International Conference on Advances in Materials, Computing and Communication Technologies
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Block Chain Technology Based Medical Healthcare System with Privacy Issues Using Blowfish Algorithm

A. George Klington[1], S. Anantha Babu[1], S. Uma Devi[2], R. Muthu Esakki[2]
[1]Professor, St. Mother Theresa Engineering College, Tuticorin, Tamil Nadu, India
[2]UG Scholar, St. Mother Theresa Engineering College, Tuticorin, Tamil Nadu, India

ABSTRACT

In the recent years the Block chain is fastest growing technology through various applications in a secure manner. The health care services industry is always showing signs of change and supporting new advancements and advances. In today's health care systems is to protect the patient's medical report against potential attackers. Hence, it is basic to have secure information that can just approve people can get to the patient's medical report. So in our proposed system have proposed Block chain technology as a disbursed approach to grant security in accessing the medical report of a patient. It's composed of three phases 1. Authentication, 2. Encryption and 3. Data Retrieval using Block Chain technology. For authentication – Quantum Cryptography, for Encryption – BLOWFISH and for Data Retrieval – SHA algorithms are used to resist the frequent attacks. Finally our result shows the proposed method ensures the protection of the patients and moreover keeps up the security and trustworthiness of the health care system.

Index Terms- AES, DES, Blowfish, Block Chain, Key generation

I. INTRODUCTION

The Block chain is the fastest growing technology through various applications in a secure manner. The various implementations make use of block chain technology among stakeholders. Banking, healthcare Services, and supply chain management utilize this Sharing management technology for its immense potential and secure data. Mainly, block chain technology plays a major role in the medical and healthcare system. Because of the decentralized and distributed technology, Block chain provides security services in healthcare [1]. Block chain innovation deals with the human service administrations to give secure information sharing among different partners, information interoperability, adaptable and speedy charging. In Today's world, the technology has a rapid growth in its upcoming future with a widespread digital transformation by making a better replacement every day. Internet of things, detecting advancements, and 5G are the quickest developing innovation gives a markable commitment to human service administrations [2].

The centralized design in current health care which provides a delay in accessing the data and it has a major risk in leakage of information. In such a case, the medical reports can be archived without the knowledge of the patient [3]. Accessing the data in a

secure manner within the network is the major issue in current health care maintaining system. For accessing the data, Block chain is the efficient way and a promised technology. Electronic, Health/Medical Record (EHR/EMR) is the current online healthcare services which play a key role in maintaining and storing the data, which has a major issue in leakage of patient's information. In block chain technology, the information is stored as a ledger feature which can monitor the patients in accessing the medical records. This becomes the major reason for the development of Block chain technology [4]. In Block chain technology, not only provides security and easy accessibility, but also gives other production elements in the administrations and furthermore pursues privacy, respectability, and verification. Thus the main aim of this research is to provide secure management in accessing the medical records using block chain technology by unique identification of the data security.

Security attacks against network are increasing significantly with time. Our communication media should also be secure and confidential. For this purpose, these three suggestions arrive in every one's mind: (i) one can transmit the message secretly, so that it can be saved from hackers, (ii) the sender ensures that the message arrives to the desired destination, and (iii) the receiver ensures that the received message is in its original form and coming from the right sender. For this, one can use two techniques, (i) one can use invisible ink for writing the message or can send the message through the confidential person, and (ii) one can use a scientific approach called "Cryptography" .Cryptography is the technique used to avoid unauthorized access of data. For example, data can be encrypted using a cryptographic algorithm in conjunction with the key management. It will be transmitted in an encrypted state, and later decrypted by the intended party. If a third party intercepts the encrypted data, it will be difficult to decipher.

The security of modern cryptosystems is not based on the secrecy of the algorithm, but on the secrecy of a relatively small amount of information, called a secret key. The fundamental and classical task of cryptography is to provide confidentiality by encryption methods. The encryption algorithms are usually summarized into two popular types: Symmetric key encryption and Asymmetric key encryption. Symmetric key algorithms are also called as secret key encryption, this symmetric key algorithm are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both encryption of plaintext and decryption of cipher text. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transformation to go between the two keys. The keys, in practice, represent a secret between two or more parties that can be used to maintain a private information link. Other terms for symmetric key encryption are secret key, single key, shared key, one key, and private-key encryption [5].

