Grenze International Journal of Engineering and Technology, Jan Issue

SCADBIN: A Blockchain-based Security Framework for Electronic Health Record Management

Fasila K.A[1,2] and Sheena Mathew[3]
[1-3]Division of Computer Engineering, School of Engineering, Cochin University of Science and Technology, Kerala, India
[2]Computer Science and Engineering, Muthoot Institute of Technology and Science, Kerala, India
Email: fasila7@gmail.com, sheenamathew@cusat.ac.in

***Abstract*—Tremendous increase in the use of distributed Internet of Things (IoT) based applications leads to the evolution of huge amount of data every second. As the volume of data and correspondingly the number of users increase, the need for protecting information also increases. Among various distributed IoT applications, healthcare industry is in the dominating position. The management of Electronic Health Record (EHR) is a serious matter of concern since this includes the patient's personal as well as health related information. This work proposes the use of an efficient security framework for EHR management. SCADBIN stands for Security using Cellular Automata, Dynamic key and Blockchain for IoT Networks. This architecture provides multilevel protection to EHRs starting from the data acquisition phase till the data access phase by a requesting node. Thus, SCADBIN assures end to end protection to EHRs. The paper explains the methodology and implementation details. The comparison of this architecture with existing methods is provided at the end with valid experimental results.**

***Index Terms*— Electronic Health Record Management; IoT security; SCADBIN; Blockchain for IoT.**

I. INTRODUCTION

Before 2000, when a patient visited a hospital, a hospital staff had to collect all the relevant information from him, prepare a record and maintain it manually. Beyond 2004, the use of Electronic Medical Records (EMR) came into existence. EMR is a digital version of the patient records which were maintained manually before. After a few years, Electronic Health Records (EHR) started replacing EMRs. EHRs contain the clinical data that were collected during the patient visit as well as the health data that are being collected regularly after monitoring the patient health. The National Alliance for Health Information Technology (NAHIT) stated that EHR can be generated, maintained, and accessed by authorized clinicians and staff across distributed healthcare organization. The records can be accessed by the doctors and other hospital staffs for clinical purpose. At the same time, patients can always keep a log of their health information. In addition to these, distributed applications opened the way to access patient data by other organizations such as insurance agencies, researchers etc. Like any other domain, shifting to the digital world made healthcare industry also vulnerable to several attacks. EHRs may contain data that are collected from the wearable devices which are connected to the patient's body. Internet of Things (IoT) is the collection of heterogeneous uniquely identifiable things [1]. The sensing devices which measure data from the patient body represent the low level IoT devices. From these devices, the collected data have to be moved to cloud storage in a protected manner. Otherwise, during each and every phase

Grenze ID:01.GIJET.9.1.637

of transmission, security of the data may be compromised. This could be accessed by any unauthorized person. Also, the cloud was responsible to perform the analytics on the collected data as per conventional architecture. But, this creates a bottleneck since all the major functionalities are to be handled by the cloud. Also, this may lead to security breaches if the cloud administrator is not trustworthy. Thus, focusing to distributed implementations become more advantageous compared to the centralized architecture. One of the latest paradigms known as blockchain [2] can be used with this motivation. Disseminating the major functionalities to blockchain will reduce the overhead of the centralized architecture and improve trustworthiness of data.

