Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.027949
Article

Tech Science Press

Multi Attribute Case Based Privacy-preserving for Healthcare Transactional Data Using Cryptography

K. Saranya[*] and K. Premalatha

Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, 638401, India
*Corresponding Author: K. Saranya. Email: saranyakbit@gmail.com

Received: 29 January 2022; Accepted: 07 March 2022

Abstract: Medical data mining has become an essential task in healthcare sector to secure the personal and medical data of patients using privacy policy. In this background, several authentication and accessibility issues emerge with an intention to protect the sensitive details of the patients over getting published in open domain. To solve this problem, Multi Attribute Case based Privacy Preservation (MACPP) technique is proposed in this study to enhance the security of privacy-preserving data. Private information can be any attribute information which is categorized as sensitive logs in a patient's records. The semantic relation between transactional patient records and access rights is estimated based on the mean average value to distinguish sensitive and non-sensitive information. In addition to this, crypto hidden policy is also applied here to encrypt the sensitive data through symmetric standard key log verification that protects the personalized sensitive information. Further, linear integrity verification provides authentication rights to verify the data, improves the performance of privacy preserving technique against intruders and assures high security in healthcare setting.

Keywords: Privacy-preserving; crypto policy; medical data mining; integrity and verification; personalized records; cryptography

1 Introduction

Personal health information system is an important paradigm in healthcare industry that collects and stores the patient data including sensitive information like demographic data, medical history, diagnostic codes, treatment plans, lab records, insurance information, immune dates, allergies, etc. [1]. Privacy preservation in medical healthcare data has gained much attention in the recent years, especially information mining analysis in big data analysis play an important role for healthcare decisions. Healthcare industry generates huge volumes of medical data which should be analyzed with caution, as the number of patterns to be processed are high. Further, this healthcare data contains both sensitive and non-sensitive information in both structured and non-structured format. So, information access during any transactions pose severe threats to individual's data security in health care industry. Most of the patients have records, directed from hospitals, and it contains their Personal Health Information (PHI) which are used before treating a person. In this context, Personal Health Information (PHI) of a patient is shared among different departments of a hospital namely, pharmacy, lab, consulting, admin etc. Such medical records contain sensitive information with regard to the patients' medical history. The chances for this information to be misused by anonymous intruders are extremely high. Private information leakage issue leads to information theft from patient's records or any other healthcare related documents. A patient's privacy and data security is breached when their healthcare data is shared without proper channel. So there is a need exists to develop a viable way that balances both healthcare data sharing as well as privacy protection [2]. In this study, a new privacy preserving framework is to be designed in the form of attribute-based protection using crypto analysis. This framework is developed for healthcare conditions and manages raw transaction datasets. A multi-attribute based protection policy is proposed using crypto policy standard to protect the raw data from segregating sensitive attributes which restrict unauthorized access and gives reverse hidden crypto policy to protect the sensitive information. This leads to the protection of sensitive medical information which is an important milestone in privacy preserving data policy.

Few privacy-preserving methods exist with an aim to protect the appropriate information of patients, while at the same time, it also maintains their private information including healthcare details. To accomplish this aim, a large number of privacy-preserving models is proposed to hide the sensitive information from public setting. Such Privacy-Preserving Data Publishing (PPDP) models are utilized to secure different types of information including socioeconomics and analysis codes with an expectation to keep the dangers of character disclosures such as trait disc1osure and enrollment disclosure as shown in Fig. 1. Further, the privacy methods have evolved with another meaning of privacy called 'k secrecy' which roughly translates into verified access from utility access logs. Being a namelessness demonstrate, it provides structure to the calculation whereas the frameworks disseminate the information, after anonymization. It secures the information that correlates to a specific substance. It principally keeps the private data away from linkage assault. Namelessness is accomplished by leveraging both concealment and speculation.

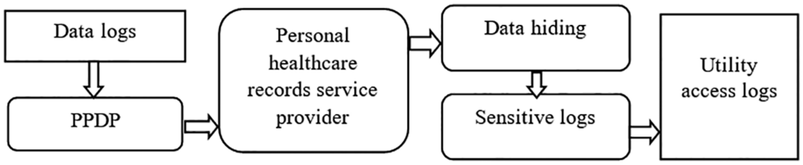

Figure 1: Privacy preserving process in EHR

Most healthcare industry processes directly make use of data about patient's healthcare information without any protection. The industries do not concentrate on the influence of attacks upon sensitive information. In this scenario, outsider access becomes sophisticated and data access becomes easy. Otherwise, encryption policy is commonly employed to unhide or hide the whole data. The attribute case is non-violent against healthcare sensitive information and so the access restriction becomes an important element to verify the log of authentication.

