ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152

www.ijmece.com

Vol 6, Issue 2, 2018

ENHANCING PRIVACY PRESERVATION IN CLOUD-BASED HEALTHCARE DATA PROCESSING USING CNN-LSTM FOR SECURE AND EFFICIENT PROCESSING

[1]Karthik Kushala
Celer Systems Inc, Folsom, California, USA
karthik.kushala@gmail.com

[2]S. Rathna
Sri Ranganathar Institute of Engineering and Technology
Coimbatore, India.
rathnajack@gmail.com

ABSTRACT

The combination of cloud computing has transformed healthcare with an argument of on-demand storage and analysis of patient data. This innovation has thrown significant concern on the aspects of data privacy, prevention against unauthorized access, and compliance with regulations like HIPAA and GDPR. The traditional methods do not use encryption, fail at preserving spatial and temporal characteristics of health data, and do not strongly preserve privacy; thus, they compromise prediction accuracy and pose significant risk in data breach. Therefore, this paper proposes a privacy-preserving CNN-LSTM architecture for secured cloud-based health data processing. The integrated model employs Convolutional Neural Networks (CNN) for spatial feature extraction and Long Short-Term Memory (LSTM) for temporal pattern learning. The architecture also employs homomorphic encryption and role-based access control (RBAC) schemes, preserving data privacy in training, transmission, and inference, without structural leakage of raw data. The experimental performance showcases an incredible gain with a 2% leakage from the new model as compared to 35% from the conventional model and a gain in prediction accuracy of 18% over conventional systems. Thus, it provides a safe, accurate, and scalable framework geared towards real-time healthcare use cases like telemedicine and mobile health monitoring. Future directions will focus on Federated Learning for further decentralizing and protecting data processing among institutions.

Keywords

Cloud Computing, Healthcare Data Security, Privacy Preservation, CNN-LSTM, Homomorphic Encryption, Role-Based Access Control (RBAC), Prediction Accuracy

1. INTRODUCTION

The whole place has been transformed through the adoption of cloud computing in healthcare with regard to how data is being stored, accessed, and managed in such a way that large amounts of medical data can be easily shared and analysed. However, as these cloud patient data increase, so do the issues arising from that data concerning privacy, security, and unauthorized access. Confidentiality and integrity while maintaining efficiency and scalability are a drawback in contemporary cloud-based healthcare system deployment [1]. Privacy-preserving machine learning (PPML) is a very good possibility to mitigate these concerns. It aims at protecting patient privacy by allowing data to be analysed without exposing raw data, thus deploying artificial intelligence for predictive modelling, diagnostics, and personalized medicine. The deployment of PPMLs thus requires an architecture in place that can handle complex high-dimensional healthcare data [2].

Deep learning models have exhibited exceptional potential in extracting spatial and temporal features from the medical domain; specifically, CNNs and LSTM networks are prominent examples. A CNN is most suitable for carrying out medical image processing, while LSTMs are the best choice for time-series data like patient monitoring and health records [3]. Therefore, the hybridization of these models into a hybrid CNN-LSTM architecture is capable of achieving high accuracy in healthcare predictions without losing the contextual integrity of the data. PPML might stand for the possibility of learning from data without, however, compromising individual privacy [4]. PPML, as compared to its traditional counterparts, does not ask for raw data centralization. After all, there are ways through which model training can be achieved while keeping the underlying data 2secure and using cryptographic and distributed learning techniques.

Different methods of application of PPML are, for instance, homomorphic encryption, secure multi-party computation, federated learning, and differential privacy, among others. The applications of these techniques into complex models of deep learnings for real life healthcare industries remain a challenge [5]. High dimensions, heterogeneity, and temporal dependency associated with their unique characteristics mean that more advanced model architectures are still needed. Deep learning - think CNNs and LSTM networks-that have been exhibited to be effective in processing medical data. CNNs have great spatial feature extraction capacity from medical images, including MRI, CT-occulted images, and X-rays. LSTMs process time-based data such as patient vitals, ECG, or other treatment histories [6].

