Table 1. Functions of BlockChain Nodes

Node Roles	**Node Functions**
Consensus	Block Generation Block Verification Consensus Process
Non-consensus	Data Transfer

B. Enrollment of devices

Every node in IoT network has to register itself with BlockChain by generating the key pair as private key handled locally and its public key will be shared and saved in BlockChain. Node generates registration event to other consensus nodes.

On receipt of registration event, consensus node will be generating new block based on other nodes authorization, verification events. Requester node has to pass data to be added, DeviceID, physical id and configuration data in order to verify in authorization step. Hash of the data, configuration data are passed on to all the nodes involved in consensus and verification.

C. A Peer to Peer Authorization

```
------------------------------------------------------------
A_Node sends connection request (ID_Node_A, M_signed_
by_Node_A) to Node_B;
------------------------------------------------------------
// Node_B QUERY KEY_Node_A AND VERIFY THE IDENTITY OF Node_A

IF (KEY_ Node_A_EXISTS _IN_LOCAL)
      VERIFY THE IDENTITY OF Node_A;
ELSE
      IF (KEY_ Node_A_EXISTS_IN_CONSENSUS_NODES)
            VERIFY THE IDENTITY OF Node_A;
      ELSE
            REJECT THE CONNECTION REQUEST OF Node_A;

------------------------------------------------------------
```

Figure 3. Peer to Peer Authorization

As an example Node_A issues a generate request with message, Node_B receives the request and validates against its public ledger using public key. Node_A public key found in local ledger then it is used to validate the identity of Node_A. If not then it will try to send the request to consensus node, even then if it’s not found public key of Node_A then request will be rejected from authentication process. Algorithm explained in Figure 3.

D. Data Integrity Mechanism

Device enrolment process ensures the basic information and critical configuration hash data is stored in public distributed Ledger about each node participating in IoT network. To ensure data integrity between nodes, Asynchronous process is enabled to automatically scan the hash of nodes and validate its critical data against Ledger.

If any deviation from the Ledger hash entry then it is assumed that node is tampered and need to disable from IoT network, same is achieved through sending the disable instruction to consensus nodes. During next authorization process, consensus nodes will reject the generation requests. System administrators also informed about the node data integrity issues. This will enable remaining network is not affected and isolated from the rest of the attacks.

V. IMPLEMENTATION

This explains implementation of proposed model and BlockChain implementation with cryptographic key generation methods. Also provides details about Merkle tree hash transactions for data storage. Finally provides details on performance evaluation using proposed model.

A. *Environmental deployment*

To enable IoT BlockChain, We used Raspberry Pi with Hyperledger Fabric open source BlockChain for private uses. Every node is enabled using Pi and connected using adhoc networks.

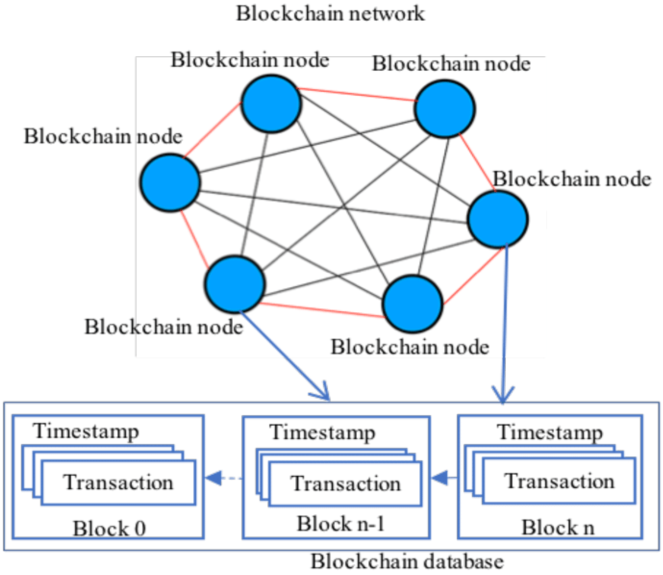

Figure 4. BlockChain Structure

Multiple layer of IoT network is arranges as clusters and each cluster works in its subnet. Each subnets can communicate with other layer as per requirements. This enables synchronous communication between clusters and consensus method effective between networks.

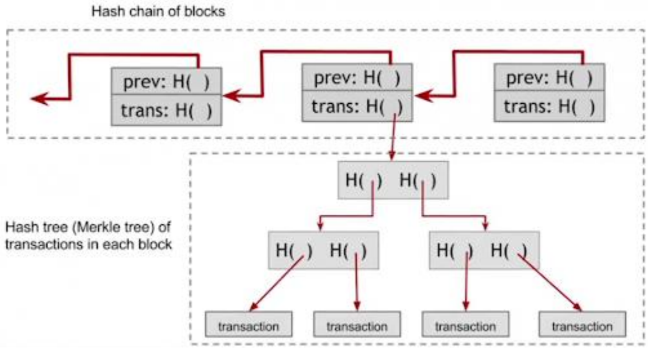

Figure 5. Data structure of the block

Transactions are stored as hashes in Blockchain and data structure followed based on Bitcoin structure. Transactions are like Device enrolment and Authorization instead of financial activities. All consensus nodes mines block header along with Timestamp, Merkle tree hash. On transaction part either Data transfer or Authorization entries present.

