Distributed Privacy Control System for Identifying Affective Data Storage in Health Care Management System

Nare Indraja[1], Rolla Chandana[2], Yedupati Spandana[3]
PG Students, Sree Venkateswara College of Engineering[123], Nellore. AP. India.

Abstract: The field of smart health has gained significant interest in recent times, thanks to the progress in information and communications technology. At the same time, the importance of medical data cannot be overstated in supporting smart health practices. However, the storage of this data is confronted with significant challenges related to security and privacy, including concerns from activists, cloud service providers, and healthcare organizations. To tackle these challenges, we introduce a new data storage solution called Derepo. Derepo aims to secure data storage through a decentralized access control system and ensure privacy using homomorphism encryption. This project leverages distributed ledger technology to enhance the access control system with features like Byzantine fault tolerance, making it more reliable. Additionally, we employ a fully homomorphism encryption scheme to safeguard data privacy and maintain the ability to perform computations. The design of Derepo is centered around the user, allowing only the data owner to set access control policies and decrypt their data. Meanwhile, authorized third parties can oversee data processing on encrypted data without having access to the original data.

Keywords: Fault tolerant, Data driven approaches, Derepo distributed privacy control system.

I.INTRODUCTION

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. If the connection to the user is relatively close, it may be designated an edge server. Moreover, medical organizations and research institutes can manage and process medical data at less cost, which can also improve the quality of medical services based on smart health. However, behind these appealing services, the security and the privacy of the medical data become a notable issue to the development of smart health due to the rapid-growth value of these data. 78.8 million Patients had their information stolen after a hack occurred on the insurance corporation named Anthem in 2015. Over 2500 data breaches for the period between 2009 and 2019 happened and millions of people were affected according to the U.S. Department of Health and Human Services Office of Civil Rights. Additionally, privacy and trust issues have become a great concern since the spread of cloud computing techniques. In the meanwhile, the cloud service providers (CSPs) can only promise to preserve the privacy at best efforts instead of the liability, which puts the data on clouds at risk. To circumvent the issue, we propose Derepo, a distributed data repository, which preserves both security and privacy for the persistence of sensitive medical data to be used for smart-health based services. In Derepo, the distributed ledger technology (DLT) is used to decentralize the access control mechanism. There is no central entity enforcing the access control mechanism, which makes the system tamper-proof to defend illegal access and prevent the single point of failure. Besides, the privacy of access control can be ensured by the decentralization structure. As another imperative aspect, the privacy of the medical data is ensured by the homomorphism 1 Introduction Fault Tolerant Data Archiving Health System With Distributed Privacy Control encryption (HE) scheme. All medical data in the repository are encrypted, which can only be decrypted by the data owners. Hence, the data owners have the overall control of their data. Moreover, Derepo provides a flexible and privacy preserving data sharing method. The third parties such as medical organizations and research institutes can perform the data processing directly on the encrypted data that is computable and meaningful without disclosing any private information. For the untrustworthy third parties such as the CSP, the encrypted data can still preserve privacy while being persisted on the cloud. Purpose

This project aims to create a, Novel data repository named Derepo to address these issues by securing the storage with the decentralized access control mechanism and preserving privacy via the homomorphism encryption scheme. Scope Furthermore, we evaluate and prove the security of Derepo with the analysis from the perspective of attackers. We also demonstrate the performance of Derepo by conducting experiments on the prototype. In addition, Derepo is not smart health specific and is capable of supporting more generalized data access, storage and sharing. In future work, we will optimize the implementation and extend the functionality to reach the industrial level. Need For The System Existing System Meanwhile, the medical data is imperative to support smart health techniques. However, the storage of medical data faces serious security and privacy issues from the hacktivists, cloud service providers and even medical institutions.

Proposed research gaps can be retrived by proposed Derepo to decentralize the access control and encrypt the data without losing computability that are two significant challenges extracted from the adversary model. The double-layered architecture is formalized together with static structures and dynamic processes. We utilize the consortium block chain to ensure the integrity of the access control mechanism, which also preserves controllability, manageability and pseudonymity. The FHE scheme is adopted to ensure confidentiality and resolve the privacy issues caused by both internal and external adversaries.

