Design of Secure Ehealth System Through Temporal Shadow using Blockchain

R Charanya, Ra. K Saravanaguru, M Aramudhan

Abstract: ***The eHealth record is a sensitive information need to protect from an unauthorized user. The privacy and security is the major issue in the eHealth record. These challenges will be overcome by a decentralized cloud. To Access the eHealth record from anywhere and at any time, the decentralized cloud is used to store the eHealth record which is generated by the medical institution and also by the individual. In proposed work, the technique which used is a temporal shadow. Each patient record is hashed with temporal shadow and the final aggregated hash value is stored it in the blockchain. Each file is authenticated by temporal hash signature. So the security of eHealth record is imporved with the help of temporal shadow and finally its stored in the blockchain.***

Index Terms*: *Temporal Shadow, Temporal hash Signature, blockchaina.

I. INTRODUCTION

The current eHealth system doesn't support to quick access and no privilege to access the patient medical history. There is no secure way to share the health record between different institutions. Presently, fax is used as a communication technology between the providers. This is a very slow process and in terms of security, no authentication techniques are used [7]. Another way to share the health record is Email which is less prone to remote attackers [6]. Due to the delay of receiving the eHealth record leads to delayed diagnosis [8]. Earlier they used the centralized cloud to store the eHealth record, Privacy and security is the major issue. The eHealth records are confidential information, need to protect from third party authority. These challenges will overcome by decentralized cloud. The decentralized cloud [5] is the peer-to-peer storage system. The copy of the health record is stored in all peers. Once stored in the decentralized cloud, it's difficult to modify, if someone tries to change the record, the changes affect the remaining record. In proposed system provides a secure framework to share the eHealth record between different institutions [1]. By using HL7 standard share the eHealth record between different providers in a secure way. Both providers should use the specified format to store the patient record. Storing the eHealth record in blockchain takes more cost, to avoid this Inter-planetary system is used. It's a protocol, it's a decentralized peer-peer technology is used. The doctor can generate the patient record in a specified format like pdf, doc, etc. This file is hashed and hashed file is sent to the blockchain. In proposed work, to make the system more secure, the temporal shadow is used, before hashing the patient record. To aggregating the hash value sufficient entropy need to be included.

II. RELATED WORK

According to research and market report, the value of Electronic health record is @23 billion in 2016 and anticipated that this should ascend to $33 billion by 2023[9]. Accordingly, there are numerous organizations overall planning to get into this exceptionally worthwhile business.

Q. Xia et al. specify the issues of accessing the sensitive data in the cloud, and how blockchain overcome this problem [2]. The history of patient information are examined and verified. The smart contract is used to specify the access policy, track the access information and revoke if there is violation to access the data.. The biggest challenge is to improve the quality of healthcare service and another issue is cost and time consuming. Most of the patients not ready to share the health record to others due to security and privacy problem. This is overcome by decentralized cloud. Initially blockchain is used for financial purpose and later its used to protect the personal data [4]. The primary focus of managing the health data in blockchain technology also focus on research studies. Some patient information are static data like gender, fingerprint, blood group, iris ,etc and some information are dynamic like age, height, weight, disease,etc, These data's can store it in blockchain, sometime data is very large then its difficult to store it in blockchain. The cost of storing the data is very high. The healthcare Data Gateway(HDG) framework [3] provide the rights to the patient to share, control and own without disregarding protection. The investigation of Medrec [2] built up decentralized health record service framework. The framework provides each patients with immutable log, and simple access of medical information between different provider. The medical chain also used blockchain to secure the medical record and transparent. The health record is encrypted with symmetry key and uploaded in the system [10]. The file is encrypted with user public key and it's uploaded in the database. Each patient record is hashed and it's stored it in the blockchain. Medichain[11] allows the user to store eHealth record in blockchain and allow to access the eHealth record by specialists, researcher, insurance companies, etc.

Revised Manuscript Received on April, 01 2019.

R Charanya, School, of Information, Technology, and Engineering, Vellore Institute of Technology, Vellore,

Dr. Ra.K Saravanaguru, School, of Computing, Science, and Engineering, Vellore Institute of Engineering, Vellore, India.

