Cloud-based Secure Healthcare Framework by using Enhanced Ciphertext Policy Attribute-Based Encryption Scheme

Siti Dhalila Mohd Satar[1]
Mohamad Afendee Mohamed[2]
Faculty of Informatics and Computing
Universiti Sultan Zainal Abidin, Terengganu, Malaysia

Masnida Hussin[3*], Zurina Mohd Hanapi[4]
Siti Dhalila Mohd Satar[5]
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia, Selangor, Malaysia

***Abstract*—Cloud computing is an emerging technology that has been used to provide better healthcare services to the users because of its convenient and economical features. Noted that the healthcare services required fast and reliable data sharing at anytime from anywhere for better monitoring and decision making in medical requirements. However, the privacy and integrity of electronic healthcare record become a significant issue during data sharing and outsourcing in Cloud. The data privacy of clients/patients is important in healthcare services where exposure of the data to unauthorized parties is unexceptional. In order to address this security loophole, this paper presents a Cloud-based Secure Healthcare Framework (SecHS) to offer safe access to healthcare and medical data. Specifically, this paper enhance the Ciphertext Policy Attribute-Based Encryption (CP-ABE) scheme by adding two more modules which aims to provide fine-grained access control and offer privacy and integrity of data. It facilitates encryption and hashing schemes. The proposed framework is compared with existing frameworks that used CP-ABE scheme. It shows the SecHS offers better features towards securing the healthcare services data. Optimistically, data security requirements such as privacy, integrity and fine-grained access control are required to effectively proposed for assuring data sharing in the Cloud environment.**

Keywords*—Cloud computing; privacy and integrity; fine-grained access control; Ciphertext Policy Attribute-Based Encryption; electronic health record

I. Introduction

Cloud technology offers an innovative computing method for delivering IT services efficiently. Cloud technology able to enhance the quality of services (QoS) in numerous fields, including healthcare and medical services[1],[2]. Basically, in the healthcare services, electronic health record (EHR) has been widely used to improve storing, accessibility, sharing and realized a collaboration of medical data among medical practitioners. The EHR includes patients' data, laboratory results, medication lists, diagnostic tests, physical assessments, and historical observations. Due to most of these records are crucial and confidential, it is recommended by the Health Insurance Portability and Accountability Act (HIPAA) [3],[4] for ensuring the data and documents are safe and protected.

Cloud adoption in healthcare services has gained many attentions as mentioned in [1], [5]–[7] and it offers superfluous benefits to the hospital and medical organization. The healthcare services through Cloud computing is expected to reduce execution cost hence might improve the services delivery. Furthermore, the resource management and system administration (infrastructure) can be effectively monitored through Cloud computing makes healthcare service is easy to maintain [8]. However, despite all the advantages, security is one of the most important challenges in Cloud computing. Particularly, the systems that have been used by the healthcare practitioner or end-users are vulnerable to many security issues. It is due to the medical data is confidential and data leaked by the irresponsible entity are unacceptable. Moreover, according to [9], [10], [11] the fact that the data is stored in the Cloud and can be resided anywhere and beyond the geographical boundary might cause the users to lose control over their own data. Other security concern includes the issue of the healthcare and medical organizations that need to have a clear agreement including security concern with the Cloud Service Provider (CSP). This involves security and access control procedures. There is very often where the Cloud users are not given a thorough explanation of their security concerns and needs in renting the Cloud services from CSP. Therefore, the need for data integrity and privacy mechanism which offer fined-grained access control are a necessity in order to provide better security services to both Cloud users and CSP.

This study proposed a Secure Healthcare Framework (SecHC) in Cloud computing using Ciphertext Policy Attribute-Based Encryption (CP-ABE). It aims to provide secure access to healthcare and medical data in the Cloud environment. In this framework, the patient's data is encrypted under Symmetric Encryption Scheme and the access policy in CP-ABE is embedded with the ciphertext. The contribution is summarized as follows:

- Provide a fine-grained access control by implementing the CP-ABE scheme which suited for a Cloud-based electronic health record system.
- Model security analysis related to security requirements in the Cloud environment includes privacy, integrity and fine-grained access control.

The remaining paper organization is as follows. Section 2 discuss on related work. In section 3, a simulation is conducted to proof the weakness of existing work. The proposed secure

*Corresponding Author

healthcare framework is provided in Section 4. Section 5 discussed the feature and security requirement analysis against other frameworks. Lastly, Section 6 provides a conclusion.

