International Journal of Computing and Mathematics
Vol. 1, Issue. 3, Sep 2024, pp. 16 ~24

Privacy-Preserving for E-Healthcare System Based on Fog Computing Using Encryption Techniques

Ebere Anastasia Tochukwu[1], Ang Ching Wen[2]
[1] Faculty of Education, Veritas University, Abuja, Nigeria
[2] School of Computer Sciences, Universiti Sains Malaysia, 11800 USM, Pulau Pinang, Malaysia.

Article Info

Article history:

Received Jul 31, 2024
Revised Aug 29, 2024
Accepted Sep 02, 2024

Keywords:

Fog Computing
Privacy Preserving
e-Healthcare
Advanced Standard Encryption

ABSTRACT

Increasing effective communication with specialist healthcare service providers, common information obtained by e-healthcare systems have substantial medical importance. However, the exchange of health data raises many security risks, like access protection and leakage of privacy, and also crucial difficulties in accessing appropriate data collection and services. So this paper proposes a fog-based privacy-preservation for e-healthcare networks to exchange medical information. Especially, for successful health data processing, it implements the fog node to group the shared data into various groups as per disease threats. In the meantime, by integrating a private security mechanism on patients and a technical access policy on the fog node for successful emergency service provision, it develops an improved Advance encryption Standard algorithm. Also, by offloading a part of the computing and storage burden from patients to the fog node, these generate large encryption consumption reduction for patients. Prevention studies illustrate that with collusion tolerance, Privacy-preserving based on fog computing recognizes confidential information and advanced access protection. Evaluations of efficiency show cost-efficient computing, storage, and energy use of encryption.

Corresponding Author:

Ebere Anastasia Tochukwu,
Faculty of Education, Veritas University, Abuja, Nigeria.

1. INTRODUCTION

As an innovative healthcare model for real-time patient data collection and health tracking with the application of information and communication technology, the e-healthcare process has evolved [1]. By 2017, different classifications of health data obtained from heterogeneous healthcare devices could hit around 12 ZBs [2], contributing to a crucial problem in the operation of big data. Cloud-assisted healthcare systems[3] have been selected for further analysis, as cloud computing may preserve and control enormous amounts of information through its efficient storage facilities and computing infrastructure. Patients use emerging healthcare devices in the Cloud-assisted healthcare systems to retrieve health information, but instead, collect it on a centralized server to discuss it with data users. Control and evaluate data access by trained healthcare providers to include healthcare resources, like disease diagnosis, personal treatment, and medical diagnosis[4].

After the exchange of data in the cloud-assisted medical systems, privacy leaks and security risks can occur[5]. For example, if it is processed to healthcare centers, patients ' blood glucose is being changed, invalidating healthcare treatments.Ciphertext- Policy Attribute-Based

Encryption [6] is evaluated and the results for health data collection to secure shared data from privacy issues, unauthorized data access, and data corruption since it might allow different data accessing frameworks with data confidentiality preservation. To encrypt your network resources, patients define security controls and give the ciphertext to the cloud server. Only if their attributes follow user access, data

users can easily access the shared data and decode the ciphertext [7]. Nevertheless, in e-healthcare networks, previous data exchange systems [8] do address many obstacles. In particular, they will only ensure easy availability of health care services and successful medical research, and also cause extreme usage of resources for encryption in resource-limited healthcare applications.

The previous concept of access policy in health data exchange systems could never provide the simultaneous availability of reliable healthcare facilities with privacy preservation[9]. To find network access as per one's abilities and development, patients can typically have their fine desires. Consequently, given the health data needs to be interpreted through competent medical experience, patients without proper healthcare experience could only identify an acceptable access policy to ensure privacy reservations and concurrently receive health care. Interestingly, the preservation of privacy and adequate healthcare facilities validate the others. When the access policy is established with "enforced" privacy preservation features, acceptable healthcare mobile operators will not be allowed to access the shared data. If "loose" features are specified in the access agreement, the data integration could be available to more healthcare providers but could raise the chances of privacy disclosure [10]. Instead, this method of exchange of health data prohibits healthcare providers from effectively evaluating multiple types of data obtained from heterogeneous sensors. Unlike the health information specifically optimized for the individual diagnosis of the disease [11], distributed e-healthcare data attributes are combined and mixed from various categories[12]. The particular form of healthcare data for the subsequent disease needs assessment could perhaps be checked for by service providers, contributing to the medical advantages of gathered healthcare data becoming difficult to excavate[13].

