International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 465-470
Published Online January 2020 in IJEAST (http://www.ijeast.com)

AN EFFICIENT AUTHENTICATION SCHEME FOR BLOCK CHAIN-BASED ELECTRONIC HEALTH RECORDS

Keerthika A.,
ME-2nd year, Department of CSE
TCET, Vandavasi-604505, Tamilnadu, India

Chendhavarayan R.,
ME., Department of CSE
TCET, Vandavasi-604505, Tamilnadu, India.

***Abstract*- In conventional Electronic Health Records (EHRs), restorative related data is for the most part independently constrained by various emergency clinics and in this way it prompts burden of data sharing. Cloud based EHRs take care of the issue of data partaking in the customary EHRs. In any case, cloud-based EHRs endure brought together issue, i.e., cloud administration focus and key-age focus. This paper takes a shot at making another EHRs worldview which can help in managing the unified issue of cloud-based EHRs. Our arrangement is to utilize the developing innovation of block chain to EHRs (signified as block chain-based EHRs for accommodation). Right off the bat, we officially characterize the framework model of block chain-based EHRs in the setting of consortium block chain. Also, verification issue is significant for EHRs. In any case, existing verification plans for block chain-based EHRs have their very own feeble focuses. Along these lines, in this work, we likewise propose a verification conspire for block chain-based EHRs. Our proposition is an identity based mark plot with different specialists which can oppose conspiracy assault out of experts. Moreover, our plan is provably secure in the arbitrary prophet model and has increasingly effective marking and confirmation calculations than existing validation plans of block chain-based EHRs.**

***Keywords*– Block Chain, Secure Outsourcing, Cloud Based Electronic Health Records, Identity Based Encryption.**

I. INTRODUCTION

There is no universal method to create a protocol for secure multi-party computation and handling aggregate queries on encrypted data is not an exception. Several holomorphic systems only support a subset of mathematical operations, like addition, or exclusive- From a security perspective, only the additive and the multiplicative are classified to be IND-CPA (stands for in distinguish ability under chosen plaintext attack).

Partially holomorphic cryptosystems are more desirable from a performance point of view than somewhat holomorphic cryptosystems, which support a limited operation depth. Fully holomorphic systems have a huge cost and cannot be deployed in practice. Sometimes the queries on HEALTH need to take into account various errors such as irrelevant mutations, incomplete specifications and sequencing errors. Therefore, the pattern of the query should be expressed using regular expressions. Many works address practical and privacy-preserving Out sourcing of this regular expression type of queries, implemented as oblivious evaluation of finite automata.

Block chain technology was formerly developed for the crypto currency Bit coin and was first presented in the Bit coin whitepaper by Nakamoto in 2008. Since block chain technology appeared, it has been celebrated as a new technological revolution just like the invention of the steam engine or the Internet because of its huge impaction on society. In a 2015 World Economic Forum report, 58% of survey respondents expected that 10% of global Gross Domestic Product (GDP) will be relevant to the block chain technology through 2025

Previously, many restrictions have been placed on sharing massive EHRs because of the risks to data security or leakage of private patient information during data exchange. Furthermore, current EHRs are managed by hospitals and providers, whereas patients are deprived of the right to freely control their own EHRs. Through utilizing block chain technology, standards for recording data and managing identity are established, and the block chain of EHRs is constructed. In addition, this technology records the auditing traces of all transactions in an immutable distributed ledger, which guarantees responsibility and transparency in the procession of data exchange. Therefore, the patient has the ability to record healthcare and diagnostic information from doctors in their own EHRs, thus reducing the number of medical accidents and preserving patient privacy

The Institute for Business Value at IBM issued a whitepaper titled, ‘‘Healthcare rallies for block chains: Keeping patients at the centres’’. This investigation shows that, for the healthcare industry, more than 70% of industry leader predict that the greatest advantage of block chain technology is contributing to manage clinical trial records, supervised compliance and EHRs. Block chain in the healthcare industry provides a secure, decentralized framework for the controlled sharing of patient EHRs, and block chain is the perfect solution to EHRs and data exchange.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 465-470
Published Online January 2020 in IJEAST (http://www.ijeast.com)