B. *IoT Node Transactions in Blockchain*

Transactions are the important data flow and also business requirement in the form of Authorization enablement for each node in IoT. Three types of transactions are enabled using Hyperledger smart contracts. Device enrolment is a write operation to chain and whereas Authentication and Verification is business validation which involves read from chain then send response to node request. Each of these transactions are placed in Hash data structure. Other Asynchronous data integrity check happens out of BlockChain and send signals to consensus node to update details in Chain. Transaction interactions explained in figure 6.

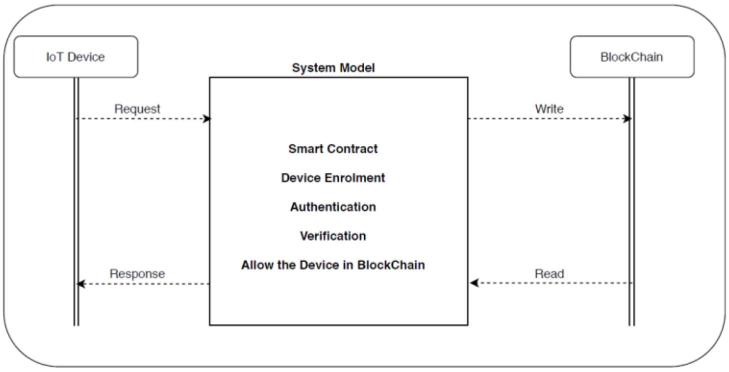

Figure 6. BlockChain – Device Interactions

C. *Key Generation Method*

In IoT network, each node is assigned with the unique device id and its corresponding public, private keys. Private Key is established using random methodology and key generated using elliptic curve algorithm.

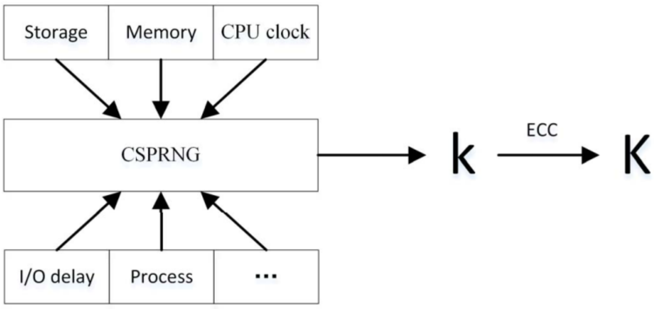

Figure 7. Key Generation Method

To ensure the randomness of the private key, we use the CSPRNG – cryptographic secure pseudo-random number generator which will provide the random number for each of the device in the IoT network. This is very critical aspect since Private Key plays role in authorization and data entries.

Apart from ensuring randomness, data is collected includes Configuration data, processing speed, clock speed and other aspects. The node data included as a seed to input mechanism.

Public Key is generated using elliptic curve method. The process is to calculate K which is public key by k*G, k is private random number generated above and G is constant. Figure 7 explains the key generation process.

D. Data integrity Verification

Distributed ledger method used in BlockChain and each file is signed in Hashes. So making the data modification and forge or stealing impossible.

Data storage method is shown in Figure 8. Hash values are used to store the data in files. Each of the hash value is used to generate the next hash making it so much difficult to interpret the hashes. This process repeats until root hash is arrived. The whole structure is called Merkle Tree which stores the data.

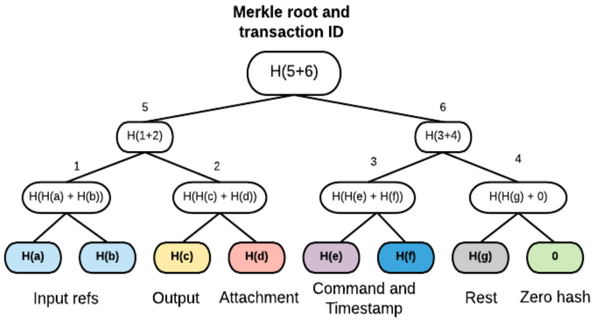

Figure 8. Merkle Hash – Storage

To verify integrity, Hash value of the file to be issued to validate signature against hash root of issued hash and current hash. This ensures data integrity.

E. Performance Evaluation

System is dependent on the Blockchain throughput and its delay so we are not discussing performance metrics. Below is the security performance evaluation against various attacks and systems advantage over it.