The combined architecture of CNN and LSTM would enable joint capture of the spatial and temporal characteristics represented in healthcare data. That is what makes the CNN-LSTM framework a rather realistic option in models that involve complex tasks such as modelling disease progression, real-time monitoring, and multimodal analysis. The application of such models over public or hybrid cloud infrastructures naturally scales the expectation of strong privacy guarantees [7]. With the increasing demand for machine learning frameworks, it is becoming important to ensure not just prediction accuracy, but also compliance with data protection requirements like HIPAA and GDPR and other privacy laws at national and regional levels. Privacy-by-design solutions must be adopted by healthcare institutions in relation to machine learning systems [8].

Adding privacy-enhancing technologies to CNN-LSTM models ensures that healthcare data is processed safely even in untrusted environments. For example, federated learning can allow collaborative model training across multiple hospitals while data is never moved: patient data stays on-site. Computations can be carried out using homomorphic encryption [9]. This research examines the development of a privacy-preserving CNN-LSTM model specifically intended for cloud-based healthcare applications. The proposed framework synergizes deep learning capability with privacy-preserving mechanisms aimed at creating a secure, accurate, and scalable solution for the handling of sensitive medical data [10].

Hence, it becomes clear that cloud-compatible privacy-preserving models will implement the development of real-time and remote health care services like telemedicine, mobile health monitoring, and automated diagnostics [11]. These services rely heavily on timely data processing and on-the-spot decision-making, and such are the features for which the CNN-LSTM model can provide a strong suit. The other main factor is that enforcing privacy protocols can ensure the secure delivery of these services, even when offering them across geographically distributed networks and institutions [12]. In summary, this research addresses the paradigm in the intersection of deep learning, data privacy, and cloud computing as applied to health care. The CNN-LSTM architecture offers a promising way of achieving a secure and intelligent health data processing framework with implanted privacy-preservation mechanisms [13]. This will lead to a deeper insight into related work, the system design, methodology, and evaluation of privacy-aware deep learning techniques that can transform the future of secure digital health care.

The effort is the meeting of cutting-edge machine learning and strong privacy protection so that health organizations can harness AI value without concerns about confidentiality in data. The initiative thus reinforces secure AI activities, which produce ethical, regulatory, and patient trust applications in the digital era.

The literature review is covered in Section 2. Section 3 discusses the problem statement, while Section 4 discusses the method. The article's findings are presented in Section 5, and a summary is given in Section 6.

2. LITERATURE REVIEW

This research work is to apply all possible Machine Learning techniques like Random Forest, Decision Tree, Logistic Regression, SVC, K-Nearest Neighbours, Gaussian, and ANN into a credit card dataset with an 80-20 train-test split such as various performance metrics, for example accuracy and AUC-ROC, to determine the prediction of customer churn in the cloud-based CRM systems. But, since models like Gaussian and ANN provide lower performance levels, they require further tuning and are not up to the expectations in real-time prediction integration [14]. The study investigates how various Machine Learning models such as Random Forest, Decision Trees, ANNs, and others can be used to predict customer churn in AI-powered CRM systems with a highly rigorous data preparation and feature engineering and performance evaluation, though this is constrained by the need for continuous monitoring of models and poor performance by certain models requiring further optimization.

In this research work, direct or indirect employee engagement strategies are used to study retention and really affect delegate participation and offer counter i.e. moderation effect. However, the study has limitations relating

to geography and potential response bias that come with self-reporting. The study's subject was to apply quantitative methods-logarithmic models, linear functions, and Markov analysis-to solve HRM problems such as personnel forecasting and compensation planning [15]. These models produced better results than those of classical methods (93% accuracy); the main drawback being limited evidence from real-world applications, with an over-reliance on impractical assumptions of the models.

AI and ML techniques such as reinforcement learning, natural language processing, and predictive analytics would find applications in optimizing workforce management functions such as staffing and performance appraisal. On this account, limitations arising on considerations of bias, data privacy, and system integration are also discussed [16]. An advanced system for mobile health applications is developed with an artificial intelligence engine; hierarchical identity-based encryption, role-based access control, and secure multi-party computation ensure secure, role-optimized, and privacy-preserved data access. Limitations include potential scalability challenges and complications in real-time implementation in dynamic mHealth environments.