Block chain is a decentralized database whose data block is connected chronologically. In the healthcare industry, there are many different parties who need to collaboratively manage personal EHRs block chain (in a model of consortium block chain), such as medical specialists, hospitals, insurance departments, etc. A variety of parties can lead to resource intensive authentication and the costly information processes for all the stakeholders involved [6]. Based on the Ethereum block chain technology, the Gem Health Network [7] was constructed to facilitate the access of different healthcare specialists and departments to patient data, reduce health resource waste and treat important illnesses rapidly. In this scenario, the EMRs (in the form of block chain) of patients should be authenticated based on ownership to avoid misdiagnoses before making accurate diagnoses into block. Furthermore, EMRs stored in block includes name, ID, allergy history and other sensitive data. According to the guidelines of the Health Insurance Portability and Accountability Act (HIPPA) [8], the privacy of patients should be preserved in the process of sharing EHRs

Block chain is considered as a new technological revolution that was introduced as the backbone of the Bit coin crypto currency. It is a peer-to-peer distributed ledger technology to record transactions, agreements, and sales. The benefits of the block chain technology are decentralized maintenance, data saving in the block-then-chain structure, secure transporting and accessing of data as well as anti-tamper and undeniable data security [28]. Taking advantage of these distinguishing features above in an EHRs system, block chain enables the management of authentication, confidentiality, accountability and data sharing while handing information related to privacy, medical resource saving and facilitating for the patient, and making population healthcare smarter.

Assuming that there is a EHRs system in a cloud storage platform, which consists of some departments, such as hospitals, pharmaceutical departments, insurance departments, disease research departments and so on, EHRs systems can be jointly managed. All departments can offer services for patients together and restrict the rights of each department to prevent EHRs abuse. Thus, a EHRs system with a block chain structure is designed. Suppose that every patient owns one block chain of healthcare alone. After being treated in a hospital, all the information including EHRs, consumption records, insurance records, etc. is encapsulated in one block. Patient treatments at different times will be generated in different blocks. Then a series of blocks. Generated according to the time sequence and a healthcare block chain of this patient is construct

Taking advantage of this technique, it achieves a perfect privacy-preserving for patient. The explicit claim of the signature reveals nothing about the identity or attributes of the patient. From another point of view, it guarantees the verifier in enforceability as well. The signature of patient whose attributes satisfy the claim cannot be generated by a collusion of parties who integrate their attributes together. Hence, it constructs a secure and controllable mechanism in EHRs system to confirm the validity of the healthcare block.

In authentication, for conforming to the characteristics of multiple departments, an attribute-based signature with multiple authorities [14] provides an effective solution to protect the privacy in EHRs systems while attesting that the endorsement derived from the correct patient.

II. RELATED WORKS

As given in the paper**" SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS IN CLOUD USING ATTRIBUTE BASED ENCRYPTION" "M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou.", Volume: 24, Issue 1 , Jan. 2015"**is Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

Moreover, this proposal allowed the user to demonstrate evidence to the verifier whether he is the right signer. Nevertheless, all these schemes have a single authority that is insufficient to meet the characteristics of the distributed system except of [14] and [18].Although these two schemes could be extended to the scenarios of multi-authority, the security and the policy supported in design is limited on account of the original ABS scheme.

The theme of the paper is **"AN SMDP-BASED SERVICE MODEL FOR INTER DOMAIN RESOURCE ALLOCATION IN MOBILE CLOUD NETWORKS", "H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng", "Volume: 14, Issue 3, Jan. 2017**"Mobile cloud computing is a promising technique that shifts the data and computing service modules from individual devices to geographically distributed cloud service architecture. In this paper, we propose a service decision making system for inter domain service transfer to balance the computation loads among multiple cloud domains. To this end, we formulate the service request decision making process as a semi-Markov decision process. The optimal service transfer decisions are obtained by jointly considering the system incomes and expenses. Extensive simulation results show that the proposed

decision making system can significantly improve the system rewards and decrease service disruptions compared with the greedy approach.