When the personalized medical information is separated as attributes in the form of sensitive and non-sensitive patient's records, it specifies the existence of highly confidential and classified sensitive information. Medical reports contain the personal information of patients in unstructured formats. It contains critical information of the patient and their caretakers such as names, telephone numbers, locality, age and furthermore the points of sicknesses.

The medical records contain the original information, directed from hospital records, based on the diagnosed information. So, the data records must be open access for anyone to read the information. The sensitive information, which are non-secure in nature, contains various types of personalized information. The information from patients include general details of the patient like name, phone number and address while these data are not sensitive in nature than the treatment and disease facts.

For example, DNA sample and drugs intake levels are sensitive information in a case record of a patient. This medical record includes the patient's original drug details and if it is accessed by the hackers through unreasonable approaches, they may exploit the data to enhance their business interests and continue to do so. However, -crypto based hidden policy hides the sensitive information excluding authorized person who possess rights to access and ensure key authentication to access the data.

With the implementation of the proposed crypto policy, the patient's information logs in healthcare industry get high security. This can be achieved by improving privacy preserving framework in the form of provable privacy security policy. During the implementation of this policy, verifiable resources are verified which contain attributes that are highly sensitive and insensitive information that does not affect the transactions done in healthcare domain, by maintaining the privacy of the patient. Masking identifiers specify the sensitive information of suffix hidden crypto encryption standard that maintains the individual records of the patient.

2 Literature Survey

Privacy preserving approach is an important technique to secure the personalized data and privacy information of individuals. This is applicable especially in case of healthcare details of the patients [3]. Though most of the privacy preserving techniques secure personalized information and are difficult to use the differential security to control information, these techniques fail in hiding private data as sensitive information. So healthcare data and the information of patients get distributed freely. This sensitive data gets uncovered which is an essential issue to be overcome. One of the data privacy protection techniques called k-namelessness is implemented based on crypto policy. In k-anonym zed dataset [4], each record is undefined from any rate whereas k −1 possesses different records regarding certain unique traits that depend upon the hiding principle.

Anonymization of restorative records is of extraordinary significance in healthcare domain, since uniform content can be easily accessible. This data about personal information of patients, accessed from healthcare specialist's records, can be protected based on Machine Learning approach named Principle Component Analysis (PCA) [5]. This is inclusive of bouncing the vulnerability of the calculated relapse and annoying the scholarly classifier with clamor that corresponds to the vulnerability [6]. When considering this approach, there are constraints present in it, when connected with other machine learning approaches. At that point, another privacy protection robust reversible calculation algorithm is discussed [7]. The proposed Scheme Against Global Eavesdropping (SAGE) can accomplish both security and provide relevant protection against global attackers. Privacy Preserving Data Publishing (PPDP) has a lot of strategies and devices to disseminate valuable data while safeguarding the information. The novel study is conducted to reveal how regression and correlation analysis can be performed on vertically-divided data using Locality Sensitive Hashing (LSH) approach [8]. As of late, PPDP has got impressive track record to look into groups, and numerous methodologies have been proposed for different types of information dissemination scenarios [9]. This sort of prerequisite is considerably harder to be addressed for dynamic and expansive scale joint efforts. Here, the quantity of access control approaches are huge in nature for both dissemination and exploration of the data [10]. In literature, Internet of Things (IoT) has been proposed to reconcile the activities that assess the application of strategies in health care applications [11].

In literature, the researchers investigated the necessities of a correspondence structure brought together from different individual entities. This study broke down the storyline based on a day in Robert's life. In the study conducted earlier [12], Secure Personal health information Sharing (SPS) was proposed which envelops personality-based cryptography to guarantee security and privacy of PHI by utilizing short advanced signature and pseudo-identity of the patient [13]. SPS reduces the burden of Health Service Provider (HSP) in terms of PHI stockpiling and administration. Further, it also supports the same by joining distributed storage administrations to electronic Health (eHealth) mind framework [14]. PHR is a sort of wellbeing record recorded and maintained by both patient and the healthcare professionals. A perfectly-maintained individual healthcare record can provide therapeutic data of the patient from various sources and help in decision making for the patient's wellbeing [15,16]. The medicinal synopsis from PHR can be accessed through Internet or other such media when there is a necessity for security and privacy.

