JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Health-Guard: Fortifying Health Records Security Through Blockchain Technology

[1]Gonella Veera Venkata Raghava Durga Pavan, [2]G Vamsi Krishna
[3]Gudise Sandhya Rani,[4]Ravi Aavula, [1,2,3]Scholar, [4]Associate Professor, Department of CSE
Guru Nanak Institutions Technical Campus, Hyderabad.

ABSTRACT: Electronic systems used for storing and sharing health records are vulnerable to security threats. To mitigate these risks, numerous countries have implemented regulations requiring healthcare information systems to adhere to certain security measures (such as confidentiality, access control, integrity, revocation, and anonymity) and additional features (like emergency access and interoperability). However, many existing solutions either have security shortcomings or only address certain aspects of these requirements. In response to this, we introduce Health-Guard, a blockchain-based protocol designed to secure health records while meeting all the primary and additional requirements stipulated in current regulations. We demonstrate the effectiveness of Health-Guard through various attack scenarios and show how it surpasses existing solutions. Additionally, we present a Health-Guard which can decrease access time of health records by 26% to 90% and reduce client-side memory overhead by up to 50%, compared to previous work.

Keywords: Blockchain, Security, Confidentiality, Access Control, Integrity, Revocation, Anonymity, Emergency Access, Interoperability, Regulations, Attack Scenarios, Access Time, Client -side Memory Overhead.

1 INTRODUCTION

Information technologies introduce several resources and benefits to the healthcare field. Electronic Health Records (EHRs), such as a patient's medical history, are one of the most widely employed resources [1], providing a wide view of a patient's medical status. EHRs are commonly originated and shared with collaborators (e.g., physicians, nurses) through cloud computing systems, which results in a more convenient approach to managing such records. Cloud-based systems, however, introduce security challenges in healthcare [2]. A recent report shows that healthcare data breaches are highly common [3], wherein several of them are classed as unauthorized access, which may lead to inappropriate use of health records (e.g., unwanted advertisements or lower chances of conquering a job opportunity). Due to security vulnerabilities, various countries (e.g., USA, Brazil, and those from European Union) have established regulations defining health records as sensitive data that should be shared only under patient consent [4]. These rules establish a set of criteria, referred to as properties of health records. For example, health records should only be accessible to those with the appropriate authorization, ensuring confidentiality and control over access. Records must also be protected from unauthorized modifications (integrity property). Furthermore, the aspects of revoking access and ensuring compatibility with other systems (access revocation and interoperability properties) must also be considered. These attributes inspire the creation of strategies to safeguard healthcare information systems.

Numerous scholarly suggestions offer frameworks that rely on centralized servers for the storage and distribution of health records. (e.g., [5], [6]). The security of such solutions relies on the fact that the server is trusted not to disclose sensitive data, such as information related to user credentials and patient records. This results in a single point that, when compromised, can make the entire system fail. Moreover, these solutions address only a subset of health record properties, Despite not meeting some basic requirements, numerous studies suggest the application of decentralized methods for safeguarding health records (for example, see references [7], [8]). Blockchain [9], for instance, is a technology that enhances data security. It permits online data transactions in a decentralized manner, thereby improving the security of the data. Although these schemes do not have drawbacks, they still lack an integrated approach that covers all of the aforementioned health records properties, then presenting security limitations. Therefore, lack of proposals in the literature that address all of the properties and afford satisfactory security to health records. Driven by the attributes outlined in the regulations, and the literature limitations, we propose Health-Guard, a protocol which secures health records by addressing all of their properties. In essence, Health-Guard is composed of a set of schemes, based on decentralized approaches (e.g., block chain and Interplanetary File System [10]) and cryptographic primitives (e.g., Cipher text-Policy Attribute-based Encryption [11] and public key encryption), which allow records to be stored and shared secur

2 SUMMARY OF THE METHODS FOUND IN THE LITERATURE

Author(s)	Technique	Advantages	Remarks
Clemens Scott Kruse, Anna Stein, Heather Thomas & Harmander Kaur1	Electronic Health Records (EHRs) usage for population health	Facilitates productivity/ efficiency in EHRs, Increased data management, and quality surveillance, and preventative care	The study found more facilitators than barriers to the use of EHR to support public health
da Costa et al. [12]	Decentralized protocol for securely storing and sharing health records	Secures health records	Proc. IEEE Int. Conf. E-Health Netw., Appl. Services (HealthCom), Bogotá, Colombia, Oct. 2019, pp. 1–6
Lee and Lee [13]	Cryptographic key management solution for HIPAA	Provides a key management solution for HIPAA	IEEE Trans. Inf. Technol. Biomed., vol. 12, no. 1, pp. 34–41, Jan. 2008
Hyperledger [23]	Hyperledger Fabric	Allows Developers to create applications with interchangeable components	Hyperledger Fabric documentation

