Privacy Assured Clinical Data Findings in Blockchain

Pushpalatha A1, Kausik M2, Logeshwaran RR3, Mohamed kamarudeen S4

M.E Phd, CSE, Sri Krishna College of Engineering and Technology, Coimbatore, India[1]
B.E, CSE, Sri Krishna College of Engineering and Technology, Coimbatore, India[2]
B.E, CSE, Sri Krishna College of Engineering and Technology, Coimbatore, India[3]
B.E, CSE, Sri Krishna College of Engineering and Technology, Coimbatore, India[4]

Abstract. EHR Data Storage is our platform which is decentralized, and privacy assured clinical data findings framework. The motive of the platform is to secure the data in the distributed storage with the 3-des cryptosystem to perform analytics without compromising the patient assets privacy. The existing methods can protect the data in case of transfer but cannot avoid the vulnerable which reveals the patient's sensitive data. Existing methods provides authority only for the data owners and makes them to distribute the decrypted keys only to authorized users. But in the proposed methodology, we introduce a efficient support called Dynamic groups where new granted users can decrypt the assets directly without the participation of data owners. Also in the proposed methodology, we ensure less transparency of assets in the centralized board but can be accessed in the decentralized storage called IPFS. The transparency is possible by Key procreation process.

Keywords—EHR, Decentralization, P2P, Blockchain, Smart contract, Clinical sensors, Data Storage, Privacy, TPA, IPFS, RL, EHR Data Storage, Truffle, Ganache, Web3 framework, Infura.

I. INTRODUCTION

A. Privacy Preserving Cloud Computing

In recent years, we have observed the extraordinary growth of remote clinical sensor organizations in the medical care manufactory. Remote clinical sensors are the state-of-the-art parts for medical services application and give radically worked on nature-of-care without relinquishing patient comfort. This network is an organization that comprises feathery gadgets with bridled memory, reduced calculation handling, less-battery power and reduced data transfer capacity. These clinical sensors (e.g., Electrocardiographic anodes, beat oxi-meter, circulatory strain, and temperature sensors) would be sent on understanding's body and gather the person's physiological information and transfers the gathered information by means of a remote channel to experts' palm-top gadgets (i.e., Personal Data Assistant, iPhone, PC, and so on) A medical practitioners can utilize these clinical sensor reports to acquire more extensive appraisal of hospital casualties wellbeing status. The patient's anatomical information might incorporate pulse rates, temperature, SpO2 level, and so forth A commonplace patient observing in emergency clinic climate.

B. Privacy exploitation on Data Storage Security in Cloud.

Putting away all asset in the cloud has turned into a pattern. An expanding unit of consumers stock their significant details in centralized servers in the cloud, excluding redundancy in their neighbourhood PCs. In some cases, the data stacked in the cloud is imperative at the point when the consumers should assure it isn't tampered. While it is uncomplicated to actually look at information after the backup information to be cross verified, localizing a lot of information only for checking information honesty is a misuse of correspondence transfer speed. Subsequently, a great deal of works has been done on planning far off information trustworthiness really looking at conventions, which permit information respectability to be verified without backing up the information. Distant information trustworthiness verification is first legitimated in which freely propose RSA-based techniques for taking care of this issue.

C. Dynamically Sustainable Data Asset in Medical Data Management

As capacity rethinking administrations and asset sharing organizations have become well known, the controversy of effectively professing the respectability of information storage at untrusted servers has been most considerable. In the PDP model, the customer checks the information and afterward sends it to a suspicious server for capacity, while holding a limited quantity of meta-information. The customer subsequently appeals that the stacked information has not been reformed or erased (without backup of the genuine information). [3] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking.

