JOURNAL OF COMPUTATION IN
BIOSCIENCES AND ENGINEERING

Journal homepage: http://scienceq.org/Journals/JCLS.php

Research Article Open Access

An Enhanced TBAHIBE-LBKQS Techniques for Privacy Preservation in Wireless Network

A.Vinodh Kumar[1] ,DR.S.Kaja Mohideen[2],A.Kathirvel[3],
[1] Anand Institute of Higher Technology ,chennai, India
[2] B.S. Abdur Rahman University,chennai, india.
[3] Misrimal Navajee Munoth Jain Engineering College, Chennai, India,
*Corresponding author: A.Kathirvel, E-mail: ayyakathir@rediffmail.com
Received: February 25, 2017, Accepted: March 27, 2017, Published: March 27, 2017.

ABSTRACT:

In recent days, providing security to the data stored in wireless network is an important and challenging task. For this purpose, several existing privacy preservation and encryption algorithms are proposed in the existing works. But, it has some drawbacks such as, high cost, required more amount of time for execution and low level security. In order to overcome all these drawbacks, this paper proposes a novel technique such as, Tiered Blind and Anonymous Hierarchical Identity Based Encryption (TBAHIBE) and Location Based Keyword Query Search (LBKQS) for providing privacy preservation to the data stored in wireless network environment. In this work, the privacy is provided to the packet data stored in the Electronic Health Record (EHR). It includes two modules such as, secure data storage and location based keyword query search. In the first module, the packet data of the egg and, receptor, doctor and lab technician are stored in the encrypted format by using the proposed TBAHIBE technique. Here, the authenticated persons can view the packet data, for instance, the doctor can view the donor and receptor packet details. In the second module, the location based search is enabled based on the keyword and query. Here, the doctor, patient and other users can fetch the packet details in a filtered format. The main advantage of this paper is, it provides high privacy to the packet data in a secured way. The experimental results evaluate the performance of the proposed system in terms of computation cost, communication cost, query evaluation, encryption time, decryption time and key generation time.

Keywords: *Wireless network Computing, Privacy Preservation, Data,Tiered Blind and Anonymous Hierarchical Identity Based Encryption (TBAHIBE) and Location Based Keyword Query Search (LBKQS), Electronic Health Record (EHR).*

.

INTRODUCTION

WIRELESS NETWORK is an emerging and demanding technology that provides different wireless network services to the user. It requires the improvement in security performance for efficient data transmission. The wireless network provides several advantages[1], including:

- Resource elasticity
- On-demand self service
- Shared pool access

The advantages are graphically represented in the following Fig 1. The main aim of wireless network is to share the data over the scalable nodes such as, user computers, wireless network services and data centers. The secure data storage plays an essential in wireless network, where the large number of wireless network users store their data in a remotely located servers. It reduces the affliction of managing and data storing within the local storage. Moreover, it can be demanded on requirement from the distributed wireless network computing. Thus, this paper selects the wireless network environment for secure data privacy preservation. Before storing the data into wireless network, it must be encrypted by the data owners to protect the data privacy.

This paper proposed a novel technique, namely, Tiered Blind and Anonymous Hierarchical Identity Based Encryption (TBAHIBE) and Location Based Keyword Query Search (LBKQS) for data privacy preservation in wireless network. The main intention of this techniques are to provide privacy for the data stored in the wireless network and, to enable the search based on the location and keyword. This work includes two modules, such as, secure data storage and location based search in wireless network. In the first module, the packet data of the egg and, receptor, doctor and lab technician are stored in the Electronic Health Record (EHR). Here, the privacy is provided for each data by using the proposed TBAHIBE technique. The donor cannot able to view the packet details of the receptor, because the data are stored in the encrypted format. Similarly, the receptors also cannot view the packet details of the donor. In the second module, the authenticated persons such as doctor, patient and other users (visitors) can fetch the normalized data from the EHR. Here, the keyword query search is enabled based on the location. After sending the query to EHR, the corresponding key is retrieved, based on this key, the filtered results are obtained by using the proposed LBKQS technique. In experiments, the performance of the proposed techniques are evaluated in terms of computation cost, communication cost, The remaining sections of this paper is organized as follows: Section II reviews some of the existing works related to privacy preservation and secure data storage in wireless network. Section III provides the detailed description for the proposed TBAHIBE mechanism. Section IV evaluates the performance of both existing and proposed techniques. Finally, this paper is concluded and the future work to be carried out is stated in Section V.