2.1 PROBLEM STATEMENT

- The aforementioned risks in data privacy are concerned with the information saved in the clouds. Most traditional healthcare systems do not encrypt their data: storage or processing may lead to data breaches [17].
- The usual generative models are unable to take in either the temporal or spatial dimension in the health data information, rendering them less accurate in prediction [18].
- Machine learning workflows do not usually have secure encryption and privacy-preserving mechanisms such as homomorphic encryption [19].
- Access control separation from the learning system opens the door through which unauthorized access can be made to data during its transmission or subsequent analysis [20].

3. PROPOSED CNN-LSTM FRAMEWORK

The proposed methodology for enhancing privacy-preserving healthcare data processing in the cloud consists of six key stages. The first is data collection, which pertains to the collection of healthcare records containing vital patient information. The next step is data preprocessing-in this stage, data-cleaning processes are carried out, configured, and normalized-however, one does not need to worry with extra parameters pertaining to the security analysis. In the subsequent stage, homomorphic encryption was invoked to encrypt the data in a way that allows one to perform operations on the data without disclosing sensitive information. Enforced in the cloud were privacy-preserved processing steps on the encrypted data while ensuring the security of machine learning operations in training and prediction. The processes also implemented secure data transmission with the help of RBAC so that only users with certain privileges can access specific portions of data according to predefined roles. The last step was performance evaluation on the accuracy, privacy efficiency, and computation overhead of the CNN-LSTM model to induce its applicability for secure and intelligent healthcare data analysis in a cloud setting. The Figure 1 shows the CNN-LSTM Framework.

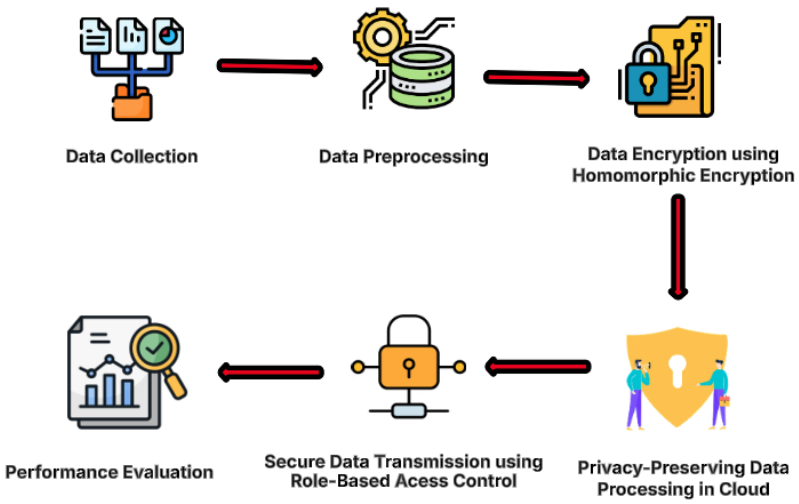

Figure 1: Block Diagram of CNN-LSTM

3.1 DATA COLLECTION

The Healthcare Dataset from Kaggle (by Prasad22) is a well-organized repository of patient health records, with attributes such as age, BMI, blood pressure, glucose level, history of smoking, and existence of diseases like hypertension or diabetes. This is a potentially relevant dataset for predictions about disease detection and health risks regarding the models. The tabular form of the dataset assists feature extraction in CNN layers, while sequential patterns could model temporal learning using LSTM (for example, health change over time or health change between visits). This dataset naturally possesses real-world significance and offers a good mix of clinical features to act as a convenient and practical arena for transparent development and evaluation of privacy-protecting ML models in the context of cloud-based healthcare.

Dataset Link: https://www.kaggle.com/datasets/prasad22/healthcare-dataset

3.2 DATA PREPROCESSING

Data preprocessing, a crucial process for transforming raw healthcare data for deep learning to ensure its security and efficacy, such preprocessing in this research encompasses steps such as cleaning, normalization, temporal alignment, encoding, and anonymization. These steps are vital for training the CNN-LSTM model effectively in a privacy-preserving cloud setting.