The representative Symmetric key cryptography algorithms include RC2, DES, 3DES, RC5, Blowfish, and AES, which use certain- or variable-length key. Public-key cryptography, also known as asymmetric cryptography, is a form of cryptography in which the key used to encrypt a message differs from the key used to decrypt it. In public key cryptography, each user has a pair of cryptographic keys a public key and a private key. The private key is kept secret, while the public key may be widely distributed and used by other users. Incoming messages would have been encrypted with the recipient's public key and can only be decrypted with his corresponding private key. The keys are related mathematically, but the user private key cannot be derived from the widely used public key (E.g. RSA and Digital Signatures)On the one hand, high security is the basic requirement of data encryption algorithm. On the other hand, encryption algorithms are known to be computationally intensive. They consume a

significant amount of computing resources such as CPU time, memory, and battery power. Especially for a wireless device, usually with very limited resources (e.g. battery) is subject to the problem of energy consumption due to encryption algorithms. Therefore, it is essential to evaluate the performance of encryption algorithms so as to ensure various applications. Both AES and blowfish algorithms are the most common cryptographic algorithm used for information security through wireless network, portable terminal, and so on. It is essential to evaluate their performance to ensure their domain application. It is also a significant work to facilitate the process of the encryption algorithm optimization In this paper, we firstly study the two most common encryption algorithm i.e. The AES and Blowfish encryption algorithm. Basically these algorithms are symmetric key encryption algorithms using block cipher. Referencing the encryption process methods, we analyse their security. We give a comprehensive performance evaluation which includes three aspects: security analysis, encryption speed, and power consumption. We design adequate experiment method for the evaluation. Based on the experimental results, we show the advantages and disadvantages for both encryption algorithms [6].

In this paper, a novel security based modified blow fish algorithm in block chain environment is suggested. The rest of this paper is organized as follows; Sect.II examines the Literature survey of security based models while Sect. III indicates system models that describes existing method AES,DES and proposed method modified blowfish algorithm working in block chain environment. Sect.IV describes the results and discussion compared with other existing methods. Sect.VI concludes the objective of the research work in the proposed method.

II. LITERATURE SURVEY

The search of the three databases provided a total of 117 records after removing duplicates. Also 11 ddff [7] studies from other sources were considered for review. After screening by title and abstract 75 ddff [7] were discarded for not accomplishing criteria, 53 were selected as relevant for full text review. Of the 53 selected for full-text examination 41ddff [7] remained to be included in the synthesis and 12 ddff [7] were discarded as they did not comply with the eligibility criteria. Features to enable syntactic interoperability while others enhanced those features to share information at a semantic level. Of the 41 ddff [5] papers reviewed 22% (n=9) described the application of medical logic and guidelines representation standards (e.g. GLIF, Arden Syntax etc.); 63% (n=26) described the use of clinical information standards such as HL7 CDA, HL7 RIM, Open EHR or HL7 VMR; 32% (n=13) employed seman- tic web technologies such as ontologies; 46% (n=19) outlined the use of standard terminologies; and 32% (n=13) reported the use of web services to offer CDS functionalities. Table 1 presents the mechanisms used to enable interoperability in the studies reviewed. It is important to notice that those categories are not disjoint but complementary [8].

Thus a particular study may pertain to several of them. Currently, several information architecture standards exist for the documentation and exchange of EHR extracts. Several works propose their use to specify the interface to interact with the CDS system. Thus, the logic references a standard information model rather than a proprietary data schema. This alle- viates the ‘curly braces’ problem Preparing the data specified in standards such as CDA or RIM to be used by the decision logic is challenging as a conse- quence of the impedance mismatch between the information model and the inference model. Works to map the RIM VMR to the guideline specification can be found in Peleg et al. [9]. Specifically, they use a mapping ontology (KDOM) to create the abstract concepts