II. Related Work

The area of healthcare and medical in Cloud computing is commonly implemented and realized. There are several approaches and techniques are used in securing the Cloud-based healthcare system in the data sharing process.

A. Healthcare and Medical in Cloud

The rapid development of Cloud computing nowadays has transformed the way of healthcare provider and even medical practitioners such as doctors and hospitals, to provide a quality and affordable service to their clients. This transformation is motivated by two major factors which are the business commanding to reduce costs and to convalesce the quality of care [12]-[14]. From the business side of view, the providers can lower their operational expenses to compensate for the increasing costs of infrastructure, administrative and pharmaceutical. Simultaneously, they also must handle requests from the government to increase the quality of healthcare and delivered a common healthcare operating standard [15], [16].

Meanwhile, on the patient side, the provider must offer a service that provides instant and top-quality access because nowadays, a patient is acquainted with the 24/7 accessibility of services especially from the online retailers and financial institutions. Furthermore, currently, the users are interested to involve in managing their own healthcare so the need for a system that could provide diagnosis, information, and treatments is in demand [3], [14]. For example, a patient would like an internet-based service from the healthcare providers that provide a platform for them to converse or consult the healthcare professionals all the time especially before, during and after any health-related procedures. This situation shows that a dire need of healthcare providers to transform themselves from a traditional to a Cloud environment to tackle the business and patient needs of an agile environment and to revolutionize their IT infrastructure.

Although the implementation of Cloud computing in healthcare sectors may seem beneficial and positive, it also fosters many detrimental situations and challenges. Despite the emergent trends of using Cloud computing as the platform to promote healthcare, the anxiety over the security and privacy of confidential information in the Cloud are intensifying over the years [17]. Data leakage and loss, phishing, hijacking of account or service, and unidentified risk profile are an example of the threats that impend the privacy and integrity of Cloud data.

Furthermore, the healthcare organizations have discovered that the existing mechanisms such as Secure Socket Layer protocol (SSL) and Transport Layer Security (TSL) protocol are not sufficient to secure EHR in Cloud because it only protects the privacy during data transmission [3][18]. Apart from it, according to [3], dishonest employees of the CSP can easily overrule a particular role with the authorization to retrieve and read the healthcare data beyond their privileges. Thus, to avoid any infringements of sensitive data by fraudulent employees and to prevent medical data from other security threats, a secure mechanism must be designed and developed to enhance the data privacy and integrity of EHR in Cloud computing.

Recently, numerous security mechanism has been proposed by researchers to protect medical data in Cloud such as encryption schemes and access control schemes [10][19]. Such schemes permit the data owner to manage the data by restricting access to specific users for a specific file with limited privileges. Fig. 1 shows example of mechanism used to secure EHR in cloud. In this figure, data owner is defined as a patient stored the records in the cloud server and the record can only be accessed and downloaded by authorized physicians. This mechanism helps the healthcare and medical organization to protect the security and privacy of cloud data.

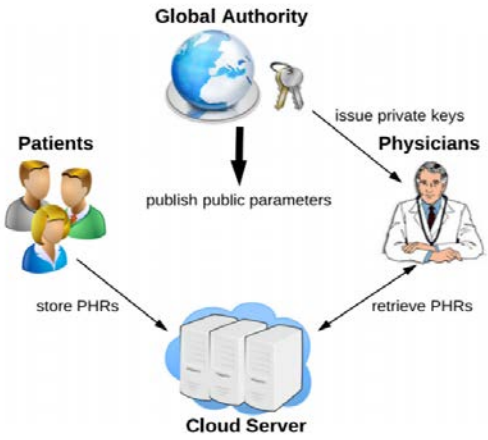

Fig. 1. Securing Electronic Health Record in Cloud [12].

B. Securing Healthcare and Medical Records in Cloud

In medical and health organizations, allowing end-users to control access to the data stored in unreliable cloud servers by using encryption schemes is an effective method to prevent data leakage, ensure safe transmission and secure from any other security threats. According to [20][21], the encryption algorithm permits end-users to encrypt data and ensure only user with the key can decrypt the data. However, this traditional encryption scheme is incapable to satisfy one-to-many encryption which is crucial in the cloud sharing scenario. One-to-many encryption permitting the data owner to encode the data once and it can be decoded or decrypted by several users that have a decryption key.