The security algorithms used in such distributed applications must always be lightweight since the low level sensing devices are having constrained resources. There are many security frameworks proposed by several researchers for EHR management. An encryption scheme was put forward in [3] for providing security during EHR exchange process. This is according to the Health Insurance Portability and Accountability Act (HIPAA) to secure EHRs. But malicious intruders can still find a way to perform an attack. As per convention, protecting data with any encryption algorithm ensures the confidentiality of data. But, this does not assure integrity and consistency of data. A Message Authentication Code (MAC) based method was proposed in [4] to ensure integrity of the message. But this code computation is slightly complex such that it cannot be used by lightweight devices. There are a lot of third party based approaches as given in [5] to ensure security of EHRs. But, as mentioned earlier, trusting a third party is not a good option in the security world. There could be a problem of single point of failure. Also, the central node may be tampered by an adversary who will compromise the data security. Elliptic Curve Cryptography based security scheme which involves some mathematical computations is propose in [6]. As authors mention, it is a good method in terms of security, but not suitable for all IoT applications. Integrity and Privacy of EHRs can be ensured using Attribute Based Encryption (ABE) as given in [7]. Encryption can be done after reaching cloud and before reaching cloud. For more performance, Patient-Centric Privacy, Health service Provider and de-duplication were also considered by the authors. PHI (Patient Health Information) record owner decide how to encrypt files and which users to retrieve access to each file. File must only be accessible to the users who are given the decryption key. But, scalability is one problem and retrieval of data is not possible if the owner is not online.

Adapting blockchain technology for Electronic Health Record management is depicted in [8-15]. Secure attribute based Signature Scheme with multiple authorities for blockchain in EHR systems is proposed in [8]. Based on this work, patient information is treated as a block. Different blocks combined on a timeline basis. This gives access to multiple authorities-service providers, treatment providers etc. Secret pseudorandom function is shared among authorities. Authors of [9] state that access along with patient privacy can be ensured using blockchain. In their work dealing with blockchain powered health record management, they propose means to avail recorded data of patients lifelong. MedRec scheme [10] uses blockchain for medical data access and permission management. The method gives patients a log of medical history. Patients are aware of their history, as well as modifications if any. Permission management on blockchain is also provided. The technique facilitates patient initiated data exchange. An advantage of this scheme is that it provides expiry date for viewership rights. A blockchain ledger can be kept to provide an auditable history. According to the method in [11], patient is the complete owner of his/her health record. They can revoke access to service providers. Providers can issue prescriptions in blockchain. Authors suggests a future modification-i.e., providers, fitness centres etc. can develop programs to reward patients for healthy behavior. There can be 2 types of implementations-permissioned blockchain and permission-less blockchain. In case of permissioned block chain, it restricts access to a predetermined group. Usage of a blockchain network based on “hyper ledger fabric”- an open source blockchain with access control designations is depicted in [12]. Wearable devices collect data (Physical activity, sleeping conditions, heart beat rate etc.). The collected data are transmitted to cloud to which blockchain network will be connected. Completely replacing cloud with the blockchain is not advised as it is not practical to use blockchain for storing big data. Also incorporating blockchain for additional functionalities like authentication, access control etc. will ensure security of the application. The unwanted modifications of are prevented by the blockchain members.

The selection of lightweight algorithms also has to be appropriate. Several Advanced Encryption Standard (AES) based encryption algorithms were proposed as shown in [16]. Even though these provide security, these are not suitable for lightweight encryption. Also, in addition to this, an authentication method has to be incorporated to provide complete security. A searchable symmetric encryption (SSE) based scheme was proposed in [17]. Proxy Re-Encryption scheme (PRES) and Proxy Re-encryption scheme based on RSA (PRER) are also given in [18, 19]. Because of the complexities involved in case of standard encryption algorithms, new classes of lightweight ciphers were introduced to provide data confidentiality in IoT networks. Lightweight stream ciphers are best suitable for IoT applications. Based on the project conducted by eSTREAM [20] by European commission, a set

of finalist candidates are Sosemanuk, Salsa 20, Lizard etc. In the last section, a comparison of the lightweight cipher used in the proposed method with all these existing algorithms is given. A cellular automata based light weight cipher was proposed in [21]. Cellular automata (CA), introduced by von Neumann and Ulam, are known to be capable of modeling complex systems, though the basic model of it is a simple grid like structure. CA can be used in lightweight cryptography because of its inherent simplicity in implementation in hardware or sensor devices. Any type of controller board can be used to implement it. The initial seed is the only requirement for its dynamic next state evolution. With appropriate selection of rule or rule vector, CA is also capable of generating chaotic sequences and pseudo random numbers (PRNs). The most important characteristic of using CA in lightweight cryptography is that prediction of the next state by looking at the initial state is next to impossible, because very similar initial state configurations also lead to totally divergent and completely different final states. Reversion of state values to any given timestamp from current state is computationally hard problem and is very costly. Strength of the algorithm lies in rule vector selection and the only disadvantage is the lack of a key management scheme.