required by the logic from the fine grained information contained in the RIM-based VMR. To solve this problem in CDA-based VMRs, Saez et al. [10] pro- posed to use a wrapper in order to link CDA documents to the CDS rules. Although both RIM and CDA can be used as in- formation models to build a VMR, they are complex and too detailed for the requirements of a CDS data schema. Kawamo- to et al. studied the requirements to create a CDS specific in- formation standard to build VMRs based on a simplification. The centralized design in current healthcare services is not so secure among the various medical services, which provides a delay in accessing the data and it has a major risk in leakage of information ,M. Puppala , T. He, X. Yu et al The medical report of a patient is viewed as relatively sensitive and wants a secure and safer ability to guard the data manner, the putting away, sharing and overseeing restorative reports can be executed in secure ways. These problems are already proposed by using a number of mechanisms, for example, numerous authentication schemes, which leads to fulfilling the need of efficient and secure access of medical reports, manageability, and other safety requirements. These options had been useful in providing a variety of protection necessities under preferred healthcare scenarios. But these strategies in current healthcare technology are no longer enough due to the fact the patient has been exploited by means of various entities via distinct means except their consent. In this research, is to discover a security solutions based on block chain based health care approaches. There have been a variety of research studies associated with efficient utilization of block chain in healthcare. Electronic medical remedy approaches for manual and remote access of medical reports and protecting the privacy of the records are the most essential fields of application where Block chain technology can create value [10[. The Med Rec in which a decentralized method for utilizing block chain mechanical skill is received to deal with the EHR/EMR and furthermore gives a potential contextual analysis of block chain usage in social insurance, which gives a model to EHR/EMR. Moreover, Med Share gives the trustless method for sharing the clinical reports among an assortment of specialist organizations utilizing block chain. Thus, the examination network characterizes the exceptional systems for accessing the records safely utilizing block chain innovations. Kahani, K. Elgazzar et,al Block chain technology as a disbursed approach to grant security in accessing the medical report of a patient. It's composed of three phases Authentication, Encryption and Data Retrieval using Block Chain technology [10]. For authentication – Quantum Cryptography, for Encryption – AES and for Data Retrieval – SHA algorithms are used to resist the frequent attacks. Fig. shows the process of securing the medical report of a patient. Initially, the patient must register their personal details in the registry and unique identification is created for the new user. If the patient already exists, then he/she can directly login to their medical account by using unique identification of the respective patient. The private key is generated for each registered patient with the help of ID. The administration of the hospital maintains the doctor's medical history and also generates the public key of each doctor. The assignment of the doctor to the patient is performed using the doctor's public key with the patient's private key. Using Quantum Cryptography, the authentication is performed to check the authorized doctor, who wants to monitor the patient's medical report. The authorized doctor can only add or retrieve the medical report with the patient's permission. But, he/she cannot modify the patient's medical history. The updated medical report is encrypted using Advanced Encryption Standard (AES) algorithm and the encrypted data is stored in the private cloud, where we can identify the location easily. The address of the encrypted data in the private cloud is stored in the block chain. Now, Data Retrieval can be performed only by the authorized doctor. After authentication, the doctor can receive the hash value

of the encrypted data. Then, the data is decrypted using the Secure Hash Algorithm (SHA). Hence, the medical report of the patient is secured by using block chain technology [11].

III. SYSTEM MODEL

3.1 Existing System

In our existing system implement the block chain architecture as a new system solution to supply a reliable mechanism for secure and efficient medical record exchanges. The Advanced Block-Chain (ABC) approach was designed to meet the demands in healthcare growth as well as in the new form of social interactive norms. It does not provide auditable e-Health records while preserving patient privacy and security .It cannot be reduce the processing time. It cannot be prevent the security based attack.

3.1.1 AES (Advanced Encryption Standard)

Advanced Encryption Standard is the new encryption standard recommended by NIST to replace DES. It was originally called Rijndael (pronounced Rain Doll). It was selected in 1997 after a competition to select the best encryption standard. It has variable key length of 128, 192, or 256 bits; default 256. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field. The Encryption and decryption process consists of a number of different transformations applied consecutively over the data block bits, in a fixed number of iterations, called rounds. The number of rounds depends on the length of the key used for the encryption process. For key length of 128 bits, the number of iteration required are10 (Nr = 10). Each of the first Nr-1 rounds consists of 4 operations: SubBytes, Shift Rows, Mix Columns & AddRoundKey.

3.1.2 DES (Data Encryption Standard)

The DES (Data Encryption Standard) algorithm is a symmetric-key block cipher created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST). The algorithm takes the plain text in 64-bit blocks and converts them into ciphertext using 48-bit keys.