Merits of proposed model

- Improving Data Privacy.
- Providing more Security to the Data.
- High efficiency.
- Ensure Confidentiality of outsourced data

II RELATED WORK

The distributed ledger technology underlying decentralized applications is the integration of multiple techniques including cryptography, distributed computing, and network engineering. With the support of consensus mechanisms such as proof-ofwork (PoW) [9], practical Byzantine fault tolerance (PBFT) [10], the decentralized applications have great integrity and capability of fault tolerance. Besides, the smart contract extends the functionality of the DLT, which widens the range of the application. Based on the DLT, decentralized applications have been applied to many fields such as [11] for IoT, Bloccess [12] for security infrastructure, Dagbase [13] for database.

Additionally, some solutions for smart health based on the DLT are also proposed. MedRec [14] is one of the earliest and feasible researches to provide a decentralized medical data management system based on the blockchain techniques. It constructed a trustworthy access control mechanism to ensure the security of medical data and data sharing. It designed a set of smart contracts running on the Ethereum virtual machine (EVM) and an incentive mechanism to make medical stakeholders participate in mining. Later, Ancile [15] was proposed to construct a secure, interoperable and efficient framework based on the permissioned blockchain to control the access to the medical records by patients, providers and third parties. Compared to MedRec, although the performance cost of Ancile is higher, the design of Ancile is more secure by allowing the providers to store more information on the blockchain such as small medical records and links to larger medical records. Additionally, some researches focus on the construction of the index engine for EHR by the blockchain techniques such as [16].

This work proposed a searchable encryption scheme for EHR data sharing based on the Ethereum. Recently, a new version of MedRec [17] was proposed for a network of trusted data repositories. The research presented a new and 4 SRS Fault Tolerant Data Archiving Health System with Distributed Privacy Control more sophisticated architecture, which is also managed by the Ethereum blockchain. However, although these researches can tackle the single point of failure and ensure integrity of data in some way, the blockchain techniques cannot be applied to the medical data persistence directly. Most of the medical data are stored off the chain due to the limited on-chain storage space. The privacy of the off-chain data can be a significant problem because the service providers cannot be fully trusted. In recent years, the HE schemes are used to preserve the privacy of the medical data. As a special form of asymmetric cryptography, HE enables computations on the encrypted data directly.

Let = (Gen, Enc, Dec) be an HE scheme, where Gen, Enc, Dec denote the key generation function, the encryption function and the decryption function respectively. Firstly, $(pk, sk) \leftarrow Gen(\kappa)$, where (pk, sk) is a pair of keys including a public key and a private key, and κ denotes the security parameter. For two plaintexts m0 and m1, HE satisfies (1). ⊕ and ⊗ represent the addition and multiplication on the ciphertext respectively. $\mathrm{Dec}(\mathrm{Enc}(m0) \oplus \mathrm{Enc}(m1)) = (m0 + m1) \vee \mathrm{Dec}(\mathrm{Enc}(m0) \otimes \mathrm{Enc}(m1)) = (m0 \times m1)$ (1) The work [18] demonstrated the feasibility of the HE scheme that can be used to compute aggregating queries on the encrypted medical data, which makes it possible to share the clinical data with the preservation of the privacy. Besides, the work [19] presented the implementation of a long-term cardiac health monitoring application based on the HE scheme, which aims to eliminate the concerns of the privacy issues on the cloud. One of the issues of using the HE mechanism simply is that the data integrity can hardly be ensured. Therefore, the integration of the blockchain techniques and the HE mechanism can provide a feasible solution to preserving both security and privacy.

