Cloud Supported Enhanced Secure Remote Health Monitoring

Nakkala Ajay Babu, S. Rama Krishna,

M-tech Student Scholar,Department of Computer Science Engineering,VRS & YRN College of Engineering & Technology, Chirala,Prakasam (Dt); Andhra Pradesh, India.

Assistant Professor &H.O.D,Department of Computer Science Engineering,VRS & YRN College of Engineering &Technology, Chirala ,Prakasam (Dt), Andhra Pradesh, India.

Abstract — Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. This paper is to address this important problem and design a cloud-assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. Moreover, the outsourcing decryption technique and a newly-proposed key private proxy re-encryption are adapted to shift the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design.

The enhancement of this system aims to improve the quality of remote health monitoring system by dynamically generating tokens to decrypt the contents of the database. These dynamically generated tokens are valid only for a certain time period and after this threshold time period they expire and do not allow the patient to view the recommended treatment. By implementing this mechanism, the quality of remote health monitoring systems is improved. Using this mechanism, the latest physiological status of the patient is presented as a query to the system and the doctor is able to recommend the required medication accordingly within the time span. Once the time span is over, the tokens are expired and the patient will have to resubmit his latest physiological status as a query to get the recommended medication/ suggestions.

Index Terms—Mobile health (mHealth), Healthcare, Privacy, Outsourcing decryption, Key private proxy re-encryption.

I. INTRODUCTION

Wide deployment of mobile devices, such as smart phones equipped with low cost sensors, has already shown great potential in improving the quality of healthcare services. Remote mobile health monitoring has already been recognized as not only a potential, but also a successful example of mobile health (mHealth) applications especially for developing countries. The Microsoft launched project "MediNet" is designed to realize remote monitoring on the health status of diabetes and cardiovascular diseases in remote areas in Caribbean countries [1]. In such a remote mHealth monitoring system, a client could deploy portable sensors in wireless body sensor networks to collect various physiological data, such as blood pressure (BP), breathing rate (BR), Electrocardiogram (ECG/EKG), peripheral oxygen saturation (SpO2) and blood glucose. Such physiological data could then be sent to a central server, which could then run various web medical applications on these data to return timely advice to the client. These applications may have various functionalities ranging from sleep pattern analyzers, exercises, physical ac-tivity assistants, to cardiac analysis systems, providing various medical consultation [2]. Moreover, as the emerging cloud computing technologies evolve, a viable solution can be sought by incorporating the software as a service (SaaS) model and pay-as-you-go business model in cloud computing, which would allow small companies (healthcare service providers) to excel in this healthcare market. It has been observed that the adoption of automated decision support algorithms in the cloud-assisted mHealth monitoring has been considered as a future trend [3].

Unfortunately, although cloud-assisted mHealth monitoring could offer a great opportunity to improve the quality of healthcare services and potentially reduce healthcare costs, there is a stumbling block in making this technology a reality. Without properly addressing the data management in an mHealth system, clients' privacy may be severely breached during the collection, storage, diagnosis, communications and computing. A recent study shows that 75% Americans con-sider the privacy of their health information important or very important [4]. It has also been reported [5] that patients' willingness to get involved in health monitoring program could be severely lowered when people are concerned with the privacy breach in their voluntarily submitted health data. This privacy concern will be exacerbated due to the growing trend in privacy breaches on electronic health data.

Although the existing privacy laws such as HIPAA (Health Insurance Portability and Accountability Act) provide base-line protection for personal health record, they are generally considered not applicable or transferable to cloud computing environments [6]. Besides, the current law is more focused on protection against adversarial intrusions while there is little effort on protecting clients from business collecting private information. Meanwhile, many companies have significant commercial interests in collecting clients' private health data [7] and sharing them with either insurance companies, research institutions or even the government agencies. It has also been indicated [8] that privacy law could not really exert any real protection on clients' data privacy unless there is an effective mechanism to enforce restrictions on the activities of healthcare service providers.