3.2 PROPOSED SYSTEM

In our proposed system propose the Block chain technology as a disbursed approach to grant security in accessing the medical report of a patient. It's composed of three phases 1.Authentication, 2.Encryption and 3.Data Retrieval using Block Chain technology. For authentication – Quantum Cryptography, for Encryption – BLOWFISH and for Data Retrieval – SHA algorithms are used to resist the frequent attacks. Initially, the patient must register their personal details in the registry and unique identification is created for the new user. If the patient already exists, then he/she can directly login to their medical account by using unique identification of the respective patient. The private key is generated for each registered patient with the help of ID. The administration of the hospital maintains the doctor's medical history and also generates the public key of each doctor. The assignment of the doctor to the patient is performed using the doctor's public key with the patient's private key. Using Quantum Cryptography, the authentication is performed to check the authorized doctor, who wants to monitor the patient's medical report. The authorized doctor can only add or retrieve the medical report with the patient's permission. But, he/she cannot modify the patient's medical history. The updated medical report is encrypted using BLOWFISH algorithm and the encrypted data is stored in the private cloud, where we can identify the location easily. The address of the encrypted data in

the private cloud is stored in the block chain. Now, Data Retrieval can be performed only by the authorized doctor. After authentication, the doctor can receive the hash value of the encrypted data. Then, the data is decrypted using the Secure Hash Algorithm (SHA). Hence, the medical report of the patient is secured by using block chain technology.

- BLOWFISH algorithm sprints faster than AES and showed poor performance results compared to BLOWFISH algorithms since it requires more processing power.
- Proposed work to ensure the protection of the patients and moreover keeps up the security and trustworthiness of the health care system

3.2.1 Modified Blowfish Algorithm

It is significantly faster than DES and provides a good encryption rate with no effective cryptanalysis technique found to date. It is one of the first, secure block cyphers not subject to any patents and hence freely available for anyone to use.

Initialization:

1. Block Size: 64-bits
2. Key Size: 32-bits to 448-bits variable size
3. Number of subkeys: 18 [P-array]
4. Number of rounds: 16
5. Number of substitution boxes: 4 [each having 512 entries of 32-bits each.

Step1: Generation of subkeys:

- ❖ 18 sub keys {P [0]…P [17]} are needed in both encryptions as well as decryption process and the same sub keys are used for both the processes.
- ❖ These 18 subkeys are stored in a P-array with each array element being a 32-bit entry.
- ❖ It is initialized with the digits of pi(?).
- ❖ The hexadecimal representation of each of the subkeys is given by:

- P[0] = "243f6a88"
- P[1] = "85a308d3"
- P[17] = "8979fb1b"

Now each of the sub key is changed with respect to the input key as: P[0] = P[0] xor 1st 32-bits of input key P[1] = P[1] xor 2nd 32-bits of input key P[i] = P[i] xor (i+1)th 32-bits of input key (roll over to 1st 32-bits depending on the key length) P[17] = P[17] xor 18th 32-bits of input key (roll over to 1st 32-bits depending on key length) The resultant P-array holds 18 subkeys that is used during the entire encryption process.

Step2: initialize Substitution Boxes:

Substitution boxes(S-boxes) are needed{S[0]…S[4]} in both encryption as well as decryption process with each S-box having 256 entries{S[i][0]…S[i][255], 0&lei&le4} where each entry is 32-bit.

- ❖ It is initialized with the digits of pi(?) after initializing the P-array.

Step3: Encryption:

The encryption function consists of two parts:

- ❖ **Rounds:** The encryption consists of 16 rounds with each round(Ri) taking inputs the plaintext(P.T.) from previous round and corresponding sub key(Pi).
- ❖ **Post-processing:** The output after the 16 rounds is processed.

