RESEARCHERID
THOMSON REUTERS

[Arslan, 6(3): March 2019] ISSN 2348 – 8034
DOI- 10.5281/zenodo.2599921 Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

PRIVACY PRESERVING SECURITY MECHANISM FOR IOT BASED DISTRIBUTED SMART HEALTHCARE SYSTEM

Farrukh Arslan
School of Electrical and Computer Engineering, Purdue University, USA

ABSTRACT

Data security and privacy are one of the key concerns in the Internet of Things (IoT). Usage of IOT is increasing in the society day-by-day, and security challenges are becoming more and more severe. From a data perspective, IOT data security plays a major role. Some of the sensitive data such as criminal record, military information, the medical record of the patients, etc. Due to the size and other features of IOT, it is almost impossible to create an efficient centralized authentication system. The proposed system focused on IoT security for distributed medical record to provide perimeter security to the patient. Building trust in distributed environments without the need for authorities is a technological advance that has the potential to change many industries, the IOT is one among them. Furthermore, it protects data integrity and availability. It improves the accessibility of data by using the indexing method along with the blockchain. Moreover, it facilitate the utility of tracking the previous history of the patient record using the hyper ledger with authorization.

Keywords: *security, Internet of Things, Health-care, Block chain, Hyper ledger.*

I. INTRODUCTION

Amount of information grows day by day but the security of the data is not maintained properly. Nowadays blockchain technology is very useful in IOT field such as smart cities, smart home system as well as it provides security [1]. Maximum of the present systems are centralized. Third parties were frequently monitoring the data and information. Blockchain provides mutual trust between people and organization because there is no trusted based third parties issues in the system. Each block contains all the recent transaction records and it provides tamper evidence decentralization and transparency [3]. The datum could be stored into many small chunks. The amount of datum stored in the block chains is more cost effective. The -middle Attacks, Replay Attacks and Impersonation Attacks are some of the attacks mainly caused high vulnerabilities. Because no mutual authentication between the system and attacks. In the protocol that provide mutual authentication of the participants is called the Authenticated Key Exchange (AKE) [8]. The essential need of an unchallengeable and auditable history is wanted to become permissions to access patient's data. Another issue is the cost of data stored in block chain. In 2020 blockchain has been implemented in many real time applications like e-voting, health care applications and bitcoin transactions. It can also be able to regularly change or modify the patient's data Blockchain stores the information in a distributed manner. However, that stores the transactional records there is also a problem of public block chain technology to overcome that private block chain is invented. It is used to prevent the unauthorized person accessing of information and it is difficult to access the data which is shared on blockchain [10]. The blockchain technology brings several Linux platforms such as Hyperledger, IBM, Corda, Ethereum, etc. [11]. Hash tables are arranged sequentially that can be linked by chains. The first block has its own hash and it does not have previous block hash **BLOCK #0. BLOCK #1** has its own hash value and previous hash value of BLOCK #0 with time stamp, nonce and transaction count [12]. Blockchain has high potential to advance the healthcare in a many number of innovative ways. Some of those samples include a Master Patient Identifier (MPI), Electronic Health Record (EHR) and the usage grown from 20% of providers using this technology in 2002. To achieve over 80% today, much of the usage handled by hospitals and crypto currency exchanges [14]. Then we have estimated a java implementation of input and output generation algorithm using Elliptic Curve Cryptography (ECC) for our method. Experimental results will help to analyse in several aspects of Health Care Record management [15]. In public blockchains there is no permission less anyone can join as new user. Moreover, all users can perform operations like transactions or contracts. In private blockchains all are permissioned blockchain [17]. Each user can have a pair of keys to perform

the transaction. Pair of keys like public and private keys [18]. Blockchains is a digital ledger system implemented in a distributed manner (i.e., without a central repository) and usually without a central authority

Each blockchain contains the transaction record. The set of transaction record contains the pair of key lists. Blockchain plays a major role for data transaction it improves the data exchange transferability with high security. Blockchain improves data availability, and makes it easier for patients to access the data. Block chain is composed of verifiable records for each and every transaction. Maintaining the transaction record is very useful to verify the exchange of data between the persons or organisation [23]. Transaction records are reached about 149GB on 2017 if we want to delete the old transaction record it is not maintained and altered by chameleon hash function. This process is called editable blockchain. Mining the block is very difficult task and power consumption of IoT devices is based on the transaction and data. Adding benefit to the block chain the data stored in the block is again encrypted using different cryptographic algorithm. But it supports only Public key cryptography. Selection of cryptographic algorithm is user friendly any method can be chosen based on the use cases. But the usage of Blockchain is mostly supports the Linux based systems some windows are support the Blockchain with preliminary necessities. Sample like Docker, fabric etc. It supports the languages like GO, JS, and also java with some jar files.