From healthcare data security perspective, healthcare data is processed through Mobile Healthcare Networks (MHN) which needs support so that the quality of access verification can be enhanced. Further, a few countermeasures can also be taken for security and privacy assurance in MHNs including privacy-preserving healthcare information integration [17], preparation of secure healthcare information, and troubles in recognizing the information. Fine-Grained and versatile information reach the control plot in light of Attribute Based Encryption (ABE). Furthermore, PHI sharing approaches might be sensitive [18] and may uncover data about hidden PHI or information senders or recipients [19]. In current study, each characteristic is allowed to have a property name along with pride. Further, it is allowed to embrace the Bloom channel to check the traits before decryption efficiently. A certifiable and unavoidable health monitoring application (inescapable fall recognition for stroke alleviation) is developed to show the adequacy and viability of haze registered across the globe in wellbeing monitoring [20]. The author proposes an Adaptive Private Security (APS) algorithm to protect the sensitive information in healthcare industry [21,22].

3 Multi Attribute Case-Based Privacy Preservation Scheme

The healthcare processes contain sufficient security resource to carry out the protection of personalized data so as to safeguard the privacy information of patients. Conventional medical data is huge in quantity while the personal information cannot be easily mined out by product developers. Hence, the current study proposes to privacy-preserving the sensitive data from patent logs using Multi Attribute Case Based Privacy Preservation (MACPP). This is proposed for the purpose of improving the security of patient data. Healthcare information is viewed as an extremely critical aspect in today's world. Such data must be handled in a sensitive manner using advanced techniques since the patient's personal information are at risk. When such data is distributed without any inhibition, the data becomes defenseless against any types of attacks. Numerous methods have been proposed earlier to safeguard the privacy of healthcare information. In current research work, a review of the models and systems proposed earlier is shown while these models are used for distributing information about patients.

In this method, preprocessing is the first step to clean the raw data from medical dataset collection. Each transaction from the medical records contains different types of sensitive information in terms of drugs. So, this healthcare information should be accessed both on a private and general level. But the usage of personal medical information is different from general information of the patient. This should be understood finely to distinguish the sensitive information and protect it through hidden policy. Such sensitive data should be represented on raw conditions themselves which need privacy protection to be accessed by unauthorized persons.

The personal data collected from patients are always in raw state and can be segregated based on sensitive attributes from patient's records. Based on these values, the mean value of average is determined for both descriptive sensitive and non-sensitive data as shown in Fig. 2. The average counts find the weightage factors for highly sensitive drug usage of the patients to use service level encryption standard that can hide the data. Finally, the linear integrity verifies the privacy terms against a user's key validation to prove the security.

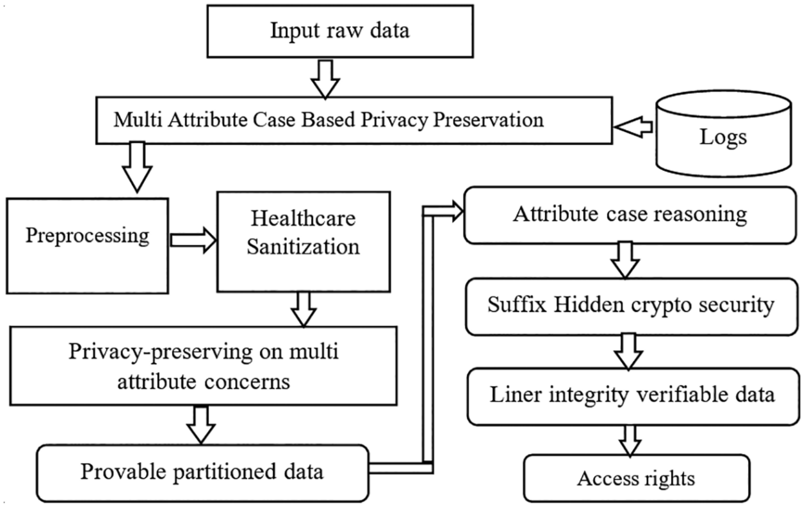
Input raw data
Multi Attribute Case Based Privacy Preservation
Logs
Preprocessing
Healthcare Sanitization
Privacy-preserving on multi attribute concerns
Provable partitioned data
Attribute case reasoning
Suffix Hidden crypto security
Liner integrity verifiable data
Access rights

Figure 2: Architecture of multi attribute case based privacy preservation

- Security and Privacy in Data Mining

Privacy is regularly characterized as a condition in which the sensitive information is secured by any means. It focuses on the utilization and administration of a person's personal information like making arrangements and setting up approval prerequisites so that the patient's personal information is gathered, shared and used in appropriate ways. By improving the security principles, the information can be partitioned in which the personalized information gets different access from general information that can be accessed by those only who has authorization. It focuses on shielding the information for authentication processes and taking information for a benefit by an authenticated person. In spite of the fact that security is imperative to ensure the information is safe, the privacy still lacks.