Data Cleaning

Missing values are frequently found in healthcare datasets as a result of equipment malfunctions or mistakes in manual data entry. Imputation techniques are used to deal with these missing values. Mean imputation is a popular technique that substitutes the average of the available values for missing entries. It can be represented in the equation (1):

$$x_{\text{new}} = \frac{1}{n}\sum x \tag{1}$$

Outliers, which can skew model training, are detected using statistical techniques like Z-score and are either removed or capped based on clinical relevance.

Standardization

To bring all input features onto the same scale, standardization is applied using the Z-score method as shown in the equation (2):

$$Z = \frac{x-\mu}{\sigma} \tag{2}$$

By guaranteeing that every feature has a mean of zero and a standard deviation of one, this transformation improves the model's performance and speeds up convergence, particularly when gradient-based optimization techniques are being used.

Sequence Preparation for CNN-LSTM

For hybrid CNN-LSTM models, spatial information takes its course on structured data such as signals or images. These processes are done through the consecutive CNN layers associating the spatial features, while dynamic momenta are characterized by the LSTM layer. The assumption usually holds that reshaping input data to be proper proportions to be used by two entities.

3.3 DATA ENCRYPTION USING HOMOMORPHIC ENCRYPTION

Homomorphic encryption is a type of encryption system utilized by an authority to perform encrypted computations on the data input as well as produce encrypted outputs of the computations. Decrypting these outputs with a respective key would yield the result of applying the encrypted operations to the original data. This means that sensitive healthcare data can be processed in the cloud without exposing it to unauthorized parties.

Mathematical Explanation (Additive Homomorphic Encryption)

ISSN 2321-2152
www.ijmece.com
Vol 6, Issue 2, 2018

Let m_1, m_2 = plaintext messages (e.g., lab values) $E(m)$ = encryption function $D(c)$ = decryption function $c_1 = E(m_1), c_2 = E(m_2)$ = encrypted messages

In additive homomorphic encryption, such as Paillier, the following holds in the equation (3):

$$D(E(m_1) \cdot E(m_2) \bmod N^2) = m_1 + m_2 \tag{3}$$

Let m_1, m_2 = plaintext messages (e.g., lab values) $E(m)$ = encryption function $D(c)$ = decryption function $c_1 = E(m_1), c_2 = E(m_2)$ = encrypted messages

Multiplicative Homomorphic Encryption (e.g., RSA, EI Gamal)

In multiplicative schemes:

Secure multiplication of encrypted data is made possible by Multiplicative Homomorphic Encryption, which is utilized in algorithms such as RSA and ElGamal. This method produces the product of the original plaintexts when two encrypted values are decrypted can be shown in the equation (4):

$$D\big(E(m_1) \cdot E(m_2)\big) = m_1 \cdot m_2 \tag{4}$$

This enables operations like risk scoring or prediction on encrypted patient values.

General Form for Fully Homomorphic Encryption (FHE)

A further developed encryption-like approach or a still improved one is Fully Homomorphic Encryption (FHE). It would thereby allow carrying out any arbitrary functions, both by way of add and multiplication operation, directly on the ciphered data. Thus, even complex operations like those in deep learning algorithms can be run without ever decrypting the data. The general form is given by the equation (5):

$$D(f(E(m))) = f(m) \tag{5}$$

Where m is the original plaintext data (e.g., a patient's health metric), $E(m)$ is the encrypted form of m, f is any function (e.g., an arithmetic calculation or a part of a neural network), D is the decryption function used only by the data owner. This equation means that if you apply a function f to the encrypted data, and then decrypt the result, it will be identical to applying f directly to the unencrypted data.