D. Productive Remote Data Asset Inspection in Critical Data Infrastructure

Really taking a look at information proprietorship in organized communities like those pinpointed with basic foundations (power officials, air fields, data vaults, guard frameworks, and so on) involves significant intention. Distant data proprietary checking conventions grant making sure that an outlying server can get to a righteous record so that the observer doesn't have to realize ahead of time the entire document that is being rooted. Lamentably, current protocol just legalizes a pre-established number of proceeding verification or are unfeasible according to the computerized viewpoint. This ideology presents another beyond information proprietorship validating convention with the motive that it grants a limitless number of document reputability proofs and its most extreme executing time can be pointed at set-up time and compromised resistant to extent at the verifier.

E. Benefits of Privacy Preserving in Clinical Sensor Findings

1) Public auditability

authorize without TPA to certify the accuracy of the cloud data on request without recovering a redundant data or conversing extra internet-based weight with the cloud consumers.

2) Capacity accuracy

to ensure not deceiving cloud server that can pass the TPA's audit without stacking clients' information flawless.

3) Security protecting

to ensure in the absence of TPA we have no clients' content from the data gathered during the inspecting system.

4) Group inspecting

empowering TPA with security to adapt in various inspecting environments with possibly huge number of various clients simultaneously.

5) Lightweight

perform scrutinizing with reduced resemblances and calculation overload without TPA.

II.RELATED WORK

In existing framework that presents Blockchain innovation was the fundamental thought was to have a cryptographically gotten and a decentralized cash that would be useful for monetary exchanges. Tragically, planning a proficient and secure information sharing plan for bunches in the IPFS (Inter Planetary File System) Monitor is not a simple undertaking. At last, this ideology of blockchain was being utilized in different forms of life; medical services area additionally being one of them plans to utilize it. Various specialists have done the exploration on this space, these examination works center around the way that whether utilizing blockchain for medical services area is attainable or not. They likewise distinguish the benefits, dangers, issues or difficulties related by the utilization of this innovation. A few analysts likewise examined the difficulties that would be confronted while really carrying out this for a bigger scope. If there should arise an occurrence of EHR frameworks, or overall medical care area is encountering this issue as specialists or emergency clinical approaches the causalities records, subsequently making it centralized. If a patient needs to get to his clinical records, he would need to follow a long and dreary cycle to get to them.

Here we present a certified safe and proficient universally practiced calculation modules to resolve this issue. This is a well-graded way for securely acquiring capacities. The peculiarity of our answer is based on mysterious distribution plan and the plan of the convention suite. The proprieties of SHAREMIND are suppositionally secured in essence Albeit the genuine however inquisitive model doesn't endure noxious members, it actually offers an expanded security conservation when heterogeneous with standard databases. [5] discussed that the activity related status data will be communicated consistently and shared among drivers through VANETs keeping in mind the end goal to enhance driving security and solace.

While standard symmetric cryptography has been overwhelmed by block figures, we have proposed an option dependent on fixed-width changes with modes based on top of the wipe and duplex development, and our substantial proposition Keccak. Our stage-based methodology is adaptable and reasonable for top-of-the-line CPUs just as asset compelled stages. The last option is outlined by the little Keccak cases and the wipe capacities Quark, Photon all tending to lightweight applications. This expansion in security permits diminishing the limit prompting a superior effectiveness. We contend that for keyed methods of the wipe and duplex developments the necessities on the basic stage can be loose, permitting to fundamentally decrease its number of rounds. At last, we present two speculations of the wipe and duplex developments that permit more opportunity in tuning the boundaries prompting much higher effectiveness.

We present a structure for a remote wellbeing observing framework utilizing remote organizations like ZigBee. Crucial insights that are accumulated utilizing a 3-layered design. The primary tier is the mobile phone carried on the body that executes various remote tests and some fundamental features like the pulse, heartrate and lethal disappointment location. Simultaneously at this stage, nearby monitoring stations utilizing the crude findings communicated by the cell phone persistently. The crude findings are additionally stacked at the server. The handled findings just as the examination results are then communicated to the specialized organization place for indicative audits just as capacity. [6] discussed because of various appealing focal points, agreeable correspondences have been broadly viewed as one of the promising systems to enhance throughput and scope execution in remote interchanges. The hand-off hub (RN) assumes a key part in helpful interchanges, and RN determination may considerably influence the execution pick up in a system with agreeable media get to control (MAC).