3 PROPOSED FRAMEWORK

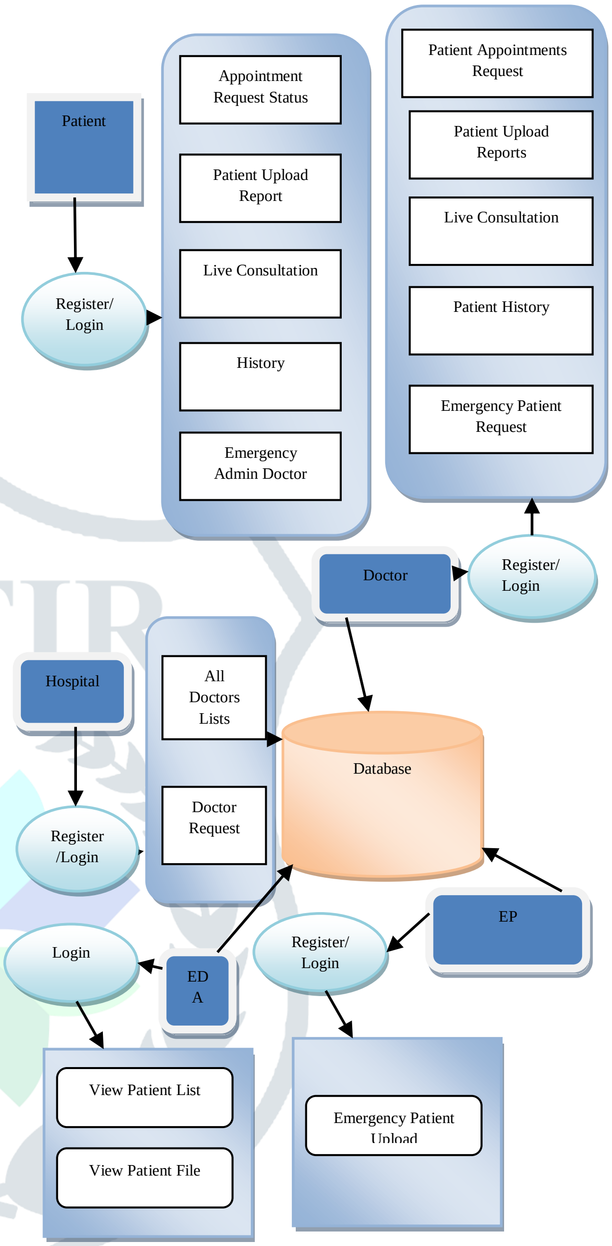


Fig 3.1. Proposed framework for Health-Guard

This ensures that message remains confidential and the intended recipient can only read it

2. AES-based Encryption: In this step, the data to be hidden is encrypted using the AES algorithm with a secret key. This key is shared between sender and the receiver. The receiver can then decrypt the hidden data using the same secret key

3. One-Way Hash Functions: A hash function is applied to the message. This function takes the message as input and outputs a fixed-size hash value. The same message will always output the same hash value. This step ensures the integrity of the message, as any changes to the message would result in a different hash value

4. CP-ABE (Ciphertext-Policy Attribute-based Encryption): In this final step, the data is encrypted with an access policy using CP-ABE. The access policy

4 METHODOLOGIES

1. Public Key Encryption: This is the first step in the process. The sender encrypts a message using the receiver's public key. Only the receiver, who has the corresponding private key, can decrypt this message.

is a tree-based structure with attributes interrelated through logical operators. The data can only be decrypted with a secret key that has attributes satisfying the access policy. This step provides fine-grained access control over the encrypted data.

This methodology provides a comprehensive approach to securing sensitive data, such as health records. It ensures confidentiality, integrity, and access control, making it suitable for use in healthcare information systems.