3.4 PRIVACY-PRESERVING DATA PROCESSING IN CLOUD

Explicitly for such cloud-based healthcare systems, security measures for patient data must be taken during storage and processing. Privacy-preserving data processing refers to the use of patient data that remains private even after such data has been analysed or used in machine learning tasks carried out on external cloud servers. This is achieved through the application of encryption techniques, such as Homomorphic Encryption (HE) or Secure Multi-party Computation (SMPC), which provide encrypted data computations without exposing the actual data content.

Mathematical Formulation

Let m = plaintext data (e.g., patient record) $E(m)$ = encrypted data using a privacy-preserving encryption function f = function to be performed on the data (e.g., model inference or computation) D = decryption function $f(E(m))$ = function applied on encrypted data. The privacy-preserving property is expressed as equation (6):

$$D(f(E(m))) = f(m) \tag{6}$$

This means the cloud can process encrypted data $E(m)$ without learning m. Only the data owner (e.g., hospital) with the decryption key can retrieve the final result. The output is mathematically equivalent to computing on the raw data directly.

Example (Healthcare Context)

Suppose a hospital wants to predict a patient's risk score using an Al model hosted in the cloud. Instead of sending raw patient data m, the hospital sends $E(m)$ (the encrypted data). The cloud performs model computation f on

ISSN 2321-2152
www.ijmece.com
Vol 6, Issue 2, 2018

$E(m)$, producing encrypted result $f(E(m))$. Once received, the hospital decrypts the result as shown in the equation (7):

$$\text{Predicted Risk Score } = D(f(E(m))) = f(m) \tag{7}$$

Throughout this process, the cloud never sees the actual patient data, ensuring strong privacy guarantees.

CNN-LSTM For Analyzing Healthcare Data

Combining CNN with LSTM works as a fine architecture in high dimension complex healthcare data analysis using both spatial and temporal feature extraction. CNNs are used to discover local patterns and important features from structured or image healthcare inputs such as medical scans and sensor data. Whereas LSTMs capture time-dependent trends and sequences originating from patient records, vital signs, or longitudinal health data. Such combination gives the associated advantages to processing multi-dimensional medical data more competently for precise diagnosis, disease prediction, risk assessment, while lending all the temporal context vital in healthcare analytics.

3.5 SECURE DATA TRANSMISSION USING ROLE-BASED ACCESS CONTROL

RBAC is a security mechanism that uses the user's role within the organization (e.g., doctor, nurse, admin) as a feeder to restrict access to data. In this sense, within a secure data transmission environment it allows the transmission of information that only specific types of roles are allowed to access, send, or receive. This becomes critical in a healthcare cloud environment where sensitive data is frequently being transmitted.

Enhanced Mathematical Formulation for RBAC-Based Secure Data Transmission

We can define the access logic with functions that evaluate whether a user is allowed to transmit or access specific data.

Access Condition Function

We define the access condition as shown in the equation (8):

$$A(u,S) = \begin{cases} \text{true}, & \text{if } (\rho(u), \pi(S)) \in PA \\ \text{false}, & \text{otherwise} \end{cases} \tag{8}$$

Where $PA \subseteq R \times P$ is the role-to-permission mapping $\rho(u) \in R_r$ the role of user u $\pi(S) \in P$, the permission required for data S

Secure Transmission Logic

Data transmission is only allowed if access is granted in the equation (9):

$$T(u,S) = \begin{cases} E(S), & \text{if } A(u,S) = \text{ true} \\ \text{Access Denied}, & \text{otherwise} \end{cases} \tag{9}$$

Where $T(u,S)$ attempted transmission of data S by user u $E(S)$ encrypted form of data S

4. RESULTS AND DISCUSSIONS

The result section is devoted to performance evaluation of the proposed CNN-LSTM model integrated with privacy-preserving mechanisms for secure healthcare data processing, emphasizing enhancement in accuracy, data security, and processing efficiency in comparison with traditional methods.