In comparison, CP-AES 's encryptions, computing, and ciphertext processing are typically utilized-demanding, growing with the number of attributes in the access policy, and bringing extreme usage of resources for e-healthcare apps constrained by resources [14]. If the quantity of cloud-based applications for encryption is used, adequate resources are not available for effective health data monitoring. The corresponding energy efficiency not just to reduce the lifetime of e-healthcare equipment, and thereby allows tremendous heat to affect the status of individuals. For successful service implementation and data management with cost-effective resource use, unique privacy-preserving health data sharing architecture is designed to resolve any such difficulties.Fog nodes are a potential approach in e-healthcare networks that enable data integration, sorting, and analysis [16], so this expands data computing from the cloud to the edge of the networkand is smarter and other powerful [2] than e-healthcare apps.

The fog node is built into the previously fog-assisted data collection system to access and re-encrypt network nodes for effective medical research. Also, for the effective pre-processing phase, the device acquires all benefits from fog computing and CP-AES for privacy protection. In this paper, suggests a privacy-preserving fog-node health data exchange structure to increase the quality of data use and facilitate efficient privacy protection availability of health services. Then, as shown by their preferences and experiences, patients encrypted their common data with a personalized access structure and the ciphertext is sent to the fog node. The fog node identifies the health data gathered into multiple groups of disease threats based on random forest classification for effective data use. The fog node determines unique characteristics to encrypt the related health entities as per the healthcare environment to any type of disease severity. After this, the latest ciphertext is sent to cloud servers and the ciphertext can be decrypted by service providers for the successful provision of healthcare services. Privacy-preserving fog-assisted health data sharing is, to their greatest effect, the next health data sharing system to attractively combine fog computing to help determine health information and encryption keys in e-healthcare systems.

We are developing a sustainable system for exchanging fog-assisted health information. Patients may obtain their health data from a customizable access protocol description from providers, and the data flows could be secured from exposure during data collection on the fog node.

With reliable preventive care access, can promise fine-grained access control. The data security initially encrypted on individuals could be obtained by approved service providers with efficient medical healthcare services by encrypting with unique characteristics of the intelligent fog node with health information. For different types of healthcare service providers, researchers help optimize data utilization. The actual data security is mainly categorized into two levels of risk factors, and the associated health products are encrypted with the characteristics of trained healthcare service providers in regards to health threats. As a consequence, it is necessary to recognize and use health data easily, and hierarchical evaluation and recovery can be accomplished by effective data exchange. Analysis of protection reveals that the suggested system protects the privacy of the health condition of patients and ensures permitted access to data during the exchange of health data, and also prevents collaboration of fog nodes with other un-authorized organizations. Also, it performs comprehensive experiments to show that with sufficient computing efficiency, Privacy-preserving fog-assisted health data sharing may ensure accurate prediction of healthcare services, and successful data analysis.

The majority of this paper is discussed in this section. The previous literature on data collection of e-healthcare structures is examined in section 2.The proposed work can be seen in Section 3. The security topics and success reviews are discussed in Sections 4 and 5, accordingly, continued by a conclusion in Section 6.

2. RELATED WORKS

Current frameworks for the exchange of health data that rely on two things are commonly proposed: protection of privacy and performance. Even though healthcare information is vulnerable to secrecy, the protection of secrecy is urgently investigated in current data sharing systems.Chen et al.[16] suggested a cloudlet-based exchange of health data, and used the Number Theory, Research Unit to encode the body information of the individual from wearable technology and provided a confidence framework to enable related patients to interact regarding their diseases with one another.Tong et al.[17], implemented threshold signed attribute-based encryption to provide intellectual activities dependent on role-based access protection to deter possible wrongdoing in e-healthcare schemes.Yang et al.[18] implemented a cloud computing, health record interface focused on the analysis of clinical data features, utilizing vertical segments of a particular data to obtain various degrees of privacy for various components of medical records. Huang et al.[19] supported a fine-grained medical records collaboration framework in cloud-assisted e-healthcare structures through similarity-based suggestions enhanced by directly impacted Hashing.