5 PROPOSED ALGORITHM

Step 1: Public Key Encryption
```
def encrypt_public_key (message, public key):
    cipher_text = E (message, public_key)
        return cipher_text
def decrypt_public_key (cipher_text, private_key)
    message = D(cipher_text, private_key)
        return message
```

Step 2: AES-based Encryption
```
def encrypt_AES (data, secret_key):
    encrypted data = AES_encrypt (data, secret_key)
        return encrypted_data
def decrypt_AES (encrypted_data, secret_key):
  Decrypt the encrypted data with the secret key
    data = AES_decrypt (encrypted_data, secret_key)
        return data
```

Step 3: One-Way Hash Functions
```
def hash_SHA256(message):
hash_value = SHA256_hash(message)
        return hash_value
```

Step 4: CP-ABE
```
def encrypt_CPABE (data, access_policy):
encrypted_data = CPABE_encrypt (data, access_policy)
        return encrypted_data
def decrypt_CPABE (encrypted_data, secret_key):
    data =CPABE_decrypt (encrypted_data, secret_key)
        return data
```

6 EXPEIMENTAL RESULTS:

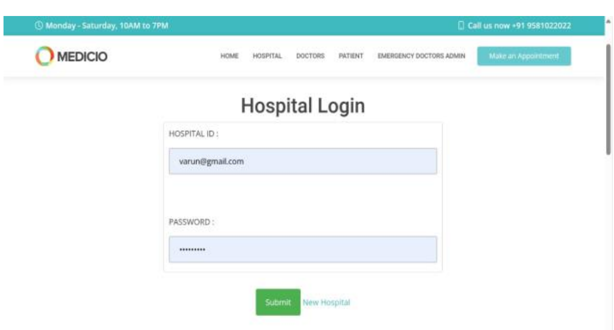
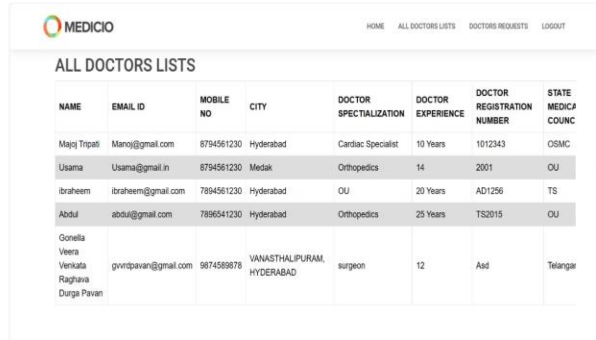
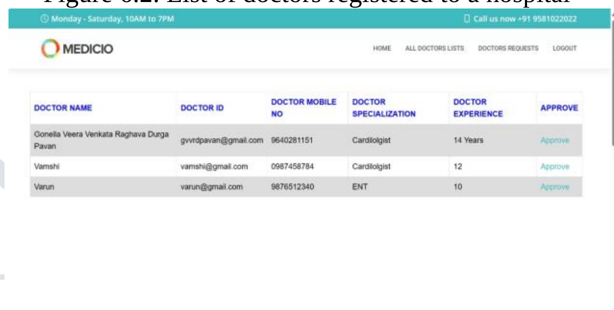


Figure 6.1. Hospital login page for doctors



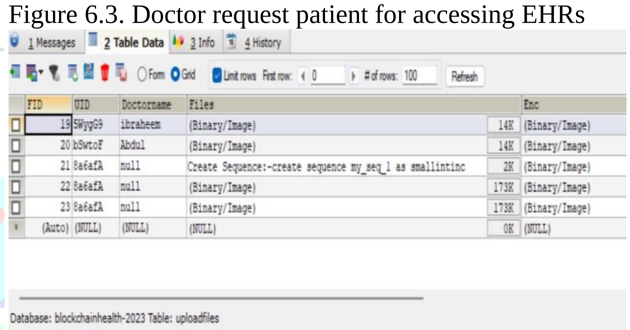
NAME	EMAIL ID	MOBILE NO	CITY	DOCTOR SPECTIALIZATION	DOCTOR EXPERIENCE	DOCTOR REGISTRATION NUMBER	STATE MEDICA COUNC
Majoj Tripati	Manoj@gmail.com	8794561230	Hyderabad	Cardiac Specialist	10 Years	1012343	OSMC
Usama	Usama@gmail.in	8794561230	Medak	Orthopedics	14	2001	OU
ibraheem	ibraheem@gmail.com	7894561230	Hyderabad	OU	20 Years	AD1256	TS
Abdul	abdul@gmail.com	7896541230	Hyderabad	Orthopedics	25 Years	TS2015	OU
Gonella Veera Venkata Raghava Durga Pavan	gvvrdpavan@gmail.com	9874589878	VANASTHALIPURAM, HYDERABAD	surgeon	12	Asd	Telangar