II. PROPOSED SYSTEM

Blockchain is a connected chain of blocks ordered in a network of peers. Each block references the previous one and contains data, its own hash, and the hash of the previous block.

Structure of block

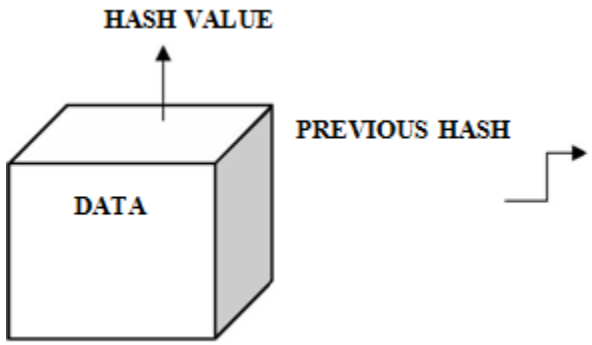

Fig 1: Structure of Block

A hash is a great method for identifying the attempts if any changes made in blocks. Anyone is allowed to join a blockchain peer-to-peer network. When new person joins a network, then that person gets a full copy of the blockchain. Distributed storage of data accompanied by effective hashing and proof-of-work mechanisms helps to prevent nearly any modification in data.

Each transaction generates a hash. It is a string of numbers and letters. Small change in transaction can create a new complete hash. It is a database which is distributed among all nodes. Whole control of the value no third party is that hold the value or limit the values. Cost to perform the transaction is very low.

Durability and robustness
It has no single point failure and controlled by any single entity.

Types of block chain
1. Private block chain
2. Consortium block chain
3. Public block chain

ISSN 2348 – 8034
Impact Factor- 5.070

Private blockchain

Private block chain is a complete reverse of public block chain, where the write permission is kept in centralized repository for one organization in a fully private block chain.

Consortium & public block chain

Any One in this world can access the data if they have an internet connection. It is a combination of public and private blockchain.

Private blockchain model

Private blockchain has one or more entities in the network. A perfect example is the hyper ledger. Blocks are linked and are securely managed by the cryptographic algorithms such as public key cryptography.

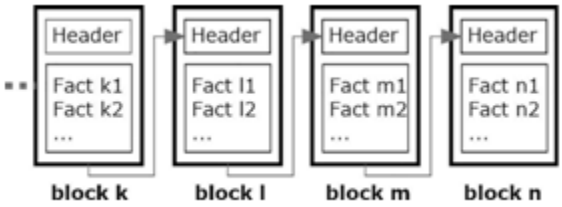

Fig 2: Structure of BLOCK with HASH Implemented Algorithm

SHA-256 is used to calculate the hash digest of the data. It is a 256-bit hash function without key cryptographic hashing method and there is no collision has been found yet.

Cryptographic hash function has primitive hashing property:

- Preimage resistant
- Second Preimage resistant
- Collision resistant

Preimage resistant

It is one way, computationally infeasible to compute the correct output find x such that hash(x) = digest

Second Preimage resistant

Cryptographic Nonce Generation

Cryptographic hash is an arbitrary number i.e., used only once

hash (data + nonce) = digest
"hash":
"000008282f34bf3f6a80b3da650f0ce54bd56aa0f05
9300cc31b2223508b40dc",
"PreviousHash":
"00000c573fe32e2032a53c3fdcdb64debe163c3316
0b86e91d022a740c497e2d", "data": " the second block", "time Stamp": 1549327096527,
"nonce": 528522

Sample SHA(SECURE HASH ALGORITHM)

SHA-256 gives an output in range of 32 bytes (i.e., 256 bits) but it displays in 64 character of hexadecimal value

ISSN 2348 – 8034
Impact Factor- 5.070

Table1: Representation of Hash value

TEXT	SHA 256 DIGEST VALUE
a	ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb
1	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b

Table2: Key Size of RSA and ECC

Recommended Key size

Symmetric Key Size	RSA and DIFFIE HELMEN	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521
NIST Recommended KEY SIZE		

III. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

It is harder to compute the mathematical calculation.In addition to that, 256 sized key security is stronger than 2048-bit classical key.

Select ***d*** it is constant (between 0 to n-1). Here n is the prime number and it generates the public key ***Q*** $Q=K*P$

Encryption:
Message **m** is distorted into affine point **M** on the curve. Plain Text is converted in to 2 cipher text such as C1 and C2. Send both the cipher text.

$$C1=K*P$$
$$C2=M+K*Q$$

Decryption:
D is used to generate the public key for decryption.

$$M=C2-D*C1$$

ECC is more effective when compared to RSA
In terms of key size and security. It provides more security with lesser key size. so, this can be utilized with lesser memory and low power consumption.