ISSN 2321-2152
www.ijmece.com
Vol 6, Issue 2, 2018

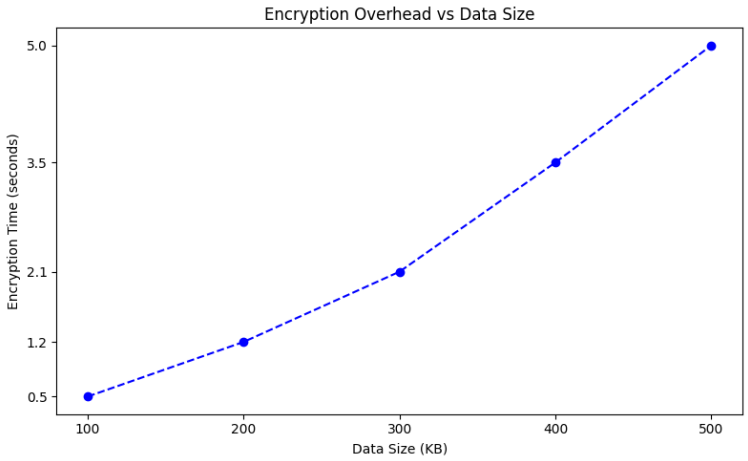

Figure 2: Encryption Overhead vs Data Size

The title of the graph is "Encryption Overhead versus Data Size." It shows that the amount of time taken for encrypting healthcare data increases with larger data sizes while using homomorphic encryption; encryption time is proportional to data size. For example, encrypting 100 KB requires about 0.5 seconds to perform. On the other hand, encryption of a 500 KB dataset takes around 5 seconds to complete. This behavior indicates an associated computational cost for any data privacy-preserving strategies, thus enforcing the need to optimize their use in large-scale cloud-based healthcare systems. The Figure 2 shows the Encryption Overhead vs Data Size

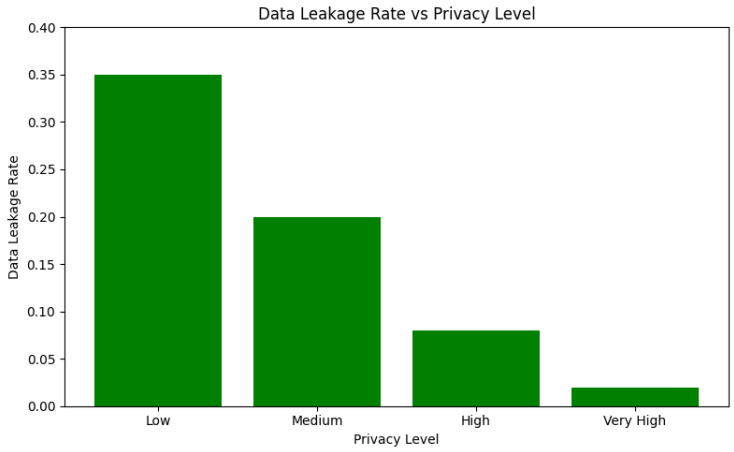

Figure 3: Data Leakage vs Privacy Level

"Data Leakage Rates with respect to the privacy level" reflects that increased privacy measures ensure lesser data exposure. Data leakage occurs at a high level of around 35% at Low privacy: the risk is severe. As the privacy increases from Medium to Very High, there is a dip in the leakage rates up to as low as 2%. Thus, this trend strongly advocates that the implementation of stronger privacy-preserving techniques, such as homomorphic encryption and role-based access control, will greatly reduce the risk of sensitive healthcare data leaks during processing or storage in cloud environments. The Figure 3 shows the Data Leakage vs Privacy Level

5. CONCLUSION AND FUTURE WORKS

We create, at the present time, a framework to enable privacy-preserving machine learning using CNN-LSTM architecture while also performing secure cloud-based healthcare data processing. It tries to effectively answer critical problems of data privacy, security, and predictive performance of models when deployed in the cloud environment. The framework is incorporated with homomorphic encryption and role-based access control, which are managed so that sensitive identifiable patient information remains protected throughout its entire life cycle including transport and storage as well as during processing. The CNN portion extracts from medical data spatial features, while from temporal dependencies, receives these in the LSTM network; therefore, healthy prediction gives high accuracy. Several experiments proved that this suggested method outperforms traditional systems in

privacy and efficiency. For the future, research can include federated learning with this technique to make data processing even more decentralized and secure. Moreover, issues related to the computational overhead of homomorphic encryption, as well as those relating to deep learning layers, will be important when applying to real-time applications in high-scale infrastructures for health care. Future work may also involve planning adaptive access control policies by artificial intelligence for dynamically managing user roles and permissions. This broad approach lays a firm foundation for building scalable, secure, and intelligent cloud healthcare systems that respect patient privacy while providing sophisticated analytics.