Yang et al.[20] recommended to such a set of individuals in cloud-based multimedia networks a data exchange strategy to accomplish privacy protection in a unique period.Li et al designed to avoid a lot of the computation mission by incorporating device public key in addition to taking partial encryption computation offline to address the high computation problem in protected data sharing. In fact, until the decryption process, a public ciphertext test approach is carried out, that removes many computing expensesdue to unauthorized ciphertexts. A Chameleon hash function is being used to produce an actual ciphertext for data protection, that is confused by the offline ciphertexts to access the final online ciphertexts.Zhang et al suggested an improved privacy-preserving data method based on encryption and spatial-anonymity in simultaneous LBSs to protect location privacy throughout information sharing, that introduced multi-level caching to minimize the chance of user information being revealed to interested LSPs. By using the main agreement and the group signatures to enable decentralized multiple devices in public clouds,Shen et al. [21] suggested a detectable group data exchange system.

Local authorities can connect securely with regards to the cryptographic algorithms in this research and, if required, the true names of members could be tracked. Even so, depending on the key agreement to allow party participants to give and preserve their data safely, a standard conference key is extracted. A privacy-enhanced data exchange system was suggested by Yin et al.[22] by enabling the data owner to create a random question trapdoor. This suggested technique will allow the cloud to conduct data sharing without collecting any valuable information by leveraging different algorithm and autoencoder pairing procedure to create a sortable database of every data file.Kang et al. used a blockchain-based smart network community technology to accomplish allowed, data sharing in the automotive network edge, and implemented an integrity-based data sharing system that ensures high-quality automotive information exchange.

Chu et al.[23] developed a modern public-key crypto scheme that provided protected data sharing consistent-size ciphertexts that would easily assign decryption privileges to every group of ciphertexts by combining secret keys into a private login. An effective hierarchy attribute-based encryption system in cloud storage was introduced by Wang et al.[24], that merged the authorization node of multiple communication standards into one for different types of health records.Li et al.[25] grouped clients in different security fields in PHR schemes, that will minimize efficient key sophistication to ensure fine-grained and flexible data access protection for operators and consumers.Liu et al suggested an online/offline attribute-based encryption healthcare information exchange mechanism to minimize the expense of encryption in mobile healthcare networks, that conducted much of the offline computing activities, and where electronic medical records are identified, an online step would easily compile the final ciphertext. Any techniques have also recommended hybrid clouds to discharge the task of cryptography into a private cloud. Some suggest hybrid systems for private use. In Paper [26], Dan et al proposedstoring sensitive data on a private cloud and less sensitive data on a public cloud to achieve data elastic properties and leverage over business data.In Paper [27], Li et al implemented a private cloud as a user-to-public cloud gateway, and also maintaining private keys for the access of users in the private cloud.

In brief, current data exchange systems have ignored the effective procurement of healthcare facilities and effective data processing, which are key factors for the beneficial use of health data in e-healthcare systems. It suggests a new effective and privacy-preserving fog-assisted data exchange in e-healthcare systems, benefiting from fog computing hybrid implemented in e-healthcare systems.

3. PROPOSED SYSTEM

The privacy-preserving fog-node health data exchange system is introduced to simply access the collected data in e-healthcare networks to influence health public services and secure data collection with privacy protection. The outline of the proposed method is shown in Figure 2. Next, e-healthcare systems or the patient's manually inputs gather the data integration and the patient encrypts the data access and afterward sends the ciphertext to the fog node. Secondly, the fog node pre-processes, the health data and identifies the health data into different groups of random forest classification after individual risk review, and also lists the health products for various disease risks. At last, the fog node re-encrypts the network resources as per disease threats with an updated access policy and then communicates the ciphertext to cloud servers. After this, the ciphertext is accessed by the network provider with, authorized attributes and decrypted. The corresponding testing methodology of privacy-preserving fog-node health data exchange system: Configuration, KeyGen, Encrypt, PreProcess, Re-Encrypt, and Decrypt.

