TEST Engineering & Management

January-February 2020
ISSN: 0193-4120 Page No. 10357 - 10365

Secured Search for Personal Health Record in Multi-Source Cloud

*N. Praveen Kumar Reddy, N. Venkateshwara Rao
**UG Scholar, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai*
Assistant Professor, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai
**praveennarala786@gmail.com, raosusipooji@gmail.com*

Article Info
Volume 82
Page Number: 10357 - 10365
Publication Issue:
January-February 2020

Article History
***Article Received**: 18 May 2019*
***Revised**: 14 July 2019*
***Accepted**: 22 December 2019*
***Publication**: 19 February 2020*

Abstract
Cloud-based Personal Health Record frameworks (CB-PHR) have incredible potential in encouraging the administration of individual wellbeing records. Security and assurance concerns are among the central obstacles for the wide gathering of CB-PHR structures. In this paper, we consider a multi-source CB-PHR system in which distinctive data providers, for instance, crisis centres and specialists are affirmed by particular data owners to move their very own prosperity data to an untrusted open cloud. The wellbeing information are submitted in an encoded structure to guarantee information security, and every datum supplier likewise submits scrambled information lists to empower inquiries over the encoded data. We propose a novel Multi-Source Order-Preserving Symmetric Encryption plan whereby the cloud can consolidate the mixed data records from various data providers without understanding the document content. It enables efficient and security sparing inquiry taking care of in that an information client can present a solitary information question the cloud can process over the encoded information from all related data providers without understanding the request content.

***Keywords:** Privacy/information privacy, Personal health record (PHR), Cloud computing*

1. Introduction

CLOUD-BASED Personal Health Record frameworks (CB-PHR) are booming. A common CB-PHR framework comprises of three substances: data proprietors, data suppliers and a cloud server. In CBPHR framework, data proprietors and data suppliers are defined as patients themselves and clinics, individually. Information proprietors can legitimately approve data suppliers to transfer their PHRs to the cloud. The CB-PHR framework enables data proprietors to get to their PHRs whenever and anyplace, be better arranged for medical appointments and unexpected emergencies, maintain a progressively complete picture about close to home wellbeing, and even accomplish fitness objectives. Data suppliers can investigate the CBPHR framework to give better therapeutic administrations by sharing, working together, and drawing in with the patients in new ways.

Protection concern is among the primary deterrents for the wide selection of CB-PHR frameworks. Specifically, numerous individuals

January-February 2020
ISSN: 0193-4120 Page No. 10357 - 10365

have profound worries that there can be unapproved access to their delicate PHRs. For instance, the cloud may have business enthusiasm for breaking down the PHRs, and it might likewise have malignant workers or even be hacked. A characteristic method to lighten the security concerns is to let information proprietors and suppliers transfer encoded PHRs to the cloud which doesn't have the unscrambling keys. Since PHRs may be in huge volume, it is very inefficient for information proprietors or suppliers to recover all the encoded PHRs from the cloud when just a little bit of them are required. To empower efficient inquiries over scrambled PHRs, the DES method is proposed to manufacture a file for every patient's PHRs. The information list enables the server of the cloud to rapidly find all the PHRs coordinating a specific information question. To additionally resolve the protection worries about information files and questions, accessible encryption plans are proposed to scramble information lists and inquiries also. These plans enable the sever of the cloud to perform efficient inquiries over encoded PHRs straightforwardly dependent on the scrambled records and questions while incognizant in regards to the list and inquiry content. Conventional accessible encryption plans are intended for nonexclusive cloud stages and not advanced for CB-PHR frameworks. Specifically, the PHRs of various information suppliers for similar information proprietor might be profoundly related and connected with similar qualities (e.g., indications). On the off chance that a conventional inquiry encryption conspire is utilized, every datum supplier needs to autonomously create the scrambled information record for accommodation to the server of the cloud. In this way, the information proprietor needs to deal with the keys with various information suppliers and furthermore present a devoted information inquiry for every datum supplier regardless of whether question conditions are actually the equivalent. A conceivable answer for this issue is to give every one of the information suppliers a chance to utilize a typical key relegated by the information proprietor to encode the information lists related with him. This strategy, be that as it may, is defenseless against the trade-off of a solitary data supplier.