To deal with this issue, a control access mechanism that supports one-to-many encryption should be implemented to prevent unauthorized access to the Cloud. The author [21] proposes a scheme to support one-to-many encryption using Attribute-Based Encryption (ABE). This scheme is based on a novel patient-centric framework for controlling access to Patient Health Records (PHR) stored in semi-trusted cloud servers.

Meanwhile, authors [13][14]15][16][18][22] proposed another variant of ABE which is CP-ABE scheme wherein the CP-ABE scheme, data owner are allowed to specify the

authorized users to access the data, by enclose the access policy to the ciphertext. In order to generate private keys associated with set of user's attributes, ABE schemes rely on reliable and trusted authorities.

In order to achieve confidentiality and authenticity simultaneously, an efficient and improving CP-ABE scheme has been introduced by [15] and [20]. They used a signature scheme to verify the authenticity of data and the owner of the data. In the meantime, authors [13] and [18] proposed a scheme to enhance the efficiency of the decryption process. They used the Attribute Bloom Filter technique to assess whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy. This technique will reduce the decryption time. However, this technique will cause a trade-off in terms of increasing computation overhead.

Besides, authors [21] also construct a scheme used CP-ABE which offers not only fine-grained access control but also providing integrity by checking the access policy of the users before they can access healthcare data. Their works also aimed to offer fast decryption by adding some redundant components to a ciphertext before the decryption stage. However, their works are not sufficient to secure the process of sharing data in the Cloud environment due to the failure to provide a fully hidden policy within the CP-ABE. The same issue applies to the researchers [23] where they proposed a privacy-aware s-health access control system that offers partially policy hiding. In the system, only the attribute value is hidden while the attribute name is sent to the Cloud with ciphertext in a readable form. This will cause data security to be compromised in the event of an attack where the attacker can find out and learn about the policy which leads to privacy leakage.

In addition, Zhang et. al., [17] proposed a privacy-preserving scheme using CP-ABE with efficient authority verification. They preserve the privacy of the data authority identification phase by determining whether the user is authorized or not. Apart from it, a study by [24] proposed a scheme using CP-ABE which successfully achieved high security by hiding the entire access policy of the EHR. However, they overlooked the additional computational cost and decryption time is high due to the newly introduced scheme on verification of the matching process.

Thus, the above literature review indicates that many works have been done to provide additional security towards the security mechanism provided by the CSP. However, according to [17], it still insufficient to protect medical and healthcare records and reduce the risk of threats in the Cloud environment. This is because there are many issues arise such as multi-authority, hidden policy and constant size ciphertext which need to be studied.

C. Framework of Health Data in Cloud

Generally, a framework is built to simplify a complex technological process. It is usually consisting of a few elements, or entities which will be integrated to become a useful process. In medical and healthcare organizations, several frameworks have been proposed to ensure administration of patients, data, staff and operations are running smoothly. For example, a security framework focusing on data delivery of patient care has been developed by Zhang et al. [25]. In this framework, Zhang has introduced three main components: data collection, secure storage and secure usage model as shown in Fig. 2. The aim of this framework is to provide a safe interaction between healthcare professionals and patients based on security needs and patient privacy in the EHR Cloud.

The first component is collection and integration of various data from various departments in organizations. These components are responsible to make sure all the data is available and safe to be used. Hence, this component needs to verify the data in term of confidentiality, integrity, and ensuring nonrepudiation as well as HIPAA compliance.

The second component is the secure storage that consists of two entities which are secure storage server and access control engine. Data is stored as ciphertext in secure storage server and only authorized user is permitted to access the data. Meanwhile access control engine use role-based and attribute-based method to grant access to the user. As a result, user that does not match the attribute will be denied the access to patient's data in Cloud Storage.

The last component is secure usage model. This component's role is to provide a safe data access by using two methods: signature and verification. Medical practitioners will sign EHR using appropriate signature algorithm before sending it to Cloud storage. Then, user will verify the authenticity of the data by using digital signature verification.

Apart from that, the work proposed by [26] introduces a framework that offers privacy of health data and provides access control to the data in Cloud. There are four entities in this framework are S-Health Authority, S-Health Cloud, Data Owner, and Data User as shown in Fig. 3.