Traditional privacy protection mechanisms by simply re-moving clients' personal identity information (such as names or SSN) or by using anonymization technique fails to serve as an effective way in dealing with privacy of mHealth systems due to the increasing amount and diversity of personal identifiable information [9]. It is worth noting that the collected information from an mHealth monitoring system could contain clients' personal physical data such as their heights, weights, and blood types, or even their ultimate personal identifiable information such as their fingerprints and DNA profiles [10]. According to [11], personal identifiable information (PII) is "any information, recorded or otherwise, relating to an identifiable individual. Almost any information, if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputation-al". In other words, the scope of PII might not necessarily be restricted to SSN, name and address, which are generally considered as PII in the traditional sense. Indeed, the state of the art re-identification techniques [12], [13] have shown that any attribute could become personal identifiable information in practice [9]. Moreover, it is also noted that although some attribute may be uniquely identifying on its own, "any attribute can be identifying in combination with others, while no single element is a (quasi)-identifier, any sufficiently large subset uniquely identifies the individual" [12]. The proposed mobile health monitoring scenario provides a good opportunity for adversaries to obtain a large set of medical information, which could potentially lead to identifying an individual user. Indeed, several recent works [14]–[16] have already shown that even seemingly benign medical information such as blood pressure can be used to identify individual users. Furthermore, it is also observed that future mobile health monitoring and decision support systems might have to deal with other much more privacy-sensitive features such as DNA profiles [17], from which an adversary may be able to re-identify an individual user [18], [19]. Traditionally, the privacy issue is tackled with anonymization technique such as *k*-anonymity or *l*-diversity. However, it has been indicated that these techniques might be insufficient to prevent re-identification attack [9]. The threat of re-identification is so serious that legal communities [20] have already been calling for more sophisticated protection mechanism instead of merely using anonymization. We believe that our proposed cryptographic based systems could serve as a viable solution to the privacy problems in mHealth systems, and also as an alternative choice for those privacy-aware users.

Another major problem in addressing security and privacy is the computational workload involved with the cryptographic techniques. With the presence of cloud computing facilities, it will be wise to shift intensive computations to cloud servers from resource-constrained mobile devices. However, how to achieve this effectively without compromising privacy and security become a great challenge, which should be carefully investigated.

As an important remark, our design here mainly focuses on insider attacks, which could be launched by either malicious or non-malicious insiders. For instance, the insiders could be disgruntled employees or healthcare workers who enter the healthcare business for criminal purpose [21], [22]. It was reported that 32% of medical data breaches in medical establishments between January 2007 and June 2009 were due to insider attacks [23], and the incident rate of insider attacks is rapidly increasing [23]. The insider attacks have cost the victimized institutions much more than what outsider attacks have caused [24]. Furthermore, insider attackers are generally much harder to deal with because they are generally sophisticated professionals or even criminal rings who are adept at escaping intrusion detection [22]. On the other hand, while outsider attacks could be trivially prevented by directly adopting cryptographic mechanisms such as encryption, it is non-trivial to design a privacy preserving mechanism against the insider attacks because we have to balance the privacy constraints and maintenance of normal operations of mHealth systems. The problem becomes especially trickier for cloud-assisted mHealth systems because we need not only to guaran-tee the privacy of clients' input health data, but also that of the output decision results from both cloud servers and healthcare service providers (which will be referred to as *the company* in the subsequent development).

In this paper, we design a cloud-assisted mHealth moni-toring system (CAM). We first identify the design problems on privacy preservation and then provide our solutions. To ease the understanding, we start with the basic scheme so that we can identify the possible privacy breaches. We then provide an improved scheme by addressing the identified privacy problems. The resulting improved scheme allows the mHealth service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely. To reduce clients' decryption complexity, we incorporate the recently proposed outsourcing decryption technique [25] into the underlying multi-dimensional range queries system to shift clients' computational complexity to the cloud without revealing any information on either clients' query input or the decrypted decision to the cloud. To relieve the computational complexity on the company's side, which is proportional to the number of clients, we propose a further improvement, leading to our final scheme. It is based on a new variant of key private proxy re-encryption scheme, in which the company only needs to accomplish encryption once at the setup phase while shifting the rest computational tasks to the cloud without compromising privacy, further reducing the computational and communication burden on clients and the cloud.

In the present system, when the user submits a query about his health status to get a recommendation, tokens are generated. The user might have the same health status without improvement and when this query is submitted, the stale token which is generated might show the same medication/ treatment over and over again which can significantly affect the quality of services provided by the remote health monitoring systems. This will have a negative impact on the health of the patient as well. By setting an expiration time on the dynamically generated tokens, we provide the opportunity to the patient to re-submit his latest physiological status and there by the doctors can review the developments and suggest appropriate medication/ treatment and thus enhancing the quality of services provided by the remote health monitoring system.