We propose a very efficient PHR system with strong privacy guarantees. In our structure, each datum owner supports distinctive data providers to submit mixed prosperity records and data records to the cloud server. Our structure contrasts from prior work in two appealing features. To begin with, each datum provider of comparable data owner uses an intriguing symmetric key for scrambling data records, along these lines contradicting single motivation behind deal. Second, every datum owner needs not manage the keys with particular prosperity providers and can show a single mixed request to the cloud server for investigating the encoded prosperity data from all of his data providers. These incorporate engages very efficient question taking care of. Our structure depends on Multi-source Encrypted Indexes Merge (MEIM), a novel technique we propose in this paper. MEIM empowers the cloud server to consolidate various encoded data records from different prosperity providers of a comparable patient without harming the patient's security. It furthermore enables the patient to make a lone encoded question over the total of his prosperity providers' mixed data set away at the cloud server. The fundamental structure square of MEIM is a novel Multisource Order-Preserving Symmetric Encryption (MOPSE) rough we make. MOPSE jam the solicitation for various data records encoded by different symmetric keys. We in like manner propose a MOPSE+ unrefined to help different leveled endorsement

January-February 2020
ISSN: 0193-4120 Page No. 10357 - 10365

requests whereby the prosperity providers with higher advantages can request the cloud server for the encoded data from those with lower benefits. Such different leveled get to structures are ordinary before long. We confirm the security and efficiency of our structure by comprehensive speculative examination and expansive investigations with a certifiable dataset. Our results show that the inquiry execution for data customers in MOPSE and MOPSE+ is faster n×4 than that in show OPSE. The inquiry execution for data providers in MOPSE and OPSE are about the proportionate and not as much as that in MOPSE+.

2. Architecture

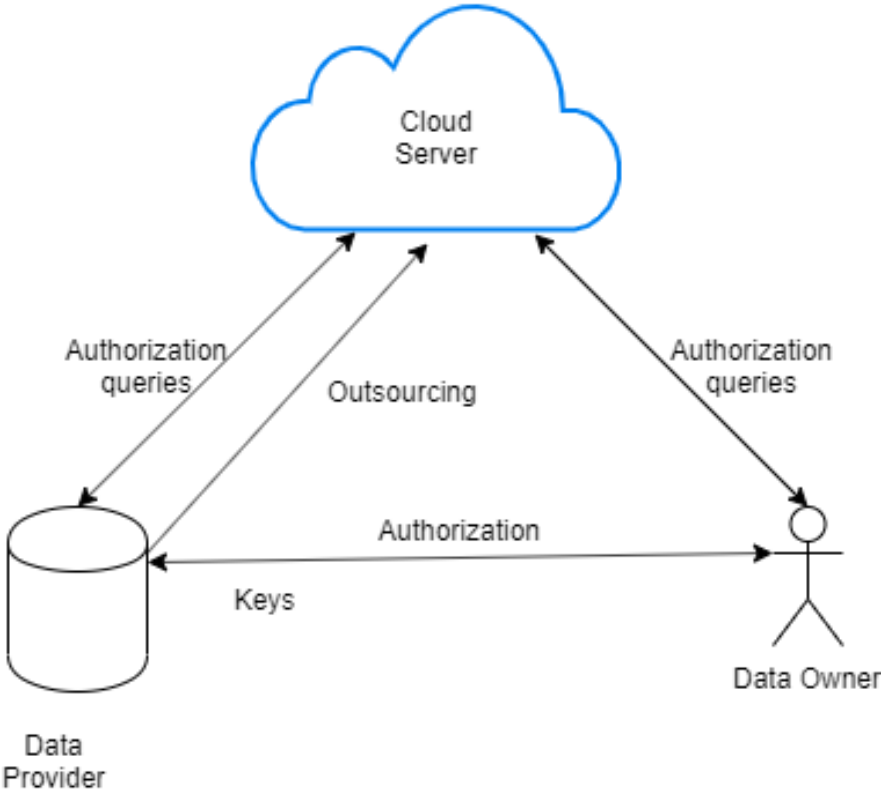

Figure 1: System Architecture

The figure 1 represents the system architecture that shows that the user logins to his/her account and uploads the data or retrieve the data through requesting the data provider who has access to the cloud. The request is considered by the data provider and relevant response is produced and generated to the user.

