Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES) – An International Journal
ISSN: 2566-932X, Vol. 2, Issue 5, August 2018
Proceedings of National Conference on Knowledge Discovery in Information Technology and Communication Engineering (KITE 18), May 2018

Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing

Shalini K M, Siddiqa Anjum, Suchitra C, Veena M, Shefali Arora
Department of Information Science, EPCET , Bangalore.

Abstract: With the advancement of wearable medical devices remote health monitoring and elderly health care has become a popular application. The data collected from patient through wearable devices (like heartbeat, blood pressure etc) has to be passed to application running in cloud to implement various services like expert advice, emergency assistance etc. The data of patients when stored in cloud can be attacked by intruders and can be stolen or corrupted. Existing solution are based on encrypting the data and storing in cloud. By these solutions can be attacked and encryption keys can be broken and all data can be still stolen. In this project we propose a cloud let based solution for providing enhanced security to patient health care data.

Keywords: Cloud; Cloudlet; Encryption; Intruders; Security; Wearable Devices

I. INTRODUCTION

The huge amount of data collected by Body area network(BAN) nodes demands scalable, on-demand, powerful, and secure storage and processing infrastructure. Cloud computing is playing a significant role in achieving the aforementioned objectives. The cloud computing environment links different devices ranging from miniaturized sensor nodes to high-performance supercomputers for delivering people-centric and context centric services to the individuals and industries. The possible integration of BANs with cloud computing will introduce viable and hybrid platform that must be able to process the huge amount of data collected from multiple BANs. This BAN-cloud will enable end users to globally access the processing and storage infrastructure at economical costs. Because BANs forward useful and life-critical information to the cloud – which may operate in distributed and hostile environments, novel security mechanisms are required to prevent malicious interactions to the storage infrastructure. Both the cloud providers and the users must take strong security measures to protect the storage infrastructure.

A. Proposed Architecture

The architecture of the system is given below Figure below shows a top level overview of our proposed Cloudlet-based BAN data collection system. The system is composed of sets of BANs. The BANs are composed of multiple users (each user is equipped with BAN), who are able to transmit the collected data by the BAN to the outside of the body, as described in Section I. A group of BAN users can be virtually clustered around one cloudlet server that is representing cloud computing capabilities in a small scale which is sufficient to handle a BAN user within the cluster, as we discussed in Section I. The cloudlet system is composed of set of physical servers with many cores and huge Gigabytes of memory. The cloudlet server system is equipped with one or more of the communication antennas that is supporting different physical layer capabilities (e.g.Wi-Fi and WiMax).

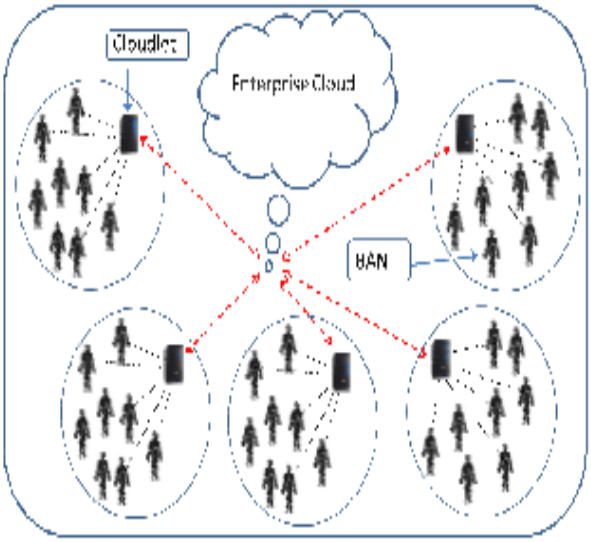

Fig 1. Mesh Topology

The most important part of the cloudlet server is the storage system. The storage system should provide scalable and reliable environment for storing large data size. Different cloudlet systems could be connected with each other using wired or wireless communication links (e.g. WiMax). Furthermore, cloudlet system could be connected directly to an enterprise cloud system using wired or wireless communication links. The enterprise cloud system is centralized management and storage point that can be accessed by different organizations that are interested in a certain type of data. Another important feature of the cloudlet system is that the ability of the bidirectional communications between many BANs users. In addition to its ability to receive data from multiple

