Journal of Biosensors & Bioelectronics
ISSN: 2155-6210

Pavan et al., J Biosens Bioelectron 2018, 9:2
DOI: 10.4172/2155-6210.1000254

Review Article Open Access

Real Medical Data Processing and Prediction of Early Disease Using Sensors, Internet of Things (IoT) and R Programming Techniques

Pavan HVS*, Maruti P, Viswanadh NR and Puhazholi

Department of Information Technology, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India

Abstract

With the recognition of wearable devices, along with the development of clouds and cloudlet technology, there has been increasing got to give higher treatment. The process chain of medical knowledge chiefly includes knowledge assortment, data storage and knowledge sharing, etc. ancient tending system often needs the delivery of medical knowledge to the cloud, which involves users sensitive info and causes communication energy consumption much, medical knowledge sharing could be a vital and difficult issue therefore during this paper, we tend to build up a completely unique healthcare system by utilizing the exibility of cloudlet. The functions of cloudlet embody privacy protection, knowledge sharing and intrusion detection within the stage of information assortment, we RST utilize range Theory analysis Unit (NTRU) methodology to encrypt users body knowledge collected by wearable devices. Firstly, those data are going to be transmitted to close cloudlet in AN energy efficient fashion. Secondly, we tend to gift a replacement trust model to assist users to select trustable partners UN agency need to share hold on knowledge in the cloudlet. The trust model conjointly helps similar patients to communicate with one another concerning their diseases. Thirdly, we divide users medical knowledge hold on in remote cloud of hospital into 3 elements, and provides them correct protection. Finally, in order to guard the tending system from malicious attacks, we develop a completely unique cooperative intrusion detection system (IDS) method supported cloudlet mesh, which may effectively forestall the remote tending massive knowledge cloud from attacks. Our experiments demonstrate the effectiveness of the projected theme. Index terms privacy protection, knowledge sharing, cooperative intrusion detection system (IDS), healthcare.

Keywords: Privacy protection; Data sharing; Collaborative intrusion detection system (IDS); Healthcare

Introduction

With the event of tending massive knowledge and wearable technology, still as cloud computing and communication technologies cloud-assisted tending massive knowledge computing becomes vital to fulfill users ever growing demands on health consultation. However, it's difficult issue to alter specific tending knowledge for numerous users in a convenient fashion.

Previous work prompt the combination of social networks and tending service to facilitate the trace of the malady treatment method for the retrieval of real time malady info, tending social platform, like Patients Like Me , will get info from different similar patients through knowledge sharing in terms of users own endings. Tho' sharing medical knowledge on the social network is benecial to each patients and doctors, the sensitive data can be leaked or purloined, that causes privacy and security issues while not efcient protection for the shared knowledge. Therefore, the way to balance privacy protection with the convenience of medical knowledge sharing becomes a challenging issue. With the advances in cloud computing, a large amount of information are often hold on in numerous clouds, including cloudlets and remote clouds , facilitating data sharing and intensive computations. However, cloud-based knowledge sharing entails the subsequent basic problems: the way to defend the protection of users body knowledge during its delivery to a cloudlet? The way to certify the data sharing in cloudlet won't cause privacy problem? As are often expected, with the proliferation of electronic medical records (EMR) and cloud-assisted applications, more and additional attentions ought to be paid to the protection issues regarding to a foreign cloud containing tending massive knowledge. How to secure the tending massive knowledge hold on in a very remote cloud? The way to effectively defend the full system from malicious attacks? In terms of the higher than issues, this paper proposes a cloudlet based mostly tending system. The body knowledge collected by wearable devices square measure transmitted to the close cloudlet. Those knowledge square measure any delivered to the remote cloud where doctors will access for malady designation. In line with data delivery chain, we tend to separate the privacy protection into three stages. Within the RST stage, user's important signs collected by wearable devices square measure delivered to a closet entrance of cloudlet. During this stage, knowledge privacy is that the main concern. In the second stage, users knowledge are going to be any delivered toward remote cloud through cloudlets. A cloudlet is made by a certain range of mobile devices whose house owners might need and/or share some specic knowledge contents. Thus, each privacy protection and knowledge sharing square measure thought-about during this stage. Especially, we use trust model to evaluate trust level between users to determine sharing knowledge or not. Considering the users medical knowledge are hold on in remote cloud, we tend to classify these medical knowledge into different sorts and take the corresponding security policy. In addition to higher than 3 stages based mostly knowledge privacy protection, we conjointly think about cooperative IDS supported cloudlet mesh to protect the cloud scheme.