II. Related work

Most of current private telemonitoring schemes [51] are based on anonymization, which are ineffective as we alluded before. Another line of work focuses on privacy preserving diagnostic programs [26], [27]. At the end of protocol run, a client obtains nothing on the diagnostic program but the diagnostic result while the company obtains no information on the client's private data. All the existing solutions require the client run multiple instances of oblivious transfer protocol with the company after setup phase, which means the company has to stay online constantly. All the current solutions [31], [26], [27] are based on garbled circuits, which implies a client must download the whole circuit to his device and complete the decryption on his own. Besides, the private computation or processing of medical information over the cloud has also attracted attention from both the security community [28], [29] and signal processing community [30], [31]. These works can be divided into two categories: providing a solution for a specific scenario such as private genomic test [29] or private classification of users' electrocardiogram (ECG) data [30], or proposing a general framework for private processing of monitored data [28] or electronic health records [31]. Although these schemes are based on cloud computing, they do not emphasize on how to transfer the workload of the involved parties to the cloud without violating the privacy of the involved parties. Since our application scenario assumes the clients hold relatively resource-constrained mobile devices in a cloud assisted environment, it would be helpful if a client could shift the computational workload to the cloud.

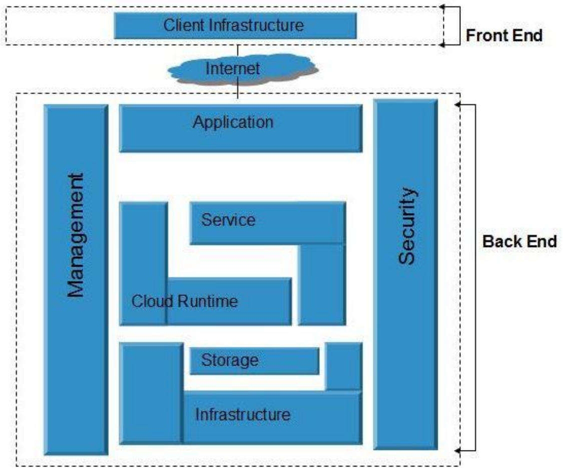
However, there seems no trivial approach to outsourcing the decryption of garbled circuit currently. Our proposed system adopts the recently proposed decryption outsourcing to significantly reduce the workload of both the company and clients by outsourcing the majority of the computational tasks to the cloud while keeping the company offline after the initialization phase [32].

The Cloud Computing architecture

The Cloud Computing architecture comprises of many cloud components, each of them are loosely coupled. We can broadly divide the cloud architecture into two parts:

- Front End
- Back End

Each of the ends are connected through a network, usually via Internet. The following diagram shows the graphical view of cloud computing architecture:



FRONT END

Front End refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, e.g., Web Browser.

BACK END

Back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

IMPORTANT POINTS

It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols.

The server employs certain protocols, known as middleware, helps the connected devices to communicate with each other.

Cloud based delivery

Software as a service (SaaS)

The software-as-a-service (SaaS) service-model involves the cloud provider installing and maintaining software in the cloud and users running the software from their cloud clients over the Internet (or Intranet). The users' client machines require no installation of any application-specific software - cloud applications run on the server (in the cloud). SaaS is scalable, and system administration may load the applications on several servers. In the past, each customer would purchase and load their own copy of the application to each of their own servers, but with the SaaS the customer can access the application without installing the software locally. SaaS typically involves a monthly or annual fee

Software as a service provides the equivalent of installed applications in the traditional (non-cloud computing) delivery of applications.

Software as a service has four common approaches:

1. single instance
2. multi instance
3. multi-tenant
4. flex tenancy

Development as a service (DaaS)

Development as a service is web based, community shared development tools. This is the equivalent to locally installed development tools in the traditional (non-cloud computing) delivery of development tools.

Platform as a service (PaaS)

Platform as a service is cloud computing service which provides the users with application platforms and databases as a service. This is equivalent to middleware in the traditional (non-cloud computing) delivery of application platforms and databases.

Infrastructure as a service (IaaS)

Infrastructure as a service is taking the physical hardware and going completely virtual (e.g. all servers, networks, storage, and system management all existing in the cloud). This is the equivalent to infrastructure and hardware in the traditional (non-cloud computing) method running in the cloud. In other words, businesses pay a fee (monthly or annually) to run virtual servers, networks, storage from the cloud. This will mitigate the need for a data center, heating, cooling, and maintaining hardware at the local level.