users, the cloudlet system is also able to communicate with multiple users based on the usage scenario. In this work, a cloudlet based solution is proposed. Using of cloudlet for security of medical data is not considered in any of work, so this work is important. After the data is collected from devices attached to patients, data is encrypted using Number theory research unit method .The data is transported to nearby cloudlet, this is major difference from existing solutions. To protect the data at cloudlet a collaborative intrusion detection method based on cloudlet mesh –whereby trust model is built across mesh to identify malicious cloudlet. The data at cloudlet can also be stored in cloud, based on user preferences but in this case , the data is split to parts, so that privacy is not leaked.

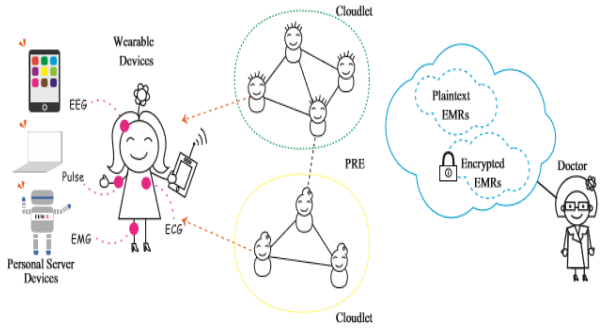

Fig 2. Illustration of the system architecture

B. Encryption at the user end

Usually, the data collected by smart clothing are all unsigned integer vectors. For example, for heart rate data, the average heart beats detected each minute is denoted by hr and the plain data shall be [hr,0,••• ,0]. We need to define clear space and cipher space for the encryption. As the definition of the polynomial ring is R := Z[x]/(xn +1), in the case of an arbitrary positive integer q, the definition of the quotient ring is known as Rq = R/qR. We define the clear space as Rp, so that the length is n and the integer vector is modulus p, which is always between 2 and 210. The cipher space is Rq, so the length is n and the integer vector is modulus p. In consideration of bandwidth, we generally make the Rq pass using the Chinese Remainder Transform (CRT) representation. For the sake of initial safety, we have n = 1024 and q = 32. We hereby describe the processes of encryption and deciphering in the following. • KeyGen()→ (pk,sk): let f ∈R,g∈ R, while f,g follows the discrete Gaussian distribution, f = 1 mod q,and f is reversible. Thus, the secret key is denoted by sk = f; the public key is denoted by pk = h = g•f−1 mod q. • Enc(pk = h,μ ∈Rp)→ c ∈Rq: let r ∈R,m∈R,m = μ mod p. Both m′ and r follow the discrete Gaussian distribution, and we have m = p•m′ + μ,c = p•r•h + m mod q. • Dec(sk = f,c∈Rq) → μ: calculate ¯ b = f •c mod q, and make it an integer polynomial b, with factors within [−q/2,q/2). Thus, we have μ = b mod p.

The encrypted data will be transmitted to the smartphone with the homomorphic processing. We assume that the clear data of heart beat is [hr,0,...,0] and the array encryption is c1. In the same way, if the blood pressure is bp, then the clear data is denoted as [0,bp,0,...,0] and the enciphered data shall be c2. This way, we can get clear data and cipher data of all sensors. Since we use a public key encryption system and homomorphic encryption(HE),the smart phone can receive data{c1,c2,...,cn} transmitted to cagg = c1 + ... + cn mod q. Therefore, after we process the data with homomorphic encryption, the bandwidth is reduced effectively before the data are uploaded to the cloudlet, thus achieving energy and bandwidth savings.

II. RELATED WORKS

A. Literature survey

Jin Sun., Yupu Hu., Leyou Zhang., "A Key Policy Attribute Based Broadcast Encyption" in The International Arab Journal of Information Technology, Vol. 10, No. 5, September 2013

In the work of Jin sun , the key policy ABE is associated with the broadcast encryption to provide a dual system encryption. With this standard model, the scheme can achieve fixed-size public criterion, force no bound on attribute set size used for encryption.