Dr. M Aramudhan, Department, of Information, Technology, PKIET, Karaikal.India

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Medichain used smart contract to set the privileges and store it in the blockchain [12].It's difficult to change the smart contract code and stored in the blockchain [13].

Medibloc is an eHealth system and it manages the medical data in a secure way [14], its purely patient-centric. Patient has the rights to share the medical record to anybody. The Qtum blockchain is used in the medibloc [15]. The access privilege is set in the smart contract, and access is given to healthcare provisional, researcher, etc., In medibloc, user mobile is used as a primary data storage, the problem arises if mobile lost. To reduce the cost of storing the health record in the blockchain, each health record is hashed and hashed record are linked by using Merkle tree. The eHealth record is more secure with the help of a hash tree. Each leave node is the hash value of the patient records, and the non-leaf node is the concatenation of the hash value of the leaf node. The root value is digitally signed with the leave node.

III. PROPOSED WORK

A. Blockchain

In 2008, the blockchain technology was invented by Satoshi Nakamoto. The blockchain is a peer-to-peer distributed ledger, blocks are connected chronologically, each block is linked with the previous block. The transactions are verified and stored in the block. Each block contains timestamp, previous hash value, and data. The data which stored in the block is verifiable and immutable. Once data stored in the blockchain cannot alter the data. The 51%of the participant validate and then block stored in the blockchain. Each peer maintains the copy of all transactions and it provides against single-point of failure.

B. IPFS

The Inter-Planetary File System(IPFS) is used for permanent file storage. This was proposed by Juan Benat. IPFS is a peer-to-peer distributed system, it connects with all peers and shares the records across the network. It replaces the HTTP with content addressing. Here it refers to a hash of files. The address of accessing the file contents itself. Each file has a unique hash address. The file size is greater than 256kb then the file is divided into subfiles, and each sub file is hashed and form a new hash this the address of the file. For hashing the file, if we use SHA 256 then hash value start with Qm0x…..This hash value is given as an input in the blockchain.

C. Temporal Shadow

Temporal shadow is considered to make the record more secure, by considering the in-time, out time, and in between time of health data is explained in fig 1. To make a more secure, temporal shadow with sufficient entropy is added in the record before aggregating the hash value. It generate the hash value, let consider the previous value, nonce value, and timing.

.

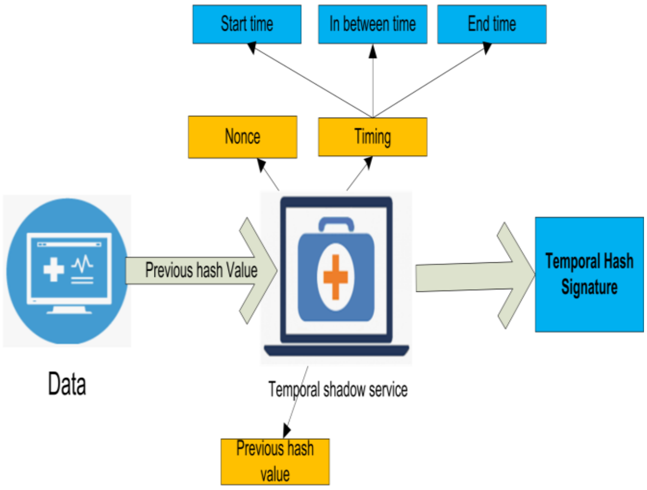


Fig 1: Temporal Shadow

D. Smart contract

The smart contract is a protocol of decentralized automation. Its digitally verify the code which runs on the blockchain. It contains the predefined rules which accept by the parties. If the condition met, automatically it gets executed. The solidity is the language which used in the smart contract. It agrees to interact with each other. No central control is involved in the smart contract. Each user is authenticated with the help of temporal hash signature. The process of verification is explained in fig 2.

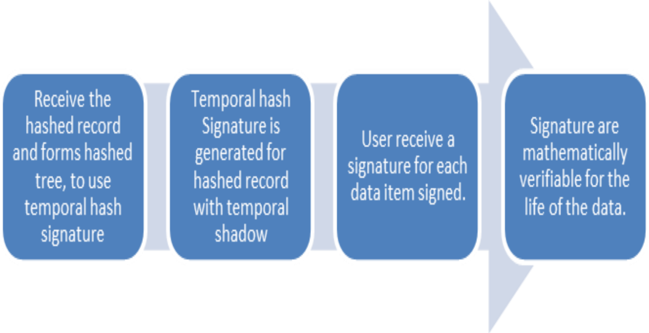

Receive the hashed record and forms hashed tree, to use temporal hash signature
Temporal hash Signature is generated for hashed record with temporal shadow
User receive a signature for each data item signed.
Signature are mathematically verifiable for the life of the data.