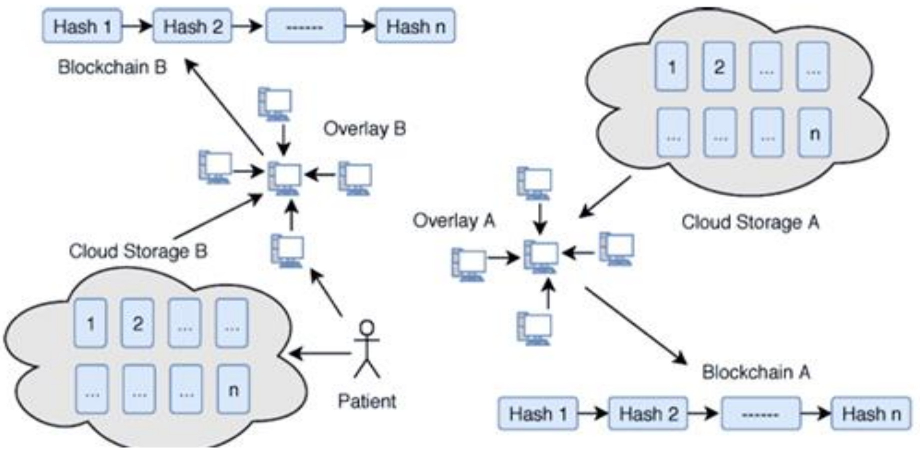
III.LITERATURE REVIEW

1. Y. Ding and H. Sato, "Bloccess: Towards Fine-Grained Access Control Using Blockchain in a Distributed Untrustworthy Environment," (2019) Access control plays a crucial role in constructing trust in a system. Particularly, it is imperative to enforce a fine-grained access control mechanism to make the access control framework flexible due to the high 5 SRS Fault Tolerant Data Archiving Health System With Distributed Privacy Control complexity of untrustworthy environments such as the Internet of Things (IoT) environments. However, traditional access control techniques can be hardly trusted on account of their centralized enforcements and improper distributed computing mechanisms while facing diverse and intricate threats. Although existing solutions based on public blockchain technology have addressed some issues, new challenges derived from public blockchain technology become noticeable such as low consensus efficiency and delicate incentive mechanism.

2. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,"(2018) Despite an increased focus on the security of electronic health records and an effort by large cities around the globe to pursue smart city infrastructure, the private information of patients is subject to data breaches on a regular basis. Previous efforts to combat this have resulted in data being mostly inaccessible to patients. Existing record management systems struggle with balancing data privacy and the need for patients and providers to regularly interact with data. Blockchain technology is an emerging technology that enables data sharing in a decentralized and transactional fashion.

3. J. L. Raisaro, J. G. Klann, K. B. Wagholikar, H. Estiri, J.-P. Hubaux, and S. N. Murphy, "Feasibility of Homomorphic Encryption for Sharing I2B2 Aggregate - Level Data in the Cloud," (2017). The biomedical community is lagging in the adoption of cloud computing for the management of medical data. The primary obstacles are concerns about privacy and security. In this paper, we explore the feasibility of using advanced privacy-enhancing technologies in order to enable the sharing of sensitive clinical data in a public cloud. Our goal is to facilitate sharing of clinical data in the cloud by minimizing the risk of unintended leakage of sensitive clinical information.

IV PROPOSED SYSTEM ARCHITECTURAL MODEL



SYSTEM ARCHITECTURE figure Describes Cloud storage is a cloud computing model that stores data on the internet through cloud computing provider who manages and operates data storage as a service. In this architecture patient should be login then user upload file in to the cloud storage. Then the system shows the results.