- Objective consideration

From the proposal, it can be considered to apply data separation based on provable partition crypto techniques so that privacy can be preserved in classifying medical data. The authors considered two approaches to ensure privacy such as vertical partition and horizontal partition. In vertical partition approach, each site utilizes a segment of credits to register its outcomes. Followed by, the appropriate outcomes are collected at a focal point which gathers huge amount of outfit strategy. In horizontal partition approach, the information is conveyed among a few locales. Each site processes a particular information and a focal trust gathers information about these outcomes.

3.1 Preprocessing Medical Datasets

Across the healthcare institutions, medical data sets are collected in the form of raw data so as to maintain the patient log. The information collected in hospitals form records with attributes that contain patient's information, drugs, suggestions and consent forms. The unavoidable yet unnecessary information is called as noise since it interrupts the information that provides much insights about the patient's health history. The attributes are nonlinear in its raw stages since it is yet to be pre-processed.

Since empty fields bring noise to the analysis, record omission is carried out so that the important records are not avoided. Further, distinct outliers from medical data records are removed.

Tab. 1 demonstrates the preprocessed dataset out of raw pharm medical. This dataset contains information on patient id, name, age, mobile number, diagnose and drugs name & dose.

Table 1: Raw pharm medical preprocessed dataset

Medical dataset attribute case process from pharm-medical raw records											
Hospital number	Patient Id	Patient name	Age	Postcode	Diagnose	Mob number	Drugs				
							Sancol	MMF	Livgen	Parctml	Misopro
KMS1	1	Raja	24	635234	Arteries	9987876	40 mg	150 mg	35 mg	50 mg	Nil
KMS2	2	Devi	26	635124	H1N1	9987453	24 mg	10 mg	20 mg	100 mg	1 mg
KMS3	3	Kumar	28	636113	Dialysis	8976254	10 mg	20 mg	80 mg	10 mg	Nil

Algorithm

```
Step 1: Input raw data Rd {rd1,rd2,…rdn}
For each rd (record set←Rs)
    Check is Empty == NULL
      Fill attribute Ac == nill to Rd
End for
Step 2: check distinct data Dt
      For each attribute Dti in the data set
          While (mismatch attribute (Ac) == Rd)
          Remove record set from rd
      Do
    End for
Step 3: check numeric and non-numeric validated attributes fields
If Rd is a numeric attribute
         Then hold discretize or eliminate the attribute;
           If Rd is a non-numeric attribute Then
                  Hold Values ←rd
Else
       Remove the non-matched noise value
    End if
End if
Step 4: keep raw data originate all fill case record fields
Step 5: validation checks for ordered records
```

The above algorithm clears the raw data (Rs), which was collected as data without any outliers. to form distinct values from sensitive and non-sensitive information. Preprocessing narrows the raw data from a conventional approach in which each record is considered as an attribute while empty case are taken as Null field to reduce the dimension and simplify the privacy principle process.

3.2 Multi Attribute Case Reasoning

The attributes are measured to ensure data dependency and segregate the transactional data as sensitive and non-sensitive attributes. The verified category of sensitive case attributes is different from standard attribute case, for example, the paramedical counts from normal patients differ from other high-risk patients. So, the physicians prescribe drugs with highly sensitive information to treat the patients. In this point of view, privacy concerns arise due to the involvement of high sensitive data. This considers multiple attributes based on the relation between drug and diagnosed disease condition, and compound molecule pattern to process the reasoning principle and protect the data. The provable partition differentiates the sensitive attributes with differential count measure of other drug average mean values.

The raw attribute is obtained from a confidential list which has a cross mean value of drug representation to combine the records as shown in Tab. 2.