Table 3: Function of Platform

Users	Functions	The solved problems
Patients	View their own medical record in freely	No rights to use his own medical record
	Decide who	Privacy leaks

ISSN 2348 – 8034
Impact Factor- 5.070

	can view this	
Hospitals	carry out treatment with fewer worries; current medical records are not Previous records can help to reliable treat;	Current medical records are not reliable
third-party research institutions	have a more formal platform to get more comprehensive data;	No legal access to get medical data
Regulatory &audit departments	smart contracts	High cost and low efficiency

We installed the jar files for accessing the functions of every modules. The manifest and the signature files are in signed jar with its SHA-1 digest.

The reason behind the use of ECC and short key size is utilizing the Less computational power, fast and secure connection and it is harder to break the ECC method when compared to RSA and DSA it states that it follows the traditional infrastructure.

Outcome of the system

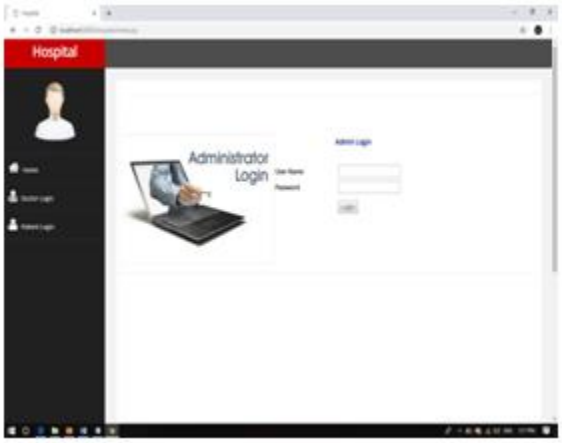

Figure3: Overview of system

Figure 3 illustrates the over view of the proposed system. It consolidates the patient, doctor and system admin roles. The security and data are maintained by the WAMP (WINDOW,APACHE,MYSQL,PHP) server.

ISSN 2348 – 8034
Impact Factor- 5.070

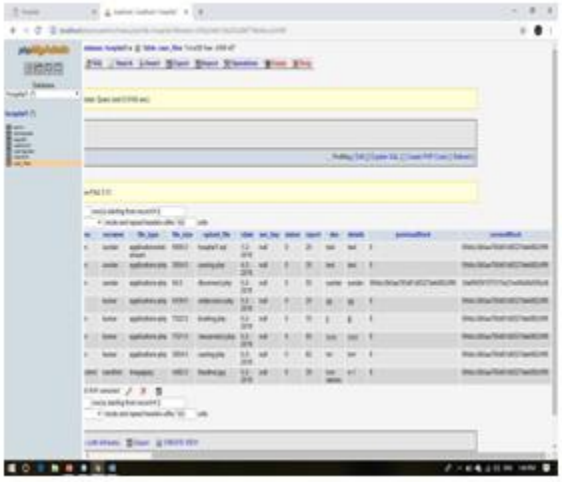

Figure4: Block and connection

Figure 4 shows that how the block is created and stored its value on blockchain and how the blocks are identified. The meta data contains the file size and type with the block connection with another block.

However, The Intruders are not able to get the data because they are evenly connected by all the blocks. Therefore, accessing of single block cannot give the permission for seeking whole data of patient record's blocks which are connected together. The connectivity of all blocks are known then only we can access the single data block, but the data is prevented by high security of using cryptographic algorithm like ECC and it can be an efficient in terms of utilising the minimum computational power. Because the key size of ECC is very small when compared to other but it gives the same strength as like other cryptographic functions.

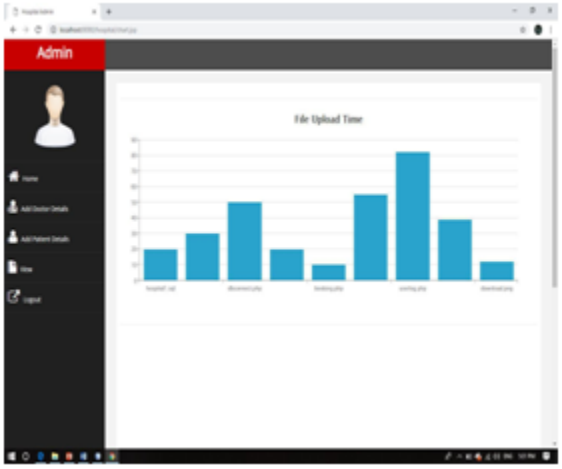

Figure3: Time taken for file uploading

When compared to ABE(Attribute Based Encryption) and RSA (Rivest, Shamir,Adleman) Block chain with SHA (Secure Hashing Algorithm) takes lesser time for encrypting the data. Moreover, the key size is smaller. However, the security level is higher than ABE,RSA,elgammal and diffie helman.