Fig 1. Advantages of wireless network

2. Related Work

This section presents some of the existing works related to encryption, data storage and local based search in wireless network. Yang, et al [2]suggested a hybrid solution to preserve the packet data during the process of data sharing in wireless network. This work includes the following components:

Vertical data partition using packet data publishing

Integrity checking Data merging for packet data

Hybrid search across plain text and cipher text

Lin, et al [3]introduced a new wireless network based framework to implement a self-caring service, namely, home diagnosis for big packet data. In this paper, the Hadoop cluster was implemented for both off line data storage and index building. The speed of packet record retrieval was improved, which was the major advantage of this paper.Dou, et al[4] developed a new model, namely, History record-based Service optimization method (HireSome-II) to improve the credibility of a composition plan. In this work, we used the k-means clustering. The advantage of this method was, it significantly reduced the time complexity. Wang, et al [5] proposed a new cryptographic technique, namely, Hierarchical Identity Based Encryption (HIBE) for multi-linear maps. Here, the secret keys were delegated at lower levels to prove the security level of the proposed technique. Wang, et al [6] introduced an efficient framework, namely, Constant-size Cipher text Policy Comparative Attribute Based Encryption (CCP-CABE) to embed the attributes into the user's key. The main objectives of this paper were listed as follows:

It provided a secure and efficient access control in a wireless network environment. It handled more expressive types of access control by integrating the wildcards and negative attributes. It minimized the computation overhead on the resource constrained data owners. Idris, et al [7] suggested a Big Data Service Engine (BISE) to provide the processing and storage services for human centric wellness data. The main objectives of this work were listed as follows:

- It offered the health care services by exploiting the big data technology.
- It maintained a physical, social and mental health services by using the service engine.
- It performed analytics and present services by handling variety of data.

Zhang, et al [8] introduced an Extended Quasi Identifier (EQI) partitioning technique to improve the privacy preservation of set valued data in hybrid wireless network. The main intention of this paper was to protect the privacy of the data during the process of data publishing. In addition, the data publication solutions were provided in this work to ensure the confidentiality of the wireless network data. The new query analysis tool was designed in this work to optimize the data query on hybrid wireless network. Nepal, et al [9] identified a solution to ensure both the data integrity and confidentiality, when storing it on a hybrid wireless network environment. In this paper, the privacy breaches from counting query, linear query and batch linear query were employed in the data querying stage. Forkan, et al [10]suggested a new model, namely, Big Data for Context aware Monitoring (BDCaM) to discover the framework for assisted healthcare. Here, the Context Management System (CMS) was utilized to store the context histories of patients. Alamri and Lee [11] proposed a new sharing system to attain the privacy and utility of desirable features. The four main entities utilized in the system are patients, Wireless network Service Provider (CSP), users and enterprise system. In this work, the security was provided against unauthorized access by removing the unique attributes in the outsourced data. In addition, two important issues such as, privacy protection and oblivious processing were analyzed within the untrusted domain. Hassanalieragh, et al [12] introduced an Internet-of-Things (IoT) based sensing method to monitor and manage the health of patients in wireless network. It includes the following processes, such as, Data acquisition,

Data transmission, Wireless network processing.

The major disadvantage of this technique was, it provided the training data for machine learning with little burden. Rajaei and Haghjoo[13] introduced an improved ambiguity based anonymization technique to preserve the data utility. In this work, different operations such as generalization, suppression, anatomization, permutation and perturbation were employed for anonymization. Moreover, the generalization based anonymization technique was applied to reduce the information while preserving the privacy requirements. Papadopoulos, et al [14] introduced a new privacy mechanism based on k Nearest Neighbor (kNN) queries to determine the notion of location privacy. The authors also suggested the following concepts to solve the problem of location privacy, which includes:

- Data transformation
- Location Obfuscation
- Private Information Retrieval (PIR)

Azraoui, et al [15] suggested a searching mechanism based on the publicly verifiable conjunctive keyword in the outsourced databases. In this work, the data owners ensured the properties of public delegatability and verifiability. Moreover, the polynomial based accumulators were utilized to represent the keywords in the database. The main contributions of this work were as follows:

It verified the correctness of the server's response in a logarithmic time. It efficiently enabled the search of outsourced database. Kuo[16] analyzed the issues and challenges in wireless network to improve the health care services. The four different aspects such as, management, technology, security and legal were discussed to evaluate the services. Zhang, et al [17] suggested a Priority Based Health Data (PHDA) aggregation system with privacy preservation to aggregate the efficiency of health data in wireless network. Based on the data priority, various forwarding strategies were utilized in this work. The advantages of this concept were, it provided lower communication overhead.Zhang, et al [18] introduced a scalable Top Down Specialization (TDS) approach to anonymize the large scale data in wireless network using MapReduce framework. A group of innovative jobs were integrated to accomplish the computation in a scalable way.Prasad, et al [19] proposed a new data sharing and security mechanism to provide privacy preservation for wireless network data. It utilized the Key Distribution Centre (KDC) mechanism to distribute and maintain the attributes and secret keys. Liu, et al [20] suggested a shared authority based authentication protocol to enable the privacy preservation in wireless network. It attained shared access authority with the security and privacy

considerations. Moreover, the proxy based re-encryption mechanism was applied to provide data sharing in wireless network. Zhang, et al [21] analyzed the key research issues to improve the process of privacy protection and preservation. Based on the wireless network service levels, the current wireless network protection and preservation processes were determined. Moreover, the issues in both customer side and server side were classified by using the key research.