***Corresponding author:** Pavan HVS, Department of Information Technology, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India, Tel: 9962732329; E-mail: pavansurya97@gmail.com

Received May 04, 2018; **Accepted** May 26, 2018; **Published** June 02, 2018

Citation: Pavan HVS, Maruti P, Viswanadh NR, Puhazholi (2018) Real Medical Data Processing and Prediction of Early Disease Using Sensors, Internet of Things (IoT) and R Programming Techniques. J Biosens Bioelectron 9: 254. doi: 10.4172/2155-6210.1000254

Literature Review

PSMPA

Gatzoulis and Iakovidis wearable and moveable E-health Systems. Patient Self-controllable and Multilevel Privacy-preserving Cooperative Authentication in Distributed m-Health care Cloud automatic data processing system [1]. Distributed m-healthcare cloud computing systems have been progressively adopted world-wide together with the European Commission activities, the USA insurance Portability and irresponsibleness Act (HIPAA) and plenty of other governments for economical and high-quality medical treatment. In m-healthcare social networks, the non-public health info is usually shared among the patients located in individual social communities full of the same malady for mutual support, and across distributed tending suppliers equipped with their own cloud servers for medical adviser. A novel licensed accessible privacy model (AAPM) and a patient self-controllable multi-level privacy protective cooperative authentication theme (PSMPA) realizing 3 different levels of security and privacy demand within the distributed m-healthcare cloud automatic data processing system.

Patient controlled encryption

Benaloh patient controlled encryption: guaranteeing privacy of electronic medical records, in CCSW, although the cloud computing model is considered to be an awfully promising internet-based computing platform, it leads to a loss of security control over the cloud-hosted assets [2]. Personal health record (PHR) is AN rising patient-centric model of health info exchange, that is usually outsourced to be hold on at a 3rd party, like cloud suppliers. However, there are wide privacy issues as personal health info might be exposed to those third party servers and to unauthorized parties. To assure the patient's management over access to their own PHRs, it's a promising methodology to cypher the PHRs before outsourcing. Yet, problems like risks of privacy exposure, quantifiability in key management, versatile access and economical user revocation, have remained the foremost important challenges toward achieving fine-grained, cryptographically enforced knowledge access management. The framework addresses the distinctive challenges brought by multiple PHR house owners and users, in this we tend to greatly reduce the complexness of key management whereas enhance the privacy guarantees compared with previous works. We tend to utilize ABE to cypher the PHR knowledge, so that patients will enable access not solely by personal users, but conjointly numerous users from public domains.

Security and privacy-enhancing multi-cloud architectures

Security challenges square measure still among the largest obstacles when considering the adoption of cloud services. The achievable security deserves by creating use of multiple distinct clouds at the same time. Numerous distinct architectures square measure introduced. Two major indications for improvement are often taken from the examinations performed in this paper. Initial of all, as long as for every sort of security downside there exists a minimum of one technical solution approach, a extremely fascinating field for future research lies in combining the approaches given here [3].

Applying agents to the data security in cloud computing

Cloud computing security associated with the survival of cloud computing, has become a key think about the event of cloud computing. This paper presents an information security model for cloud computing, and introduces agents to data security module so as to supply additional reliable services. In any reducing the user waiting time, speeding up knowledge access and any increasing knowledge availability. It's conjointly planned to enhance agents ability to satisfy the special demands of cloud computing [4].

K-Means clustering: K means that agglomeration is AN unsupervised learning rule that tries to cluster knowledge supported their similarity. Unsupervised learning means there's no outcome to be expected, and the rule simply tries to search out patterns within the knowledge. In k means clustering, we've the specify the amount of clusters we tend to want the information to be sorted into. The rule willy-nilly assigns every observation to a cluster, and finds the centre of mass of each cluster. Then, the rule iterates through 2 steps: Reassign knowledge points to the cluster whose center of mass is nearest. Calculate new centre of mass of every cluster. These 2 steps square measure repeated until the intervals cluster variation can't be reduced any further. That intervals cluster variation is calculated because the add of the geometer distance between the information points and their respective cluster centroids (Figure 1).