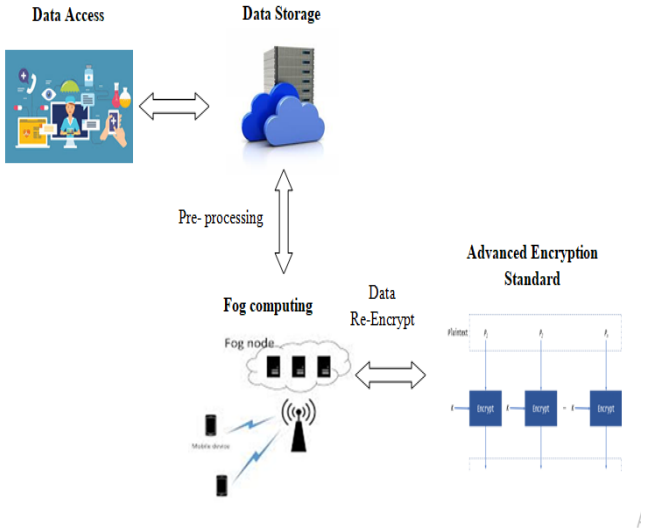

Figure 1. Architecture of the Proposed System

The initial stage of the framework involves Configuration and KeyGen techniques. The group similarly defines the system in this stage and creates keys for the fog node and the provider of the service. The trustworthy authority inserts the attributes I into the scheme as an input. It selects between them two multipliers primary sequence ‘s’ types B and BQ and a bilinear map: B * B →B_Q. The generator of similar group components “b” and “I”; c_1, c_2,…c_i ∈ B, which is correlated in the scheme with standard features I. The attribute collection, i.e., c_1, c_2,…c_i, is general to all providers, but the trustworthy authority does not keep them confidential. They are connected in the scheme to standard characteristics and are components of public keys. Besides that, the trustworthy authority selects a random integer, ρ, t ∈ A_e.The trustworthy authority generates P_K, of the public key and PD_K of the program master key,

P_K = b, b^t, m$(b, b)^{\rho}$, c_1, ……,c_i …… (1)

$PD_K = b^t$ …… (2)

The Trusted Authority uses the KeyGen approach to optimize the service provider's hidden keys. The service provider refers to the trustworthy authority his or her features collection H. The trustworthy opportunity to reveal the MSK framework master key as an input extracts a random f ∈ A_e, and then computes the H_K, private key using the C_K (r ∈ H), public keys related to the service provider's attributes. Here, P_K = (K, K_r), where r ∈ H,

K = b^t, b^{tf}, r ∈ $HK_r = c_r^f b^t$ …… (3)

By using the Advanced Encryption Standard, the shared data is encrypted with a content key. The customer, whereas, encrypts the data key with a personalized access policy for the secure exchange of data. Even with the decryption key and appropriate characteristics, the fog node, cloud storage, and unauthorized service providers could never decode the shared ciphertext, so that privacy-preserving fog-node health data exchange systems may hold shares data secret from the truth but interested fog node and cloud storage. Also,

because the encrypted data is transferred from patients to cloud servers via the fog node via the protected network, privacy-preserving fog-node health data exchange systems avoid data interfering from any unauthorized organizations.

Determination of patient-centric access since the exchange of health data from the two specific dimensions. As shown by his personal preferences, the patient will specify his or her shared data to be viewed by the health service provider. The data sharing encryption key is encrypted with the access treeδ, which contains the access tree T_{tree}, that maintains the patient's access policy developed corresponding to his or her experiences and desires. Just the service provider with characteristics that followsT_{tree}, can fulfill the access tree and receive the access key, just so the customer can choose to access his or her shared data through the service provider that meets his or her unique criteria.

4. PERFORMANCE ANALYSIS

In this article, PPFC performance is evaluated in terms of system cost, storage cost, and energy cost, that are calculated using version 0.3.1 of the RELIC archive for a 256-bit Bareto-Naehrig curve. Since the patient is loaded with different types of e-healthcare equipment, it tests PPFC on two traditional e-healthcare systems: a smartphone and a sensor. In category B_m, let F_m, indicate an exponential function. The primary expense is bilinear processes, so it neglects small variables like arithmetic in A_e. The bytes-length of the item in groupC_i, is denoted by PC_i. Irepresent the set of universal attributes. m indicates the time for paring.F contains the frequency of features in the access structure which could even decrypt the network storage; F_1reflects the number of attributes in the individual access structure; and F_2identifies the number of attributes in the skilled access policy, where $F = F_1 + F_2$. Let $Y = \frac{F_1}{F_2}$, be the ratio of the characteristics of individual power in all control attributes. The number of types of health data on the fog node represents f. Individual performance criteria are chosen from the electronic medical records and database area of Reference [28] that contains technical and personal data of health practitioners, but also individuals, like a hospital, service, years of employment, age, city, and gender. For e-healthcare networks, certain characteristics are generic. As each attribute I is identified bya hi public key in group G before actually being used in costly computations, the encryption evaluation system is not connected to the particular feature. In certain instances, the size of the sample used in each encrypted communication instance, may not exceed 30 [17], so we test the output with up to 50 attributes. To minimize the effect of encryption time and storage expense, as seen in Table 1, it examines the research aspects of PPFC and CP-AES [6] and also illustrates the efficiency of the expense of computing, storage cost, and energy usage as below.