3.Proposed Method

This section presents the detailed description for the proposed Tiered Blind and Anonymous Hierarchical Identity Based Encryption (TBAHIBE) based privacy preservation mechanism.The main intention of this work is to securely store the data in wireless network with privacy preservation. Here, the application of egg and is considered. This work includes the following modules:

- Secure storage in wireless network
- Location privacy search in wireless network

At first, the users such as, doctor, patient and lab technician registered their accounts. Then, the personal profile will be created for them and it will be stored in the Wireless Network Electronic Health Record (HER) database. Here, a novel encryption technique, namely, Tiered Blind and Anonymous Hierarchical Identity Based Encryption (TBAHIBE) mechanism is proposed for data encryption, which generates the individual key for the encrypted data. After encryption, the secrecy will be maintained for each data stored in the database. Moreover, the Quasi and sensitive identifiers are utilized to provide the privacy for the preserved data. In the second module, the doctor, patient and other users (visitors) login into their account using the unique ID and password. If it is an authenticated account, the normalized data will be retrieved by using the proposed Location Based Keyword Query Search (LBKQS) technique. Here, the data are searched based on the location. Finally, the filtered data will be obtained based on the similarity search. The detailed description is provided in the following stages:

Secure Storage in Wireless network

In this paper, the packet application of egg and, receptor is taken for analysis. The main aim of this process is to hide the privacy data of both the donor and receptor. The flow of the secure storage in wireless network is shown in the following Fig 2. Initially, the registration process is performed by creating the login account for doctor, patient and lab technician. Then, the personal profile is generated for each wireless network user, who registered their accounts. Here, the data is stored in the encrypted format by using the proposed TBAHIBE. It generates the individual key for user and it stores the encrypted data in the wireless network EHR database. Here, the lab technician will update the packet details of the patient with anonymity. Then, the Quasi and sensitive identifiers are utilized to retrieve the data from the EHR. Normally, the quasi identifier is used to uniquely identify the tuples in the table. Moreover, it links the anonymized dataset other datasets. The sensitive identifiers reveal the sensitive information of individuals by linking with the external data. The main intention of blinding is to offer perfect confidentiality of a message and its corresponding signature.

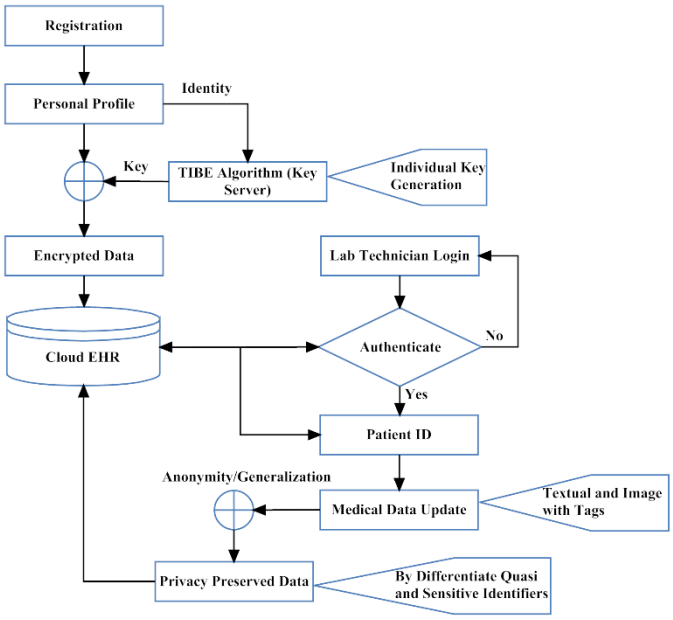

Fig 2. Secure storage in wireless network

Algorithm I –Tiered Blind and Anonymous Hierarchical Identity Based Encryption (TBAHIBE)

// Register

Users (U_i = 1 to N)

For each U_i ← Register into the wireless network database (C_d);

Hierarchical Identity = $\{Hosp_{ID}, D_{ID}, U_{LOC}, U_{ID}\}$;

Key ← Identity;