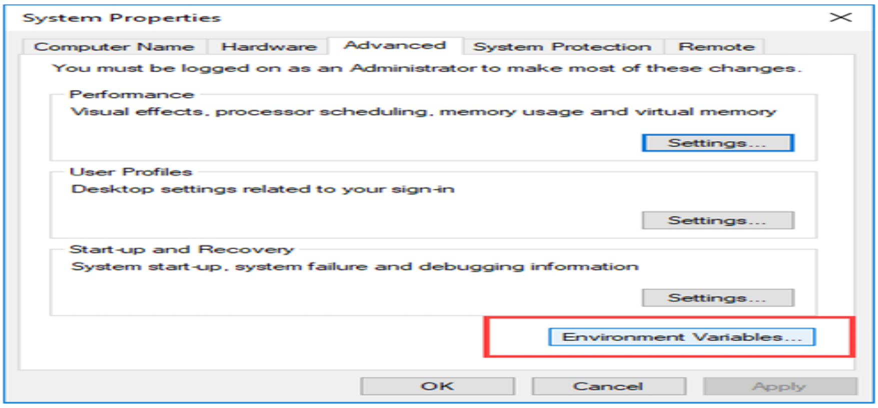
V PROPOSED ALGORITHMS

Related Work Existing Algorithms Encryption In Cryptography, Encryption is the process of encoding a message or information in a way that only authorized parties can access it and those who are not authorized cannot. Encryption happens at sender's end. Any message to be encrypted using a secret key or public key. Proposed Algorithms Decryption Decryption happens at receiver's send any message to be decrypted using a secret key or private key.

RESEARCH METHODLOGY PROCESS

Cloud Service Providers • Cloud Service Provider can login into the system with their credentials. After login he/she can view the Users, checking who is active and inactive, and View user uploaded files, Checking Threats (External: (Remove the threats and protect the files) and Internal), View Attacked list and protect the files and then logout from the system. 2. Data Consumer .

VI RESULTS

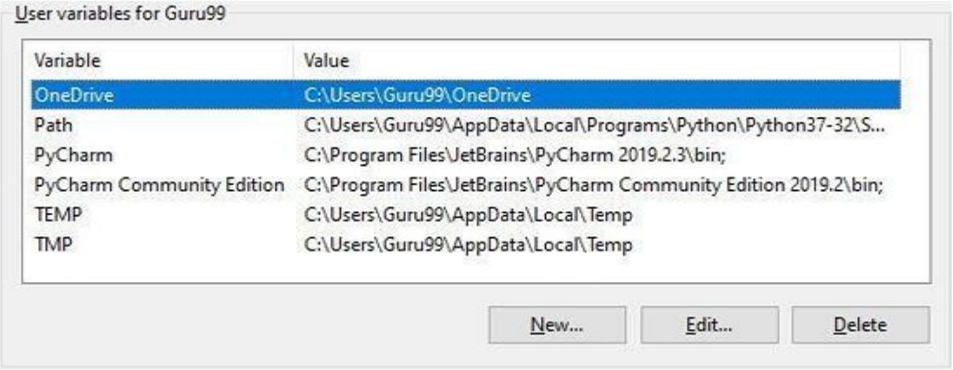


You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage and virtual memory

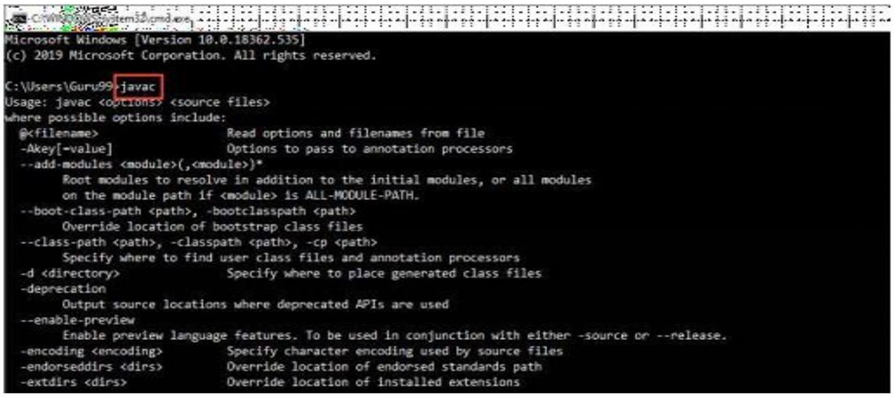
Desktop settings related to your sign-in

System start-up, system failure and debugging information



User variables for Guru99

Variable	Value
OneDrive	C:\Users\Guru99\OneDrive
Path	C:\Users\Guru99\AppData\Local\Programs\Python\Python37-32\S...
PyCharm	C:\Program Files\JetBrains\PyCharm 2019.2.3\bin;
PyCharm Community Edition	C:\Program Files\JetBrains\PyCharm Community Edition 2019.2\bin;
TEMP	C:\Users\Guru99\AppData\Local\Temp
TMP	C:\Users\Guru99\AppData\Local\Temp