Security using cellular Automata, Dynamic Key and Blockchain for IoT Networks (SCADBIN) framework uses the principles of cellular automata for random number generation. It is a framework using the best known lightweight stream cipher ChaCha 20 and No Share Key Exchange (NSKE) method. The architecture utilizes blockchain for authentication checks and access control verifications. Next sections of this paper arranged as follows. Following sections give the detailed explanation of proposed model, implementation and results. Finally, a comparison study is provided.

II. METHODOLOGY

The proposed method provides a patient centric health record management system. Initially, when a patient visits a hospital, the EHR is added to the cloud by the hospital employee. During the registration process, the patient has the freedom to choose the information that can be shared with others. This is given as consent fields in the registration form. Only those features which are selected by the patient will be shared with others. Since the details are entered by the hospital staff, there is a possibility for an insider attack. To avoid this, a confirmation message is sent to the registered mail ID. After getting approval from the patient only, the status of data will be updated to “shared” or “unshared”. See Fig 3.1. The content of an EHR is then protected using SCADBIN framework. Different phases of the framework are detailed in [22].

Based on this, multilevel encryption is provided using the lightweight ChaCha 20 stream cipher [23] technique. The data-owner gateway node will assign priority levels to the data while uploading an EHR. If the data item is of higher priority, then it is encrypted with the intended recipient’s public key. Otherwise, the data will be protected using ABE Scheme. Attributes will be specified by the owner gateway node. The wearable sensing devices connected to a patient’s body can also send data to the owner gateway node in encrypted form. ChaCha 20 lightweight stream cipher is the best suitable encryption algorithm in this scenario since the encryption is done by constrained devices. The gateway devices will form a blockchain network. Even though the owner uploads an EHR to the cloud for the first time, any gateway device can add more data if this update request is approved by the blockchain members. This modification will be considered as a new transaction by the blockchain. Any communication between two entities in SCADBIN framework is preceded by a mutual authentication phase. After completing this phase successfully, the nodes will be able to upload data.

The key used for encryption by the low level device is known as a master key. This is device specific and will be shared with the intended recipient using the NSKE method [24]. Also, a second level encryption is done by using a dynamic group key which is provided by the owner gateway node. This group key is updated for every session and the same is done by applying the random number generator based on cellular automata. After this multilevel encryption, data will be uploaded to the cloud. After successful uploading to the cloud, any time another gateway node can send a request to access the same, as shown in Fig 3.2. When a data access request comes, initially, that will be processed by the blockchain members. An initial check is done to see whether the requested item is in the list of shared items. If not, the request is immediately rejected. If the data which are being requested belong to higher priority category, that will be encrypted using the public key of intended recipient. Hence, the requesting node will be given access if it is authenticated. If the data belong to lower priority category, the attributes of the requesting node are compared with the attributes specified during the uploading phase. Request is granted when both match. Here, the additional functionalities like verification of data modification, access control and authentication checks are disseminated to blockchain. The key management phase of SCADBIN is based on No-Share Key Exchange (NSKE) algorithm and the random numbers required for the stream cipher implementation are generated using the principles of cellular automata.