Fig 2 Process of Temporal hash signature

IV. SYSTEM ARCHITECTURE

The doctor can upload a patient health record to IPFS but only give access to the patient. The patient health record is encrypted with the patient public key. T Patient can retrieve the encrypted file and decrypt by using the patient private key. A malicious party cannot decrypt the file because of a lack of a patient private key.

To identify the data is generated by the authorized user, the digital signature is appended in the file. Any file type like pdf, doc, etc. can upload in IPFS network. The encrypted file is put in the working directory, which generates the hash of files. The hash file is available in the IPFS network. In the proposed system, the temporal shadow is added before linking the hashing value explained in fig 3. The hash chain is extracted from the Merkle tree,

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

each node contains the hash value of the other node. The temporal shadow eliminates the complication of a brute-force attack. The records are hashed with temporal shadow, the attacker finds the difficulty to identify the pattern of the hash value. The temporal shadow is added before hashing the record. While hashing the patient record, the following component need to be considered like hashed record r(i), temporal shadow ts(i), leaf hash value z(i), random number n(i), timing t(i), previous hash value z(i-1), non leave node z(i,j).

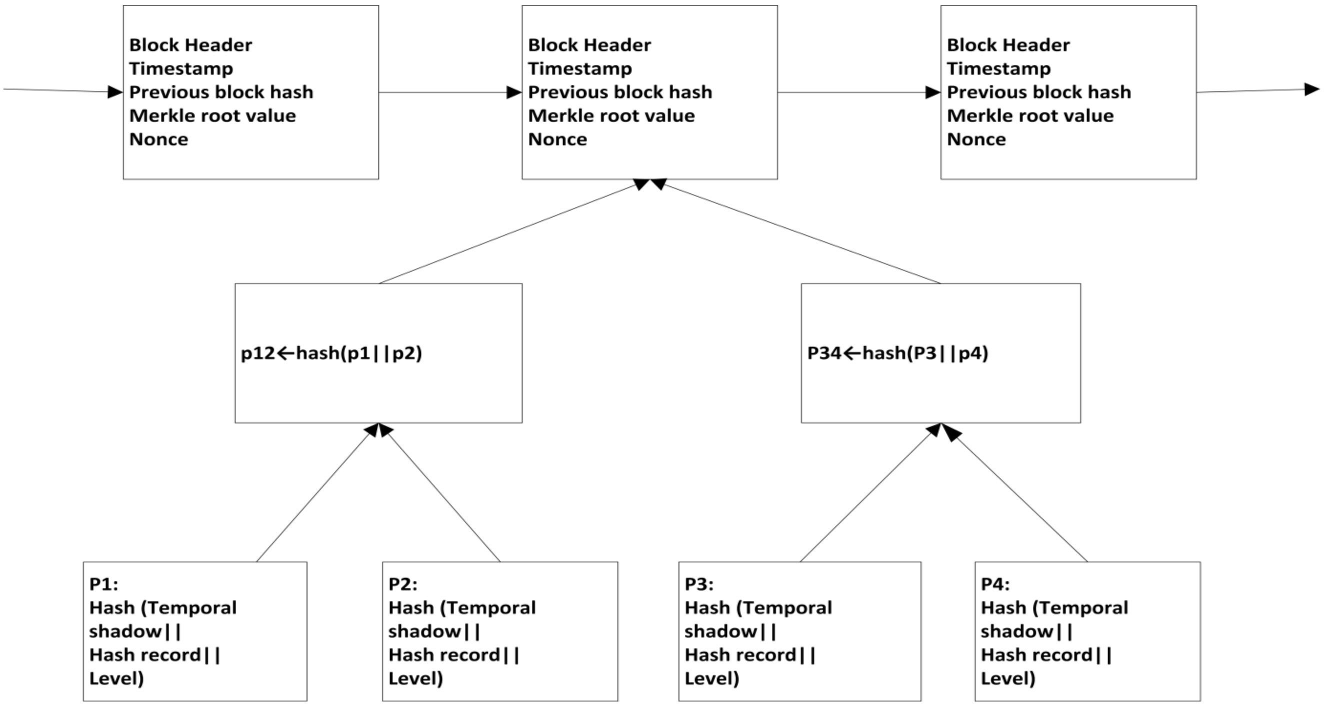
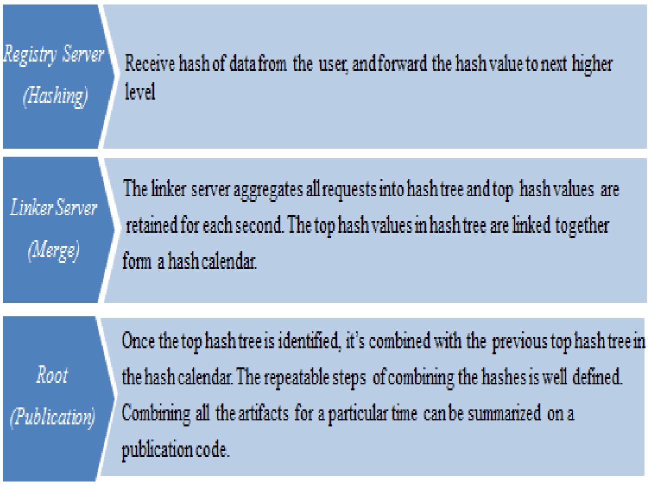