Jaatun, M.G., Zhao, G., and Rong, C., "Identity Based Authentication for Cloud Computing", (Eds.): CloudCom 2009, LNCS 5931, pp. 157–166, 2009.© Springer-Verlag Berlin Heidelberg 2009

In this work, SSL Authentication Protocol is applied in cloud computing, will become so complicated that users will undergo a bulk point both in computation and communication. It based on the identity-based hierarchical model for cloud computing

Vishnu sekar. R., Nandhini. N., Bhanumathy. D., Hemalatha. M., "Identity based authentication for data stored in cloud", in international journal of Advanced research in Computer science and software engineering, vol 5, No.2, March 2015.

the authors proposed a dynamic authentication protocol that can support dynamic operations in cloud. This enables only valid users to authenticate in cloud.

Cong Wang., Qian Wang., KuiRen., "Privacy Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions On Computers, vol. 64, no. 5, may 2012.

In this work, Wang proposed public auditing scheme which provides aentire outsourcing result of data not only the data itself, but also its integrity checking. It involves public auditability to allow TPA to verify the correctness of the cloud data and also ensure that there exists no cheating cloud server.

Qian Wang., Cong Wang., Jin Li1., Kui Ren1., and Wenjing Lou., "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing" in

Proc. of ASI-ACRYPT'08. SpringerVerlag, 2008, pp. 90–107.

In this work ,qianwang proposed a Merkle hash tree technique to improve the proof of retrievability. A hash tree is a tree of hashes in which the leaves are data blocks hashes in, for instance, a file or set of files. Nodes added up in the tree are the hashes of their corresponding children.

B. Improvement Approach

Our work is closely related to cloud-based privacy preserving and cloudlet mesh based collaborative IDS. We will give a brief review of the works in these aspects.

a) Cloud-based Privacy Preservation :

Despite the development of the cloud technology and emergence of more and more cloud data sharing platforms, the clouds have not been widely utilized for healthcare data sharing due to privacy concerns [14]. There exist various works on conventional privacy protection of health care data [11], [12]–[15]. In Lu et al. [15], a system called SPOC, which stands for the secure and privacy-preserving opportunistic computing framework, was proposed to treat the storage problem of healthcare data in a cloud environment and addressed the problem of security and privacy protection under such an environment. The article [12]proposed a compound resolution which applies multiple combined technologies for the privacy protection of healthcare data sharing in the cloud environment. In Cao et al. [11], an MRSE (multi keyword ranked search over encrypted data in cloud computing) privacy protection system was presented, which aims to provide users with a multi-keyword method for the cloud's encrypted data. Although this method can provide result ranking, in which people are interested, the amount of calculation could be cumbersome. In Zhang et al. [14], a priority based health data aggregation (PHDA) scheme was presented to protect and aggregate different types of healthcare date in cloud assisted wireless body area network (WBANs).The article[15]investigates security and privacy issues in mobile healthcare networks, including the privacy-protection for healthcare data aggregation, the security for data processing and misbehavior. [10] describes a flexible security model especially for data centric applications in cloud computing based scenario to make sure data confidentiality, data integrity and fine grained access control to the application data. [07] give a systematic literature review of privacy-protection in cloud-assisted healthcare system.

b) Collaborative IDS based on cloudlet mesh

A number of prior works [08] have studied different intrusion detection systems with quite some advances. For example, [09] proposed a behaviour-rule specification-based technique for intrusion detection. The main contribution is the performance outperforms other methods of anomaly-based techniques. [13] proposed a collaborative model for the cloud environment based on distributed IDS and IPS (intrusion prevention system). This model makes use of a hybrid detection technique to detect and take corresponding measures for any types of intrusion which harm the system, especially distributed intrusion. However, collaborative IDS based on the cloudlet mesh structure is a new kind of intrusion detection technique, which was first proposed in Shi et al. [11]. The authors demonstrated that the detection rate of the intrusion detection system established on the basis of a cloudlet mesh is relatively high. [12] describes design space, attacks that evade CIDSs and attacks on the availability of the CIDSs, and introduces comparison of specific CIDS approaches. [13] describes the IDS for privacy cloud. The authors give an overview of intrusion detection of cloud computing and provide a new idea for privacy cloud protection

III. RESULT

The problem of privacy protection and sharing large medical data in cloudlets and the remote cloud. We developed a system which does not allow users to transmit data to the remote cloud in consideration of secure collection of data, as well as low communication cost. However, it does allow users to transmit data to a cloudlet, which triggers the data sharing problem in the cloudlet.