III. IMPLEMENTATION DETAILS

An EHR management application was developed in Python using Django framework. Since, the application was dealing with a distributed scenario, as mentioned in the previous sections; blockchain paradigm was used to implement it. Here, it was implemented with the Hyperledger fabric platform. A screenshot of the same is given in Fig 3.3. Hyperledger fabric is a type of consortium blockchain. In this, all participating entities will be having known identities. Since we are forming blockchain of gateway nodes that are already part of an IoT application, all nodes will be having their own identities. Two gateway nodes were created for participation as blockchain members. The Hyperledger Fabric implemented was supported by nodejs, Docker and Go installations.. Two gateway nodes were added as organizations with two peers each. When added to the blockchain, each organization will be assigned a public key-private key pair. As an example, we consider a gateway node is associated with the patient. Another gateway device is associated with the hospital. When the data are collected from the sensors connected to patients, gateway device will be uploading the contents to the storage after performing encryption. This means, EHR is uploaded to the cloud only after multilayer encryption as per the SCADBIN framework. Here, MongoDB was used as the storage platform.As shown in Fig 3.1, an approval page will be displayed in the home page of patient. The patient can decide with who the data items are to be shared. After encryption phases, the data will be uploaded to the storage.

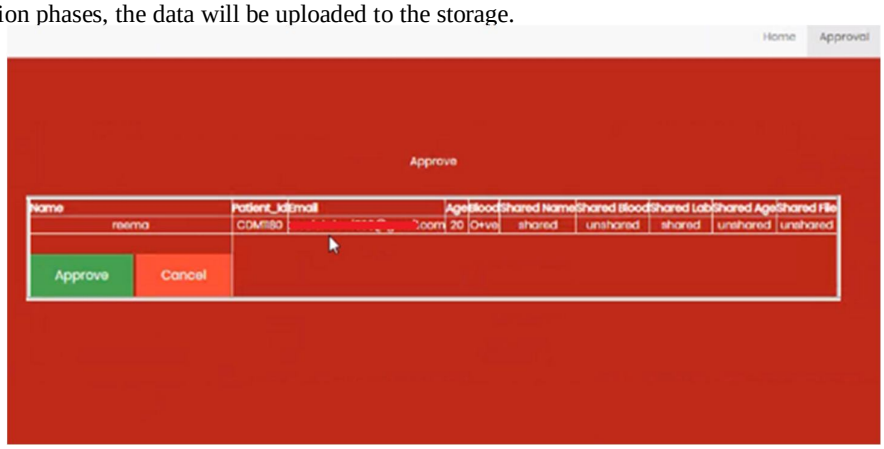

Fig 3.1: Approval page in patient's login

Now, another stakeholder such as a doctor may request the data item associated with the same patient. Initially, it will be checked whether the permission has been granted from the patient. If this first level authentication is satisfied, the decryption parameters will be shared with the requesting node. All these kinds of verifications are done by the blockchain consortium of gateway nodes.