In this framework, S-Health Authority is responsible for system initialization and authorization where it uses attribute-based access to permit authorized user to store or access data in Cloud. Meanwhile, for data owner they manage their EHR by performing encryption process to secure the record. They stored the ciphertext and its access policy in the S-Health Cloud. To enhance the security, they partially hide access policy to prevent untrusted entities take advantages of the access policy.

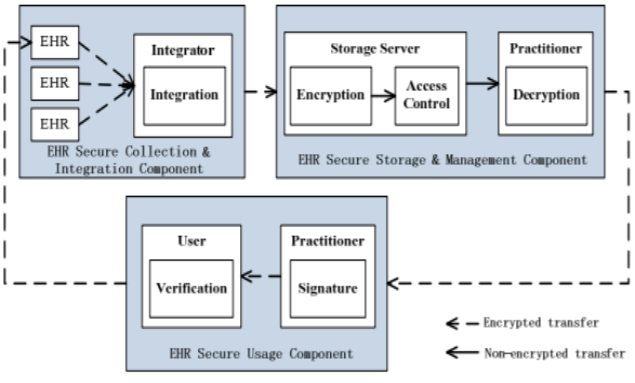

Fig. 2. Security Framework Focusing on Data Delivery of Patient Care [25].

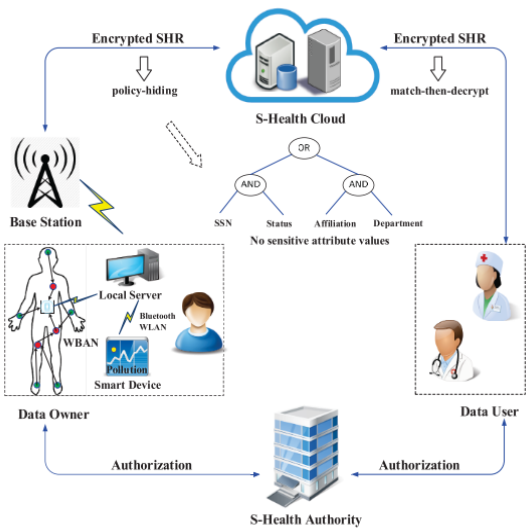

Fig. 3. Framework of the Privacy-Aware S-Health Access Control System [26].

In addition, to make the process efficient, they implement match-then decrypt procedure in the decryption phase. In this phase, data user will use to his secret key to check whether his attributes match the underlying access policy, and then decrypt the encrypted EHR only if the matching is successful.

Using this framework, the system achieved security requirement by offering fine-grained access control using CP-ABE scheme. They also provide confidentiality using encryption algorithm and offer data privacy using hidden access policy.

However, both frameworks proposed by [25] and [26] can be improved by incorporating other mechanisms such as hashing algorithms which are used to ensure data integrity. In addition, to ensure the privacy of data, fully hidden access policy must be implemented to solve user distrust issues.

III. Preliminaries Work

This section describes the preliminaries related to the proposed work by [21]. In Zhang's work, they used CP-ABE to provide fine-grained access control to the health data in Cloud storage. The proposed solution was successfully delivered data verifiability and fast decryption by providing the validation of decrypted message. However, the access policy was sent to the Cloud together with the ciphertext in a readable form which led to the data privacy leakage.

In this preliminaries work, a simulation of transferring a file that contained an access policy using FileZilla Tool is conducted. To transfer the file from a client to a server, a File Transfer Protocol (FTP) without encryption is used as shown in Fig. 4.

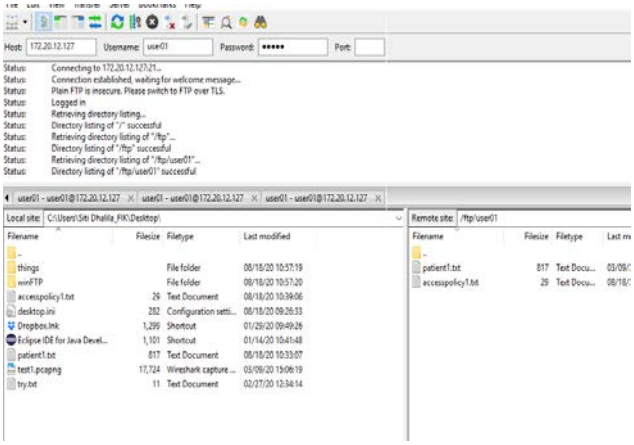

Fig. 4. Transferring a File using FTP in FileZilla Tool.