Table 1. An Theoretical Analysis of PPFC and CPAES

Analysis	PPFC	CPAES
Encrypt	✓	✓
Re-Encrypt	✓	
Total Encrypt	✓	✓
Patients Data	✓	✓
Fog Node Data	✓	✓

One encryption and decryption based on democratic processes, one elliptic curve point inclusion procedure, one hash analysis on c_1, several hash tests on c_2, but each set of random data is included in their proposed technique. All of these equations belonging to one entity only, and quantify the user operations in our case. Thus, 3 elliptic curves based on democratic processes, 3 elliptic curve point inclusion services, 3 hash tests on c_1, nine hash tests on c_2, and 3 phases of random data are the cumulative computing value for all key stakeholders collected. We could never quantify the functions of the server component, that's why we have nothing about operating modular division, operating modular multiplication, and operating modular extension. On the healthcare provider and the fog node, in both, we measure the storage cost. The smartphone and sensor computing costs are compared between CP-AES and PPFC, separately, when the feature

percentage is shown in Figure 2 and Figure 3. The encryption time of the smartphone and the device increases with the number of attributes, as seen both in Figure 2 and Figure 3.

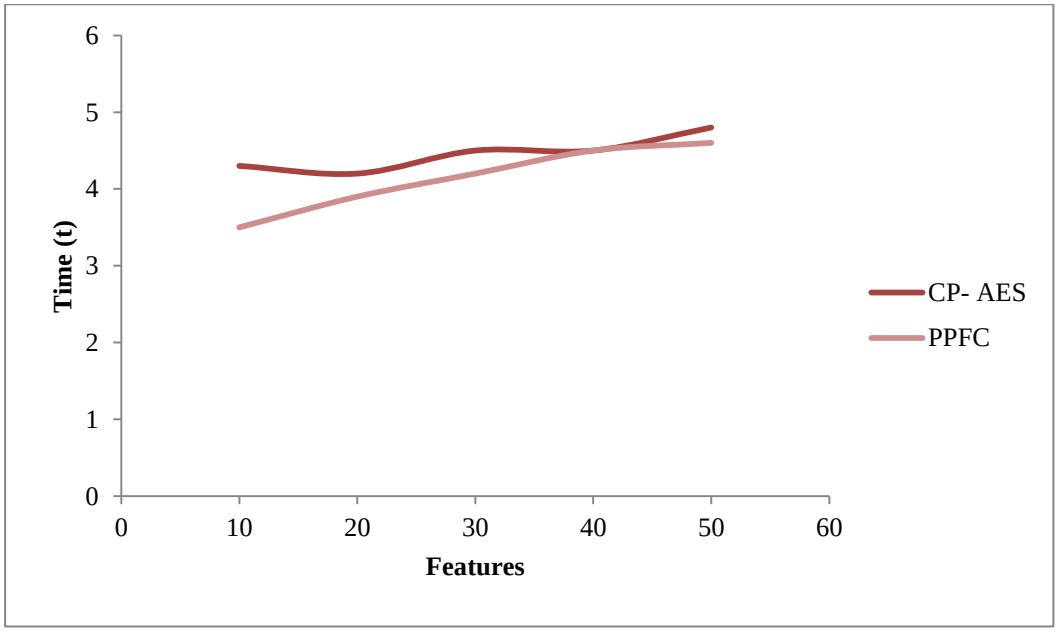

Figure 2. Performance Evaluation on Smartphone using Encryption

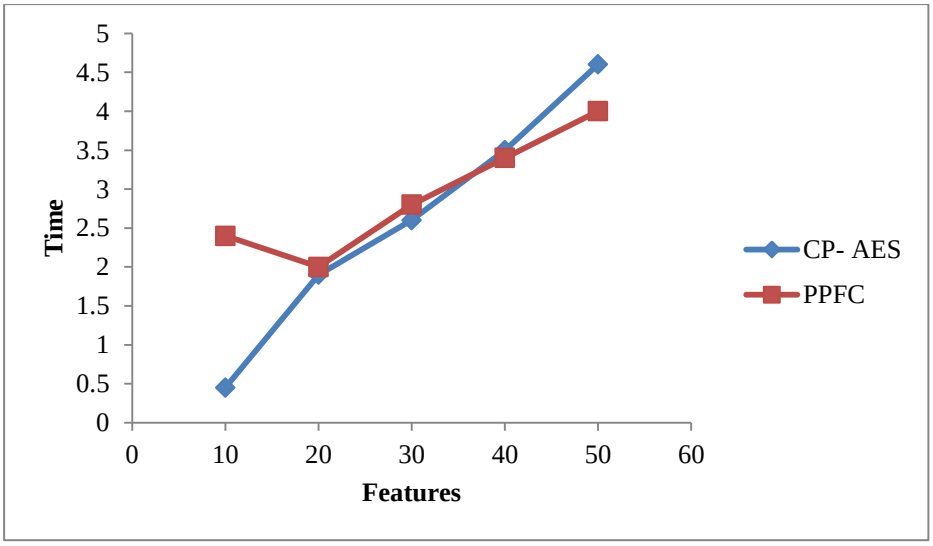

Figure 3. Performance Evaluation on Fog Computing using Encryption

The encryption time on the smartphone and the sensor refers to the number of attributes, as seen in both Figure 4 and Figure 5. Due to the separation of a fog node, no ciphertext processing in CP-AES is required for storage costs on the fog node. The storage costs for the patient defined as the number of attributes, as seen in Figure 4 The encryption time of PPFC at the same set of attributes is less than and inversely proportional to R factors of the encryption time in CP-AES. The storage cost on the fog node and the entire storage cost on CP-AES increase with the set of attributes, as seen in Figure 5. As several disease risk classes are defined in PPFC, the fog node requires additional storage costs, although the total processing costs in CP-AES is constant as disease severity classes improve. The storage cost on the fog node in PPFC is higher than the entire storage cost on CP-AES from both Figure 4 and Figure 5 because the classified shared ciphertext needs considerable storage devices, that is fair and necessary because health data identification providers may achieve successful data usage.