January-February 2020
ISSN: 0193-4120 Page No. 10357 - 10365

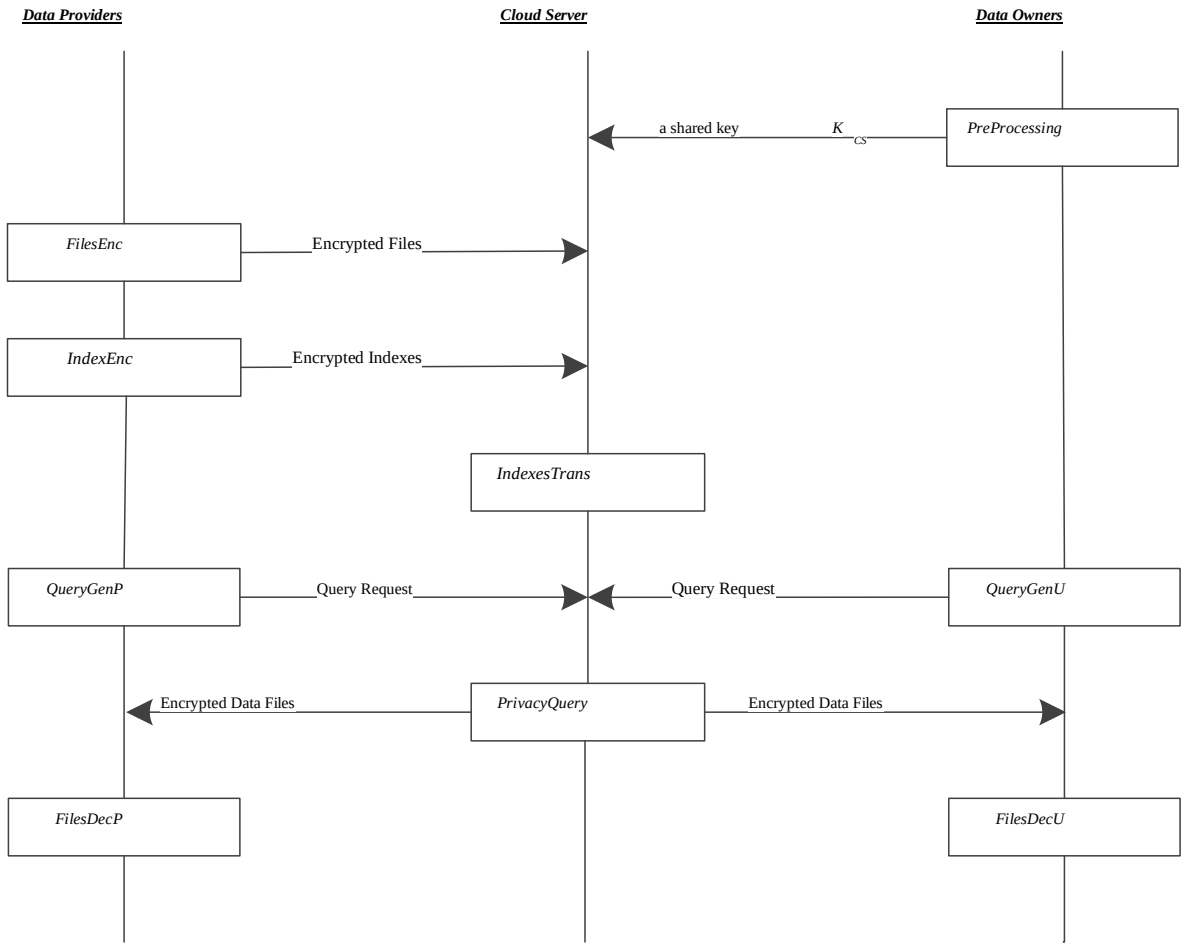

Figure 2: Sequence diagram

The figure 2 represents the flow of the process which is occurred in the system. It explains clearly how each and every function in the system and how the roles and their activities related to the functions are involved in the system.

Kaletsch & Sunyaev / Personal Health Records in Cloud Computing Environments
Thirty Second International Conference on Information Systems, Shanghai 2011 5physicians and patients have an exigent need to use personal health records, which offer various functions and are also affordable. (ii) By analyzing existing literature we examined PHRs and CC technologies in detail. Moreover, by performing several case studies on existing online platforms, we added a practical perspective to our research. Further upcoming research: (iii) A new artifact will be created, which will allow utilizing CC for PHR purposes. The framework will support providers, who want to create new PHRs, but also allow improving existing healthcare IT services in order to be ready for cloud environments. (iv) A web-based prototype will be used for the evaluation of our framework. Tests in laboratories as well as with physicians' practices are planned. (v) The findings of these tests will be used for further improvement of future framework.

3. Top Threats

Obviously, it is a fact that there are incredible chances, which accompany social capacities, similar to "patients enable patients", there may be significantly more serious dangers: E.g., it is

January-February 2020
ISSN: 0193-4120 Page No. 10357 - 10365

conceivable that clients even in a de-distinguished condition uncover themselves by giving recognizable data. In addition, they may likewise inadvertently or deliberately give bogus data to different patients. In such cases, authoritative structures may help, as directing remarks or guaranteeing that solitary individuals with same conditions meet. The contextual investigations indicated that there are numerous PHRs, which depend on selling therapeutic data. Generally, the suppliers ensure de-recognizable proof and collection of information sold. Nonetheless, the creators were always unable to locate an unequivocal rundown of the information things imparted to outsiders. Henceforth, clients are left in obscurity about what is in actuality finished with their medicinal data. Additionally, they are regularly not illuminated about the dangers that could show up through re-recognizable proof. Notwithstanding selling restorative data, publicizing is frequently utilized by outsiders to pick up income from a PHR. Frequently, administrations are used, which check the substance of the website page with outer programming so as to give focused on publicizing. The substance exhibited to the client and, the medicinal data showed, could hole to the outside. Web investigation regularly utilize comparable innovations to publicizing. Client conduct is followed by outside devices to be assessed later on. We found numerous situations where not just outsider JavaScript was incorporated, yet also straightforward pictures were utilized to follow clients. One PHR even included JavaScript from a non-secure source into a safe domain. Shockingly, this condition was just recognized by one internet browser we utilized.