Data (P_{DT}, M_{DT}, M_{Key})

$C_d \leftarrow Load\ (Denc)$

// Encryption

For any ($U_i||D_i||L_i$) // Where, user or doctor or lab technician

Attr (key) ← $\{Hosp_{ID}, D_{ID}, U_{LOC}, U_{ID}\}$;}

D = Encrypt (Denc, Attr (key),$Skey_i$)

If ($D_i||L_i$)

View $Any_{DT} \leftarrow C_d$

If (U_i)

View Org_{DT}

End if;

End if;

End for;

The Algorithm I shows the clear procedure of TBAHIBE encryption technique. It includes two processes such as, registration and encryption. The packet data of each user is stored in the wireless network database. This information was arranged in a hierarchical manner like hospital ID, doctor ID, user location and user ID. After loading the data, it will be stored in the encrypted format. Algorithm II shows the process of data accessing from wireless network database. After storing the data, it will be accessed by the authenticated persons, who have the unique ID and password. Here, the authenticated key is generated with the location and time stamp for login verification. Based on the user ID and password, the data can be retrieved from the wireless network database.

Algorithm II - Data accessing from wireless network database

Input: Uniqid (U_{ID}) and pass word P_w;

Output: Key for authentication;

Generate the authentication key (Key_{Au}) with the location and the time stamp (Loc, T) for login verification;

Verify (U_{ID}, P_w);
$Key_{Au} \leftarrow Gen\ (U_{Loc}, Cur_T)$;
If (U_{ID} in need of Donor)
Gen (Dnr_{ID}, U_{ID});
RL ← add (Dnr_{ID});
If (U_{ID} in wish to Donate)
Gen ($Recp_{ID}, U_{ID}$);
DL ←add $Recp_{ID}$;
End if;
End if;

Algorithm III describes the procedure of best match identification of donor for a receptor. Here, the donor list and the receptor list are given as the input, based on this, the best match of donor to receptor is identified. At first, the donor with least count are extracted and arranged in an alphabetical order. Then, it will be prioritized with least count. For each receptor in RL list, the donor with least count is loaded. Based on the location, gender and race, the match will be identified.

Algorithm III - Best Match Identification of Donor for a Receptor
Input: Donor List (DL), Receptor List (RL);
Output: Best match of donor to receptor;
Step 1: Extract the donor with least count (Dcount);
Step 2: Dmin = min count (DI);
Dlp← Ascending (Dl) based on Dmin;
Step 3: Prioritize the DL (Donor with least domain count →First);
Step 4: For each ($Recp_{ID}$) in RL
Load Donors (Dnr_{ID}) from DL with least donation count i = 1, 2, … N;
If (Dnr_{ID}&R^*) // * represents the opposite gender in RL;
If (Dnr_{ID} location == R^* location)
If (Dnr_{ID} race == $Recp_{ID}race$)&& other physical features
Suggest donor to the receptor;
Else if
Load the next donor ($Dnr_{ID} + 1$);
Continue the above steps until all the receptors assigned with the donors;

Else

Put receptor in the waitlist;

Wait ←($Recp_{ID}$);

End if;

End if;

End for;

Location Privacy Search in Wireless network
The flow of the location based keyword query search is shown in Fig 3. In this module, the doctor, patient and other users will login into their accounts. If it is an authenticated account of doctor, the required patient ID and the patient packet information will be retrieved to fetch the normalized data. If it is an authenticated account of patient, the normalized data will be fetched by retrieving the patient ID from the database. If it is an authenticated account of other user, the query is requested to the database based on the location. Then, the corresponding results will be forwarded to the user and the cipher query will be generated based on the similarity search. Finally, the filtered results are retrieved by using the location based searching algorithm.

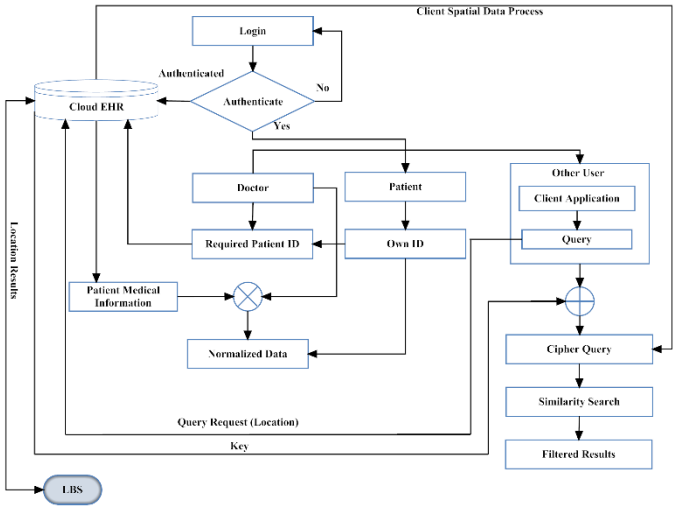

Fig 3. Location privacy search in wireless network

Algorithm IV shows the procedure of location based keyword query search. In this stage, the visitors who have the valid ID and password can request the query to the database. If the keywords and the corresponding key stored in the database are matched, the results are retrieved from the database. Moreover, the authentication, correctness and freshness processes are performed to provide the data in a filtered format.