The theme of the paper is **"EXPLOITING GEO DISTRUBUTED CLOUDS FOR E HEALTH MONITORING SYSTEM WITH MINIMUM SERVICE DELAY AND PRIVACY PRESERVATION"**, "**Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo.","Volume: 34, Issue 1, Jan. 2015"**In this paper, we propose an e-health monitoring system with minimum service delay and privacy preservation by exploiting geo-distributed clouds. In the system, the resource allocation scheme enables the distributed cloud servers to cooperatively assign the servers to the requested users under the load balance condition. Through the numerical analysis, we show the efficiency of the proposed traffic-shaping algorithm in terms of service delay and privacy preservation. Furthermore, through the simulations, we demonstrate that the proposed resource allocation scheme significantly reduces the service delay compared to two other alternatives using jointly the short queue and distributed control law.

With reference to the paper **"ACHIEVING USABLE AND PRIVACY ASSURED SIMILARITY SEARCH OVER OUTSOURCED CLOUD DATA", "C. Wang, K. Ren, S. Yu, and K. M. R. Urs","Volume: 18, Issue 8, Jan. 2018",** In this paper, we investigate the problem of secure and efficient similarity search over outsourced cloud data. Similarity search is a fundamental and powerful tool widely used in plaintext information retrieval, but has not been quite explored in the encrypted data domain. We formally prove the privacy-preserving guarantee of the proposed mechanism under rigorous security treatment. To demonstrate the generality of our mechanism and further enrich the application spectrum, we also show our new construction naturally supports fuzzy search, a previously studied notion aiming only to tolerate typos and representation inconsistencies in the user searching input. The extensive experiments on Amazon cloud platform with real data set further demonstrate the validity and practicality of the proposed mechanism.

III. MOTIVATION

3.1 EXISTING SYSTEM

The Existing System, all medical related data are digitized and stored in the server of hospital. Then, when a patient goes back to the hospital, he or the hospital can search previous information, including names of the patient and doctor, time, diagnosis, and so on. As an important application in the medical field, EHRs have attracted wide attention. Many standards have been proposed for EHRs. In addition, many papers considered the security and privacy issues in EHRs systems. However, there exists many problems in traditional EHRs. First of all, generally, medical-related data are independently stored in different hospitals or research institutions since they have their own independent database. Therefore, when a patient transfers from a hospital to another one, he needs to obtain medical examinations once again. This obviously will lead to waste of medical information resources and increase patients' body and financial burdens. Secondly, in EHRs systems, only the authorities, such as hospitals, have data. Hence, if there is a dispute between hospital and patient, then the hospital will always win since it can tamper the medical records or even delete them. It is not fair for patients.

3.2 DEMERITS

- The Medical related data are independently stored in different hospitals or research institutions since they have their own independent database.
- This obviously will lead to waste of medical information resources and increase patients body and financial burdens.
- Patient access permissions to HER are very limited, and patients are typically unable to easily share these data with researchers or providers.
- Without coordinated data management and exchange the health records are fragmented instead of cohesive.

3.3 PROPOSED SYSTEM

The Proposed System works on creating a new EHRs paradigm which can help in dealing with the problems in cloud-based EHRs. Our solution is to make use of the emerging technology of block chain which is derived from Bit coin. Generally speaking, block chain can be seen as a decentralized and distributed database. There is authority in traditional network architectures or application systems, such as KGC, cloud service provider, and so on. The decentralized feature of block chain gets rid of such dependence on authority. Therefore, many people considered the applications of block chain in different types of real-world scenarios, including EHRs, we call it block chain-based EHRs. As we proposed, with the trained set of patient data by SVM Specified and spited the data into sensitive and insensitive data. In SVM Specified using the separate sensitive case from the block chain and uploaded to cloud by holomorphic encryption. For example, the works of designed a broad framework for block chain based EHRs made use of encryption technology to protect the confidentiality of the medical records focus on the privacy issue of EHRs and designed a new framework based on block chain and holomorphic encryption.

3.4 MERITS

- Authentication is very important for block chain based EHR.
- In the healthcare industry there are many different parties.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 465-470
Published Online January 2020 in IJEAST (http://www.ijeast.com)

- An identity based signature scheme with multiple authorities.
- Which has both efficient signing and verification algorithms and can resist collusion attack?
- Which guarantees responsibility and transparency in the procession of data exchange?
- Thus reducing the number of medical accidents and preserving patient privacy.