Firstly, we can utilize wearable devices to collect users' data, and in order to protect users privacy, we use NTRU mechanism to make sure the transmission of users' data to cloudlet in security. Secondly, for the purpose of sharing data in the cloudlet, we use trust model to measure users' trust level to judge whether to share data or not. Thirdly, for privacy-preserving of remote cloud data, we partition the data stored in the remote cloud and encrypt the data in different ways, so as to not just ensure data protection but also accelerate the efficacy of transmission. Finally, we propose collaborative IDS based on cloudlet mesh to protect the whole system. The proposed schemes are validated with simulations and experiments.

IV. CONCLUSION

A large scale BANs system in the presence of cloudlet-based data collection is presented in this paper. The goal was objective to minimize end-to-end packet cost by dynamically choosing data collection to the cloud using cloudlet based system. The goal is to have the monitored data of BANs to be available to the end user or to the service provider in reliable manner.

REFERENCES

[1] Yun Liang, AbhikRoychoudhury, and TulikaMitra, "Timing Analysis of Body Area Network Applications." 30-Dec-2008.

[2] D. Simic, A. Jordan, Rui Tao, N. Gungl, J. Simic, M. Lang, Luong Van Ngo, and V. Brankovic, "Impulse UWB Radio System Architecture for Body Area Networks," in Mobile and Wireless Communications Summit, 2007. 16th IST, 2007, pp. 1–5.

[3] M. Quwaider and S. Biswas, "Delay Tolerant Routing Protocol Modelling for Low Power Wearable Wireless Sensor Networks," Netw. Protoc. Algorithms, vol. 4, no. 3, pp. 15–34, 2012

[4] P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST Spec. Publ., vol. 800, no. 145, p. 7, 2011.

[5] M. Quwaider and A. Plummer, "Real-time posture detection using body area sensor networks," in Proc. 13th IEEE Int. Symp. Wearable Comput.(ISWC), 2009.

[6] D. Chappell, "Introducing the Azure services platform," White Pap. Oct, vol. 1364, no. 11, 2008.

[7] E. Jovanov and A. Milenkovic, "Body area networks for ubiquitous healthcare applications: opportunities and challenges," J. Med. Syst., vol. 35, no. 5, pp. 1245– 1254, 2011.

[8] M. Quwaider, J. Rao, and S. Biswas, "Transmission power assignment with postural position inference for on-body wireless communication links," ACM Trans Embed ComputSyst, vol. 10, no. 1, pp. 14:1–14:27, Aug. 2010.

[9] M. Abousharkh and H. Mouftah, "Service oriented architecture-based framework for WBAN-enabled patient monitoring system," in Proceedings of the Second Kuwait Conference on e-Services and eSystems, New York, NY, USA, 2011, pp. 18:1–18:4.

[10] M. Quwaider, M. Taghizadeh, and S. Biswas, "Modelling on-body DTN packet routing delay in the presence of postural disconnections," EURASIP J. Wirel. Commun. Netw., vol. 2011, p. 3, 2011.

[11] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia. Commun. Tech. Comm. MMTC E-Lett., vol. 6, no. 10, pp. 27–31, 2011.

[12] D. Fesehaye, Y. Gao, K. Nahrstedt, and G. Wang, "Impact of Cloudlets on Interactive Mobile Cloud Applications," in Enterprise Distributed Object Computing Conference (EDOC), 2012 IEEE 16th International, 2012, pp. 123–132.

[13] T. Soyata, R. Muraleedharan, C. Funai, M. Kwon, and W. Heinzelman, "Cloud-Vision: Real-time face recognition using a mobile-cloudlet-cloud acceleration architecture," in