While transferring a file in FileZilla, Wireshark tool is execute by running a passive attack to sniff the packet as shown in Fig. 5.

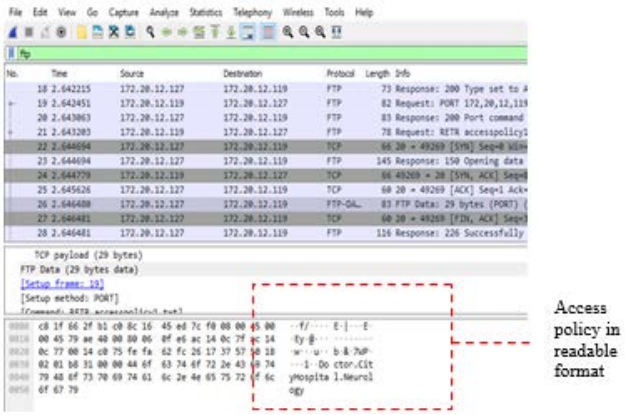

Fig. 5. Packet Sniffing using Wireshark.

In this simulation, because of the access policy was sent in a readable form, the attacker can read packet and gain the information in the access policy. Based on the simulation, it is necessary to provide a framework that can help user to secure their data than preserve the privacy of an access policy.

IV. Enhancement of Ciphertext Policy Attribute-Based Encryption (CP-ABE) Scheme

This section describes in detail on how the ciphertext policy attribute-based encryption (CP-ABE) scheme has been utilized to design the proposed framework; called as SecHC. The proposed framework provides security components in order to ensure the healthcare and medical data can securely exchange among healthcare organizations through Cloud environment. The SecHC framework (Fig. 6) have four entities involved are Data Owner, Data User, Attribute Authority and Secure Health Cloud.

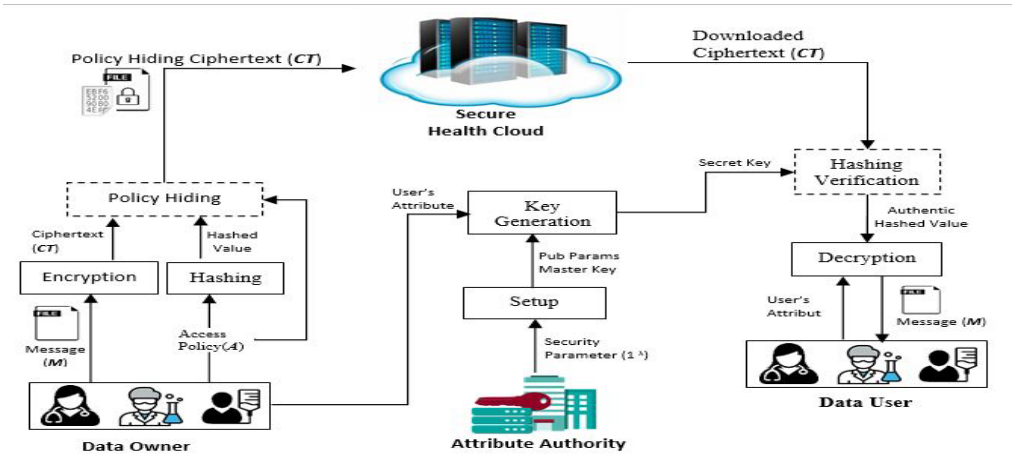

Fig. 6. Cloud-based Secure Healthcare Framework (SecH).

The general framework for CP-ABE scheme has four modules are (i) setup, (ii) key generation, (iii) encrypt and (iv) decryption. The data owner in CP-ABE scheme is been set to some access policy before it been encrypted. Data owners then outsourced the encrypted data along with access policy to the Cloud storage. If the receiver satisfied the defined access policy, the data then will be decrypted. Even though ciphertext attribute-based encryption is a prominent access control scheme however it suffers from privacy preservation of policy. It is because the defined policy is appended to the ciphertext in readable format which can lead to user's information leakage. So, the adversaries can learn confidential information from readable access policy. To address the issue, this work enhance Ciphertext Policy Attribute-Based Encryption (CP-ABE) scheme by adding other components to secure the healthcare data for designing the Secure Healthcare Framework (SecHC). The proposed framework provides security and integrity of data using encryption and hashing scheme. It also provides a policy hiding scheme to ensure access control with privacy-preserving.