Algorithm IV – Location based keyword query search
For each user who visit C_d
Register ($Ur_{VID,}Ur_{Loc}$);
Load Query (Q);
Identify ($K_w from\ Q$) with Dynamic Cuckoo Hashing (DCH); // K_w represents the keywords;
Match (I_{Key}, K_w);
If Index matched
Genkey ()
$Skey(Vid)_i \leftarrow (Ur_{VID}, Ur_{Loc})$
Results (R) ← Process (Q, Ur_{VID});
$D_{dec}(Denc_{Results}, Skey(Vid)_i)$
If (R ← Retrieval (C_d))
Check (Correctness (R));
Check (Completeness (R));
Check Freshness (R));
View $Any_{rst} \leftarrow (Ur_{VID}, Ur_{Loc})$;
End if;
//Correctness ($\boldsymbol{Any_{rst}}$)
If ($Any_{rst} \leftarrow C_d$) &&$Ur_{Loc} \leftarrow Reg_{Loc}$)
Ensure proof of correctness;
Else
Perform authentication;
//Completeness ($\boldsymbol{Any_{rst}}$)
If ($Any_{rst} \leftarrow C_d$) &&$Ur_{Loc} \leftarrow Reg_{Loc}$)
Match (Q, Any_{rst});
If (Partial (Any_{rst}))
Repeat search with more specific query;
Else
Ensure completeness;
End if;
//Freshness ($\boldsymbol{Any_{rst}}$)
Extract $Any_{rst} \leftarrow C_d$;
Set L_{max} with respect to Cur_T;
If (Any_{rst}within L_{max})
Ensure proof of freshness;

Else

Repeat query search;

4. Performance Analysis

This section presents the results of both existing and proposed techniques. Here, the packet application is taken for the analysis with own dataset. The data are stored into the dataset in the encrypted format. The existing encryption and search based techniques considered in this work are, target snapshot top k-queries, moving snapshot top k-queries, Secure Data Outsourcing (SDO), Baseline Method (BM), Reverse top-k Boolean Spatial Keyword (RKBSK), Enhanced RKBSK (ERKBSK), Traditional Rivest Shamir Adelman (RSA) and Modified RSA. The performance of these techniques are evaluated in terms of,

- Computation cost
- Communication cost
- Query evaluation
- Query time
- Computation time
- Encryption time
- Decryption time
- Key generation time

Computation Cost

The computation cost is the amount of cost required for the process of query search. Here, it is calculated by varying the number of keywords from 0 to 100, which is shown in below:

$$Computation\ Cost = \frac{N_H}{\mathrm{T}} \quad (1)$$

Where, NH represents the number of hash computation to verify query results and T indicates the required amount of time. Fig 4 graphically represents the amount of required computation cost for both existing and proposed location based searching techniques. When compared to the existing target snapshot top k-queries and moving snapshot top k-queries techniques[22], the proposed LBKQS requires the minimum computation cost.

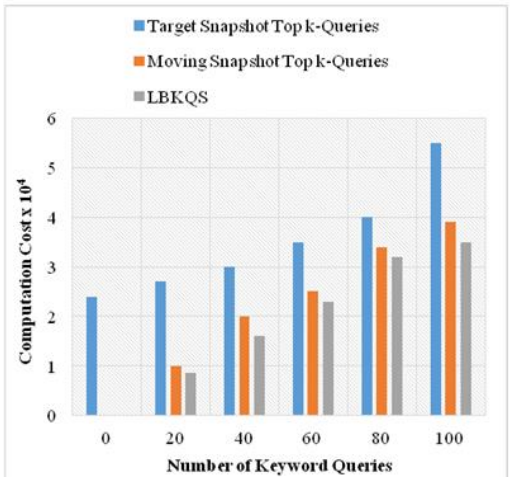

Fig 4. Computation cost of both existing and proposed techniques

Communication Cost

Communication cost is defined as the cost required to retrieves the query results from the database. Fig 5 shows the communication cost required for both existing target snapshot top k-queries, moving snapshot top k-queries and proposed LBKQS techniques. The communication cost is calculated by varying the number of keyword queries, which is shown in below:

$$Communication\ Cost = \frac{Q_R}{N_K} \quad (2)$$

Where, QR represents the query region size to retrieve the query results and NK indicates the number of keyword queries. From the results, it is observed that the proposed LBKQS technique requires low cost, when compared to the existing techniques.