Cloud networking

Generally, the cloud network layer should offer:

- High bandwidth (low latency)
  Allowing users to have uninterrupted access to their data and applications.

III. EXISTING SYSTEM

Existing Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. CAM consists of four parties: the cloud server (simply the cloud), the company who provides the mHealth monitoring service (i.e., the healthcare service provider), the individual clients (simply clients), and a semi-trusted authority (TA). The company stores its encrypted monitoring data or program in the cloud server. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud server through a mobile (or smart) device. A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model. The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual interest with the company. However, the company and TA could collude to obtain private health data from client input vectors.

IV. PROPOSED SYSTEM

In the present system, when the user submits a query about his health status to get a recommendation, tokens are generated. The user might have the same health status without improvement and when this query is submitted, the stale token which is generated might show the same medication/ treatment over and over again which can significantly affect the quality of services provided by the remote health monitoring systems. This will have a negative impact on the health of the patient as well. By setting an expiration time on the dynamically generated tokens, we provide the opportunity to the patient to re-submit his latest physiological status and there by the doctors can review the developments and suggest appropriate medication/ treatment and thus enhancing the quality of services provided by the remote health monitoring system.

V. CONCLUSION

In this paper, we design a cloud-assisted privacy preserving mobile health monitoring system, called CAM, which can effectively protect the privacy of clients and the intellectual proerty of mHealth service providers. To protect the clients' privacy, we apply the anonymous Boneh-Franklin identity-based encryption (IBE) in medical diagnostic branching pro-grams. To reduce the decryption complexity due to the use of IBE, we apply recently proposed decryption outsourcing with privacy protection to shift clients' pairing computation to the cloud server. To protect mHeath service providers' programs, we expand the branching program tree by using the random permutation and randomize the decision thresholds used at the decision branching nodes. Finally, to enable resource-constrained small companies to participate in mHealth busi-ness, our CAM design helps them to shift the computational burden to the cloud by applying newly developed key private proxy re-encryption technique. Our CAM has been shown to achieve the design objective. By implementing the above discussed quality improvement mechanism, we were able to monitor the patient's health more effectively.

REFERENCES

[1] P. Mohan, D. Marin, S. Sultan, and A. Deen, "Medinet: personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony." Conference Proceedings of

the International Conference of IEEE Engineering in Medicine and Biology Society, vol. 2008, no. 3, pp. 755–758. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/19162765

[2] A. Tsanas, M. Little, P. McSharry, and L. Ramig, "Accurate telemoni-toring of parkinson's disease progression by noninvasive speech tests," Biomedical Engineering, IEEE Transactions on, vol. 57, no. 4, pp. 884– 893, 2010.

[3] G. Clifford and D. Clifton, "Wireless technology in disease management and medicine," Annual Review of Medicine, vol. 63, pp. 479–492, 2012.

[4] L. Ponemon Institute, "Americans' opinions on healthcare privacy, available: http://tinyurl.com/4atsdlj," 2010.

[5]A. V. Dhukaram, C. Baber, L. Elloumi, B.-J. van Beijnum, and P. D. Stefanis, "End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust," in PervasiveHealth, 2011, pp. 478–484.

[6] M. Delgado, "The evolution of health care it: Are current u.s. privacy policies ready for the clouds?" in SERVICES, 2011, pp. 371–378.

[7] N. Singer, "When 2+ 2 equals a privacy question," New York Times, 2009.

[8] E. B. Fernandez, "Security in data intensive computing systems," in Handbook of Data Intensive Computing, 2011, pp. 447–466.

[9] A. Narayanan and V. Shmatikov, "Myths and fallacies of personally identifiable information," Communications of the ACM, vol. 53, no. 6, pp. 24–26, 2010.

[10] P. Baldi, R. Baronio, E. D. Cristofaro, P. Gasti, and G. Tsudik, "Coun-tering gattaca: efficient and secure testing of fully-sequenced human genomes," in ACM Conference on Computer and Communications Security, 2011, pp. 691–702.

[11] A. Cavoukian, A. Fisher, S. Killen, and D. Hoffman, "Remote home health care technologies: how to ensure privacy? build it in: Privacy by design," Identity in the Information Society, vol. 3, no. 2, pp. 363–378, 2010.