Figure 6.2. List of doctors registered to a hospital



DOCTOR NAME	DOCTOR ID	DOCTOR MOBILE NO	DOCTOR SPECIALIZATION	DOCTOR EXPERIENCE	APPROVE
Gonella Veera Venkata Raghava Durga Pavan	gvvrdpavan@gmail.com	9640281151	Cardilolgist	14 Years	Approve
Vamshi	vamshi@gmail.com	0987458784	Cardilolgist	12	Approve
Varun	varun@gmail.com	9876512340	ENT	10	Approve

Figure 6.3. Doctor request patient for accessing EHRs



FID	UID	Doctorname	Files		Enc
19	5WygG9	ibraheem	(Binary/Image)	14K	(Binary/Image)
20	bSwtoF	Abdul	(Binary/Image)	14K	(Binary/Image)
21	8a6afA	null	Create Sequence:-create sequence my_seq_1 as smallintinc	2K	(Binary/Image)
22	8a6afA	null	(Binary/Image)	173K	(Binary/Image)
23	8a6afA	null	(Binary/Image)	173K	(Binary/Image)
(Auto)	(NULL)	(NULL)	(NULL)	0K	(NULL)

Figure 6.4. Patients data stored in data base with proposed encryption scheme

Comparing The Experimental Results With Related Works

Execution Time: Health-Guard outperforms related work in execution time, especially with 10 CP-ABE attributes, achieving **0.36s** for storage and **0.17s** for sharing phases. It remains efficient even with 100 attributes.

Memory Usage: While Health-Guard introduces more memory overhead in storage, it uses less memory than related work for sharing, particularly with smaller health records.

Comparative Efficiency: Compared to da Costa et al.'s protocol, Health-Guard is more efficient in sharing phase, reducing execution time by at least **26%** and memory usage by up to **50%**.

Overall Performance: Despite being less efficient in memory usage during storage, Health-Guard's sharing phase is generally faster and more memory-efficient than similar protocols.

Research	Storage phase		Sharing phase	
	10 attributes	100 attributes	10 attributes	100 attributes
Rahul amathavan et al.[31]	0.5s		0.23s	
Liu et al.[26]	0.01s	0.01s	10s	100s
da Costa et al.[9]	0.19s	1.28s	0.38s	0.79s
Sec-Health	0.36s	0.89s	0.17s	0.4s
Health-Guard	0.35s	0.87s	0.15s	0.3s

Table 1. Experimental values obtained for various research works.

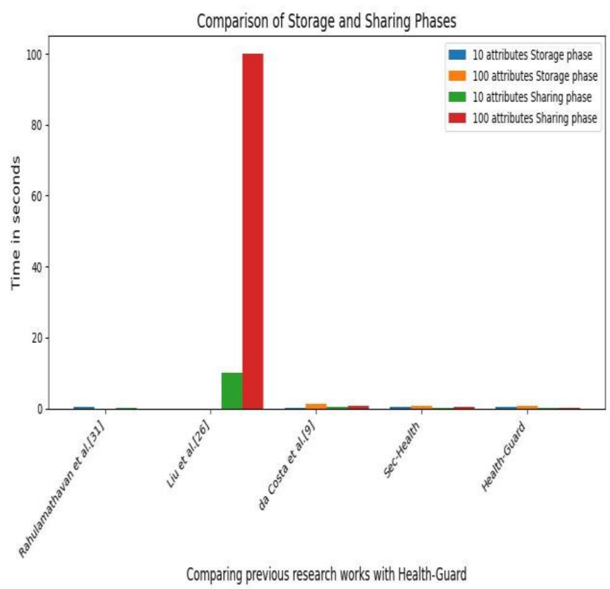


Figure 2. Graph showing experimental results of research works based on their execution time

7 CONCLUSION

In this work, we proposed Health-Guard, a blockchain-based protocol that secures health records while addressing all of their main properties, namely confidentiality, access control, integrity, access revocation, emergency access, Health-Guard shows security advantages compared to related proposals that present highly security mechanisms. While those proposals are generally based on a server, Health-Guard affords several features, preventing one single entity from compromising the healthcare system. Furthermore, compared to solutions, our protocol addresses the challenging problem of fulfilling all the main properties of health records, whereas other solutions focus on offering mechanisms for specific only. Experimental evaluations of a Health-Guard demonstrated the practical feasibility of our protocol.