1) Malicious node Attacks

Peer to Peer authentication using the BlockChain is implemented. It ensures all the nodes should provide the authorization to do any activity so malicious nodes are eliminated and would not be allowed to enter in IoT network

2) DDoS Attack Mitigation

Distributed Ledger is shared among the nodes and if few of the nodes under attack, still the IoT network remains in active mode. Node under attack will be reported during Asynchronous scan which will scan firmware and configuration data. On the report from process administrator can take the action.

3) Firmware intrusion Mitigation

BlockChain utilized to ensure Authentication and firmware configuration data stored in the Blocks. Integrity validation process will enable the identification process of Firmware upgrade or configuration change, Process will disable the consensus or data generation request if finds any violation.

.

VI. CONCLUSIONS

In this paper, identified security vulnerabilities of existing Authentication mechanisms and provided BlockChain oriented immutable authentication using DeviceId and firmware data stored in Block itself. HyperLedger model explained the working of proposed mechanism and advantage over conventional approaches of authentication. Lightweight devices can also be enabled to use BlockChain based approaches and its implementation is simple, low-cost, provides proven security.

To further improve the approach, real time key phrase from user can be pulled to store the hashed value into blocks, Okta Identity management with real-time integration of IoT Device, Users and BlockChain can be enterprise level security mechanism.

VII. REFERENCES

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[2] Alexopoulos N, Daubert J, Mühlhäuser M, et al. Beyond the Hype: On Using Blockchains in Trust Management for Authentication[J]. 2017:546-553.

[3] Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: a new Blockchain based access control framework for the Internet of Things[J]. Security & Communication Networks, 2017, 9.

[4] Xu Q, Jin C, Rasid M F B M, et al. Blockchain-based decentralized content trust for docker images[J]. Multimedia Tools & Applications, 2017(239):1-26.

[5] Rodrigues B, Bocek T, Lareida A, et al. A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts[C]// IFIP International Conference on Autonomous Infrastructure, Management, and Security. Springer, Cham, 2017:16-29.

[6] Zyskind G, Nathan O, Alex. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]// IEEE Security and Privacy Workshops. IEEE Computer Society, 2015:180-18.

[7] Kumari S, Karuppiah M, Das A K, et al. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers[J]. Journal of Supercomputing, 2017(4):1-26.

[8] Lee B, Lee J H. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment[J]. Journal of Supercomputing, 2017, 73(3):1-16.

[9] Moinet A, Darties B, Baril J L. Blockchain based trust & authentication for decentralized sensor networks[J]. 2017.

[10] Lundbaek L N, D'Iddio A C, Huth M. Optimizing Governed Blockchains for Financial Process Authentications[J]. 2017.

[11] Yin W, Wen Q, Li W, et al. An Anti-Quantum Transaction Authentication Approach in Blockchain[J]. IEEE Access, 2018, 6(99):5393-5401.

[12] Zhang L, Li H, Sun L, et al. Poster: Towards Fully Distributed User Authentication with Blockchain[C]//Privacy-Aware Computing (PAC), 2017 IEEE Symposium on. IEEE, 2017: 202-203.

[13] ZHOU Zhicheng,LI Lixin,LI Zuohui. Efficient cross-domain authentication scheme based on blockchain technology[J]. Journal of Computer Applications, 2018, 38(2): 316-320.

[14] Abdullah N, Hakansson A, Moradian E. Blockchain based approach to enhance big data authentication in distributed environment[C]// Ninth International Conference on Ubiquitous and Future Networks. IEEE, 2017:887-892.

[15] Zhao J L, Fan S, Yan J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue[J]. Financial Innovation, 2016, 2(1):28.

[16] Callegati, F., Cerroni, W., Ramilli, M.: Man-in-the-middle attack to the HTTPS protocol. IEEE Security & Privacy 7(1), 78–81 (2009), https://doi.org/10.1109/MSP.2009.12

[17] Weaver, A. C.: Biometric authentication. Computer, 39(2):96–97, Feb 2006, ISSN 0018-9162.

AUTHORS PROFILE

Mrs. D.M Sheeba, Completed MSc in 2012 at Sun College of Engineering and Technology, Kanniyakumari and at present working as an Assistant Professor in Dept of Computer Science, New Prince Shri Bhavani Arts & Science College, Chennai. She is currently pursuing PhD in Computer Science at VISTAS, Pallavaram. Her Area of interest and research includes Network Security, and Cryptography, Internet of Things. She has been actively taken part and presented and published various papers in International and National Conferences in his research area.

Dr. S. Jayalakshmi working as Professor in the Department of Computer Applications, Vels Institute of Science, Technology and Advanced studies (VISTAS), Pallavaram, Chennai. She has more than 14 years of experience in both Industry and Educational Institute. Her area of research includes Natural Language Processing (NLP) and Data Mining. She has published more than 25 Research Papers in National and International journals. She is interested in writing textbooks for the students to make them understand any concept in an easy way. She is a recognized supervisor, guiding M.Phil. and PhD scholars.