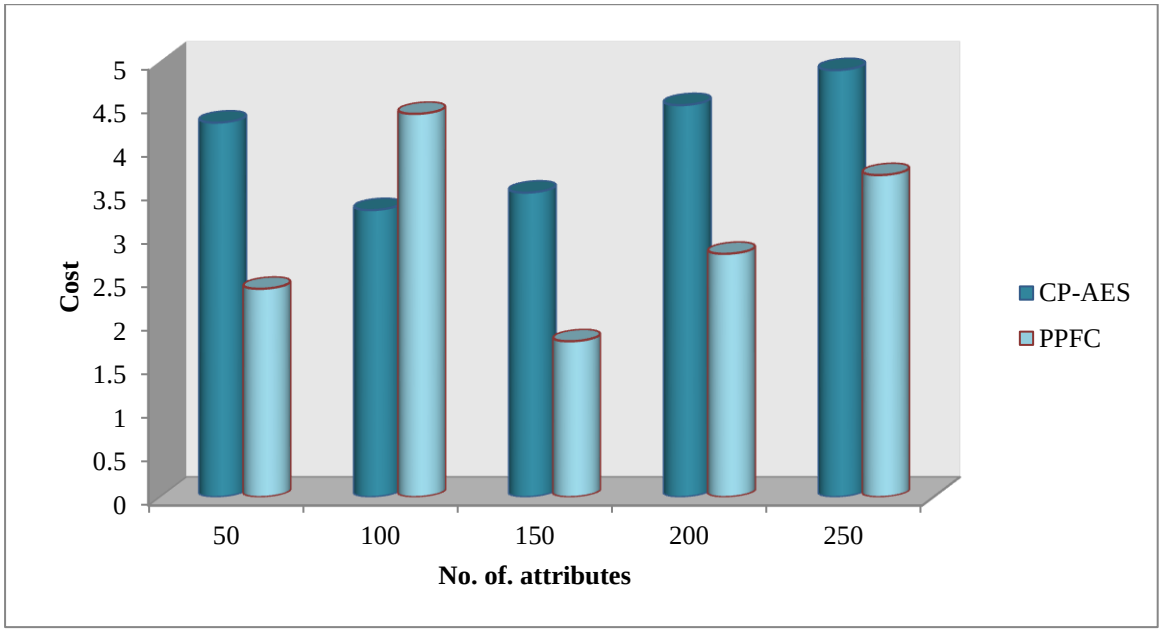

Figure 4. Patients Storage Data Analysis

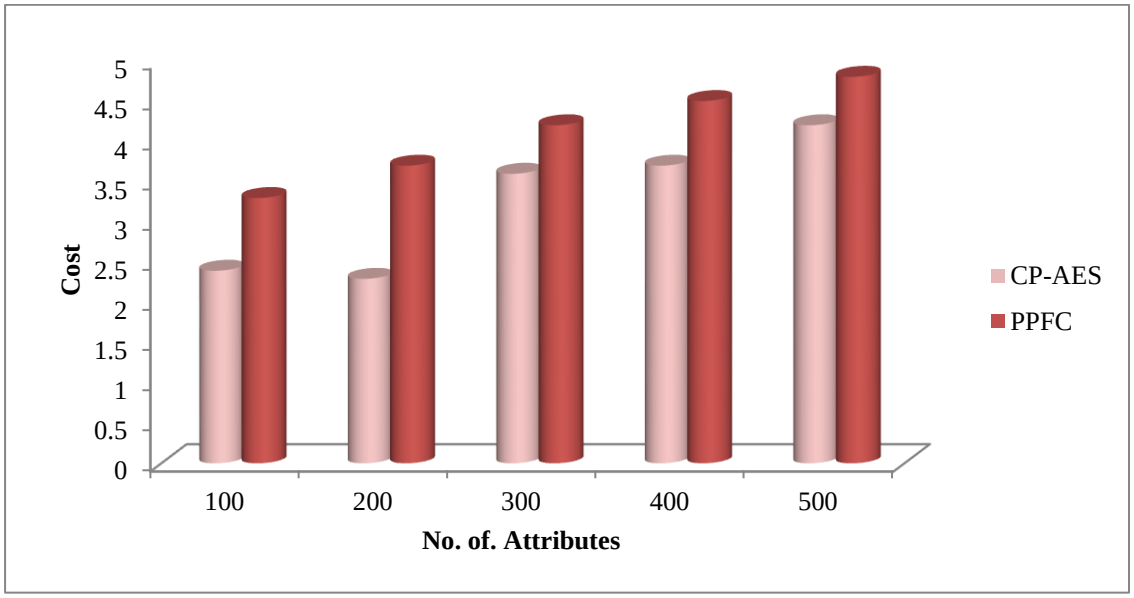

Figure 5. Fog Data Storage Analysis

Energy use, fitted with resource-limited e-healthcare systems, is a big problem for encryption working on the patient. It usesPowerTutor to control energy usage in PPFC by using built-in battery voltage sensors and battery degradation behavior information to determine energy consumption.

5. CONCLUSION

This paper also suggested PPFC that may support the effective distribution of medical services and effective use of data through cost-efficient consumption of resources. First, related to the specialist access policies across the fog node, PPFC facilitates effective health care coverage for patients. Second, by identifying health data into different groups and indexing health risk components, PPFC improves data analysis effectiveness for service providers. Third, below the coordination of the fog node and other organizations, PPFC maintains the integrity of health data and access control for patients during the exchange of health data. Finally, in form of cryptography computing, ciphertext handling, and energy usage, PPFC decreases the capital usage of patients. In future work, during data exchange, it should recognize medical emergencies and include appropriate updating and elimination of access policies.

REFERENCES