Specifically, two more modules have been added in encryption phase namely hashing and policy hiding while for decryption phase, the added module is hashing verification. In the encryption phase, the hashing module is to ensure there is no tampering data while maintaining the data integrity. In the policy hiding module, the access policy will be hidden from the unauthorized users that might be led to privacy leakage. Meanwhile in the decryption phase the hashing verification is introduced which is to verify the authenticity of the access policy. This module aims to accelerate hashing verification thus reducing the time for decryption. Each of the functions is described as follows.

A. Setup Algorithm

The setup algorithm involves a security parameter as an input and produces a public parameter key and a master key as the outputs. Both will be utilized as the input in the key generation algorithm. In this setup algorithm, Bilinear Pairing will be used to create a public key which generated by Attribute Authority.

B. Key Generation

The key generation algorithm is executed by the Attribute Authority. It will take input users' attributes, public parameters, and master key then perform an operation to the inputs to generate a secret key. Later, this secret key will be employed by the data user to decrypt the ciphertext.

C. Hashing

This is the new module introduced in SecHC. The hashing algorithm used a mathematical function to generate a hash value from the input by the user. It used to verify the integrity of a file after it has been transferred from one place to another. In this module, the attributes of access policy will be hashed using the MD5 algorithm. According to [27], MD5 is very efficient and it operates faster than other algorithms. Then, after the hashing process, the hashed value will be sent to the Cloud along with ciphertext.

D. Encryption

In the encryption phase, the algorithm takes the inputs from the Data Owner to be encrypted and produce a ciphertext. Advanced Encryption Standard (AES) is used as an encryption algorithm to converts data into unreadable forms. The data owner will outsource the ciphertext along with the hashed value in the Cloud to be shared with the other users.

E. Access Policy Hiding

In traditional CP-ABE, the access policy is sent along with the ciphertext to the Cloud in readable form. Therefore, anyone who accesses the ciphertext can learn about the access policy which leads to weak policy privacy. Hence, to overcome this issue, an access policy hiding scheme is proposed and developed in SecHC to provide fully hidden access policy. In this module, the Logical Connective Operator is used to hide the attribute names and its values into meaningless values. Then, this meaningless value will be sent to Cloud along with ciphertext and hashed value.

F. Extracting Hidden Access Policy

Data Users need to extract the hidden access policy before he/she can access and download the file from Cloud. In this module, reverse process of hidden access policy from meaningless value to the access policy will be performed.

Then, after extracting the access policy, hashing verification will take place.

G. Hashing Verification

Hashing verification scheme is used to determine the authenticity of ciphertext and access policy. This module is to ensure the transferred ciphertext is not corrupted. In this module, the user needs to perform a calculation (hashing verification algorithm) to access policy. If the hash value of access policy (before and after downloaded from the Cloud) is the same, then the transferred file is an identical copy. So, the user can proceed to the decryption module. But if the values are not the same, the process will be ended.

H. Decryption

The decryption module is taking place after the hashing verification process produced the authentic hashing value. The decryption scheme takes a public parameter, secret key (associated with the user's attributes) and ciphertext as input and produces the message.

V. Comparison with Other Frameworks

In this section, a comparative analysis of the proposed scheme with some typical CP-ABE schemes has been conducted. By considering the characteristics of the proposed scheme satisfied, only selected schemes [21][26][28][29] that are strongly relevant to the proposed scheme for comparison is discussed.

Based on findings reported in Table I, a comprehensive comparison according to important features is presented including policy hiding, privacy-preserving, data integrity, and fine-grained access control.

By comparing the proposed framework with the schemes by the authors in [21][29] it definitely a different strategy is used for improving CP-ABE. In [21], the enhancement of CP-ABE scheme only achieves partly hiding policy which leads to failure to protect the privacy of the data. However, they accomplish to offer integrity using a hashing scheme. Yet, their scheme can be improved in terms of decryption procedure which focuses on the decryption test.

TABLE I. Comparative Summary between Schemes

Technique	Hidden Policy	Privacy-Preserving	Integrity	Fine-grained Access Control
CP-ABE [26]	Partial	√	X	√
Improvised CP-ABE [21]	Partial	X	√	√
CP-ABE [28]	No	√	X	√
Improvised CP-ABE [29]	Partial	X	√	√
SecHC CP-ABE scheme	Fully	√	√	√

Meanwhile, in [29], their CP-ABE scheme focused more on the decryption phase where they introduced KeyGen.out, Decrypt.out, Decrypt.user. Their scheme is designed to broadcast encryption techniques and used outsourcing techniques to realize policy-hide, direct revocation, and secure delegation simultaneously. However, their scheme failed to provide a fully hidden access policy and unable to keep it private.