[12] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008, pp. 111–125.

[13] "De-anonymizing social networks," in IEEE Symposium on Secu-rity and Privacy. IEEE Computer Society, 2009, pp. 173–187.

[14] I. Neamatullah, M. Douglass, L. Lehman, A. Reisner, M. Villarroel, W. Long, P. Szolovits, G. Moody, R. Mark, and G. Clifford, "Automated de-identification of free-text medical records," BMC medical informatics and decision making, vol. 8, no. 1, p. 32, 2008.

[15] S. Al-Fedaghi and A. Al-Azmi, "Experimentation with personal identi-fiable information," Intelligent Information Management, vol. 4, no. 4, pp. 123–133, 2012.

[16] J. Domingo-Ferrer, "A three-dimensional conceptual framework for database privacy," Secure Data Management, pp. 193–202, 2007.

[17] T. Lim, Nanosensors: Theory and Applications in Industry, Healthcare, and Defense. CRC Press, 2011.

[18] X. Zhou, B. Peng, Y. Li, Y. Chen, H. Tang, and X. Wang, "To release or not to release: evaluating information leaks in aggregate human-genome data," Computer Security–ESORICS 2011, pp. 607–627, 2011.

[19] R. Wang, Y. Li, X. Wang, H. Tang, and X. Zhou, "Learning your identity and disease from research papers: information leaks in genome wide association study," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 534–544.

[20] P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," UCLA Law Review, vol. 57, p. 1701, 2010.

[21] P. Institute, "Data loss risks during downsizing," 2009.

[22] P. Dixon, "Medical identity theft: The information crime that can kill you," in The World Privacy Forum, 2006, pp. 13–22.

[23] K. E. Emam and M. King, "The data breach analyzer," 2009, [Available at: http://www.ehealthinformation.ca/dataloss].

[24] E. Shaw, K. Ruby, and J. Post, "The insider threat to information systems: The psychology of the dangerous insider," Security Awareness Bulletin, vol. 2, no. 98, pp. 1–10, 1998.

[25] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts," in Usenix Security, 2011.

[26] M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A. Sadeghi, and T. Schneider, "Secure evaluation of private linear branching programs with medical applications," Computer Security–ESORICS 2009, pp. 424–439, 2009.

[27] M. Barni, P. Failla, R. Lazzeretti, A. Sadeghi, and T. Schneider, "Privacy-preserving ecg classification with branching programs and neural net-works," Information Forensics and Security, IEEE Transactions on, vol. 6, no. 2, pp. 452–468,

2011.
[28] G. Danezis and B. Livshits, "Towards ensuring client-side computational integrity," in Proceedings of the 3rd ACM workshop on Cloud computing security workshop. ACM, 2011, pp. 125–130.
[29] E. De Cristofaro, S. Faber, P. Gasti, and G. Tsudik, "Genodroid: are privacy-preserving genomic tests ready for prime time?" in Proceedings of the 2012 ACM workshop on Privacy in the electronic society. ACM, 2012, pp. 97–108.
[30] R. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection."
[31] V. Danilatou and S. Ioannidis, "Security and privacy architectures for biomedical cloud computing," in Information Technology and Applications in Biomedicine (ITAB), 2010 10th IEEE International Conference on. IEEE, 2010, pp. 1–4.
[32] CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring, IEEE Transactions on Cloud Computing 2013

AUTHOR'S PROFILE

AJAY BABU .NAKKALA received M.C.A from Bapatla Engineering College, Bapatla, Gutur Dst, Andhra Pradesh. and currently pursuing M.Tech in Computer Science Engineering at VRS & YRN College of Engineering &Technology, Chirala; Prakasam (Dt), Andhra Pradesh. His areas of interest area include Cloud Computing.

MR. S. RAMA KRISHNA is presently working as Associate professor and Head of CSE Department in VRS & YRN College of Engineering & Technology, Chirala, AP, India. He completed his B.Tech degree in Computer Science and Engineering from JNTUH, Hyderabad. And then completed his M.Tech. in Computer Science and Engineering as his specialization from JNTUH, Hyderabad. Now he is pursuing his Ph.D Degree in Computer Science and Engineering from JNTUH, Hyderabad. His research areas include Cloud Computing and Security. He has a teaching experience of 10 years. He published papers in 3 International Journals and 1 National Conference.