PRIVACY-PRESERVING PRIORITY CATEGORIZATION ON PATIENT PHYSICAL CONDITION DATA IN REMOTE E-HEALTH CARE SYSTEM

G.VenuMadhava Rao Assoc.Professor, Dept of CSE, Jawaharlal Nehru Technological University, Ananthapuramu.

V.SriKavya G.Gayathri G.Divya P.Harshitha

ABSTRACT

The Distributed Area Network (DAN) has attracted considerable attention and become a promising approach to provide a 24-hour on-the-go healthcare service for users. However, it still faces many challenges on privacy of users' sensitive personal information, confidentiality of healthcare center's Disease models. For this reason, many privacy-preserving schemes have been proposed in recent years. However, the efficiency and accuracy of those privacy-preserving schemes become a big issue to be solved. In this project, we propose an efficient and privacy-preserving priority categorization scheme, named PPC, for Categorizing patients' encrypted data at the DAN-gateway in a remote e-healthcare system. Specifically, to reduce the system latency, we design a non-interactive privacy-preserving priority categorization algorithm, which allows the DAN-gateway to conduct the privacy-preserving priority categorization for the received Users' medical data(reports) of the users and relay these data according to their priorities. Detailed Security analysis shows that the PPC scheme can achieve the priority classification and reports relay without disclosing the privacy of the users' personal information and confidentiality of the healthcare center's Disease models.

KEYWORDS: DAN,PPC

INTRODUCTION

With the pervasiveness of smartphones and the Distributed area network (DAN), the remote E-Healthcare system has received considerable attention and become more popular. A variety of DAN schemes and applications have been proposed in recent years, including energy-e_cient medium access protocol for DAN using the listen-before transmit manner , data forwarding framework between biosensors and the gateway considering the presence of body shadowing, prioritized adaptive resource allocation algorithm for DAN based on patients' medical situation. Considering the limited resource of the sensors, the collected data streams cannot be transmitted directly to the healthcare center. As shown in Fig. 1, the sensors in each user's wearable health system periodically collect the users' physiological data, send these raw data to the his/her smartphone for preprocessing. The smartphone assembles a medical packet containing the user's preprocessed physiological data, and sends it to a DAN-gateway nearby. The medical packets from different users will be randomly aggregated in DANgateways. Then the DAN-gateways relay all the medical packets to the remote healthcare center.

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. If the connection to the user is relatively close, it may be designated an edge server.

Clouds may be limited to a single organization (enterprise clouds), or be available to many organizations (public cloud).Cloud computing relies on sharing of resources to achieve coherence and economies of scale.

Advocates of public and hybrid clouds note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand, providing the burst computing capability: high computing power at certain periods of peak demand.

Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models.

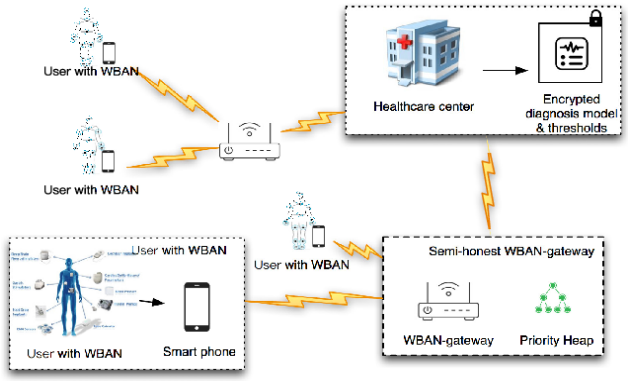

Fig.1 Achieving the PPC Scheme

1.LITERATURESURVEY

TITLE	ADVANTAGES	DISADVANTAGES
1.Enabling Efficient and Privacy-Preserving Health Query over Outsourced Cloud.	1. Health service provider has abundant of health data. 2. Diagnosis models for multiple diseases. 3. Outsources the encrypted data to the cloud.	1. The collected data streams cannot be transmitted remotely to a service provider like healthcare center or cloud service provider.
2. A Secure Privacy-Preserving Data Aggregation Scheme based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems.	1. SPPDA scheme is proven under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. 2.Data confidentiality, data authenticity, and data privacy. 3. Health Insurance Portability and Accountability (HIPAA).	1. Scarce resources in terms of memory, energy, and storage. 2. The LPU has more resources than sensors. 3. Uses the battery and communicates wirelessly with the medical server.
3.Ensuring Access Control in Cloud Provisioned Healthcare Systems.	1. By tapping into the cloud infrastructure, users can gain fast access to best-of-breed applications. 2.Improve the information technology's agility and reliability.	1.Cloud computing paradigm moves computing and storage tasks from individual systems into the cloud. 2.Cloud computing facilities cannot be employed for e-Health platforms to provide information flow between multiple entities.
4.Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguish ability Obfuscation.	1.The published values can be used in multiple NIKE environments setup by different organizations. 2.Public-key broadcast encryption using candidate multi linear maps.	1.Indistinguishability obfuscation is a powerful cryptographic primitive: it can be used to build public-key encryption from pseudorandom functions, selectively-secure short signatures, deniable encryption.
5.A WBAN-basedSystem for Health Monitoring at Home.	1.Proliferation of systems prove crucial in promoting proactive approaches to healthcare.	1. Proliferation of wireless sensor network applications will result in commoditization of wireless sensor network components.