ISSN 2348 – 8034
Impact Factor- 5.070

IV. CONCLUSION

Implementing the concepts in block chain is the latest technology.It would be expected to arise 80% in 2020. It achieves high level security when comparing with other methods. Moreover, without any third party it gains the security while having the transaction between any two or more organisations.Though, ECC provide the better security when compared to others and utilises less computational power. In future, it can be implemented in real time hardware platform on the same medical data sets to compare the performance.

REFERENCES

1. *Qi Liu, Kenli, "Decentration Transaction method based on block chain technology", International Conference on Intelligent Transportation, Big Data & Smart City*
2. *Leonardo Aniello, Roberto Baldoni, "A Prototype Evaluation of a Tamper-resistant High Performance "Blockchain-based Transaction Log for a Distributed Database", European Dependable Computing Conference 2017*
3. *Xing Liu, "A Small Java Application for Learning Blockchain", IEEE 2018*
4. *Hailong Yao, Caifen Wang "Homomorphic Hash and Blockchain Based Authentication Key Exchange Protocol for Strangers", IEEE 2018*
5. *Ilya Sukhodolskiy, Sergey Zapechnikov, "A Blockchain-Based Access Control System for Cloud Storage", IEEE 2018*
6. *Cosmas Krisna Adiputra, Rikard Hjort, "A Proposal of Blockchain-based Electronic Voting System", IEEE 2018*
7. *Hailong Yao, Caifen Wang, "A Novel Blockchain-Based Authenticated Key Exchange Protocol and Its Applications", IEEE 2018*
8. *Jieying Chen, Xiaofeng Ma, "A Blockchain Application for Medical Information Sharing".*
9. *Tomas Mikula and Rune Hylsberg Jacobsen,"IdentityandAccess Management with Blockchain in Electronic Healthcare Records", 21st Euromicro Conference on Digital System Design,2018*
10. *Thein Than Thwin and Sangsuree Vasupongayya," Blockchain Based Secret-Data Sharing Model for Personal Health Record System", IEEE 2018*
11. *Navaneeth Krishnan, Roopesh Jenu, "Blockchain Based Security Framework for IoT Implementations", International CET Conference on Control, Communication, and Computing, 2018*
12. *Qi Feng, Debiao He, Sherali Zeadally, "A survey on privacy protection in blockchain system", Journal of Network and Computer Applications,2018*
13. *Liehuang Zhu, Yulu Wu, "Controllable and trustworthy blockchain-based cloud data management", Future Generation Computer Systems,2018*
14. *Ramzi Abujamra, David Randall, "Blockchain applications in healthcare and the opportunities and the advancements due to the new information technology Framework.*
15. *Abdullah Al Omar, Md Zakirul Alam Bhuiyan, "Privacy-friendly platform for healthcare data in cloud based on blockchain Environment", 2018*
16. *Clare Sullivan, Eric Burger, "E-residency and blockchain",2018*
17. *Fran Casinoa, Thomas, "A systematic literature review of blockchain-based applications: Current status, classification and open issues", 2019*
18. *Huige Li, Haibo Tian, "Blockchain-based searchable symmetric encryption scheme",2019*
19. *Harish Sukhwani, Nan Wang, "Performance Modeling of Hyperledger Fabric", IEEE 2018*
20. *AratiBaliga,NiteshSolanki, "Performance Characterization of Hyperledger Fabric", Crypto Valley Conference on Blockchain Technology 2018*
21. *Kaiwen Zhang "Towards Dependable, scalable and pervasive Distributed Ledgers with Block Chain", IEEE 2018*
22. *William J. Gordon, Christian Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability", ELSEIVER*
23. *Peng Jiang, Fuchun Guo, "Searchain: Blockchain-based private keyword search in decentralized Storage", ELSEIVER 2017*

24. *Huaqun Wang, Debiao He, "Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography" ,2017*
25. *James Brogan, "Authenticating Health Activity Data Using Distributed Ledger Technologies", 2018*
26. *Xu Wang, Xuan Zha, "Survey on blockchain for Internet of Things", 2019*
27. *Huihui Yang, Bian Yang, "A Blockchain-based Approach to the Secure Sharing of Healthcare Data", 2017*
28. *Surendiran Balasubramanian, "Elliptic curve cryptography for secured text encryption", 2017*
29. *Dylan Yaga, Peter Mell, "Blockchain Technology Overview", 2018*
30. *Chao Yuan, Mixue Xu, "Blockchain with Accountable CP-ABE: How to Effectively Protect the Electronic Documents", IEEE 2017.*