Table 2: Raw attribute values

Medical dataset attribute case process from pharm-medical raw records											
Hospital number	Non sensitive attribute			Sensitive attribute							
	Patient Id	Patient name	Post code	Age	Diagnose	Mob number	Sancol	MMF	Livgen	Parctml	Misopro
KMS1	1	Raja	635234	24	Arteries	9987876	40 mg	150 mg	35 mg	50 mg	Nil
KMS2	2	Devi	635124	26	H1N1	9987453	24 mg	10 mg	20 mg	100 mg	1 mg
KMS3	3	Kumar	636113	28	Dialysis	8976254	10 mg	20 mg	80 mg	10 mg	Nil

Algorithm

```
Input: preprocessing dataset Dt
Output: portioned category non-sensitive and sensitive
Step 1: Data Dt initialization attribute set Dt→At
Step 2: For attribute At→no sensitive attribute list.
        Find sensitive terms mean value.
Mn = $m \sum_{i}^{n=0} asensitiveattributeidentityfromlist$Attribute
            For each Cl→At mean value
        Average margin rate Cl = $\int_{i=1}^{N} \sum (Ai(Dtmax) - Ai(Dtmin))2$
            End
            Add sensitive list St
        End
Step 3: Identify relative closeness of attribute similarity
        At → for each case attribute
```

(Continued)

Algorithm (continued)

```
            Mean count SC = $\int_{i=1}^{N} \sum Dt(At) \geq marginalvalue$
        End
          Identify the patronal semantic closeness attribute list Ati← dt
End
```

The above algorithm splits the attributes into sensitive (Si) and non-sensitive (Nsi) based on results of relative mean analyses obtained from sensitive factors.

3.3 Hidden Crypto Security Analysis

In this stage, privacy principles verify the nature of outsourced data based on access principle so that cryptographic principle can be applied. This makes the sensitive information safer and its fortunes of privacy information cannot be misused. So, the suffix patterns are hidden to encrypt the data. In healthcare industry, patient's private information is highly important since it involves drugs and prescriptions that are hidden based on specified principles and access rights. The hidden crypto policy encrypts the sensitive information from logical suffix representation of each attribute. In records, it can be reversed to hide the information with specific characters using symmetric key verification standards.

The sensitive attribute enriches the least maximum of suffix value and secures the information from unauthorized access. Tab. 3 shows the suffix hidden crypto policy for personal health information which is divided into sensitive and non-sensitive attributes.

Table 3: Suffix hidden crypto policy

Medical data set attribute case process from pharm-medical Raw records												
Hospital number	Non sensitive attribute			Sensitive attribute								
	Patient Id	Patient name	Post code	Age	Gender	Diagnose	Mob number	Sancol	MMF	Livgen	Parctml	Misopro
KMS1	1	Raja	635234	XX	*	Arteries	998XXX	40X	**	**	50XX	-
KMS2	2	Devi	635124	XX	*	H1N1	998XXX	24X	**	**	10XX	**
KMS3	3	Kumar	636113	XX	*	Dialysis	897XXX	10X	**	**	10XX	-

Algorithm

```
Input: marginal portioned dataset
Step 1: start
Step 2: for each record Dt←attribute
            Read sensitive term attribute Rst
          For Rst→count attribute length Ct
              Find suffix terms length Slt←term-2index
              Encrypt suffix term Est
```

(Continued)

Algorithm (continued)

```
              Generate key index Symmetric Si ← attribute Ati
              Ct++;
            End for
For each attribute
            Create suffi index sensitive and sensitive
              For each sensitive term listStl
                  Hide Est term ← Ati additional prescription
              End.
End
End
            Assign the suffix term key index to record set Dt ← si
Step 3: stop.
```

From the above table, the patient's information is secured using hidden crypto privacy policy. In patient information, the sensitive information such as drug and other medical information are categorized as 'miso'. In special case, the private information specified from the prescription are hidden compared to other patient drug information. So this information is considered as a private one to be preserved.

3.4 Linear Integrity for Verifiable Outsource Data

Linear integrity verifies the attribute case records which are sensitive in nature in terms of access rights on verification and validation against hackers. These hackers attempt to encrypt and decrypt the information on symmetric standard and hold the information constructs based on confirmation. Further, the trustworthiness of such data needs to be checked and the outsourced data must be reworked to meet the customer's demand. In addition, secure data sensitivity approach is proposed with enhanced security. This plan too helps in gaining extensive evidence and ensure dynamic skill activity simultaneuosly.