4. Existing System

Individual wellbeing record (PHR) is viewed as an essential part in improving patient results. Anyway the reception rate by the overall population still stays low. To discover the hindrances in embracing PHR, we have overviewed articles identified with individual wellbeing record framework (PHRS) from 2008 to 2016 and classified them into 6 unique classifications, for example, inspiration, obstructions, proprietorships, interoperability, protection, and security and conveyability. To accomplish fine-grained and adaptable information get to control for PHRs, we are using property based encryption (ABE) strategies to encode every patient's PHR record. Unique in relation to past works in secure information redistributing, we center around the different information proprietor situation, and gap the clients in the PHR framework into numerous security areas that extraordinarily lessens the key administration multifaceted nature for proprietors and clients. A high level of patient protection is ensured at the same time by abusing multiauthority ABE.

5. Proposed System

This framework can give a decent security to the clients to store their own wellbeing records in their very own records. This framework will have a superior confirmation where in the accreditations are part separated into certain pieces, and each lump is encoded utilizing distinctive calculation. Along these lines the qualifications are put away in the database safely and it will be not able decode by the unapproved clients. The main objective of this project is to provide privacy to the users and their health records and several other details related to him. Also to avoid various attacks, such as insider attack, the off-line password guessing attack, the user illegal attack, the

January-February 2020
ISSN: 0193-4120 Page No. 10357 - 10365

server attack and man-in-the-middle attack. The project is to protect the transmitted data with the help of encryption and decryption techniques. This project investigates the security of well-known cryptographic primitive applications of cloud storage. DES technique is used for both encryption and decryption process. Firebase is used to store the data of the users. The data stored in the database are in encrypted format.