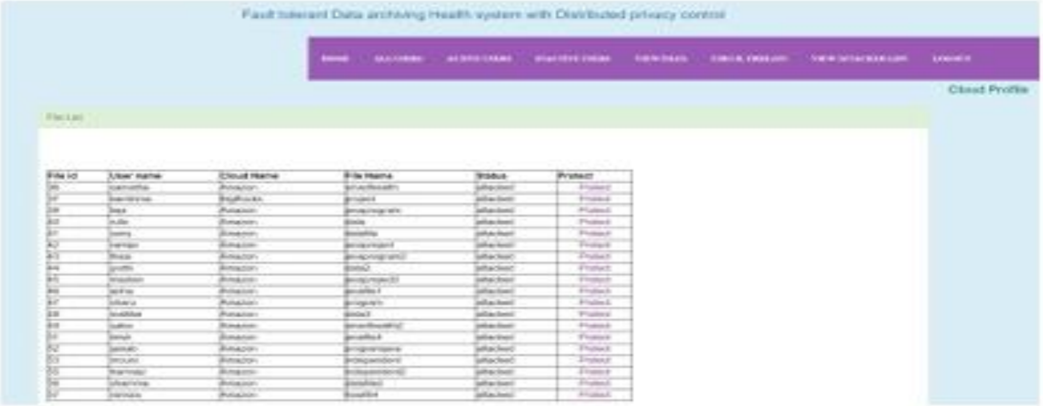
```
Microsoft Windows [Version 10.0.18362.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Guru99>javac
Usage: javac <options> <source files>
where possible options include:
  @<filename>                  Read options and filenames from file
  -Akey[=value]                Options to pass to annotation processors
  --add-modules <module>(,<module>)*
        Root modules to resolve in addition to the initial modules, or all modules
        on the module path if <module> is ALL-MODULE-PATH.
  --boot-class-path <path>, -bootclasspath <path>
        Override location of bootstrap class files
  --class-path <path>, -classpath <path>, -cp <path>
        Specify where to find user class files and annotation processors
  -d <directory>               Specify where to place generated class files
  -deprecation
        Output source locations where deprecated APIs are used
  --enable-preview
        Enable preview language features. To be used in conjunction with either -source or --release.
  -encoding <encoding>         Specify character encoding used by source files
  -endorseddirs <dirs>         Override location of endorsed standards path
  -extdirs <dirs>              Override location of installed extensions
```

- Data Consumers are register into the system and then he can able to login into the system.
- After Logging, the Data Consumer will send key to the data user and, then logout from the system.

3. Data User

- Data Users are register into the system and then he can able to login into the system.
- After Logging, the Users upload the file and view the uploaded files and share with all/some particular persons and he/she can also cancel the shared file, and send a request for a file to data owner, then get a master key from data owner to download a file.
- Attacker Login with their credentials, view cloud protected attacked list, then logout from the system