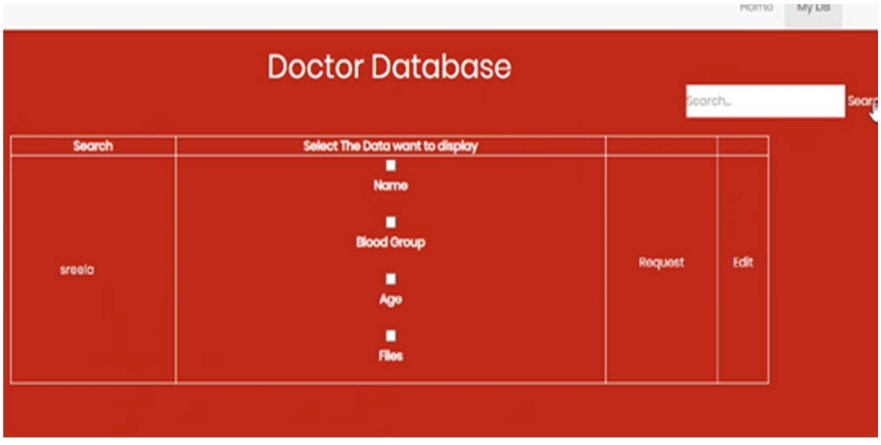

Fig3.2: User Interface page of a requesting node

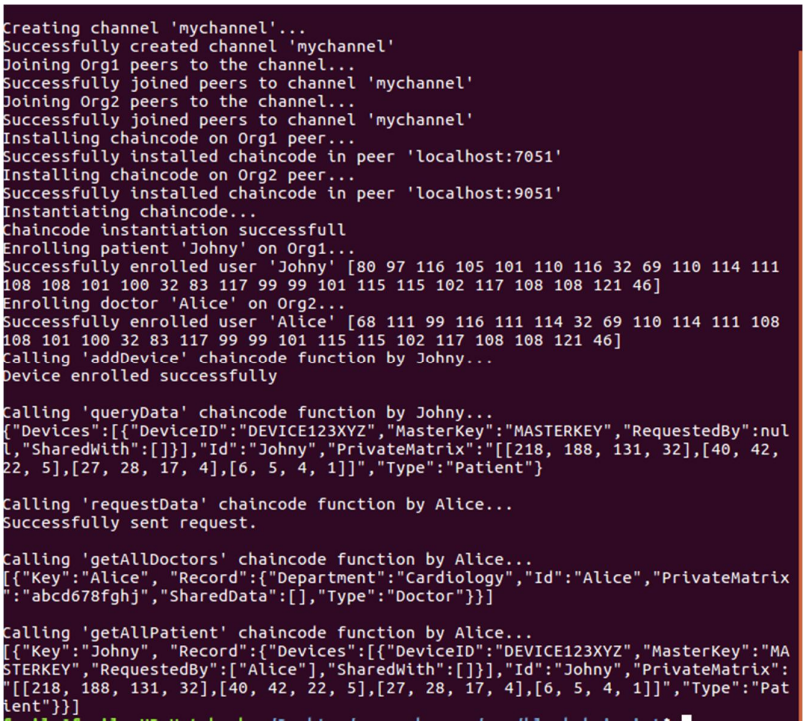

Fig 3.3: Blockchain set-up

IV. Results and Discussion

The authentication and key establishment phases of the proposed scheme are compared with two related schemes such as a matrix based key management scheme in [25] and a Lightweight Device Authentication and Key Management Scheme (LDAKM) in [26], in terms of computational cost.As mentioned in [27] and [28], computational cost of a security scheme depends on encryption, decryption and the hash computations for authentication. Cost of an AES encryption/decryption with 128 bits key would be 9μJ (milli Joules). Cost of a hash operation is 40mJ. Cost of encryption is less compared to the cost of hash operations. The cost of the proposed scheme for authentication and key establishment are less compared to the same phases in matrix based key management scheme and LDAKM. As it is clear from the Fig 4.1, our proposed scheme is having better performance in terms of computational cost compared to these two.

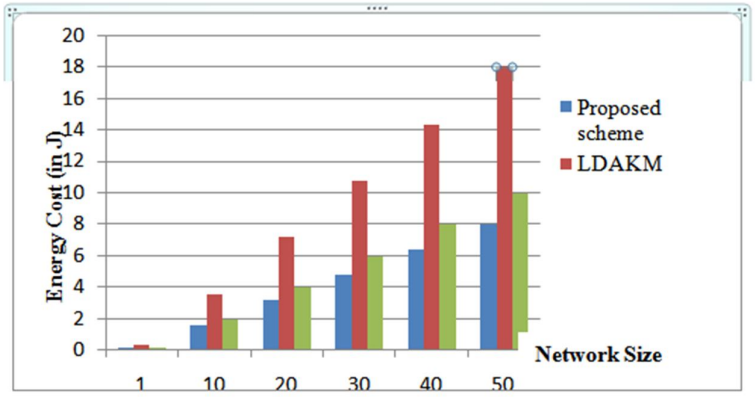

Fig 4.1. Comparison between Key exchange methods

The proposed algorithm is fast and efficient in terms of encryption time involved. The encryption algorithm CA-based ChaCha 20 cipher has been compared with the existing ciphers in terms of execution time. The data size used for encryption is 128 KiloBytes. The results are shown in Fig 4.2. Further enhancements on this system can be done on the storage optimizations. In addition to this, the feasibility of machine learning based methods for malicious node detection can be analyzed.