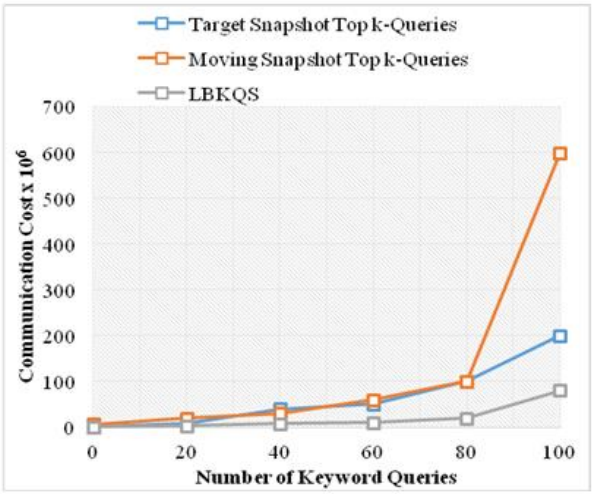

Fig 5. Communication cost of both existing and proposed techniques

Query Evaluation

Fig 6 shows the cost of query evaluation with respect to different key size (KB). Moreover, the cost is calculated for both existing SDO [23]and proposed LBKQS techniques. From this analysis, it is evaluated that the proposed LBKQS technique requires low cost, when compared to the other technique. It is calculated as follows:

$$cost = \frac{Q_D}{T} \quad (3)$$

Where, QD represents the decryption of query results for the requested query region and T is the required amount of time.

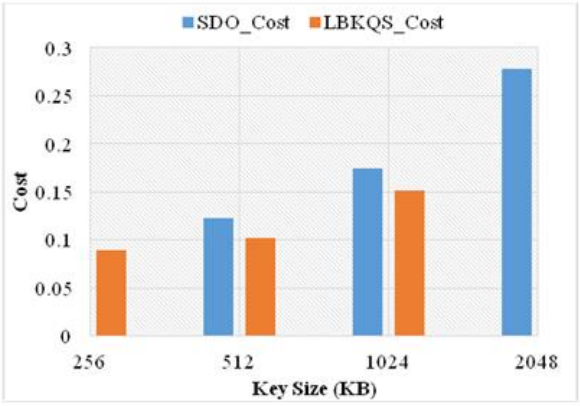

Fig 6. Query evaluation Vs Cost

Query Time

Fig 7 depicts the query time of existing BM, RKBSK, ERKBSK[24] and proposed LBKQS techniques. The time is

estimated by varying the number of query keywords. The query time is calculated as follows:

$$Query\ time = \frac{K_Q}{M_T} \quad (4)$$

Where, KQ indicates the number of keyword queries and MT indicates the maximum time to execute the query for all keywords. When compared to the existing techniques, the proposed LBKQS technique requires minimized query time.

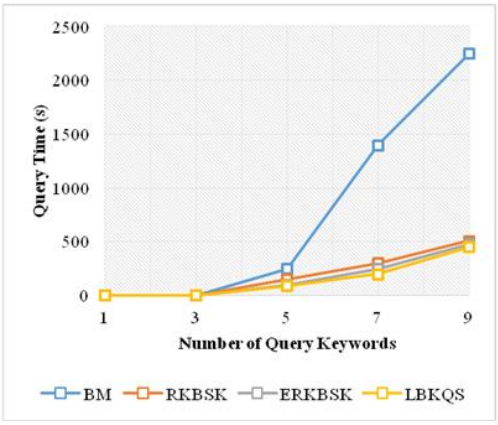

Fig 7. Query time

Computation Time

Fig 8 shows the computation time required for both existing MDE [2]and proposed TBAHIBE encryption techniques. The amount of time required to process to number of EHRs from 50000 to 200000. Here, the colored lines indicate the number of attributes. From this evaluation, it is obtained that the proposed TBAHIBE requires less time, when compared to the existing MDE technique.