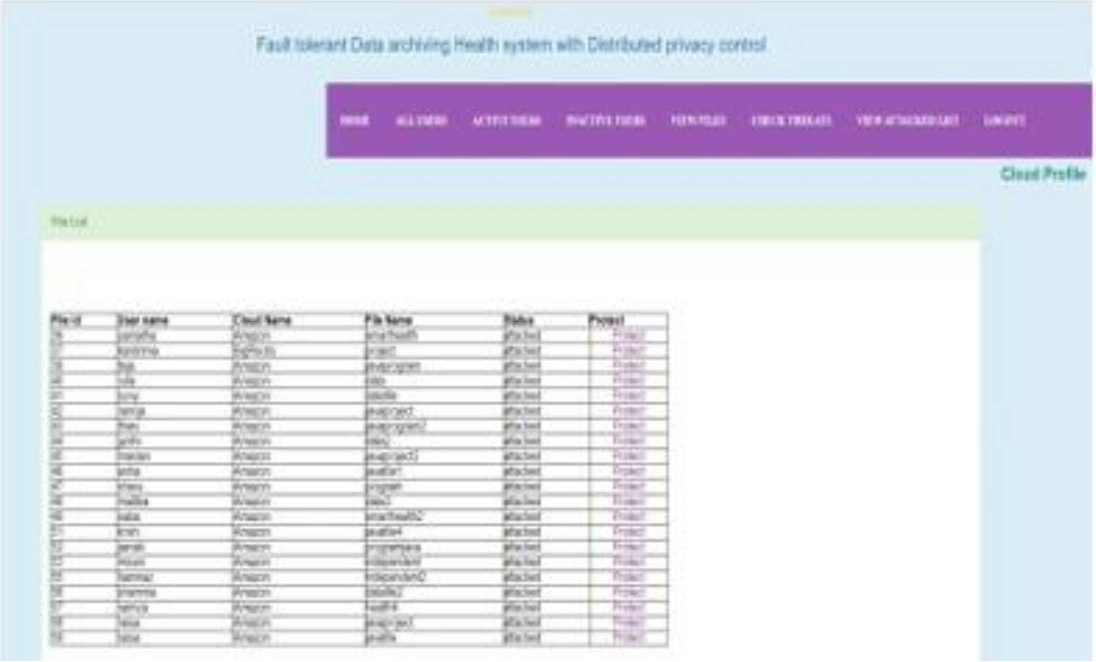
View Attacked List



File List

File id	User name	Cloud Name	File Name	Status	Protect
36	[illegible]	Amazon	smarthealth	attacked	Protect
37	[illegible]	[illegible]	project	attacked	Protect
39	[illegible]	Amazon	javaprogram	attacked	Protect
40	[illegible]	Amazon	data	attacked	Protect
41	[illegible]	Amazon	datafile	attacked	Protect
42	[illegible]	Amazon	javaproject	attacked	Protect
43	[illegible]	Amazon	javaprogram2	attacked	Protect
44	[illegible]	Amazon	data2	attacked	Protect
45	[illegible]	Amazon	javaproject3	attacked	Protect
46	[illegible]	Amazon	javafile1	attacked	Protect
47	[illegible]	Amazon	program	attacked	Protect
48	[illegible]	Amazon	data3	attacked	Protect
49	[illegible]	Amazon	smarthealth2	attacked	Protect
51	[illegible]	Amazon	javafile4	attacked	Protect
52	[illegible]	Amazon	programspara	attacked	Protect
53	[illegible]	Amazon	independent	attacked	Protect
55	[illegible]	Amazon	independent2	attacked	Protect
56	[illegible]	Amazon	datafile2	attacked	Protect
57	[illegible]	Amazon	health4	attacked	Protect

View cloud protected attacker List



File List

File id	User name	Cloud Name	File Name	Status	Protect
36	[illegible]	Amazon	smarthealth	attacked	Protect
37	[illegible]	[illegible]	project	attacked	Protect
39	[illegible]	Amazon	javaprogram	attacked	Protect
40	[illegible]	Amazon	data	attacked	Protect
41	[illegible]	Amazon	datafile	attacked	Protect
42	[illegible]	Amazon	javaproject	attacked	Protect
43	[illegible]	Amazon	javaprogram2	attacked	Protect
44	[illegible]	Amazon	data2	attacked	Protect
45	[illegible]	Amazon	javaproject3	attacked	Protect
46	[illegible]	Amazon	javafile1	attacked	Protect
47	[illegible]	Amazon	program	attacked	Protect
48	[illegible]	Amazon	data3	attacked	Protect
49	[illegible]	Amazon	smarthealth2	attacked	Protect
51	[illegible]	Amazon	javafile4	attacked	Protect
52	[illegible]	Amazon	programspara	attacked	Protect
53	[illegible]	Amazon	independent	attacked	Protect
54	[illegible]	Amazon	independent2	attacked	Protect
56	[illegible]	Amazon	datafile2	attacked	Protect
57	[illegible]	Amazon	health4	attacked	Protect
58	[illegible]	Amazon	javaproject	attacked	Protect
59	[illegible]	Amazon	javafile	attacked	Protect