8 REFERENCES

[1] C. S. Kruse, A. Stein, H. Thomas, and H. Kaur, ‘‘The use of electronic health records to support population health: A systematic review of the literature,’’ J. Med. Syst., vol. 42, no. 11, p. 214, Nov. 2018.

[2] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, ‘‘EHealth cloud security challenges: A survey,’’ J. Healthcare Eng., vol. 2019, pp. 1–15, Sep. 2019.

[3] HIPAA Journal. December 2021 Healthcare Data Breach Report. Accessed: Sep. 2, 2022. [Online]. Available: https://www.hipaajournal. com/december-2021-healthcare-data-breach-report/

[4] I. M. Lopes, T. Guarda, and P. Oliveira, ‘‘General data protection regulation in health clinics,’’ J. Med. Syst., vol. 44, no. 2, p. 53, Feb. 2020.

[5] S. Mhatre and A. V. Nimkar, ‘‘Secure cloud-based federation for EHR using multi-authority ABE,’’ Progress in Advanced Computing and Intelligent Engineering (Advances in Intelligent Systems and Computing), vol. 714. Singapore: Springer, 2019. [Online]. Available

[6] R. Ganiga, R. Pai, M. Pai, and R. Sinha, ‘‘Security framework for cloud based electronic health record (EHR) system,’’ Int. J. Electr. Comput. Eng., vol. 10, pp. 455–466, Feb. 2020.

[7] V. Patel, ‘‘A framework for secure and decentralized sharing of medical imaging data via blockchain consensus,’’ Health Informat. J., vol. 25, no. 4, pp. 1398–1411, Dec. 2019.

[8] B. Shen, J. Guo, and Y. Yang, ‘‘MedChain: Efficient healthcare data sharing via blockchain,’’ Appl. Sci., vol. 9, no. 6, p. 1207, Mar. 2019.

[9] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: Sep. 7, 2022. [Online]. Available.

[10] J. Benet, ‘‘IPFS—Content addressed, versioned, P2P file system,’’ 2014, arXiv:1407.3561. [11] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute-based encryption,’’ in Proc. IEEE Symp. Secur. Privacy, Oakland, CA, USA, Dec. 2007, pp. 321–334.

[12] L. da Costa, B. Pinheiro, R. Araujo, and A. Abelem, ‘‘A decentralized protocol for securely storing and sharing health records,’’ in Proc. IEEE Int. Conf. E-Health Netw., Appl. Services (HealthCom), Bogotá, Colombia, Oct. 2019, pp. 1–6.

[13] W. B. Lee and C. D. Lee, ‘‘A cryptographic key management solution for HIPAA privacy/security

regulations,'' IEEE Trans. Inf. Technol. Biomed., vol. 12, no. 1, pp. 34–41, Jan. 2008.

[14] LGPD. (2018). Lei no 13.709, de 14 de Agosto de 2018 (in Portuguese). Accessed: Sep. 7, 2022. [Online]. Available: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

[15] K. Yang, X. Jia, and K. Ren, ''Attribute-based fine-grained access control with efficient revocation in cloud storage systems,'' in Proc. 8th ACM Symp. Inf., Comput. Commun. Secur. (ASIA CCS), K. Chen, Q. Xie, W. Qiu, N. Li, W.-G. Tzeng, Eds. Hangzhou, China, May 2013, pp. 523–528.

[16] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, ''Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system,'' Inf. Sci., vol. 479, pp. 567–592, Apr. 2019.

[17] R. L. Rivest, A. Shamir, and L. M. Adleman, ''A method for obtaining digital signatures and public-key cryptosystems (reprint),''Commun. ACM, vol. 26, no. 1, pp. 96–99, 1983.

[18] FIPS. (2002). Secure Hash Standard. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/fips/180/2/archive/2002-08- 01/documents/fips180-2.pdf

[19] M. Jakobsson and A. Juels, ''Mix and match: Secure function evaluation via ciphertexts,'' in Advances in Cryptology—ASIACRYPT (Lecture Notes in Computer Science), vol. 1976, T. Okamoto, Ed. Kyoto, Japan: Springer, Dec. 2000, pp. 162–177.