[1] Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., &Alamri, A. (2017). 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, 5, 22313-22328.

[2] Liu, W., & Park, E. K. (2014, February). Big data as an e-health service. In 2014 International Conference on Computing, Networking and Communications (ICNC) (pp. 982-988). IEEE.

[3] Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., &Alamri, A. (2015). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Systems Journal, 11(1), 88-95.

[4] Zhang, K., Liang, X., Ni, J., Yang, K., &Shen, X. S. (2016). Exploiting social network to enhance human-to-human infection analysis without privacy leakage. IEEE Transactions on Dependable and Secure Computing, 15(4), 607-620.

[5] Harel, Y., Gal, I. B., &Elovici, Y. (2017). Cyber security and the role of intelligent systems in addressing its challenges.

[6] Waters, B. (2011, March). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In International Workshop on Public Key Cryptography (pp. 53-70). Springer, Berlin, Heidelberg.

[7] Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X., &Luo, H. H. (2015). Security and privacy for mobile healthcare networks: from a quality of protection perspective. IEEE Wireless Communications, 22(4), 104-112.

[8] Wang, S., Zhou, J., Liu, J. K., Yu, J., Chen, J., &Xie, W. (2016). An efficient file hierarchy attribute-based encryption scheme in cloud computing. IEEE Transactions on Information Forensics and Security, 11(6), 1265-1277.