IV. IMPLEMENTATION

Authorized entity might look over the health records of this patient by means of his block chain, and has powerless to tamper the data in established block (such as drug allergy and dosage). When the patient goes to be treated in other clinical departments or hospitals next time, the new entity needs to identify this patient and authenticate his available block chain, which could save the medical resources and avoid the repeated detection.

To meet the requirement of distributed structure in EHRs system, we employ attributes based signature with multiple authorities to address the above application. A MA-ABS scheme is a protocol that a signature attests not to the identity of the patient who endorsed a message, but instead to a claim (like access policy) regarding the attributes delegated from some authorities he possesses. Suppose that a patient Alice wishes to anonymously publish a block with sensitive data on EHRs system. To give credibility to her block she decides to take the following claim to endorse message.

Alice would acquire these attributes from the different attribute authorities, who may not trust or even be aware of each other. In the special cases, a party of the attribute authorities may be corrupted. Under this case, it should not impede the acquirement of attributes from the other hornet's authorities. Alice is allowed to endorse her message under the claim above, without having to reveal how she meets the claim. Authorities jointly guarantee her signature for Alice, while guaranteeing it for herself in the identity-based signature scheme.

Taking advantage of this technique it achieves a perfect privacy preserving for patient. The explicit claim of the signature reveals nothing about the identity or attributes of the patient. From another point of view it guarantees the verifier in enforceability as well. The signature of patient whose attributes satisfy the claim cannot be generated by collusion of parties who integrate their attributes together. Hence it constructs a secure and controllable mechanism in HER system to confirm the validity of health block

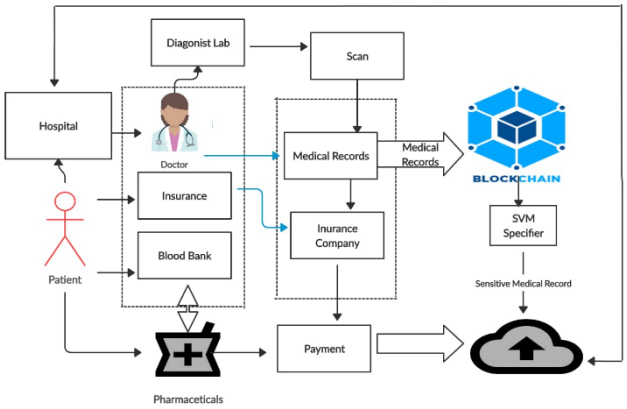

Fig 1: Block Diagram

These blocks on MoD services are connected in series into a block chain that belonged to Alice. Because of the small size of index, it does not exceed the limitation of the storage space in every block. According to this model, any changes about the original healthcare data in cloud would cause that the corresponding index in the block chain is altered, and each entity including Alice and all authorities will discover these variations. This technique achieves a global view of Alice's medical history in an efficient, verifiable and permanent method. Hence, the block chain technique is benefit to providing the integrity protection on the healthcare data in cloud.

Although it shows a lot of advantages to the medical services, cloud computing also brings some security challenges [13]–[19]. In the cloud, all the sensitive data related to patient is controlled by CSP, such as name, address, social security number, allergic history and so on. Normally, the service provider is a commercial enterprise (such as Amazon and IBM) that cannot be trusted completely. These enterprises enable to access users' privacy at any time, and alter or delete data accidentally or deliberately. Consequently, it is necessary to restrict the behaviours of curious CSP and unauthorized users, and prevent the information stored in cloud from being tampered.

V. EVALUATION

5.1 Unique Id and Key Verification.

When an every doctor must have a unique hospital details and doctor list

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 465-470
Published Online January 2020 in IJEAST (http://www.ijeast.com)

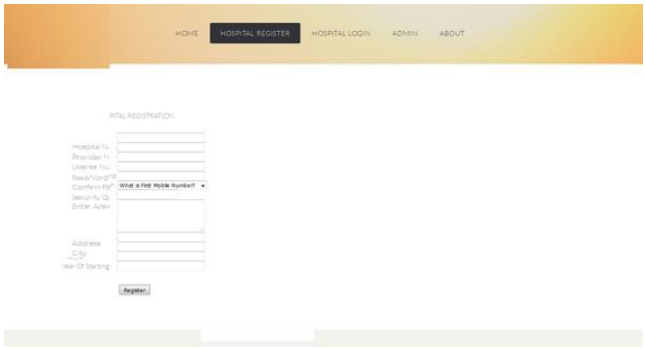

Fig 2: Hospital.