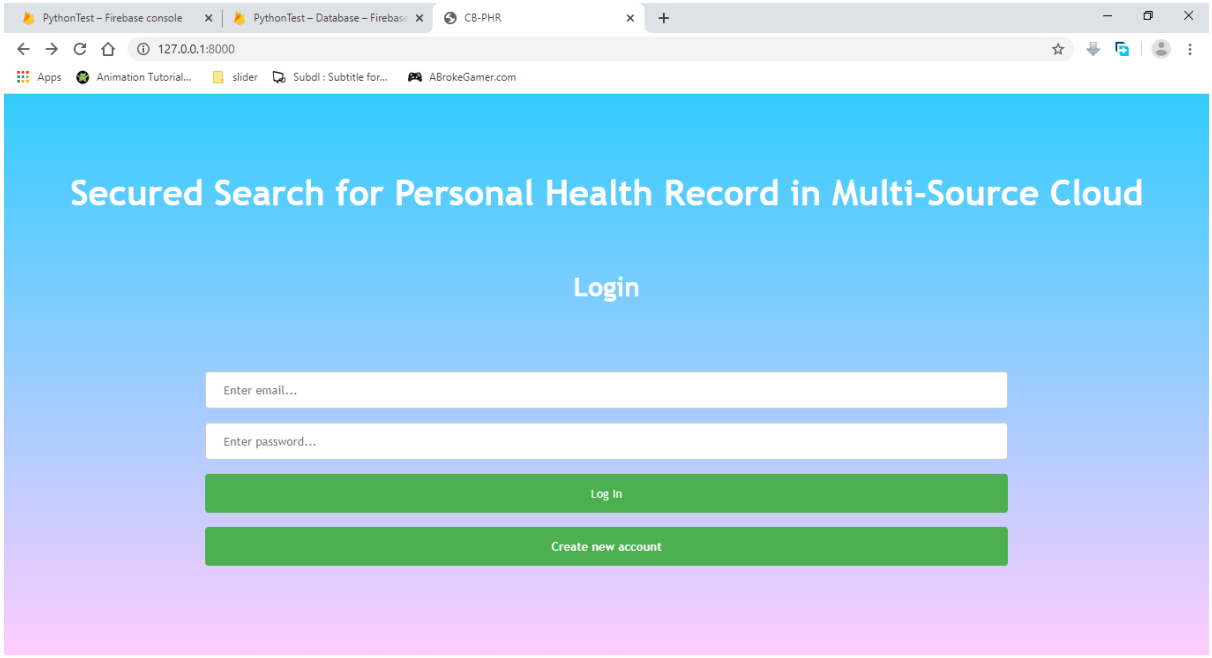

Figure 3: Login Page

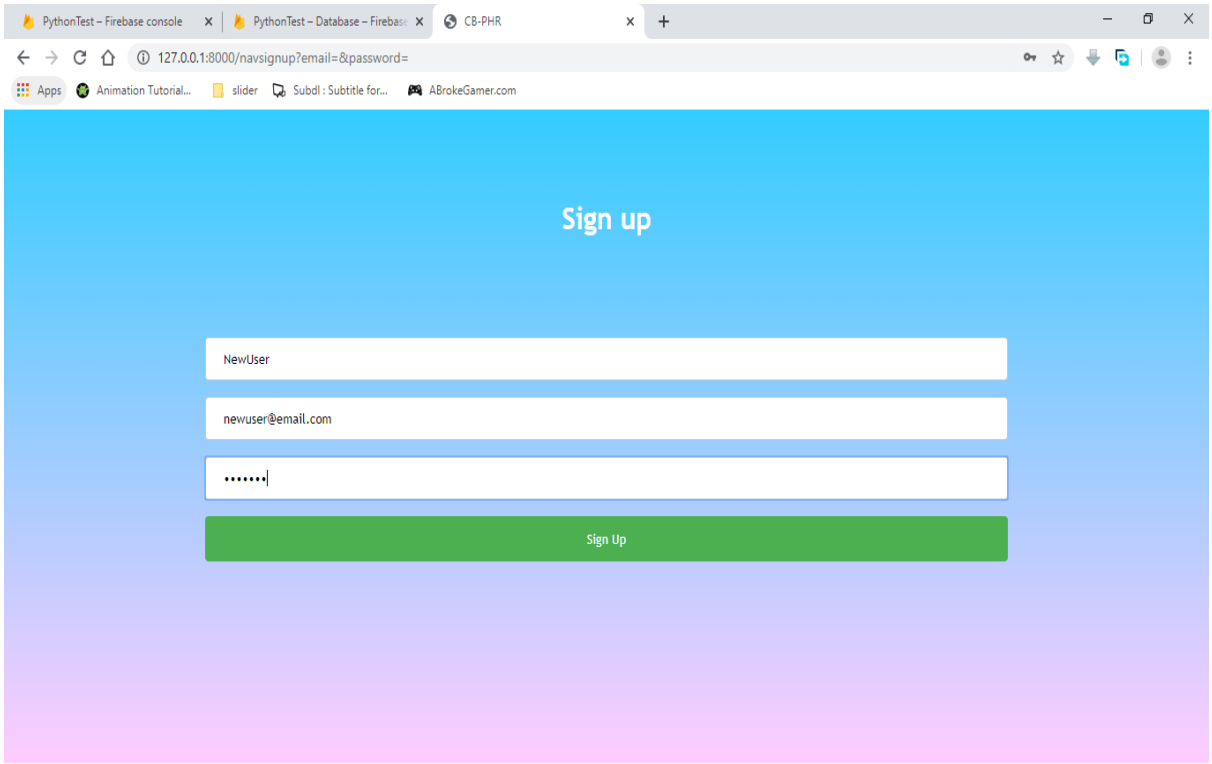

Figure 4: Sign Up Page

January-February 2020
ISSN: 0193-4120 Page No. 10357 - 10365

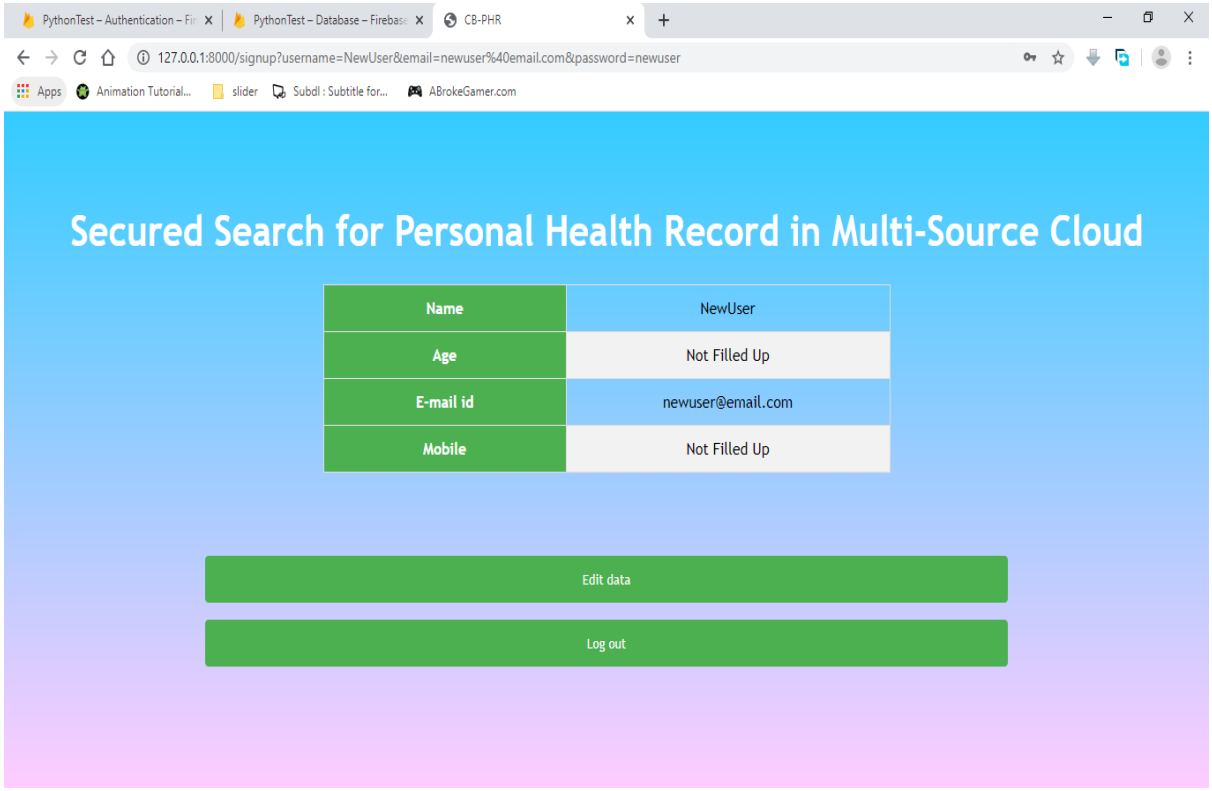

Figure 5: User Account

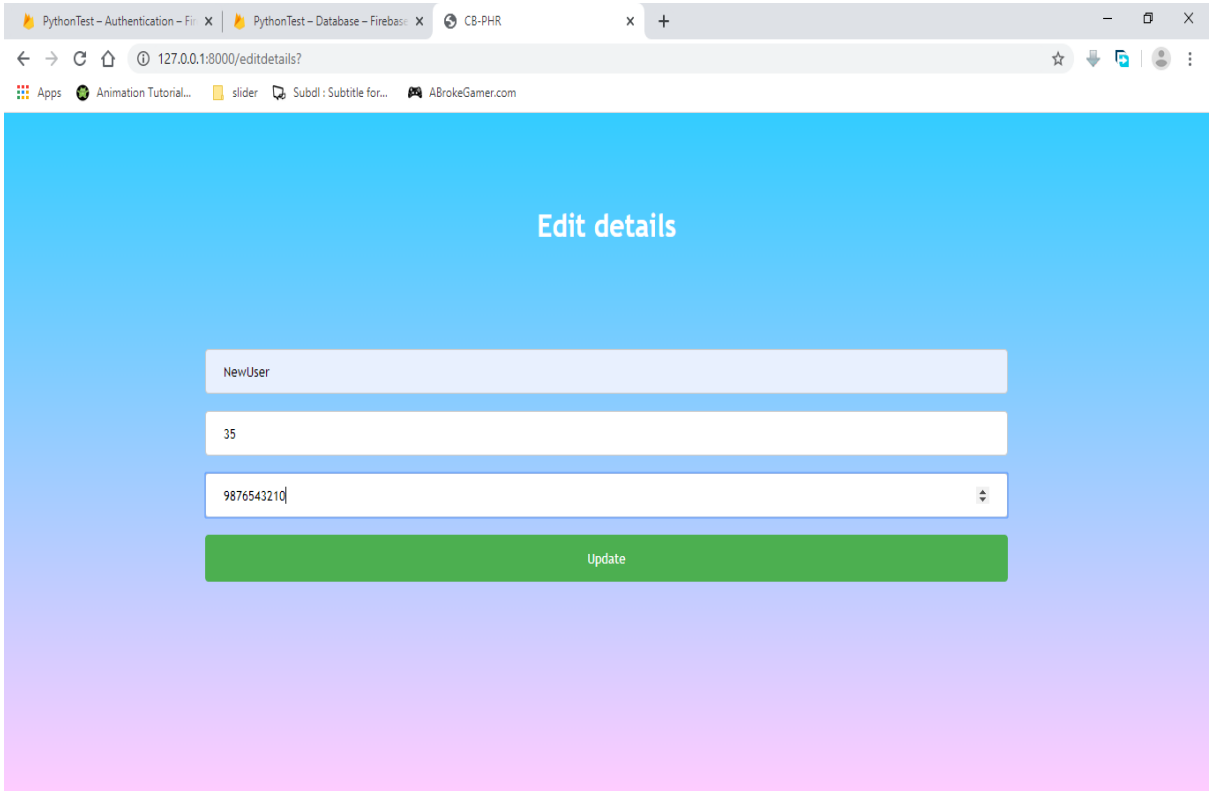

Figure 6: Edit Information Page

January-February 2020
ISSN: 0193-4120 Page No. 10357 - 10365

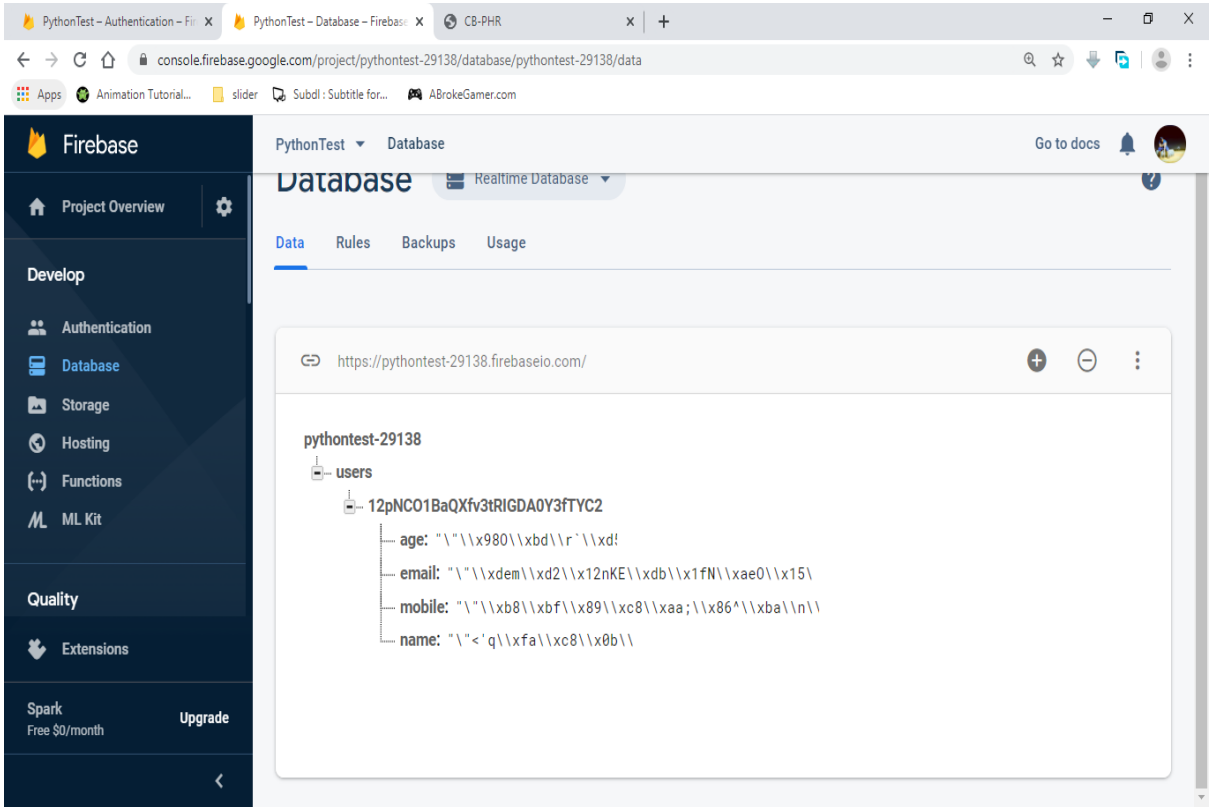

Figure 7: Firebase Database after storing data

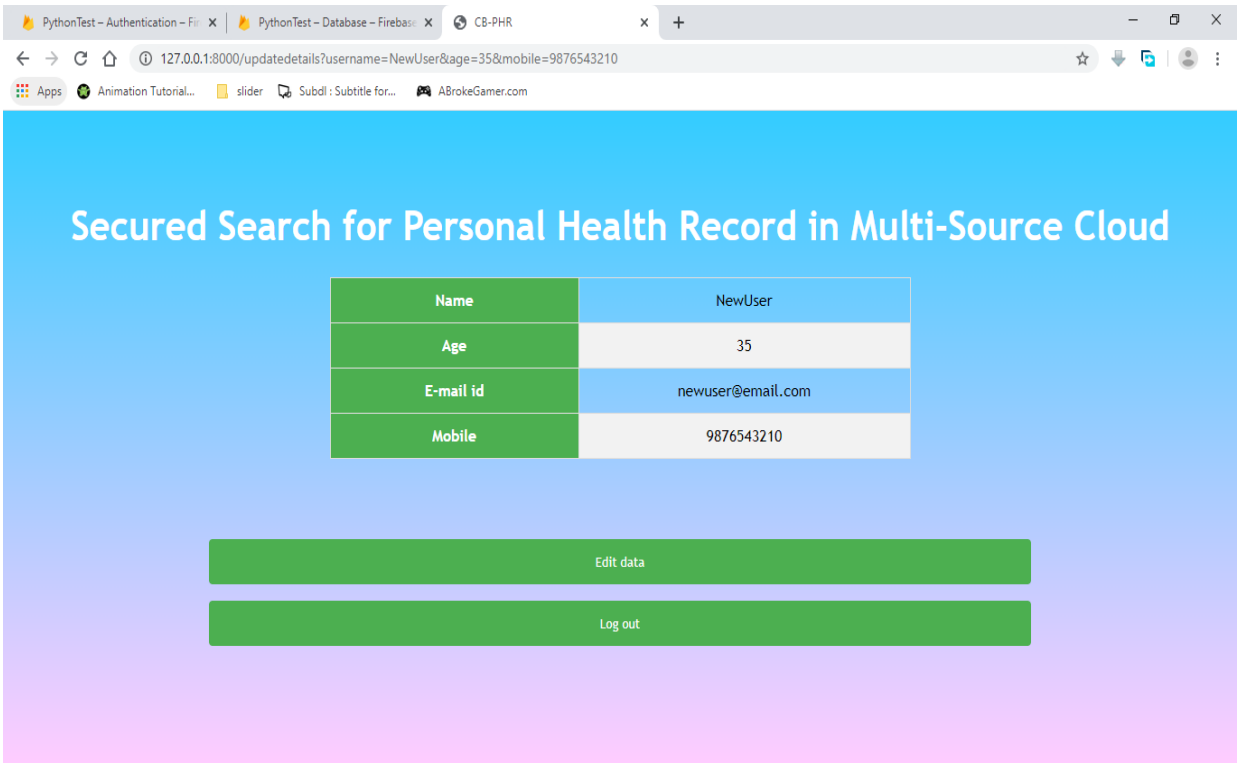

Figure 8: User Account after updating details

January-February 2020
ISSN: 0193-4120 Page No. 10357 - 10365

6. Conclusion

I hereby conclude that this project can open a new way of understanding huge amount of data and reduce and even replace the human effort in the field of personal health record system. This system can be used for secure authorization for the users to store their health records and prevent access to unauthorised users from stealing personal information.