This review presents a medical services checking engineering combined with multi-purpose sensor frameworks and an ecological sensor network for observing old or persistent patients in their home. The multi-purpose portable sensor framework, incorporated into a texture belt, comprises of different clinical sensors that gather an opportune arrangement of physiological wellbeing pointers sent by means of low energy remote correspondence to portable processing gadgets. Three application situations are carried out utilizing the proposed network architecture. Adaptive security issues for information transmission are performed dependent on various remote capacities. This concentrate additionally presents a checking application model for catching sensor information from remote sensor hubs. The executed plans were checked as performing effectively and quickly in the proposed network architecture.

III.PROPOSED METHODOLOGY

We propose a safe multi-view administrative information sharing methodology. It suggests that any dependents can safely disclose information to others by the IPFS Monitor. Our proposed conspire can uphold dynamic convocations productively. In particular, new conceded dependents can forthrightly decode documents transferred. User repudiation can be effectively accomplished through clever denial list without refreshing the mystery keys of the excess clients. The size and calculation overhead of encryption are steady and free with the quantity of repudiated clients. We give robust saving access control to dependents, which ensures any findings or crude data to secretly use the IPFS Monitor asset. Also, the genuine personalities of information proprietors can be uncovered by the gathering director when debates happen.

A. Cluster Members Signup And Signin Process.

In this component, the principal client entered his user credentials, riddle phrase, and picks id then, at that point, register with Data IPFS Monitor. Group signature plot permits any individual from the gathering to sign messages while keeping the character mysterious from verifiers. Besides, the assigned gathering director can uncover the personality of the mark's originator when a question happens, which is indicated as discernibility.

B. Cluster Level Signature Key Procreation

In this component, each user induces their respective keys by means of Data encryption Key Generator Process. Digital signs utilize a sort of deviated cryptography. For messages sent through a channel, an appropriately carried out advanced sign gives the recipient motivation to accept that the message was sent by the guaranteed sender. Advanced signs are identical to free-handwritten signs in many regards; appropriately executed computerized signs are harder to fashion than the transcribed sort. Computerized signature plans in the sense utilized here are cryptographic based and should be executed appropriately to be tenable.

C. *Upload Files to IPFS Monitor*

Some Uber drivers use bogus identities and shared accounts and at least 14000 trips were made by unauthorized drivers. This has caused great concern for the users of these types of centralized applications. This allows organizations to reduce fees for significant benefits. [8] emphasized that Security is an important issue in current and next-generation networks. Blockchain will be an appropriate technology for securely sharing information in next-generation networks.

D. *Download Files from IPFS Monitor*

In this component, As the end user needs to download a assets, he provides the base name and in return gets the secret key. Mark check might be accomplished by any party utilizing the endorser's public key. An endorser may desire to attest that the figured mark is right, prior to dispatching the marked message to the expected grantee. The expected grantee inspects the mark to opt its reputation. Former validating the sign of a notable message, the space boundaries, and the affirmed endorser's public key and persona will be made accessible to the observer in an attested manner. The public key may, for instance, be stumbled on as an endorsement endorsed by a confided in substance or in a face-to-face reunion with the public key proprietor.