[20] D. Johnson, A. Menezes, and S. Vanstone, ''The elliptic curve digital signature algorithm (ECDSA),'' Int. J. Inf. Secu-r., vol. 1, no. 1, pp. 36–63, Aug. 2001.

[21] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, ''Survey on blockchain for Internet of Things,'' Comput. Commun., vol. 136, pp. 10–29, Feb. 2019.

[22] G. W. Peters and E. Panayi, ''Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the Internet of Money,'' 2015, arXiv:1511.05740.

[23] Hyperledger. Hyperledger Fabric. Accessed: Sep. 7, 2022. [Online]. Available.

[24] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea, and M. S. Hossain, ''A robust and lightweight secure access scheme for cloud based Ehealthcare services,'' Peer-Peer Netw. Appl., vol. 14, no. 5, pp. 3043–3057, Sep. 2021.

[25] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, ''Secure and fine-grained access control on E-healthcare records in mobile cloud computing,'' Future Gener. Comput. Syst., vol. 78, pp. 1020–1026, Jan. 2018.

[26] M. Kumar and S. Chand, ''A secure and efficient cloud-centric Internet-of Medical-things-enabled smart healthcare system with public verifiability,'' IEEE Internet Things J., vol. 7, no. 10, pp. 10650–10659, Oct. 2020.

[27] H. Qiu, M. Qiu, M. Liu, and G. Memmi, ''Secure health data sharing for medical cyber-physical systems for the healthcare 4.0,'' IEEE.

[28] V. Vijayakumar, M. K. Priyan, G. Ushadevi, R. Varatharajan, G. Manogaran, and P. V. Tarare, ''E-health cloud security using timing enabled proxy re-encryption,'' Mobile Netw. Appl., vol. 24, no. 3,pp. 1034–1045, Nov. 2022.

[29] I. Abunadi and R. Kumar, ''BSF-EHR: Blockchain security framework for electronic health records of patients,'' Sensors, vol. 21, no. 8, p. 2865,Apr. 2021.

[30] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, ''A patient-centric health information exchange framework using blockchain technology,'' IEEE J. Biomed. Health Informat., vol. 24, no. 8, pp. 2169–2176, Aug. 2020.

[31] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, ''Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption,'' in Proc. IEEE Int. Conf. Adv. Netw. Telecom mun. Syst. (ANTS), Bhubaneswar, India, Dec. 2017, pp. 1–6.

[32] M. Zghaibeh, U. Farooq, N. U. Hasan, and I. Baig, ''SHealth: A blockchain-based health system with smart contracts capabilities,'' IEEE Access, vol. 8, pp. 70030–70043, 2020.

[33] M. T. de Oliveira, A. Bakas, E. Frimpong, A. E. D. Groot, H. A. Marquering, A. Michalas, and S. D. Olabarriaga, ''A break□glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud,'' Ann. Telecommun., vol. 75, nos. 3–4, pp. 103–119, Apr. 2020.

[34] Design and Implementation of sensor and IoT based Remembrance system for closed one R Aavula, AB Deshmukh, VA Mane, GH Chavhan, KKS Liyakat Telematique, 2769-2778 2022.

[35] XBPF: an extensible breast cancer prognosis framework for predicting susceptibility, recurrence and survivability R Aavula, R Bhramaramba Int. J. Eng. Adv. Technol 8 (5), 2249-8958 2019

[36]A survey on latest academic thinking of breast cancer prognosis R Aavula, R Bhramaramba Int J Appl Eng Res 13, 5207-5215 2018

[37] Smart Health Consulting Android System R Aavula, M Kruthini, N Raviteja, K Shashank International Journal of Innovative Research in Science, Engineering and 2017

[38] Towards a framework for breast cancer prognosis: risk assessment R Aavula, R Bhramaramba ICCCE 2020: Proceedings of the 3rd International Conference on 2021

[39] A Comprehensive Study on Data Mining Techniques used in Bioinformatics for Breast Cancer Prognosis R Aavula, R Bhramaramba, US Ramula Journal of Innovation in Computer Science and Engineering 9 (1), 34-39 2019

[40] A Machine Learning based Fine-Tuned and Stacked Model: Predictive Analysis on Cancer Dataset R AAVULA CSA) International Journal of Advanced Computer Science and Applications, 9 2018