[9] Prasad, A., Liang, X., &Kotz, D. (2014, June). Poster: Balancing disclosure and utility of personal information. In Proceedings of the 12th annual international conference on Mobile systems, applications, and services (pp. 380-381).

[10] Xu, Z., &Stoller, S. D. (2014). Mining attribute-based access control policies. IEEE Transactions on Dependable and Secure Computing, 12(5), 533-545.

[11] Liu, Q., Yan, B. P., Yu, C. M., Zhang, Y. T., & Poon, C. C. (2013). Attenuation of systolic blood pressure and pulse transit time hysteresis during exercise and recovery in cardiovascular patients. IEEE Transactions on Biomedical Engineering, 61(2), 346-352.

[12] Nobles, A. L., Vilankar, K., Wu, H., & Barnes, L. E. (2015, October). Evaluation of data quality of multisite electronic health record data for secondary analysis. In 2015 IEEE International Conference on Big Data (Big Data) (pp. 2612-2620). IEEE.

[13] Xu, C., Ren, J., Zhang, Y., Qin, Z., &Ren, K. (2017). DPPro: Differentially private high-dimensional data release via random projection. IEEE Transactions on Information Forensics and Security, 12(12), 3081-3093.

[14] Ambrosin, M., Conti, M., &Dargahi, T. (2015, May). On the feasibility of attribute-based encryption on smartphone devices. In Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems (pp. 49-54).

[15] Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., &Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, 641-658.

[16] Chen, M., Qian, Y., Chen, J., Hwang, K., Mao, S., & Hu, L. (2016). Privacy protection and intrusion avoidance for cloudlet-based medical data sharing. IEEE transactions on Cloud computing.

[17] Tong, Y., Sun, J., Chow, S. S., & Li, P. (2013, October). Towards auditable cloud-assisted access of encrypted health data. In 2013 IEEE Conference on Communications and Network Security (CNS) (pp. 514-519). IEEE.

[18] Yang, J. J., Li, J. Q., &Niu, Y. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Generation computer systems, 43, 74-86.

[19] Huang, C., Lu, R., Zhu, H., Shao, J., & Lin, X. (2016, May). FSSR: Fine-grained EHRs sharing via similarity-based recommendation in cloud-assisted eHealthcare system. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (pp. 95-106).

[20] Yang, K., Liu, Z., Jia, X., &Shen, X. S. (2016). Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach. IEEE Transactions on Multimedia, 18(5), 940-950.

[21] Shen, J., Zhou, T., Chen, X., Li, J., &Susilo, W. (2017). Anonymous and traceable group data sharing in cloud computing. IEEE Transactions on Information Forensics and Security, 13(4), 912-925.

[22] Yin, H., Qin, Z., Ou, L., & Li, K. (2017). A query privacy-enhanced and secure search scheme over encrypted data in cloud computing. Journal of Computer and System Sciences, 90, 14-27.

[23] Chu, C. K., Chow, S. S., Tzeng, W. G., Zhou, J., & Deng, R. H. (2013). Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE transactions on parallel and distributed systems, 25(2), 468-477.

[24] Wang, S., Zhou, J., Liu, J. K., Yu, J., Chen, J., &Xie, W. (2016). An efficient file hierarchy attribute-based encryption scheme in cloud computing. IEEE Transactions on Information Forensics and Security, 11(6), 1265-1277.

[25] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE transactions on parallel and distributed systems, 24(1), 131-143.

[26] Dobre, D., Viotti, P., &Vukolić, M. (2014, November). Hybris: Robust hybrid cloud storage. In Proceedings of the ACM Symposium on Cloud Computing (pp. 1-14).

[27] Bost, R., Popa, R. A., Tu, S., &Goldwasser, S. (2015, February). Machine learning classification over encrypted data. In NDSS (Vol. 4324, p. 4325).
[28] Dugas, M., Neuhaus, P., Meidt, A., Doods, J., Storck, M., Bruland, P., & Varghese, J. (2016). Portal of medical data models: information infrastructure for medical research and healthcare. Database, 2016.
[29] Tong, Y., Sun, J., Chow, S. S., & Li, P. (2013, October). Towards auditable cloud-assisted access of encrypted health data. In 2013 IEEE Conference on Communications and Network Security (CNS) (pp. 514-519). IEEE.