Naive Bayes algorithm: Naive Thomas Bayes could be a classification rule for binary (two-class) and multi-class classification issues. The technique is best to know once delineate victimization binary or categorical input values. It's referred to as naive Bayes-Bayes-Thomas Thomas Bayes-mathematician or simpleton Bayes because the calculation of the chances for every hypothesis are simplified to form their calculation tractable. Instead of attempting to calculate the worth's of every attribute value P(d1, d2, d3h), they're assumed to be not absolutely freelance given the target worth and calculated as P(d1h) * P(d2H)and so on. This can be a awfully robust assumption that's most unlikely in real knowledge, i.e. that the attributes don't act. Nevertheless, the approach performs amazingly well on knowledge where this assumption doesn't hold [5]. Illustration employed by Naive Bayes-Bayes-Thomas Thomas Bayes-mathematician Models. The illustration for naïve Bayes is probabilities. A listing of chances square measure holds on to file for a learned naive Thomas Bayes model. This includes: category Probabilities: The probabilities of every category within the coaching dataset [4]. Conditional Probabilities: The

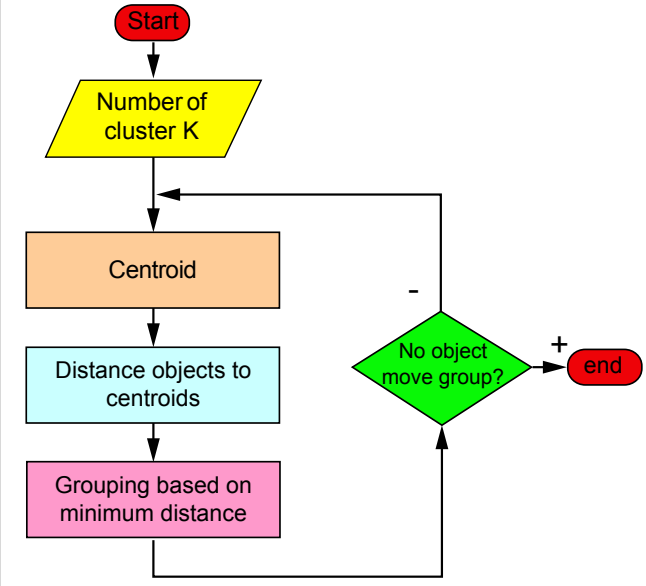

Figure 1: K-Means Diagram.

conditional chances of every input value given every category worth (Figure 2).

System framework: The framework of the projected cloudlet-based tending system is shown. The client's physiological knowledge square measure selected by wearable devices like sensible vesture. Then, that knowledge square measure delivered to cloudlet. The subsequent 2 important issues for health care knowledge protection are taken into account. The downside is health care knowledge privacy protection and sharing data, as shown in Figure 1the second downside is to develop effective counter measures to stop the health care info from being intruded from outside, that is shown in Figure 1 we address the RST downside on health care encryption and sharing as follows [6,7] (Figure 3).

Client data encryption: We tend to utilize the model given and take the advantage of to protect the client's physiological knowledge from being leaked or abused. This theme is to guard the users privacy once transmitting the information from the smartphone to the cloudlet [8].

Cloudlet based data sharing: Generally, users geographically near one another hook up with a similar cloudlet. Its possible for them to share common aspects, for example, patients suffer from similar reasonably malady exchange information of treatment and share connected knowledge. For this purpose, we tend to use users similarity and name as input data. After we obtain users trust levels, a certain threshold is set for the comparison. Once reaching or Olympian the threshold, it's thought-about that the trust between the users is enough for knowledge sharing. Otherwise, the information won't share with low trust level l [9].

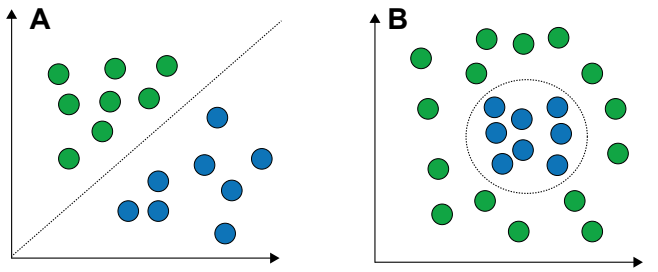

Figure 2: Naive Bayes Diagram.

Remote cloud data privacy protection: Compared to users daily knowledge in cloudlet, the information hold on remote contain larger scale medical knowledge, e.g., EMR, which will be hold on for an extended term. We tend to use the ways presented in to divide EMR into specific identier (EID), quasi-identier (QID) and medical info(MI), which is able to be mentioned in four. Once classifying, proper protection is given for the information containing users sensitive info [10].

Collaborative IDS based on cloudlet mesh: There is a vast volume of medical knowledge hold on within the remote cloud, it is vital to use security mechanism to guard the database from malicious intrusions. During this paper, we develop specie countermeasures to ascertain a defense system for the massive medical info within the remote cloud storage. Specially, cooperative IDS supported the cloudlet mesh structure is employed to screen any visit to the database as a protection border. If the detection shows a malicious intrusion before, the cooperative IDS will is AN alarm and block the visit, and vice-versa. The collaborative IDS, as a guard of the cloud info, can protect an enormous range of medical knowledge and certify of the security of the info [11].