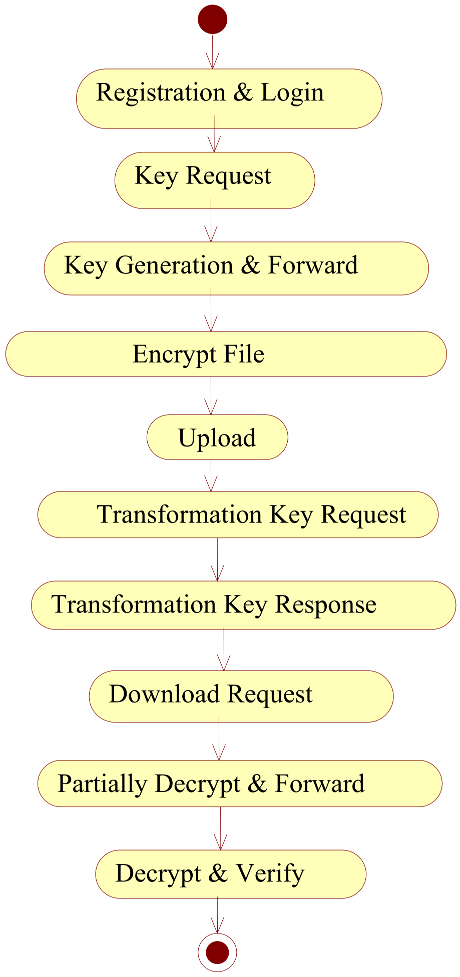


Figure 1- Activity Diagram

IV.EXPERIMENTAL SETUP

Our proposed key is a blend of secure asset repositing parallel to the granular access rules for those assets which in turn makes less complicated for the clients to utilize and discern. Each exchange on Ethereum embraces an information payload field. Information payload is remembered for that exchange which is intended to summon keen agreement capacities. This information payload is in the hex-episodic design and has bytes related to it. Here we would examine two capacities from set of rules to intuit the information payload remembered for the exchanges being generated. Information payload is the discretionary plot of an exchange which is possibly utilized where some type of collaboration with contract capacities Smart agreements are a truly accommodating component in this framework as they guarantee straightforwardness, accuracy and trust on the exchanges being effectuated. The records being put away and gotten to in the framework are just open by the confided in parties. Any dubious newbie attempting to get to the framework is denied admittance by the framework. With the data being kept as private from outsider access the structure would cert that it would be part of invulnerability also.

V.USE CASE DIAGRAM

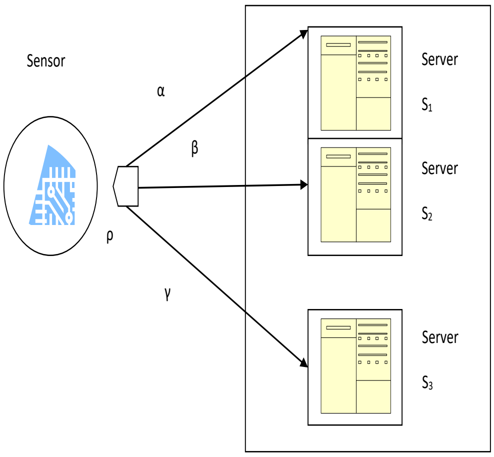


Figure 2-Data Architecture

VI.IMPLEMENTATION OF SMART CONTRACT

The End user or Decentralized Application user will connect with the blockchain via web3 which helps us in developing and interacting with the Ethereum smart contracts and nodes. In order to connect to the blockchain, metamask plays a major role which acts as a private wallet and makes us consider our browser as decentralized browser. In this project, without playing around with real money assets we will be using a local deployment network called the Ganache. It provides us clones of accounts which we can use for our transaction. To migrate our smart contract in the ganache blockchain we use a framework called as Truffle. If we need to connect to the Ethereum node with RPC, we need access. So, we use a service platform called Infura which assists us in providing remote Ethereum nodes as a complimentary. Web3 catches block Id, chain Id, block Number, accounts, gas price and so on.

The end user interacts with truffle framework which will add our smart contracts to the blockchain. Then we will connect with blockchain through web3 and ganache. The document is published in a decentralized stack called IPFS which in turn return the document hash. The document hash is added to the smart contract and gets the transaction approvement via metamask. After transaction approvement, we can view or download the document from IPFS.