Meanwhile, in SecHC framework, the proposed CP-ABE scheme capable of supporting fully hidden access policy using data hiding technique, provide integrity using hashing scheme and provision fine-grained access control. Most of the researchers have improvises the CP-ABE scheme except the authors in [26] and [28] which cause them unable to achieved hidden policy and provide data integrity.

VI. Data Security Requirement Analysis of SecHC Framework

Particularly, in medical and healthcare organizations, sharing information in the Cloud environment has raised many security problems related to security requirements such as confidentiality, integrity, privacy and so on. Thus, the SecHC framework is developed to meet and satisfy the security requirement for the Cloud environment. The analysis of security requirements is described as follows.

A. Data Privacy

The proposed framework is fully privacy-preserving. It protects users' privacy by using the encryption algorithm. The proposed framework adopted the encryption algorithm in CP-ABE scheme to provide data privacy in a secure health Cloud. The electronic health record's privacy is achieved when the user uploads the encrypted record with hidden policy to the cloud.

B. Data Integrity

In the proposed framework, the hashing algorithm is used to protect the accuracy and consistency of data from any modification, deletion or fabrication. To achieve data accuracy, only correct and trustworthy data must be stored in the Cloud while consistency can be attained when outsourced data is not tampered, changed or maliciously deleted. Based on the framework, the medical and health record will be encrypted, and the access policy will be hashed. This hashing process is to ensure there is no modification that has been made on ciphertext stored in Cloud. If there is any modification on ciphertext, the user could not perform the decryption process. This process proves that the proposed framework offers to protect the integrity of data in a secure health Cloud.

C. Fine-Grained Access Control

In a healthcare Cloud, all users do not have the same privileges to retrieve medical data. This privilege depends on the degree to which a user is involved or specialized in treatment. Therefore, this framework ensures a different user will have different access privileges which defined by access policy imposed by attribute authority. The CP-ABE scheme used in this framework helps us achieve fine-grained access control. This means that all the attributes must be matched with

the user access policy structure to be able to access the required information.

VII. Conclusion

In the ever-increasing era of a data breach, Cloud computing is required to provide a security solution to protect sensitive information and transactions. This solution can prevent a third party from eavesdropping or tampering with the data while it is being transmitted. In this work, the Secure Healthcare Framework (SecHC) is designed by enhancing the Ciphertext Policy Attribute-Based Encryption (CP-ABE) scheme. It can further promote the Cloud privacy and integrity to both users and providers in the healthcare and medical organizations. The SecHC framework supports privacy and integrity of healthcare and medical data and offers fine-grained access control strategy. It is provided by using combination of prior and new components in the CP-ABE scheme. Such components offer a fully hidden access policy and provide fast decryption. Analysis of security requirements shows that this framework satisfies the privacy and integrity of healthcare data. In the near future, let the proposed framework to handle the real healthcare and medical data over the Cloud environment.

References

[1] O. Ali, A. Shrestha, and S. Fosso, International Journal of Information Management, "Cloud computing-enabled healthcare opportunities, issues , and applications : A systematic review," vol. 43, no. April, pp. 146–158, 2018.

[2] F. Shiferaw and M. Zolfo, "The role of information communication technology (ICT) towards universal health coverage: the first steps of a telemedicine project in Ethiopia," Global health action, 5(1), 15638, no. June 2014, pp. 0–8, 2012.

[3] J. J. Yang, J. Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Futur. Gener. Comput. Syst., vol. 43–44, pp. 74–86, 2015.

[4] A. Jemai, R. Attia, N. Kaaniche, S. Belguith, and M. Laurent, "PHOABE: Securely outsourcing multi-authority attribute-based encryption with policy hidden for cloud assisted IoT," Comput. Networks, vol. 133, pp. 141–156, 2018.

[5] N. Sultan, "International Journal of Information Management Making use of cloud computing for healthcare provision: Opportunities and challenges," Int. J. Inf. Manage., vol. 34, no. 2, pp. 177–184, 2014.