VII CONCLUSION

It suggested that Derepo decentralize access control and encrypt the data without compromising computability, two key challenges taken from the adversary model, in order to address the security and privacy concerns of medical data persistence in smart health. Static structures and dynamic processes are formalized alongside the double-layered architecture. which also maintains pseudonymity, controllability, and manageability. In order to guarantee confidentiality and address privacy concerns brought on by both internal and external adversaries, the FHE scheme was implemented.

FEATURE WORK: Additionally, the project uses an analysis from the attacker's point of view to assess and demonstrate Derepo's security. By experimenting with the prototype, it also shows off Derepo's performance. Furthermore, Derepo is not unique to smart health and can help .

VIII.REFERENCES

[1]. C. S. Wood, M. R. Thomas, J. Budd, T. P. Mashamba-Thompson, K. Herbst, D. Pillay, R. W. Peeling, A. M. Johnson, R. A. McKendry, and M. M. Stevens, "Taking connected mobile-health diagnostics of infectious diseases to the field," Nature, vol. 566, no. 7745, pp. 467–474, 2019, iSBN: 1476-4687 Publisher: Nature Publishing Group.

[2]. J. Li, Q. Ma, A. H. Chan, and S. S. Man, "Health monitoring through wearable technologies for older adults: Smart wearables acceptance model," Applied ergonomics, vol. 75, pp. 162–169, 2019, iSBN: 0003- 6870 Publisher: Elsevier.

[3]. R. M. Sadek, S. A. Mohammed, A. R. K. Abunbehan, A. K. H. A. Ghattas, M. R. Badawi, M. N. Mortaja, B. S. Abu-Nasser, and S. S. Abu- Naser, "Parkinson's Disease Prediction Using Artificial Neural Network," 2019.

[4]. P. Romero-Aroca, A. Valls, A. Moreno, R. Sagarra-Alamo, J. BasoraGallisa, E. Saleh, M. Baget-Bernaldiz, and D. Puig, "A clinical decision support system for diabetic retinopathy screening: creating a clinical support application," Telemedicine and e-Health, vol. 25, no. 1, pp. 31–40, 2019, iSBN: 1530-5627 Publisher: Mary Ann Liebert, Inc., publishers 140 Huguenot Street, 3rd Floor New ....

[5]. N. Menachemi and T. H. Collum, "Benefits and drawbacks of electronic health record systems," Risk management and healthcare policy, vol. 4, p. 47, 2011, publisher: Dove Press.

[6]. N. Akpan, "Has health care hacking become an epidemic," PBS Newshour, 2016.

[7]. "U.S. Department of Health & Human Services - Office for Civil

[8]. S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in 2010 IEEE Second International Conference on Cloud Computing Technology and Science. IEEE, 2010, pp. 693– 702.

[9]. C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in Annual International Cryptology Conference. Springer, 1992, pp. 139–147.

[10]. M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in OSDI, vol. 99, 1999, pp. 173–186, issue: 1999.

[11]. D. Pavithran, K. Shaalan, J. N. Al-Karaki, and A. Gawanmeh, "Towards building a blockchain framework for IoT," Cluster Computing, pp. 1–15, 2020, iSBN: 1573-7543 Publisher: Springer.

[12]. Y. Ding and H. Sato, "Bloccess: Towards Fine-Grained Access Control Using Blockchain in a Distributed Untrustworthy Environment," in 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud). IEEE, 2020, to appear.

[13]. Y. Ding and H. Sato, "Dagbase: A Decentralized Database Platform Using DAG-Based Consensus," in 2020 IEEE 44rd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2020, to appear.

[14]. 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). IEEE, 2016, pp. 25–30.

[15]. G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," Sustainable cities and society, vol. 39, pp. 283–297, 2018, iSBN: 2210-6707 Publisher: Elsevier.