3.2.2 Proposed Architecture:

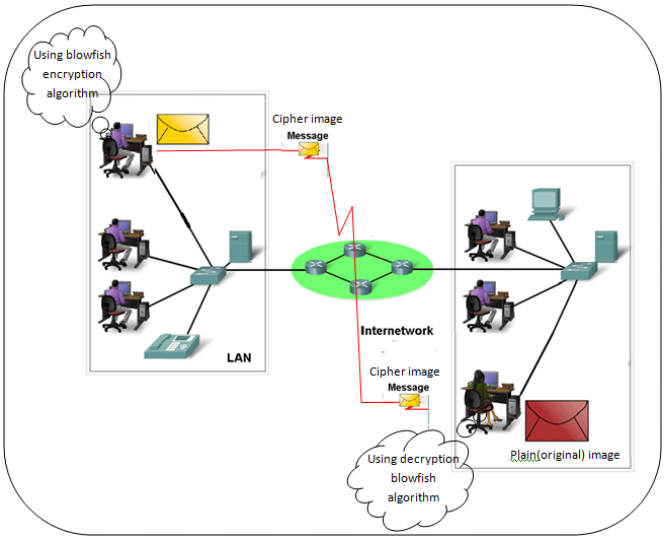

Fig1. Proposed Blowfish Architecture

3.2.3 OVERALL ARCHITECTURE

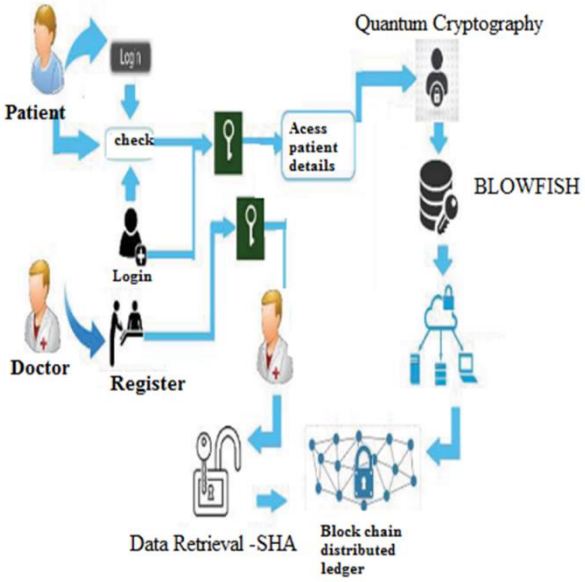

Fig 2. Overall Architecture

3.2.4 Procedure for secure the medical record

Step 1 : Patient(P) came to Hospital(H)

Step 2 : if(patient == new user) then Register with personal informationcreate unique ID(idp), public key(Pkp), private key(Skp) using LCG login(idp, Skp, Pkd) else directly login using ID(idp)

Step 3 : Assign specialist and register(Idd ,Skp, Pkd) in the registry

Step 4 : Assigned doctor responsible for treatment of patient and add information to patient's records(PR)

Step 5 : Authenticate doctor using Blowfish algorithm

Step 6 : if doctor wants to add details then get permission from patient

Step 7 : if (permission == granted) then validate data by patient update(record)

Step 8 : Encrypt data using AES using key provided by patient, Ek(PR, k)

Step 9 : Encrypted data is stored in private cloud with timestamp, PC(PR, T)

Step 10 : Location Address is stored in Block chain BC

Step 11 : New doctor(D) wants to retrieve the medical report

Step 12 : Get address from BC

Step 13 : Authenticate the doctor if(authentication == true) then retrieve address of the record from BC

Step 14 : Get(Encrypted data) using retrieved address

Step 15 : Decrypt using SHA Dk(PR, SKp, idp)

IV. RESULTS AND DISCUSSION

Encryption algorithm plays an imperative task for information security guarantee in recent mounting internet and network application. In this paper, we studied two symmetric key encryption algorithms: AES and BLOWFISH. We assessed encryption speed, throughput and power burning up for their performance. The simulation results showed that Blowfish has superior performance than AES since Blowfish has not any known security weak points so far, it can be considered as an excellent standard encryption algorithm. BLOWFISH algorithm sprints faster than AES and showed poor performance results compared to BLOWFISH algorithms since it requires more processing power. Thus Blowfish algorithm maybe more appropriate for wireless set-up which swaps small size packets.

4.1.1. Encryption Process

The encryption process can be done with the help of blowfish algorithm. Blowfish is a symmetric encryption algorithm which has a specification in encryption of electronic data. For encryption, plain text and secret key (K) is required in Blowfish engine and also the same secret key is used for decryption. The datas are encrypted with the patient's private key Ek(PR, k). The private key of the patient is used to prevent the medical record in a secure manner. Thus, the encrypted data Ek(PR, k) is stored in a private cloud(PC) with the timestamp(T) PC(PR, T). The address of the encrypted data which is stored in private cloud is added to the block chain(BC).

4.1.2. Decryption Process

The data can be retrieving only by the authorized doctor. The authenticated doctor can perform data retrieval using SHA algorithm. SHA is a cryptographic hash function, there is no direct way decode. Hashed data is very easy and efficient to decrypt. If authentication is true, then hash value of encrypted data is received. Using the hash value, the decryption is preceded using secure hash algorithm. Fig 3 shows the comparison of proposed method of encryption and decryption mechanism with computation time.