References

[1] Tang, Paul; Ash, Joan; Bates, David; Overhage, J.; Sands, Daniel (2006). "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption". Journal of the American Medical Informatics Association. 13 (2): 121–126. doi:10.1197/jamia.M2025. PMC 1447551. PMID 16357345.

[2] "Computerisation of personal health records". Health Visitor. 51 (6): 227. June 1978. PMID 248054.

[3] Dragstedt, CA (14 April 1956). "Personal health log". Journal of the American Medical Association. 160 (15): 1320. doi:10.1001/jama.1956.02960500050013. PMID 13306552.

[4] AHIMA e-HIM Personal Health Record Work Group (July 2005). "The Role of the Personal Health Record in the EHR". Journal of AHIMA. 76 (7): 64A–D. PMID 16097127. Archived from the original on 20 September 2008.

[5] Personal Health Working Group (1 July 2003). Connecting for Health: A Public-Private Collaborative (PDF) (Report). Markle Foundation. Archived from the original (PDF) on 4 January 2007.

[6] America's Health Insurance Plans (13 December 2006). "What are Personal Health Records (PHRs)?". Archived from the original (DOC) on 5 March 2009.

[7] Flaumenhaft, Y.; Ben-Assuli, O. (2018). "Personal health records, global policy and regulation review". Health Policy. In Press (8): 815–826. doi:10.1016/j.healthpol.2018.05.002. PMID 29884294.

[8] "Personal Health Records and the HIPAA Privacy Rule" (PDF). Office of Civil Rights. U.S. Department of Health and Human Services. 15 December 2008. Archived (PDF) from the original on 17 February 2017.

[9] "MyChart". Cleveland Clinic. Retrieved 29 March 2011.

[10] Archer, N.; Fevrier-Thomas, U.; Lokker, C.; et al. (2011). "Personal health records: A scoping review". Journal of the American Medical Informatics Association. 18 (4): 515–22. doi:10.1136/amiajnl-2011-000105. PMC 3128401. PMID 21672914.

[11] Assadi, V.; Hassanein, K. (2017). "Consumer Adoption of Personal Health Record Systems: A Self-Determination Theory Perspective". Journal of Medical Internet Research. 19(7): e270. doi:10.2196/jmir.7721. PMC 5553007. PMID 28751301.

[12] Ford, E.W.; Hesse, B.W.; Huerta, T.R. (2016). "Personal Health Record Use in the United States: Forecasting Future Adoption Levels". Journal of Medical Internet Research. 18(3): e73. doi:10.2196/jmir.4973. PMC 4830902. PMID 27030105.

[13] Kaelber, David C.; Jha, Ashish K.; Johnston, Douglas; Middleton, Blackford; Bates, David W. (Nov–Dec 2008). "A Research Agenda for Personal Health Records (PHRs)". Journal of the American Medical Informatics Association. 15 (6): 729–36. doi:10.1197/jamia.M2547. PMC 2585530. PMID 18756002.

[14] Roehrs, A.; da Costa, C.A.; da Rosa Righi, R.; de Oliveira, K.S.F. (2017). "Personal Health Records: A Systematic Literature Review". Journal of Medical Internet Research. 19 (1): e13. doi:10.2196/jmir.5876. PMC 5251169. PMID 28062391.