Private assets are hidden in the patient or doctor components which can be audited in IPFS which is our ultimate goal of privacy.

```
// SPDX-License-Identifier: UNLICENSED

pragma solidity ^0.8.2;
contract EHRStorage {
string public name = 'EHRDataStorage';
uint public fileCount = 0;
mapping(uint => File) public files;
mapping(string => string[]) public fileAccess;
mapping(string => string[]) userFileAccessList;
address payable wallet;
struct File {
uint fileId;
string patientReferred;
uint age;
string gender;
string fileHash;
uint fileSize;
string fileType;
string fileName;
string fileDescription;
uint uploadTime;
address payable uploader;
}
event FileUploaded(
uint fileId,
string patientReferred,
uint age,
 string gender,
string fileHash,
uint fileSize,
string fileType,
string fileName,
string fileDescription,
uint uploadTime,
address payable uploader
);
function addFileAccessArray(string memory _id, string memory _address) public {
```

```
fileAccess[_id].push(_address);
userFileAccessList[_address].push(_id);
}
function getUserFileList(string memory _id) external view returns (string[] memory) {
return userFileAccessList[_id];
}
function removeFileAccessArray(string memory _id, string memory _address) public {
for (uint i=0; i < fileAccess[_id].length; i++) {
if (keccak256(bytes(fileAccess[_id][i])) == keccak256(bytes(_address))){
fileAccess[_id][i] = fileAccess[_id][fileAccess[_id].length - 1];
fileAccess[_id].pop();
break;
}
}
}
function getFileAccessArray(string memory _id) external view returns (string[] memory) {
return fileAccess[_id];
}
 function uploadFile(string memory _patientReferred, uint _age, string memory _gender,
string memory _fileHash, uint _fileSize, string memory _fileType, string memory _fileName,
string memory _fileDescription) public{
require(bytes(_fileHash).length > 0);
require(bytes(_fileType).length > 0);
require(bytes(_fileDescription).length > 0);
require(bytes(_fileName).length > 0);
require(msg.sender!=address(0));
require(_fileSize>0);
fileCount ++;
wallet = payable(msg.sender);
// Add File to the contract
files[fileCount] = File(fileCount, _patientReferred, _age, _gender, _fileHash, _fileSize,
_fileType, _fileName, _fileDescription, block.timestamp , wallet);
// Trigger an event
emit FileUploaded(fileCount, _patientReferred, _age, _gender, _fileHash, _fileSize,
_fileType, _fileName, _fileDescription, block.timestamp , wallet);
}
}
```

VII. IMPLEMENTATION OF SIMULATION

A. Login and Registration

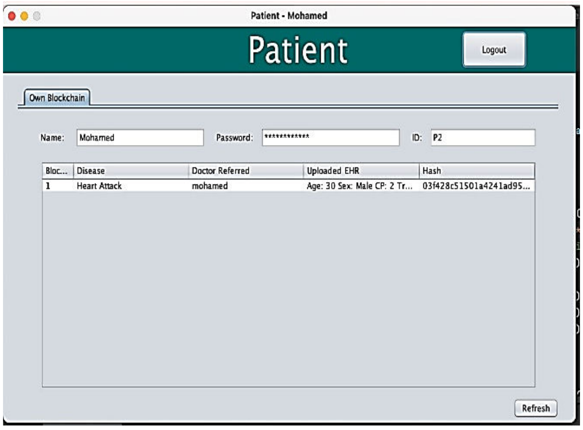
In this module, user can login with their respective username and password only after registration. If you are a new user, they must register in the platform by clicking register button in login frame which will navigate them to the register page.

B. *Doctor Form*

In Doctor form, doctors will update patients' details including disease affected, Age, Gender, Cholesterol, Heart Rate etc. Key Generation generates private and public key for doctor user which is confidentially carried out by doctors. Encryption and Hash generation generates a hash code which is displayed in EHR server instead of displaying the original data to ensure privacy. After generation process, data will be uploaded in the server.