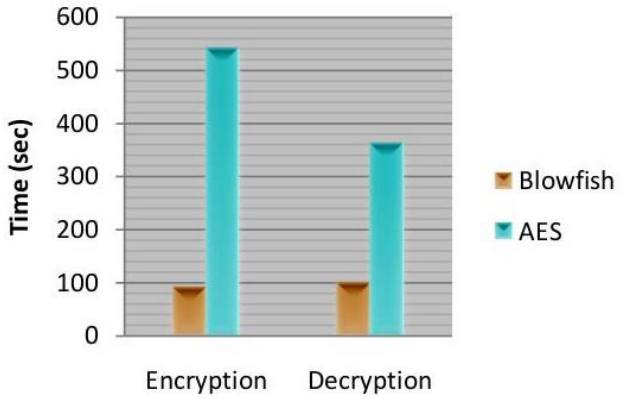

Fig 3. Computation Time for Encryption and Decryption Process

4.1.3. Comparison with other Existing Methods

Table 1. Comparison with existing Methods

Input Bytes	Encryption			Decryption		
	AES	DES	Modified Blowfish	AES	DES	Modified Blowfish
49	56	52	36	64	62	38
59	42	38	36	62	58	26
100	62	60	37	64	62	52
321	92	90	37	63	62	52
899	223	258	64	221	171	102
5345.28	1235	1237	122	658	655	149
7310.33	1346	1366	107	1005	882	140
223	135	135	155	998	885	190
35	8	0				
42000	1530	1423	165	998	994	190
99000	7890	1720	190	1345	1208	210
Average Time	520	502	91	458	360	98

In our proposed methods reveals that quickest computation time compared with other existing standard security mechanism. AES average time computation with secured files with 520 seconds when compared with proposed method outperforms the computation results 91 seconds to complete with secured way transferred information in block chain technology.

V. CONCLUSION

Block chain in medicinal services frameworks has gotten gigantic open doors terms of not just giving secure and productive data putting away, sharing and access yet additionally creates a potential degree in the social insurance business for an assortment of partners. In this paper, the principle center is to verify and effective information get to instrument for present day social insurance frameworks utilizing square chain innovation. Moreover, we investigated that our proposed plan can satisfy the prerequisites of trustworthiness, secrecy and validation in this medicinal services situation.

VI. REFERENCES

[1]. M. Puppala, T. He, X. Yu, S. Chen, R. Ogunti, and S. T. C. Wong, “Data security and privacy management in healthcare applications and clinical data warehouse environment,” in2016 IEEE-EMBS International Conference on

Biomedical and Health Informatics (BHI), Feb 2016, pp. 5– 8.

[2]. K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A review," Procedia Computer Science, vol. 113, pp. 73 – 80, 2017, the 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017) / The 7th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2017) / Affiliated Workshops.

[3]. N. Kahani, K. Elgazzar, and J. R. Cordy, "Authentication and access control in e-health systems in the cloud," in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security ril 2016, pp. 13–23.

[4]. Christo MS, Meenakshi S. Enhancing security properties of Rumor Riding protocol under various attacks scenario in P2P network. In2016 International Conference on Communication and Signal Processing (ICCSP) 2016 Apr 6 (pp. 1130-1135).

[5]. Christo, M.S. and Meenakshi, S., 2018. Enhancing Rumor Riding protocol in P2P network with Cryptographic puzzle through challenge question method. Computers & Electrical Engineering, 65, pp.122-138.

[6]. Christo, M.S. and Rathinam, J.J., 2018, April. Enhancing Authenticated Intermediate Node in Rumor Riding Protocol. In 2018 International Conference on Communication and Signal Processing (ICCSP) (pp. 0023-0027). IEEE..

[7]. F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, "Trust C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" IEEE Cloud Computing, vol. 5, no. 1, pp. 31–37, Jan 2018. S. P. Bingulac, "On the compatibility of adaptive controllers (Published Conference Proceedings style)," in Proc. 4th Annu. Allerton Conf.Circuits and Systems Theory, New York, 1994, pp. 8–16.

[8]. P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralizedapps," in 2017 IEEE 19th International Conference one-Health Networking, Applications and Services (Healthcom),Oct 2017, pp. 1–4..

[9]. M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in 2016 IEEE 18th International Conferenceon e-Health Networking, Applications and Services (Healthcom),Sept 2016, pp. 1–3.G. W. Juette and L. E. Zeffanella, "Radio noise currents n short sections on bundle conductors (Presented Conference Paper style)," presented at the IEEE Summer power Meeting, Dallas, TX, June 22–27, 1990, Paper 90 SM 690-0 PWRS.

[10]. W. Liu, S. Zhu, T. Mundie, and U. Krieger, "Advanced blockchain architecture for e-health systems," in e-Health Networking,Applications and Services (Healthcom), 2017 IEEE 19thInternational Conference on. IEEE, 2017, pp. 1–6..

[11]. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 25–30. deleted from the biography.