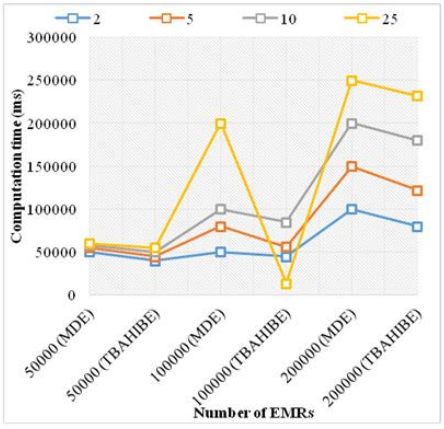

Fig 8. Computation time

Encryption Time

Encryption is defined as the process of converting the original data into an unknown format. Encryption time is the amount of time required to encrypt the given data. In this paper, the packet details of the egg receptor are stored in EHR in the encrypted format. Here, the encryption time is calculated for both traditional RSA, modified RSA, ESRKGS[25] and proposed TBAHIBE techniques.

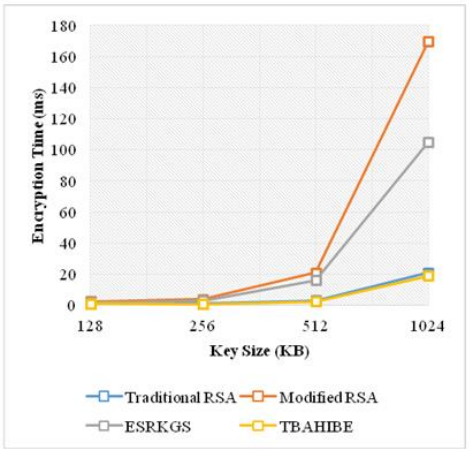

Fig 9. Encryption time

From Fig 9, it is observed that the proposed TBAHIBE technique requires minimized encryption time. It is calculated as follows:

$$Encryption\ time = \frac{N_A}{T} \quad (5)$$

Where, NA represents the number of attributes in N number of packet records and T indicates the amount of time taken to encrypt.

. Decryption Time

Decryption is defined as the process of converting the encrypted text into the original text. Decryption time is the amount of required to convert the encrypted data into the original data. Fig 10 shows the decryption time of both existing and proposed techniques with respect to different key size (KB). When compared to the existing techniques, the proposed TBAHIBE requires minimized decryption time (ms).

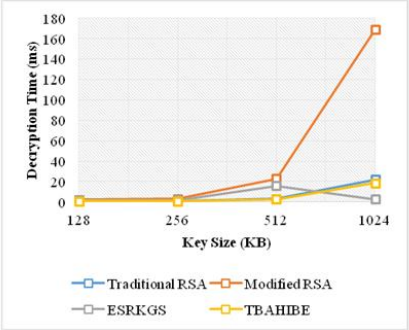

Fig 10. Decryption time

Key Generation Time

Key generation time is the amount of time required to generate the key for retrieving the data from EHR. Fig 11 shows the key generation time of both traditional RSA and modified RSA, ESRKGS and proposed TABHIBE techniques. Here, the colored line indicates the key size in terms of KB. From this evaluation, it is observed that the proposed TABHIBE requires minimum

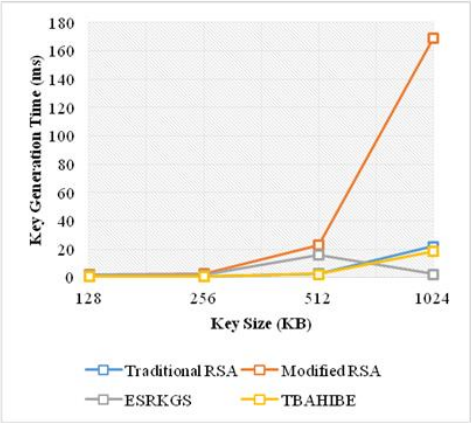

Fig 11. Key generation time (ms)

5. CONCLUSION AND RECOMMENDATION

This paper proposed a novel scheme, TBAHIBE-LBKQS techniques to provide privacy preservation for packet data. The main intention of this work is to provide high privacy to the data stored in EHR. Here, the packet data of the egg receptor are stored in the wireless network environment. This work includes two modules, such as, secure storage in wireless network and location based search. At first, the registration process is performed by updating the patient's personal information in the encrypted format by using the TBAHIBE technique. In the second module, the user can query a keyword based on the location to retrieve the data by using the LBKQS technique. Finally, the authenticated users retrieved the filtered packet information. The main advantages of this work are, high security, privacy, low cost and minimum processing time. Moreover, the proposed techniques are compared with some of the existing techniques used for encryption and location based search. The results are analyzed and evaluated in terms of computation cost, computation cost, query evaluation, encryption time, decryption time, query response time and computation time. From this analysis, it is proved that the proposed TBAHIBE-LBKQS technique provides better results, when compared to the existing techniques.

In future, this work will be extended to device specific with location coordination based searching.