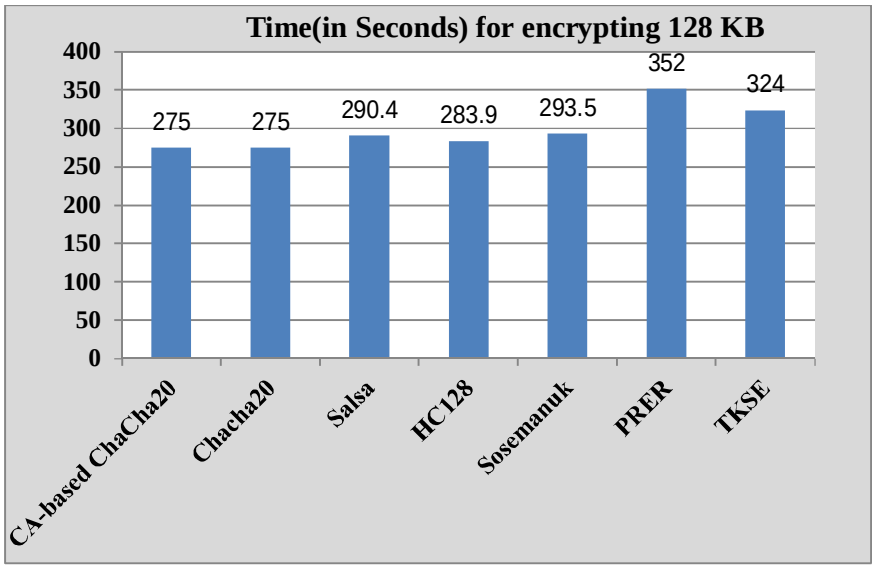

Fig 4.2: Encryption time comparison

V. Conclusions

The security of EHRs has become really crucial as the world has shifted to digital platform after the pandemic. The work proposed an efficient architecture SCADBIN for protecting EHRs using the best known algorithms such as ChaCha 20 based on the principles of cellular automata. Updating the session key at regular intervals improves security. The comparison study has proved that the algorithms used in SCADBIN architecture is having better performance compared to other existing schemes. All the major phases such as encryption, key exchange, mutual authentication etc. have lightweight operations. Use of blockchain improves the security by ensuring integrity and authentication.

References

[1] [1] P. Raj and A.C. Rajan, “Demystifying the IoT paradigm,” in The Internet of Things: Enabling Technologies, Platforms and Use cases, CRC Press, Taylor & Francis Group, Florida, USA, pp. 1–38, 2017.

[2] [2] S. Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”. [Online]. Available: https://bitcoin.org/bitcoin.pdf, Accessed on: 12-07-2019.

[3] [3] C.J. Wang, D.J. Huang. “The HIPAA conundrum in the era of mobile health and communications”, in JAMA. Vol. 310, no. 11,pp.1121–1122, 2013.

[4] [4] S.Aldossary, W. Allen. “Data Security, Privacy, Availability, and Integrity in Cloud Computing: Issues and Current Solutions”, in (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016 pp.485-498.

[5] [5] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, (2013) pp. 362–375, Feb 2013.

[6] [6] Debiao He and SheraliZeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare”, IEEE Internet of Things Journal 2(1):72-83, 2015.

[7] [7] R.ShinySharon,R Joseph Manoj, “E-Health Care Data Sharing Into The Cloud Based On De- duplication And File Hierarchical Encryption”, IEEE International Conference on Information Communication and Embedded Systems (ICICES), DOI: 10.1109/ICICES.2017.8070739, 2017.

[8] [8] RuiGuo ,Huixian Shi, Qinglan Zhao, Dong Zheng, “Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems”, IEEE Access, vol. 776, pp. 11676–11686, 2018.