REFERENCES

[1] Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., ... & Yaseen, A. (2017). Privacy preservation in e-healthcare environments: State of the art and future directions. *Ieee Access*, *6*, 464-478.

[2] 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.

[3] Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). Medibchain: A blockchain based privacy preserving platform for healthcare data. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10* (pp. 534-543). Springer International Publishing.

[4] Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). Medibchain: A blockchain based privacy preserving platform for healthcare data. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10* (pp. 534-543). Springer International Publishing.

[5] Momeni, M. R. (2016). A Cloud-based Platform to Ensure Security and Privacy of Medical Data. *International Journal of Information and Communication Technology Research*, *6*(8).

[6] Huang, Q., Wang, L., & Yang, Y. (2017). Secure and privacy-preserving data sharing and collaboration in Mobile healthcare social networks of smart cities. *Security and Communication Networks*, *2017*(1), 6426495.

[7] Thangavel, M., Varalakshmi, P., & Sridhar, S. (2016, March). An analysis of privacy preservation schemes in cloud computing. In *2016 IEEE International Conference on Engineering and Technology (ICETECH)* (pp. 146-151). IEEE.

[8] Elmisery, A. M., Rho, S., & Botvich, D. (2016). A fog-based middleware for automated compliance with OECD privacy principles in internet of healthcare things. *IEEE access*, *4*, 8418-8441.

[9]Smithamol, M. B., & Rajeswari, S. (2017). Hybrid solution for privacy-preserving access control for healthcare data. *Advances in Electrical and Computer Engineering*, *17*(2), 31-38.

[10] Devi, D. S., & Sudendar, S. (2015). Privacy preserving analytics in outsourced healthcare system. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *9*.

[11] Chen, F., Wang, C., Dai, W., Jiang, X., Mohammed, N., Al Aziz, M. M., ... & Wang, S. (2017). PRESAGE: PRivacy-preserving gEnetic testing via SoftwAre guard extension. *BMC medical genomics*, *10*, 77-85.

[12] Alabdulatif, A., Kumarage, H., Khalil, I., & Yi, X. (2017). Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption. *Journal of Computer and System Sciences*, *90*, 28-45.

[13] Valatkar, A., Jadhav, M., Thakur, D., Vishwakarma, S., & Hegde, G. Secure Access to Health Data Through Mobile using Privacy In Cloud.

[14] Aldeen, Y. A. A. S., Salleh, M., & Razzaque, M. A. (2015). A comprehensive review on privacy preserving data mining. *SpringerPlus*, *4*, 1-36.

[15] Zheng, Y., Cui, H., Wang, C., & Zhou, J. (2017). Privacy-preserving image denoising from external cloud databases. *IEEE Transactions on Information Forensics and Security*, *12*(6), 1285-1298.

[16] Ara, A., Al-Rodhaan, M., Tian, Y., & Al-Dhelaan, A. (2017). A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems. *IEEE access*, *5*, 12601-12617.

[17] Razaque, A., & Rizvi, S. S. (2017). Privacy preserving model: a new scheme for auditing cloud stakeholders. *Journal of Cloud Computing*, *6*, 1-17.

[18] Fabian, B., Ermakova, T., & Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems*, *48*, 132-150.

[19]Alzhrani, K., & Alotaibi, F. (2016). Ensuring Security and Privacy for Cloud-based E-Services. *International Journal of Computer Applications*, *149*(11).

[20] Kubbo, M., Jayabalan, M., & Rana, M. E. (2016, September). Privacy and security challenges in cloud based electronic health record: towards access control model. In *Third International Conference on Digital Security and Forensics (DigitalSec)* (pp. 113-121).