C. *EHR Server*

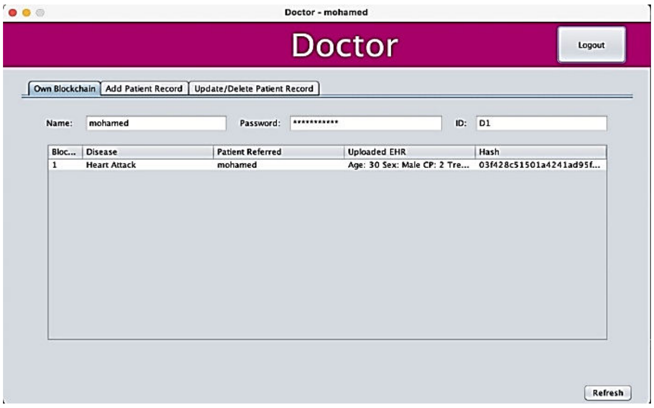
EHR server displays the data uploaded by doctors with privacy ensured by key generation and Encryption hash generation process. View Blockchain button is used to display the user details with respect to user tab selected.



Name: Mohamed Password: ************ ID: P2

Bloc...	Disease	Doctor Referred	Uploaded EHR	Hash
1	Heart Attack	mohamed	Age: 30 Sex: Male CP: 2 Tr...	03f428c51501a4241ad95...

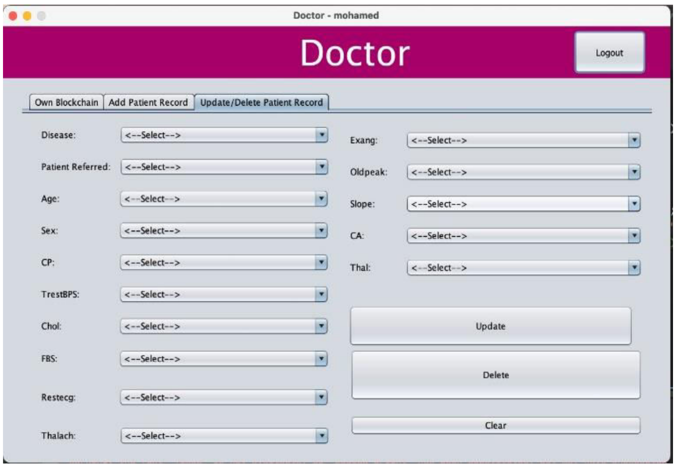
Figure 3- Patient Dashboard



Name: mohamed Password: *********** ID: D1

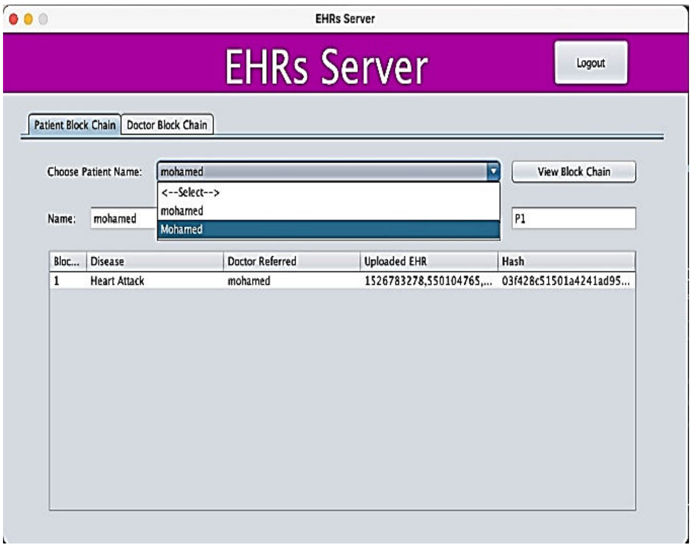
Bloc...	Disease	Patient Referred	Uploaded EHR	Hash
1	Heart Attack	mohamed	Age: 30 Sex: Male CP: 2 Tre...	03f428c51501a4241ad95f...