REFERENCES

1. Advantages of wireless network computing. google images
2. J.-J. Yang, et al., "A hybrid solution for privacy preserving packet data sharing in the wireless network environment," Future Generation Computer Systems, vol. 43, pp. 74-86, 2015.
3. W. Lin, et al., "A wireless network-based framework for Home-diagnosis service over big packet data," Journal of Systems and Software, vol. 102, pp. 192-206, 2015.
4. W. Dou, et al., "HireSome-II: Towards Privacy-Aware Cross-Wireless network Service Composition for Big Data Applications," IEEE Transactions on Parallel and Distributed Systems, vol. 26, pp. 455-466, 2015.
5. H. Wang, et al., "Hierarchial Identity-Based Encryption Scheme from Multilinear Maps," in 2014 Tenth International Conference on Computational Intelligence and Security (CIS), 2014, pp. 455-458.
6. Z. Wang, et al., "Efficient Attribute-Based Comparable Data Access Control," IEEE Transactions on Computers, vol. 64, pp. 3430-3443, 2015.
7. M. Idris, et al., "Big Data service engine (BISE): Integration of Big Data technologies for human centric wellness data," in 2015 International Conference on Big Data and Smart Computing (BigComp), 2015, pp. 244-248.
8. H. Zhang, et al., "Towards Privacy Preserving Publishing of Set-valued Data on Hybrid Wireless network," IEEE Transactions on Wireless network Computing, pp. 1-14, 2015.
9. S. Nepal, et al., "Trustworthy Processing of Healthcare Big Data in Hybrid Wireless networks," IEEE Wireless network Computing, vol. 2, pp. 78-84, 2015.
10. A. Forkan, et al., "BDCaM: Big Data for Context-aware Monitoring-A Personalized Knowledge Discovery Framework for Assisted Healthcare," IEEE Transactions on Wireless network Computing, pp. 1-14, 2015.
11. F. S. Alamri and K. D. Lee, "Secure sharing of health data over wireless network," in Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on, 2015, pp. 1-5.
12. M. Hassanalieragh, et al., "Health monitoring and management using internet-of-things (iot) sensing with wireless network-based processing: Opportunities and challenges," in Services Computing (SCC), 2015 IEEE International Conference on, 2015, pp. 285-292.
13. M. Rajaei and M. S. Haghjoo, "An improved Ambiguity+ anonymization technique with enhanced data utility," in Information and Knowledge Technology (IKT), 2015 7th Conference on, 2015, pp. 1-7.
14. S. Papadopoulos, et al., "Nearest neighbor search with strong location privacy," Proceedings of the VLDB Endowment, vol. 3, pp. 619-629, 2010.
15. M. Azraoui, et al., "Publicly verifiable conjunctive keyword search in outsourced databases," in 2015 IEEE Conference on Communications and Network Security (CNS), 2015, pp. 619-627.
16. M.-H. Kuo, "Opportunities and challenges of wireless network computing to improve health care services," Journal of packet Internet research, vol. 13, p. e67, 2011.
17. K. Zhang, et al., "PHDA: A priority based health data aggregation with privacy preservation for wireless network assisted WBANs," Information Sciences, vol. 284, pp. 130-141, 2014.
18. X. Zhang, et al., "A Scalable Two-Phase Top-Down Specialization Approach for Data Anonymization Using MapReduce on Wireless network," IEEE Transactions on Parallel and Distributed Systems, vol. 25, pp. 363-373, 2014.
19. K. Prasad, et al., "Data sharing security and privacy preservation in wireless network computing," in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, 2015, pp. 1070-1075.
20. H. Liu, et al., "Shared authority based privacy-preserving authentication protocol in wireless network computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 26, pp. 241-251, 2015.
21. G. Zhang, et al., "Key research issues for privacy protection and preservation in wireless network computing," in Wireless network and Green Computing (CGC), 2012 Second International Conference on, 2012, pp. 47-54.
22. R. Zhang, et al., "Secure spatial top-k query processing via untrusted location-based service providers," IEEE Transactions on Dependable and Secure Computing, vol. 12, pp. 111-124, 2015.

23. M. Li, et al., "Scalable and secure sharing of personal health records in wireless network computing using attribute-based encryption," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, pp. 131-143, 2013.
24. Y. Gao, et al., "Efficient reverse top-k boolean spatial keyword queries on road networks," Knowledge and Data Engineering, IEEE Transactions on, vol. 27, pp. 1205-1218, 2015.
25. M. Thangavel, et al., "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)," Journal of Information Security and Applications, vol. 20, pp. 3-10, 2015.

Citation: A.Kathirvel, *et al*. (2017). An Enhanced TBAHIBE-LBKQS Techniques for Privacy Preservation in Wireless Network. J. of Computation in Biosciences and Engineering. V3I3. DOI: 10.15297/JCLS.V3I3.02