Fig 3: Structure of Temporal Shadow merkle tree.

The Temporal shadow is calculated with the previous hash value, nonce value, and timing. Here timing represents the start time, end time and in-between time. For example patient walk in the thread mill, start time is calculated on the start time of walk and end time is calculated based on the end time of the walk and in-between time is an intermediate value between the start time and end time of the walk. The temporal shadow is used to generate the hash value for the medical record. Here timing is calculated based on the generation of the patient record. For example, the patient went to the hospital, and explained the symptoms to the doctor, based on the symptoms, prescription given by the doctor. Start time is calculated when the doctor starts entering the details and end time is calculated when the doctor submit the details, in-between time is calculated based on the start time and end time. In fig 5 the initial hash value is received by registry server and linking all the hash values by linker server and form the root value, root value is stored in the root server.



Receive hash of data from the user, and forward the hash value to next higher level

The linker server aggregates all requests into hash tree and top hash values are retained for each second. The top hash values in hash tree are linked together form a hash calendar.

Once the top hash tree is identified, it's combined with the previous top hash tree in the hash calendar. The repeatable steps of combining the hashes is well defined. Combining all the artifacts for a particular time can be summarized on a publication code.

Fig4: Different Servers

The advantage of adding the nonce value is to increase security and also reduce the computational burden . Each record is appended with the height of the node. In the existing technique, there is no option to share the health record between providers. In proposed work, HL7 standard is used to securely share the eHealth record between the providers