5.2 Uploading the Patient Data Set.

When a patient booked his doctor along with hospitality and Doctor Specialist.

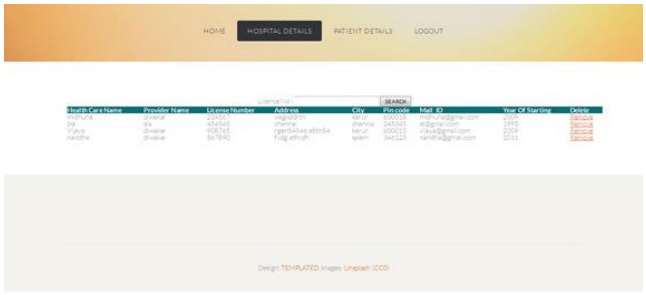

Fig 3: Uploading the Patient Data Set.

5.3 Doctor Counselling.

That means doctor will update patient details according to daily basic report and patient.

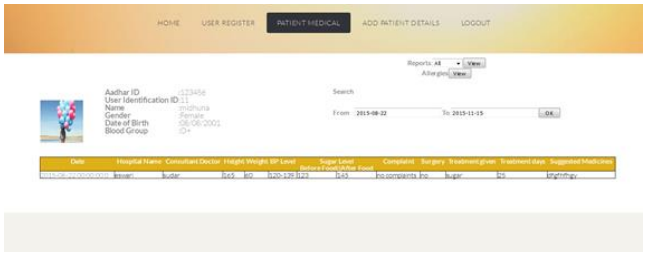

Fig 4: Doctor Counselling Report.

5.4 Patient Access:

Patient personal information to all roles in an application to prevent that we had proposed to use identity based encryption.

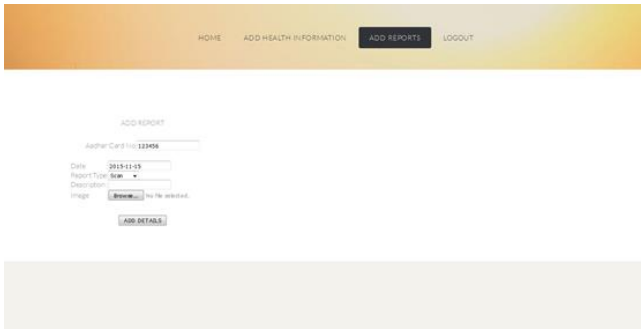

Fig 5: Patient Records.

5.5 Medical Data in Block Chain.

Patients to assign access rule for their medical data and permitting specific researchers to access parts of their data and importing medical data using block chain.