Conclusion

In this paper, we tend to investigate the matter of privacy protection and sharing giant medical knowledge in cloudlets and therefore the remote cloud. Firstly, we tend to develop a system that doesn't enable users to transmit knowledge to the remote cloud in thought of secure assortment of information, still as low communication value. However, it will enable users to transmit knowledge to a cloudlet, which triggers the information sharing downside within the cloudlet. Firstly, we are able to utilize wearable devices to gather users data, and so as to guard users privacy, we tend to use NTRU mechanism to form positive the transmission of users knowledge to cloudlet in security. Secondly, for the aim of sharing data within the cloudlet, we tend to use trust model to live users trust level to evaluate whether or not to share knowledge or not. Thirdly, for privacy-preserving of remote cloud knowledge, we tend to partition the data hold on within the remote cloud and cypher the information in different ways that, thus on not simply guarantee knowledge protection but conjointly accelerate the efficacy of transmission. Finally, we propose cooperative IDS supported cloudlet mesh to guard the whole system. The projected schemes square measure valid with simulations and experiments.

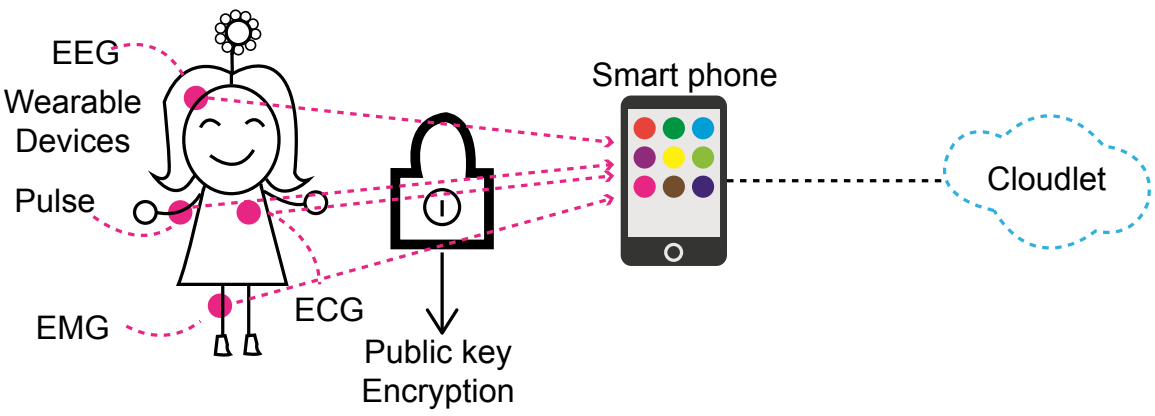

Figure 3: Collection of data.

Acknowledgment

We would prefer to categorical our deepest feeling to our guide, Mrs. Puhazholi her valuable steering, consistent encouragement, personal caring, timely facilitate and providing me with a wonderful atmosphere for doing analysis. All through the work, in spite of her busy schedule, she has extended cheerful and cordial support to Maine for finishing this analysis work.

References

1. Gatzoulis L,Iakovidis I (2007) Wearable and Portable eHealth Systems. IEEE Eng Med Biol Mag 26:51-56.
2. Benaloh J, Chase M, Horvitz E, Lauter K (2009) Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records. The ACM Cloud Computing Security Workshop.
3. Hung K, Zhang Y, Tai B (2004) wearable medical devices for tele home healthcare, in Engineering in medication and Biology Society. Twenty sixth Annual International Conference of the IEEE.
4. Zhao J, Wang L, Tao J, Chen J, Sun W, et al. (2014) A security framework in G-Hadoop for giant data computing across distributed cloud knowledge centres. J Comput Syst Sci 80: 994-1007.
5. Hossain MS, Muhammad V (2016) Cloud-assisted industrial web of things (IIOT)- Enabled framework for health monitoring. Comput Netw 101: 192202.
6. He K, Chen J, Du R, Wu Q, Xue G, et al. (2016) Deypos: Deduplicatable dynamic proof of storage for multi-user environments.
7. Grifn L, DeLeastar E (2009) Social networking healthcare, in Wearable small and Nano Technologies for personalised Health (pHealth). 6th International Workshop on IEEE.
8. https://elearningindustry.com/applications-r-programming-r-eal-world
9. Khorsheed MSM (2000) Automatic recognition of words in arabic manuscripts.
10. Dmytro Terletskyi, Alexandr Provotar (2002) object-oriented dynamic networks. Computational models for business and engineering domains PP: 123-136.
11. Lumley T (2006) R Fundamentals and Programming Techniques.R Core Development Team and UW Dept of Biostatistics.