4 Result and Discussion

Multi attribute case-based privacy preservation algorithm was proposed and implemented in this study to assess its effectiveness upon patients' health care records sourced from UCI web repository. The proposed privacy principle implemented a context-aware multi attribute relational analysis with hidden crypto model to deduce a set of privacy fields from a user's Electronic Health Records (EHR). The proposed method produced efficient results on context-aware clustering and improved the performance too. Principle Component Analysis (PCA), Locality Sensitive Hashing (LSH) and Adaptive Private Security (APS) are some of the algorithms used for comparison and its parameters are tabulated herewith.

Tab. 4 shows the details of data set used to evaluate the performance of the proposed Multi-Attribute Provable Partition-based approach. The performance of MAPPC was evaluated through privacy accuracy (cs), precision rate, recall rate and time complexity.

$$\text{Privacy accuracy (cs)} = \sum_{k=0}^{k=n} \frac{\text{Retrived number of interest terms cluster(Cds)predictedlinks}}{\text{Total related datsets(Tr)from search links}} \tag{1}$$

In Fig. 3, the comparison results for privacy-preserving accuracy are shown which infer that the proposed method produced the highest performance than other methods.

Table 4: Details of dataset

Parameter	Value
EHR	Medical records
Total records	3000
Tools used	Microsoft .net framework

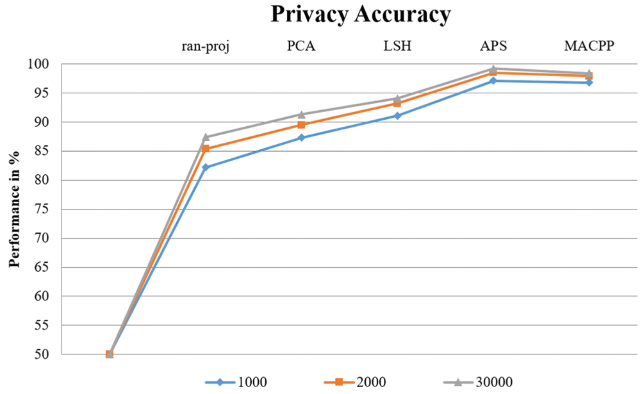

Figure 3: Comparison of privacy accuracy

Tab. 5 shows the comparison results of privacy preserving accuracy achieved by the proposed method against existing techniques. The proposed model achieved privacy preserving accuracy values such as 96.8%, 97.9%, and 98.4% under 1000, 2000, and 3000 records respectively.

Table 5: Comparison of privacy-preserving accuracy

	Impact of privacy accuracy in %				
Methods/number of records	Random projection	PCA	LSH	APS	MACPP
1000 records	82.2	87.3	91.1	96.1	96.8
2000 records	85.4	89.5	93.2	97.5	97.9
3000 records	87.4	91.3	94.1	98.1	98.4

4.1 Analysis of Precision Rate

Precision (Pr) is defined as the proportion of total number of relevant sensitive information from healthcare dataset, where R is the relevant margin rate calculated and A is the total number of sensitive data.

$$\text{Precision, } (\text{Pr}) = \frac{sensituivelistmeanvalue\ (R)}{Totalnumberofattributes(A)} \times 100 \tag{2}$$

Fig. 4 shows the comparison results for precision rate produced by the proposed method against existing methods. The results infer that the proposed method produced an excellent performance rate than other methods.

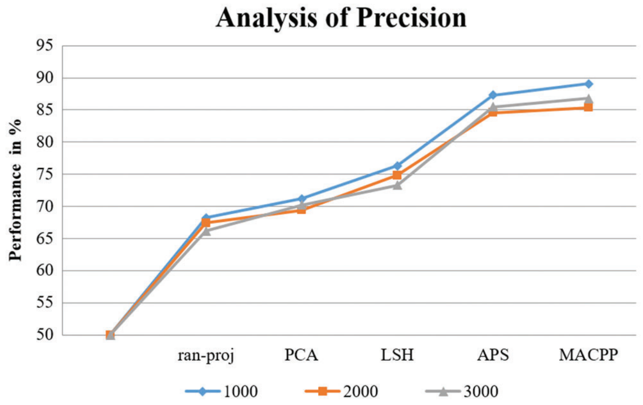

Figure 4: Comparison of a precision rate

Tab. 6 shows the results accomplished by the proposed approach i.e., high performance ratios such as 89.1%, 85.4%, and 86.8% under 1000–3000 records respectively.