[6] N. Y. Lee and B. H. Wu, "Privacy Protection Technology and Access Control Mechanism for Medical Big Data," Proc. - 2017 6th IIAI Int. Congr. Adv. Appl. Informatics, IIAI-AAI 2017, pp. 424–429, 2017.

[7] L. Ibraimi, M. Asim, and M. Petko, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," Proc. 6th Int. Work. Wearable, Micro, Nano Technol. Pers. Heal., pp. 71–74.

[8] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography," IEEE Access, pp. 22313–22328, 2017.

[9] T. Kajiyama, M. Jennex, and T. Addo, "To cloud or not to cloud: how risks and threats are affecting cloud adoption decisions," Inf. Comput. Secur., pp. 00–00, 2017.

[10] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues," Futur. Gener. Comput. Syst., vol. 72, pp. 273–287, 2017.

[11] Satar, S.D., Hussin, M., Hanapi, Z., & Mohamed, M.A. (2018). Data Privacy and Integrity Issues Scheme in Cloud Computing: A Survey. International journal of engineering and technology, 7, 102.

[12] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, and D. S. Wong, "Designing cloud-based electronic health record system with attribute-based encryption," Multimedia Tools and Applications, 74(10), 3441-3458.2014.

[13] K. Yang, Q. Han, H. Li, K. Zheng, Z. Su, and X. Shen, "An Efficient and Fine-Grained Big Data Access Control Scheme with Privacy-Preserving Policy," IEEE Internet Things J., vol. 4, no. 2, pp. 563–571, 2017.

[14] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.

[15] S. Sabitha and M. S. Rajasree, "Access control based privacy preserving secure data sharing with hidden access policies in cloud," J. Syst. Archit., vol. 75, pp. 50–58, 2017.

[16] H. Wang, X. Dong, and Z. Cao, "Multi-value-Independent Ciphertext-Policy Attribute Based Encryption with Fast Keyword Search," IEEE Transactions on Services Computing vol. 1374, no. c, 2017.

[17] L. Zhang, Y. Cui, Y. Mu, and S. Member, "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing," IEEE Systems Journa, pp. 1–11, 2019.

[18] Q. Han, Y. Zhang, and H. Li, "Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things," Futur. Gener. Comput. Syst., vol. 83, pp. 269–277, 2018.

[19] Abd Hamid, N., Ahmad, R. and Selamat, S.R., 2017. Recent Trends in Role Mining Algorithms for Role-Based Access Control: A Systematic Review. World Applied Sciences Journal, 35(7), pp.1054-1058.

[20] F. Deng, Y. Wang, L. I. Peng, H. U. Xiong, and Z. Qin, "Ciphertext-Policy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records," IEEE Access, vol. 6, pp. 39473–39486, 2018.

[21] L. Zhang, G. Hu, Y. Mu, and F. Rezaeibagha, "Hidden Ciphertext Policy Attribute-Based Encryption with Fast Decryption for Personal Health Record System," IEEE Access, vol. 3536, no. c, pp. 1–1, 2019.

[22] D. Slamanig and C. Stingl, "Privacy Aspects of eHealth," pp. 1228–1235, 2008.

[23] Z. Ying, L. U. Wei, Q. I. Li, X. Liu, and J. I. E. Cui, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud," vol. 6, 2018.

[24] N. Muhammad, J. M. Zain, and M. Mohamad, "Current Issues in Ciphertext Policy-Attribute Based Scheme for Cloud Computing : A Survey," International Journal of Engineering & Technology, vol. 7, pp. 64–67, 2018.

[25] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," Proc. - 2010 IEEE 3rd Int. Conf. Cloud Comput. CLOUD 2010, pp. 268–275, 2010.

[26] Y. Zhang, D. Zheng, and R. H. Deng, "Security and Privacy in Smart Health : Efficient Access Control," IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, 2018.

[27] Rachmawati, D., Tarigan, J. T., & Ginting, A. B. C. (2018, March). A comparative study of Message Digest 5 (MD5) and SHA256 algorithm. In Journal of Physics: Conference Series (Vol. 978, No. 1, p. 012116).

[28] S. Sharaf and N. F. Shilbayeh, "A Secure G-Cloud-Based Framework for Government Healthcare Services," IEEE Access, vol. 7, pp. 37876–37882, 2019.

[29] H. Xiong, Y. Zhao, L. Peng, H. Zhang, and K. Yeh, "Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing," Futur. Gener. Comput. Syst., vol. 97, pp. 453–461, 2019.