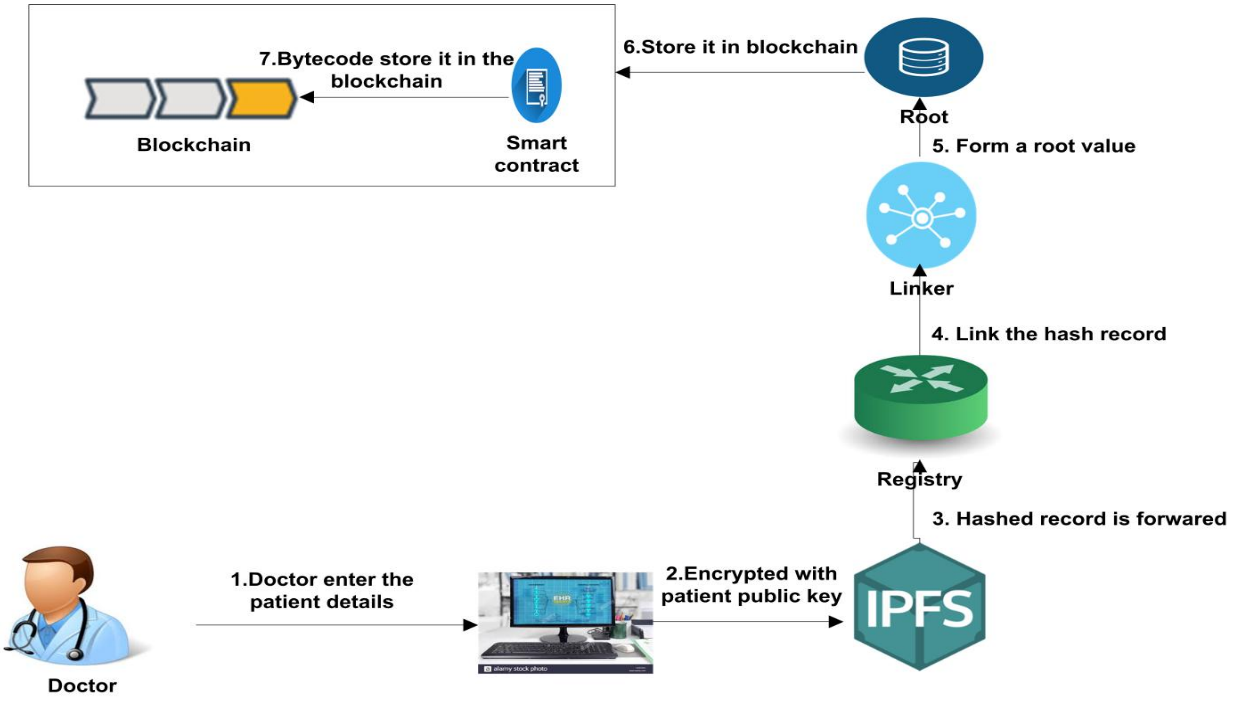

7.Bytecode store it in the blockchain
Blockchain
Smart contract
6.Store it in blockchain
Root
5. Form a root value
Linker
4. Link the hash record
Registry
3. Hashed record is forwarded
1.Doctor enter the patient details
2.Encrypted with patient public key
IPFS
Doctor

Fig 5: System Architecture

Algorithm 1:

Parameter:

z(i): Patient Health Record z(i-1): previous hash value
Ts(i): temporal shadow n(i) : Nonce l(i): level

Input: Set of Medical record received from the user.

Output: One time Signature X

Process:

```
1. Health record ‘r’ in proper format.
2. Health records r1, r2, r3, etc.
3. for (i←0; i<l;i++)
        z(i) ← hash((i)) // hashed health record   SHA256 algorithm
         t(i) ← hash(st(i)||et(i)||ib(i))// timing
         ts(i) ←hash(t(i)||n(i)||z(i-1))  //temporal shadow
         z(i) ←hash(t(i)||z(i)||l(i))     // hash the patient record with temporal shadow
4. Leaves node of the hash value is concatenated and form a root node by using merkle tree.
5. End for
6. System sends the signature token ths(i) to user, which is path from leaf node to root node
```

V. IMPLEMENTATION

The doctor can upload the patient file in the decentralized cloud. The doctor encrypts the file with the patient public key using RSA algorithm. A digital signature is appended with the file to know the file is generated by an authenticated doctor. The file can be accessed by content addressing. Then the encrypted file is hashed using SHA 256 algorithm, before hashing the temporal shadow need to be appended with the file. Temporal shadow is hashing the previous hash value, random number and timing. Temporal shadow is appended before hashing the record. ReactJS has used a front end and it's connected with dApp builder. It’s a decentralized application which is used to deploy it in Ethereum blockchain. The transactions agreement is written in a smart contract. Each transaction is validated against a smart contract. The solidity is the language which is used to develop a smart contract. The advantage of a smart contract is difficult to change the agreement. The smart contract is compiled and two components are generated like bytecode and application binary interface (abi). The bytecode is deployed in the blockchain and application binary interface defines a contract and invoke any function in the contract. In Fig 6 specifies about the time taken to execute the different file with different size is mentioned.

The x-axis is represent with file size and y-axis represent with time. According to the result, in terms of security, temporal shadow hashing is better than the existing hashing techniques. The temporal shadow provides secure storage of health record.