6.An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing.	1. An efficient and privacy preserving biometric identification scheme which can resist the collusion attack. 2. Attackers can only observe the encrypted data stored in the cloud.	1.Doesn't implement Biometric Identification Scheme. 2.No affective privacy preserving encryption techniques.
7.Low-Complexity Privacy-Preserving Compressive Analysis Using Subspace-Based Dictionary for ECG Telemonitoring System.	1. In off-line stage, the subspace-based dictionary is built by dividing signal space into discriminative and complementary subspace. 2.In on-line stage, the encryption and decoding protocol is proposed using the pre-trained dictionary.	1. Insufficient privacy: Even though CS-based encryption can achieve a computational notion secrecy through the set of measurement matrices. 2.High complexity decryption: These frameworks decrypt signal through recovering the measurements.
8.Data Security and Privacy in Wireless Body Area Networks.	1. Confidentiality. 2. Dynamic integrity assurance. 3. Dependability.	1. The signature size is small, and computation and storage overhead are low. 2.A drawback is that it does not allow a third party to carry out integrity checks.

2.ISSUES IN THE SYSTEM

In the existing system of privacy preserving priorityon patient data,

- The access control policies are proper techniques used for privacy-preserving. Most of time, hybrid access control policies are adopted to propose a privacy-preserving access control mechanisms.
- It is common to use the combination of the access control and the pseudonymization in one privacy-preserving scheme, which stores the users' data in an anonymized manner, and shared the anonymized data according to the access control policies.
- A patient monitoring scheme was proposed to give patients control over who can access their protected health information (PHI).
- The privacy-preserving healthcare schemes based on the encrypted data have some issues like accuracy and efficiency to be solved.
- Seriously raises concerns about leaking and misusing of users' sensitive privacy data
- Some attackers may crack the users' smartphones or the wban-gateways, and steal the sensitive users' personal information and the healthcare center's intellectual properties.

3.CONSTRUCTION

- Some attackers may crack the users' smartphones or the WBAN-gateways, and steal the sensitive users' personal information and the healthcare center's intellectual properties medical packets to the healthcare center through WBANgatways.
- First, we propose the PPC scheme, an efficient privacypreserving non-interactive priority classification scheme for users' medical packets in WBAN-gateways. Particularly, The WBAN-gateways derive the priorities of the medical packets and relay the packets in a priority heaps.
- The results show that the proposed PPC scheme is efficient in both computational cost and communication overhead.

- The security analysis also demonstrates that our proposed PPC scheme can preserve the privacy of the users' personal information and the confidentiality of the healthcare center's disease models.

4.SYSTEMARCHITECTURE

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required

4.1 PROPOSED ARCHITECTURE

The proposed architecture contains user, Gateway,Healthcarecenter.The proposed architecture is as follows.

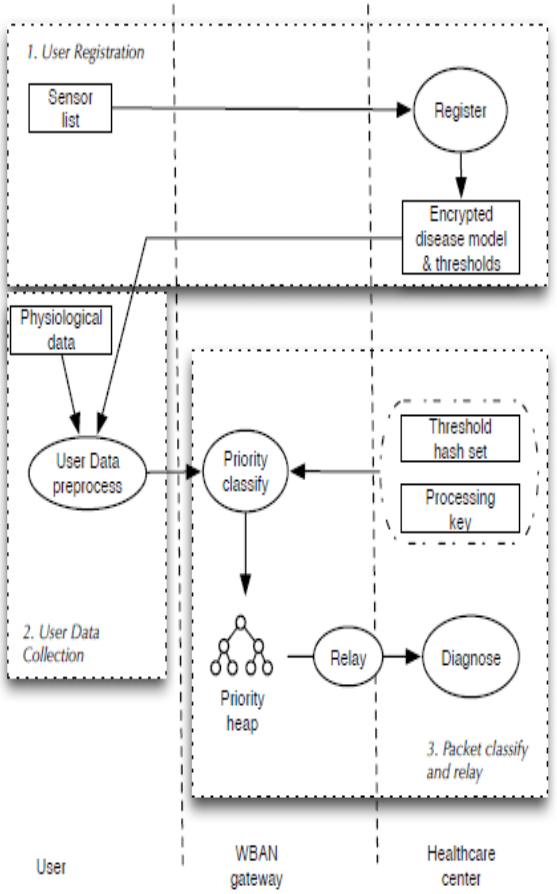

Fig.4.1 Proposed Architecture

- The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
- The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
- DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

- DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

5.IMPLEMENTATION DETAILS

The algorithms used in the proposed system are,

- Attribute Based Encryption
- Ciphertext-Policy Attribute Based Encryption

5.1 ATTRIBUTE BASED ENCRYPTION

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country in which they live, or the kind of subscription they have). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. A crucial security aspect of attribute-based encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

The concept of attribute-based encryption was first proposed by AmitSahai and Brent Waters and later. Recently, several researchers have further proposed Attribute-based encryption with multiple authorities who jointly generate users private keys. Attribute-based encryption (ABE) can be used for log encryption.Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients attributes. This primitive can also be used for broadcast encryption in order to decrease the number of keys used.Attribute-based encryption methods are also widely employed in vector-driven search engine interfaces.

5.2 CIPHERTEXT-POLICY ATTRIBUTE BASED ENCRYPTION

CP-ABE (Ciphertext-Policy Attribute-Based Encryption) with hidden access control policy enables data owners to share their encrypted data using cloud storage with authorized users while keeping the access control policies blinded.CP-ABE (Ciphertext-Policy Attribute-Based Encryption) is more appropriate, as it enables the data owner to more freely define the access control policy. Moreover, because the access control policy itself may leak critical information, efforts have been made to hide the access control policy by blinding the attributes within it.

However, the data owner may unavoidably release some data onto the cloud storage whereby either there may exist a conflict of interest or one can derive sensitive or confidential data from the released data. For example, the data owner may release two data objects (a data object refers to an encryption data unit in CP-ABE scenario, e.g., a file, a message) and to the cloud, to which the Chinese Wall security policy should be applied, as and are competitors. Any authorized user of the two data objects can freely access either data object, but once he/she has accessed one of them, he/she can no longer access the other. In the CP-ABE scenario, it is inappropriate to split all users into two mutually disjoint sets beforehand by choosing an access structure for the two data objects. This is because an authorized user is initially supposed to be able to access either of the two data objects freely. The relations among the data released to the cloud storage are substantially more complicated. Other types of data sets exist as well. We emphasized the situation in which a user's consecutive access to any data out of may yield a conflict of interest or disclosure of some sensitive data. This type of data set has been studied in primary access control constraints such as SOD (Separation of Duty) of RBAC (Role-Based Access Control) and the Chinese Wall security policy; we call this kind of data set a sensitive data set in this paper. The handling of the sensitive data set problem for cloud storage should be considered. Some work has been conducted on such data sets. However, for cloud storage, where the access control is realized via CP-ABE, there remains no such mechanism for effectively controlling a user's successive access to data objects from a data owner's sensitive data set to prevent commercial fraud, mistakes, or the leakage of critical information.

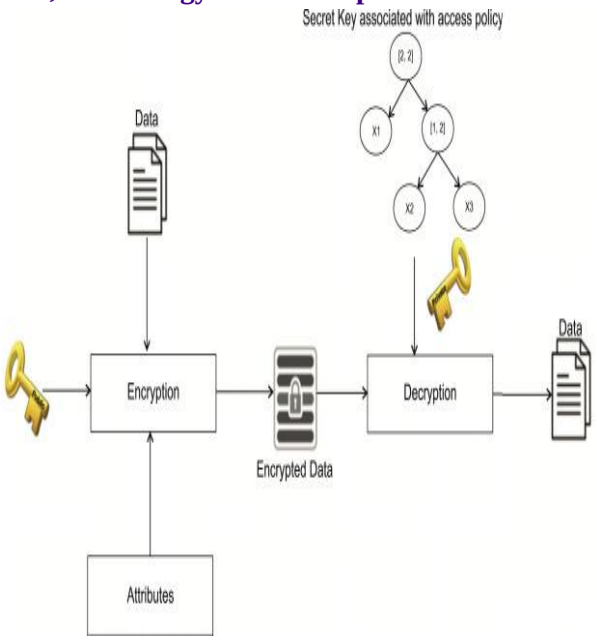

Fig.5 Attribute Based Encryption

6.CONCLUSION

In this paper, we have proposed an efficient privacy preserving priority classification (PPC) scheme on patient healthcare data in remote e-Healthcare system. The proposed PPC scheme achieves the priority classification and packets relay tasks, while preserving the privacy of the users and the confidentiality of the healthcare center's disease models. Because it is a non-interactive procedure, the communication cost is low.