Table 6: Comparison of precision rate

	Impact of precision in %				
Methods/number of users	Random projection	PCA	LSH	APS	MACPP
1000 records	68.2	71.2	76.3	87.3	89.1
2000 records	76.4	69.4	74.8	84.6	85.4
3000 records	66.2	70.2	73.2	85.5	86.8

4.2 Analysis of Recall

Recall (Rc) is defined as the proportion of matched drug items within relevant drugs against the total drugs with high sensitivity.

$$\text{Recall (Rc)} = \frac{totalcountofsesntivedrug(RA)}{totaldrugitems\ (R)} \times 100 \tag{3}$$

Fig. 5 shows the comparison results of false recall ratio produced by the proposed method against other methods. The proposed method achieved excellent performance over other methods.

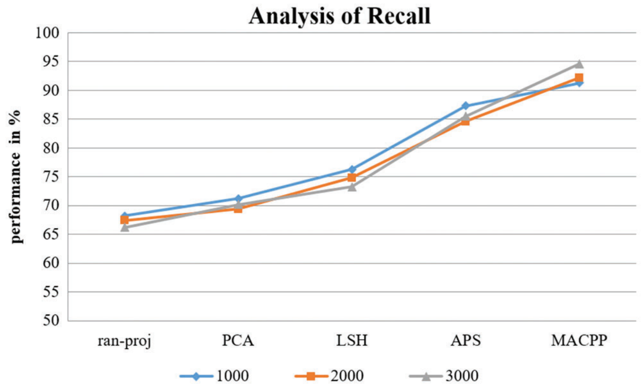

Figure 5: Comparison of recall

Fig. 6 shows the comparison results of time complexity achieved by both the proposed method and other methods considered for the study. The proposed approach produced less time complexity compared to other methods.

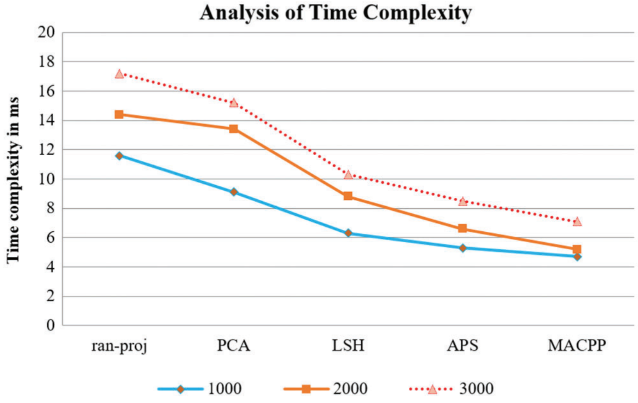

Figure 6: Comparison of time complexity

Tab. 7 shows the comparison results of recall value which infer that the proposed method accomplished the highest performance compared to other methods.

Table 7: Comparison of recall

Impact of recall in %					
Methods/number of records	Random projection	PCA	LSH	APS	MACPP
1000 records	68.2	71.2	76.3	87.3	91.3
2000 records	67.4	69.4	74.8	84.6	92.2
3000 records	66.2	70.2	73.2	85.5	94.6

4.3 Analysis of Time Complexity

$$\text{Time complexity }(\text{Tc}) \ = \sum\nolimits_{k=0}^{k=n} \times \frac{\text{precsion }(\text{pr}) + \text{recall}(\text{rc})}{\text{Time taken}(\text{Ts})} \tag{4}$$

Tab. 8 shows the comparison of time complexity of the proposed precision clustering which offered time complexity values such as 4.7, 5.2 and 7.1 ms under 1000–3000 records respectively.

Table 8: Comparison of time complexity

Impact of time complexity in Mille seconds (ms)					
Methods/number of records	Random projection	PCA	LSH	APS	MACPP
1000 records	11.6	9.1	6.3	5.3	4.7
2000 records	14.4	13.4	8.8	6.6	5.2
3000 records	17.2	15.2	10.3	8.5	7.1

5 Conclusion

Healthcare privacy techniques focus on sensitive information collected from patient logs such as drug information, patient's medical history. So, such sensitive information must be protected from intruders. The current study proposed a multi attribute sensitive protection method using relational analyses using benchmark healthcare data. The proposed MACPP considered radical patient-centric information from drugs category with sensitive personal prescription in order to achieve provable linear partition and enhance the level of security. The performance of the proposed framework, in terms of accuracy, was found to be higher compared to other methods. The proposed method improved the performance of privacy accuracy by 96.8%, with a least time complexity of 4.7 milliseconds. The experimental results established the privacy-preserving ability of state-of-the-art model which is phenomenal and better than existing methods. In future, hybrid deep learning models can be employed to further improve the security of sensitive data.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. M. Chong, "Privacy-preserving healthcare informatics: A review," in *ITM Web of Conf.*, Malaysia, 36, pp. 4005, 2021.