[9] [9] G. Mgyar, “Block-chain: solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in helath data management”, 2017 IEEE 30th Neumann Colloquium (NC), Budapest, pp. 000135-000140, 2017.
[10] [10] AsaphAzaria ; Ariel Ekblaw ; Thiago Vieira ; Andrew Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management”, 2016 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp.25-30.
[11] [11] Guy Zyskind ; Oz Nathan ; Alex Sandy Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data”, 2015 IEEE Symposium on Security and Privacy Workshops (SPW), San Jose, CA, 2015, pp.180-184.
[12] [12] Juan Zhao, Sachin Shetty, Jihong Liu, Danyi Li, “Securing Mobile health Data Transmissions with BlockchainTexhnology”, https://innovate.ieee.org/innovation-spotlight/blockchain-mobile-health-data-wearables, 2018, Accessed: 11-07-2019.
[13] [13] RJ Krawiec, Mark White, “Blockchain: Opportunities for health care”, https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html,2016, Accessed: 11-07-2019.
[14] [14] Matthias Mettler, “Blockchain technology in healthcare: The revolution starts here”, 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich 2016, pp.1-3.
[15] [15] Ariel Ekblaw, Asaph Azaria, John D. Halamka, Andrew Lippman, “A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data”, https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf, 2016, Accessed: 11-07-2019.
[16] [16] N. Benhadjyoussef, H. Mestiri, M. Machhout, and R. Tourki, “Assessing CPA resistance of AES with different fault tolerance mechanisms,” in Proc. Design Autom. Conf. (ASP-DAC), Jan. 2016, pp. 661–666.
[17] [17] Aldiabat K, Kwekha Rashid AS, Talafha H, Karajeh A, “The extent of smartphones users to adopt the use of cloud storage”. J ComputSci 14(12):1588–1598, 2018.
[18] [18] KamelBoulosMN, Wilson JT, Clauson KA, “Geospatial blockchain: promises, challenges, and scenarios in health and healthcare”. Int J Health Geogr, 2018..
[19] [19] Zhou L, Wang L, Sun Y, “MIStore: a blockchain-based medical ınsurance storage system”. J Med Syst., 2018.
[20] [20] “eSTREAM: the ECRYPT Stream Cipher Project” ,Available: https://www.ecrypt.eu.org/stream/, Accessed: 26 October 2021.
[21] [21] Satyabrata Roy, UmashankarRawat, JyotirmoyKarjee, ”A Lightweight Cellular Automata Based Encryption Technique for IoT Applications”, IEEE Access Special Section on Security and Privacy for Cloud and IoT, March 2019.
[22] [22] K. A. Fasila and S. Mathew, "Fast and efficient security scheme for blockchain-based iot networks," Computers, Materials & Continua, vol. 73, no.1, pp. 2097–2114, 2022.
[23] [23] Ali F, Mathew S. 2022. “An efficient multilevel security architecture for blockchain-based IoT networks using principles of cellular automata”. PeerJ Computer Science 8:e989 https://doi.org/10.7717/peerj-cs.989.
[24] [24] Mahalingam P.R. and Fasila K.A., “Zero-Share key management for secure communication across a channel”, in Design and Analysis of Security Protocol for Communication. Scrivener Publishing. 2020. Ch.4.
[25] [25] M.Nafi ,S.Bouzefrane and M.Omar, “Matrix-based key management scheme for IoT networks” in Ad Hoc Networks , vol. 97, pp.102003, 2020.
[26] [26] M.Wazid, A.K.Das, S.Shetty, J.J.P.C. Rodrigues and Y. Park, “LDAKM-EIoT: Lightweight Device Authentication and Key Management Mechanism for Edge-Based IoT deployment”, Sensors. vol. 19. no. 24. 2019.
[27] [27] G. D. Meulenaer , F. Gosset , F.X. Standaert and O. Pereira , “On the energy cost of communication and cryptography in wireless sensor networks” , Networking and Communications, 2008. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/?doi=10.1.1.157.34 8&rep=rep1&type=pdf.
[28] [28] A.S. Wander , N. Gura , H. Eberle , V. Gupta and S.C. Shantz , “Energy analysis of public-key cryptography for wireless sensor networks”, in Proc. Third IEEE International Conference on Pervasive Computing and Communications. Kauai, HI, USA. pp. 324-328, 2005.