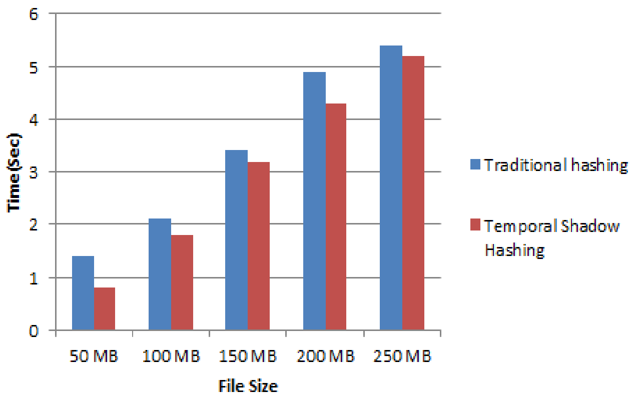


Fig 6:Compare Traditional hashing and Temporal shadow hashing

I. CONCLUSION

In this paper, temporal shadow is used in the proposed work which allow to access the eHealth record in secure way. This system is patient centric, it allows the patient to access the medical history. The temporal blockchain is used to store the anonymous health information. The temporal value is generated based on the previous hash value, random value and timing. The start time, end time and in-between time are considered for the timing. The user can access the patient record by giving the temporal hash signature.

REFERENCES

1. Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757-14767.
2. Xia, Q., Sifah, E., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2), 44.
3. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40(10), 218.
4. Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.
5. Satoshi Nakamoto. (2008, March). Bitcoin: A peer-to-peer electronic cash system. Technology, Economy and Finance.
6. Hanley, M., & Tewari, H. (2018, October). Managing Lifetime Healthcare Data on the Blockchain. In 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 246-251). IEEE.
7. Recommendation, T. (1988). Facsimile coding schemes and coding control functions for group 4 facsimile apparatus. International Telecommunication Union, Geneva.
8. V. Traynor, “2.5m award for terminally-ill woman over missed cancer,” Apr 2018. [Online]. Available: ttps://www.rte.ie/news/courts/2018/0425/957122-vicky-phelan/
9. “Electronic health records (ehr) market by product, type, application and end user - global opportunity analysis and industry forecast, 2017-2023,” Research And Markets, January 2018. [Online]. Available: https://www.researchandmarkets.com/research/65n56m
10. “Blockchain for electronic health records.” [Online]. Available: https://medicalchain.com/
11. “Medichain.” [Online]. Available: https://medichain.online/
12. Bacina, M. (2018). When two worlds collide: Smart contracts and the australian legal system. Journal of Internet Law, 21(8), 1-27.
13. Sklaroff, J. M. (2017). Smart contracts and the cost of inflexibility. U. Pa. L. Rev., 166, 263.
14. “Reinventing your healthcare experience!” [Online]. Available: https: //medibloc.org/en/
15. “Qtum the blockchain made ready for business.” [Online]. Available: https://qtum.org/en/

AUTHORS PROFILE

R Charanya has been associated with Vellore Institute of Technology (VIT), Vellore since June 2010 and presently working as Assistant Professor in School of Information Technology and Engineering (SITE). She has eleven years of teaching experience. She is doing her Ph.D in Computer Science and Engineering in the field of securing the ehealth system in blockchain. Her area of interest include cloud computing, Software Engineering, Blockchain. She published more research papers and conference papers in reputed journals.

Dr. RA K Saravanaguru has been associated with Vellore Institute of Technology (VIT), Vellore since June 2004 and presently working as Associate Professor in School of Computer Science and Engineering (SCOPE) and Assistant Dean Academics. He has sixteen years of teaching experience. He completed his Ph.D in Computer Science and Engineering in the field of Context aware middleware for vehicular adhoc network. His area of interest include context aware systems, middleware, web services, VANET, data science and network security.

Dr M Aramudhan received his B.E in Computer Science and Engineering from the Regional Engg. College, Trichy in 1997. In 2001 he completed his M.E in Computer Science and Engineering from Regional Engg. College, Trichy. He received his Doctor of Philosophy in Computer Science & Engineering at Anna University, Chennai in 2008. He is currently working as an Associate Professor in the Department of Information Technology at Perunthalivar Kamarajar Institute of Engineering and Technology since 2009. His area of interest is Computer Networks, Web Technology, Operating System, Data structure, Programming Languages, DBMS. He published more journals and conference paper in the reputed journal.