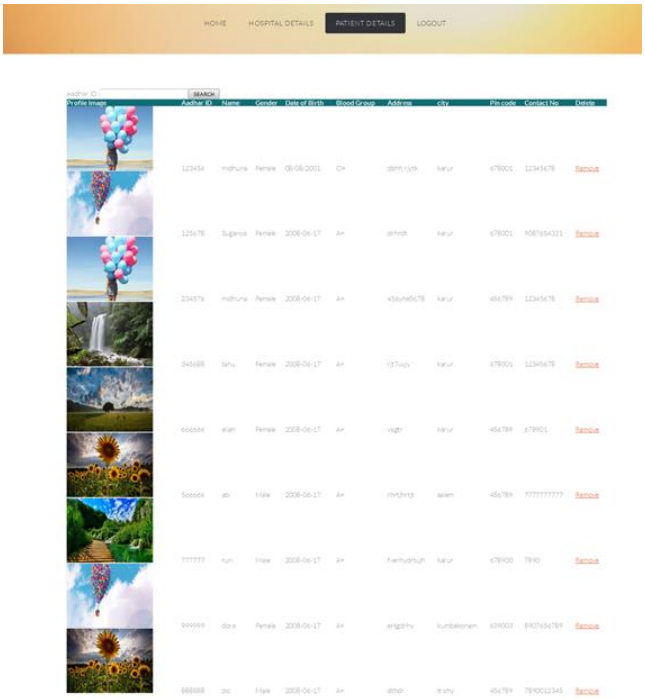

Fig 6: Medical Data Set

VI. CONCLUSION

Aiming at preserving patient privacy in an EHRs system on block chain, multiple authorities are introduced into ABS and put forward a MA-ABS scheme, which meets the requirement of the structure of block chain, as Pwell as guaranteeing the anonymity and immutability of the information. PRF seeds are needed among authorities and the patient private keys need to be constructed, $N - 1$ corrupted authorities cannot succeed in collusion attacks. Finally, the security of the protocol is proven under the CBDH assumption in terms of enforceability and perfect privacy. The comparison analysis demonstrates the performance and the cost of this protocol increases linearly

with the number of authorities and patient attributes as well. A non-monotone predicate could be used in many distributed system applications, which enriches the representation of the predicate. Supporting general non-monotone predicates in block chain technology is the direction of future work.

VII. REFERENCES

[1]Li M., Yu S., Zheng Y., Ren K., and Lou W. et al.(2013) "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, (pp. 131–143).

[2] Liang H., Cai L.X., Huang D., Shen, X. and Peng D. et al.(2012). "An smdp based service model for inter domain resource allocation in mobile cloud networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 5, (pp. 2222–2232).

[3]Shen Q., Liang X., Shen X., Lin X., and Luo H. et al.(2014)."Exploiting geo distributed clouds for e-health monitoring system with minimum service delay and privacy preservation," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 2, ((pp. 430–439).

[4]Yang Y., Li H., Wenchao L., Yang H., and Mi W. et al. (2014). "Secure dynamic searchable symmetric encryption with constant document update cost," *in Proceedings of GLOBECOM. IEEE*, (pp. 775–780).

[5]Wang C., Ren K., Yu S., and Urs K M R. et al. (2012)."Achieving usable and privacy-assured similarity search over outsourced cloud data," *in Proceedings of IEEE INFOCOM*, (pp. 451–459).

[6]Boneh D., Di Crescenzo G., Ostrovsky R., and Persiano G , et al. (2004., "Public key encryption with keyword search," in *Advances in Cryptology–Eurocrypt. Springer*), (pp. 506–522).

[7] Curtmola R., Garay J., Kamara S., and . Ostrovsky R., et al. (2006). "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proceedings o ACM CCS*,(pp. 79—88).

[8] Ren K., Wang C., and Wang Q. , et al. (Jan 2012). "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, (pp. 69–73).

[9]Song D.X., Wagner D., and Perrig A. , et al. (2000). "Practical techniques for searches on encrypted data," *in IEEE Symposium on Security and Privacy*, (pp. 44–55).

[10]Hahn F. and Kerschbaum F. , et al. (2014). "Searchable encryption with secure and efficient updates," in *Proceedings of CCS. ACM*, (pp. 310–320).

[11] Yuan X., Wang X., Wang C., Squicciarini A., and Ren K. , et al. (2014). "Enabling privacy-preserving image-centric social discovery," in *Proceedings of IEEE ICDCS*, (pp. 198–207).

[12] Lu-Chou Huang, Huei-Chung Chu, Chung-Yueh Lien, Chia-Hung Hsiao, Tsair Kao, et al. (2009). "Privacy preservation and information security protection for patients'portable electronic health records", *Computers in Biology and Medicine*, vol. 39, no. 9, (pp. 743-750).

[13]Usman Iqbal, Cheng-Hsun Ho, Yu-Chuan(Jack) Li, Phung-Anh Nguyen, Wen-Shan Jian, Hsyien-Chia Wen, et al. (2013). "The relationship between usage intention and adoption of electronic health records at primary care clinics", *Computer Methods and Programs in Biomedicine*, vol. 112, no. 3, (pp. 731-737).