Figure 4- Doctor Dashboard



Disease: <--Select-->
Patient Referred: <--Select-->
Age: <--Select-->
Sex: <--Select-->
CP: <--Select-->
TrestBPS: <--Select-->
Chol: <--Select-->
FBS: <--Select-->
Restecg: <--Select-->
Thalach: <--Select-->
Exang: <--Select-->
Oldpeak: <--Select-->
Slope: <--Select-->
CA: <--Select-->
Thal: <--Select-->

Figure 5- Doctor Dashboard



Choose Patient Name: mohamed

Name: mohamed

P1

Bloc...	Disease	Doctor Referred	Uploaded EHR	Hash
1	Heart Attack	mohamed	1526783278,550104765,...	03f428c51501a4241ad95...

Figure 6- EHR Server

VIII. CONCLUSION

By the end we came to know how blockchain technology can be valuable for the medical industry and how it might be utilized for electronic wellbeing records. In the face of progress in the Clinical care and technological advancement in EHR frameworks they gone through a little spikes that were tended by this original innovation, i.e., blockchain. But in the proposed methodology, we introduce a efficient support called Dynamic groups where new granted users can decrypt the assets directly without the participation of data owners. It makes such a framework that is more straightforward for the clients to utilize and comprehend. The clinical data assets are stored in a distributed storage platform called Interplanetary File System(IPFS) which itself will generate hash of each document assets and each assets assures privacy with the advancement of smart contracts. Blockchain and Key Generation Process helps the framework as the clinical records are simply accessible to the authorized and trusted people. We can also improve the upgrade of the platform for not just spectacles but for all kinds of products.

IX. REFERENCE

[1] D. Bogdanov, S. Laur, J. Willemson. Sharemind: A Framework For Fast Privacy-Preserving Computations. In Proc. Esorics' 08, Pages 192-206, 2008crypto++ .6.0 Benchmarks. Http://Www.Cryptopp.Com/Benchmarks. Html.

[2] R. Chakravorty. A Programmable Service Architecture For Mobile Medical Care. In Proc. fourth Annual Ieee International Journal On Pervasive Computing And Communication Workshop (Persomw'06), Pisa, Italy, 13-17 March 2006.

[3] Christo Ananth, M.Danya Priyadharshini, “A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks”, International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254).

[4] S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, N. Challa. Continuous And Secure Wireless Health Monitoring. Int. J. Telemed. Appl. 2008, Doi: 10.1155/2008/135808. .

[5] Christo Ananth, Dr.S. Selvakani, K. Vasumathi, “An Efficient Privacy Preservation in Vehicular Communications Using EC-Based Chameleon Hashing”, Journal of Advanced Research in Dynamical and Control Systems, 15-Special Issue, December 2017,pp: 787-792

[6] Christo Ananth, Dr. G. Arul Dalton, Dr.S.Selvakani, “An Efficient Cooperative Media Access Control Based Relay Node Selection In Wireless Networks”, International Journal of Pure and Applied Mathematics, Volume 118, No. 5, 2018,(659-668).

[7] X. H. Le, M. Khalid, R. Sankar, S. Lee. An Efficient Mutual Authentication And Access Control Scheme For Wireless Sensor Network In Healthcare. J. Organizations 27: 355-364, 2011

[8] Christo Ananth, Denslin Brabin, Sriramulu Bojjagani, “Blockchain based security framework for sharing digital images using reversible data hiding and encryption”, Multimedia Tools and Applications, Springer US, Volume 81,Issue 6, March 2022,pp. 1-18.

[9] S. Raazi, H. Lee, S. Lee, Y. K. Lee. Bari+: A Biometric Based Distributed Key Management Approach For Wireless Body Area Networks. Sensors 10: 3911-3933, 2010.

[10] W. Diffie And M. Hellman. New Directions In Cryptography. Ieee Transactions On Information Theory, 22 (6): 644-654, 1976

[11] Digital Signature Standard (Dss). Fips Pub 186-4, July 2013.

[12] P. Kumar And H. J. Lee. Security Issues In Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. Sensors 12: 55-91, 2012

[13] MetaMask, Dec.2019,[online]Available: https://medium.com/metamask