6.1 FUTURE ENCHANCEMENT

The future scope for the proposed method might be thedevelopment of an enhanced PPC scheme that canhave the authentication module along with encryptionand decryption. Meanwhile the work can be enhancedfor further data for security. Similarly the PPC scheme technique can be developed for effective security in the remote E-healthcare system.

The further work may contain combination of thismethod to message digesting algorithms. Further workincludes adapting the free parameters of the logisticchaotic map using soft computing techniques as chaos systems are highly sensitive to initial conditions.

REFERENCES

1) C. A. Otto, E. Jovanov, and A. Milenkovic, "A wban-based system for health monitoring at home," in Ieee/embs International Summer School on Medical Devices and BIOSENSORS, 2006, pp. 20–23.
2) O. Omeni, A. Wong, A. J. Burdett, and C. Toumazou, "Energy efficient medium access protocol for wireless medical body area sensor networks," IEEE Transactions on Biomedical Circuits & Systems, vol. 2, no. 4, p. 251, 2008.
3) A. Argyriou, A. C. Breva, and M. Aoun, "Optimizing data forwarding from body area networks in the presence of body shadowing with dualwireless technology nodes," Mobile Computing IEEE Transactions on, vol. 14, no. 3, pp. 632–645, 2015.
4) S. Rezvani and S. A. Ghorashi, "Context aware and channel-based resource allocation for wireless body area networks," Iet Wireless Sensor Systems, vol. 3, no. 1, pp. 16–25, 2013.
5) N. Mcdonald, D. Atkinson, Y. Khmelevsky, and S. Mcmillan, "Sport wearable biometricdata encrypted emulation and storage in cloud," in Electrical and Computer Engineering, 2016, pp. 1–4.
6) M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Communications, vol. 17, no. 1, pp. 51–58, 2016.
7) Z. Chen, H. Hu, and J. Yu, "Privacy-preserving large-scale location monitoring using bluetooth low energy," in International Conference on Moile Ad-Hoc and Sensor Networks, 2016, pp. 69–78.
8) C. Y. Chou, E. J. Chang, H. T. Li, and A. Y. Wu, "Low-complexity privacy-preserving compressive analysis using subspace-based dictionary for ecgtelemonitoring system," IEEE Transactions on Biomedical Circuits & Systems, vol. PP, no. 99, pp. 1–11, 2018.

9) C. Dwork and M. Naor, “On the difficulties of disclosure prevention in statistical databases or the case for differential privacy,” Journal of Privacy & Confidentiality, 2008.

10) M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart, “Privacy in pharmacogenetics: an end-to-end case study of personalized warfarin dosing,” in Usenix Conference on Security Symposium, 2014, pp. 17–32.

11) B. Dan and M. Zhandry, “Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation,” in Cryptology Conference, 2014, pp. 480–499.

12) M. V. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, Fully Homomorphic Encryption over the Integers. Springer Berlin Heidelberg, 2010.

13) B. Dan, E. J. Goh, and K. Nissim, “Evaluating 2-dnf formulas on ciphertexts,” in International Conference on Theory of Cryptography, 2005, pp. 325–341.

14) D. Harrison, S. Boyce, P. Loughnan, P. Dargaville, H. Storm, and L. Johnston, “Skin conductance as a measure of pain and stress in hospitalised infants,” Early Human Development, vol. 82, no. 9, pp. 603–608, 2006.

15) G. Wang, R. Lu, and C. Huang, “Pguide: An efficient and privacypreserving smartphone-based pre-clinical guidance scheme,” in IEEE Global Communications Conference, 2015, pp. 1–6.

16) P. Anooj, “Clinical decision support system: Risk level prediction of heart disease using weighted fuzzy rules,” Journal of King Saud UniversityComputer and Information Sciences, vol. 24, no. 1, pp. 27–40, 2012.

17) J. B. G. Jr, “Regression analysis and forecasting models,” Introduction to Financial Forecasting in Investment Analysis, pp. 277–301, 2007.

18) A. Ara, M. Al-Rodhaan, T. Yuan, and A. Al-Dhelaan, “A secure privacypreserving data aggregation scheme based on bilinear elgamal cryptosystem for remote health monitoring systems,” IEEE Access, vol. 5, no. 99, pp. 12 601–12 617, 2017.

19) G. Wang, R. Lu, and C. Huang, “Pslp: Privacy-preserving single-layer perceptron learning for e-healthcare,” in International Conference on Information, Communications and Signal Processing, 2016, pp. 1–5.

20) G. Wang, R. Lu, and Y. Guan, “Enabling efficient and privacy-preserving health query over outsourced cloud,” IEEE Access, vol. PP, pp. 1–1, 11 2018