[2] C. Li, M. Dong, J. Li, G. Xu, X. Chen *et al.,* "Healthchain: Secure EMRs management and trading in distributed healthcare service system," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7192–7202, 2021.

[3] C. Li, G. Xu, Y. Chen, H. Ahmad and J. Li, "A new anti-quantum proxy blind signature for blockchain-enabled Internet of Things," *Computers Materials & Continua*, vol. 61, no. 2, pp. 711–726, 2019.

[4] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou and J. Li, "A New lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2019.

[5] G. Szarvas, R. Farkas and R. B. Fekete, "State-of-the-art anonymization of medical records using an iterative machine learning framework," *Journal of the American Medical Informatics Association*, vol. 14, pp. 574–580, 2007.

[6] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[7] X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.

[8] A. F. Karr, X. Lin, A. P. Sanil and J. P. Reiter, "Privacy-preserving analysis of vertically partitioned data using secure matrix products," *Journal of Official Statistics*, vol. 25, no. 1, pp. 125–138, 2009.

[9] B. C. M. Fung, K. Wang, R. Chen and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," *ACM Computing Survey*, vol. 42, no. 4, pp. 1–53, 2010.

[10] D. Lin, P. Rao, E. Bertino, N. Li and J. Lobo, "EXAM: A comprehensive environment for the analysis of access control policies," *International Journal of Information Security*, vol. 9, no. 4, pp. 253–273, 2010.

[11] N. Bui and M. Zorzi, "Health care applications: A solution based on the internet of things," in *ISABEL '11: Proc. of the 4th Int. Symp. on Applied Sciences in Biomedical and Communication Technologie*, Barcelona, Spain, pp. 131–135, 2011.

[12] D. Sánchez, M. Bates and A. Viejo, "Automatic general-purpose sanitization of textual documents," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 853–862, 2013.

[13] M. Barua, R. Lu and X. Shen, "SPS: Secure personal health information sharing with patient-centric access control in cloud computing," in *2013 IEEE Global Communications Conf. (GLOBECOM)*, Atlanta, GA, pp. 647–652, 2013.

[14] C. Li, M. Hay, G. Miklau and Y. Wang, “A data- and workload-aware algorithm for range queries under differential privacy,” *Proceedings of the VLDB Endowment*, vol. 7, no. 5, pp. 341–352, 2014.

[15] T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau *et al.,* “Secure dynamic access control scheme of PHR in cloud computing,” *Journal of Medical Systems*, vol. 36, no. 6, pp. 4005–4020, 2012.

[16] R. Zhang, L. Liu and R. Xue, “Role-based and time-bound access and management of EHR data,” *Security and Communication Networks*, vol. 7, no. 6, pp. 994–1015, 2014.

[17] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen *et al.,* “Security and privacy for mobile healthcare networks: From a quality of protection perspective,” *IEEE Wireless Communications*, vol. 22, no. 4, pp. 104–112, 2015.

[18] S. Jiang, X. Zhu and L. Wang, “Epps: Efficient and privacy-preserving personal health information sharing in mobile healthcare social networks,” *Sensors*, vol. 15, no. 9, pp. 22419–22438, 2015.

[19] W. Liu and E. K. Park, “Big data as an e-Health service,” in *2014 Int. Conf. on Computing, Networking and Communications (ICNC)*, Honolulu, HI, USA, pp. 982–988, 2014.

[20] Y. Zhou, W. Tang, D. Zhang, X. Lan and Y. Zhang, “A case for software-defined code scheduling based on transparent computing,” *Peer-to-Peer Networking and Applications*, vol. 11, no. 4, pp. 668–678, 2018.

[21] Y. Cao, P. Hou, D. Brown, J. Wang and S. Chen, “Distributed analytics and edge intelligence: Pervasive health monitoring at the era of fog computing,” in *Mobidata '15: Proc. of the 2015 Workshop on Mobile Big Data*, New York, NY, United States, pp. 43–48, 2015.

[22] A. Alnemari, C. J. Romanowski and R. K. Raj, “An adaptive differential privacy algorithm for range queries over healthcare data,” in *2017 IEEE Int. Conf. on Healthcare Informatics (ICHI)*, Park City, UT, USA, pp. 397–402, 2017.