www.ijatir.org

International Journal of Advanced Technology and Innovative Research

ISSN 2348–2370
Vol.10,Issue.12,
December-2018,
Pages:1124-1132

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

PATAN NAUSHAD KHAN[1], SUBHANI SHAIK[2], JALAIAH SAIKAM[3]
[1]PG Scholar, Dept of CSE, St. Mary's Group of Institutions, Chebrolu, Guntur, AP, India,
E-mail: naushad.khan1212@gmail.com.
[2]Associate Professor & HOD, Dept of CSE, St. Mary's Group of Institutions, Chebrolu, Guntur, AP, India,
E-mail: subhanicsehod@stmarysgroup.com.
[3]Assistant Professor, Dept of CSE, St. Mary's Group of Institutions, Chebrolu, Guntur, AP, India,
E-mail: jalaiahcse@gmail.com.

Abstract: With the popularity clouds and cloudlet technology, there has been increasing need to provide better medical care. The processing chain of medical data mainly includes data collection, data storage and data sharing, etc. Traditional healthcare system often requires the delivery of medical data to the cloud, which involves users' sensitive information and causes communication energy consumption. Practically, medical data sharing is a critical and challenging issue. Thus in this paper, we build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet include privacy protection, data sharing and intrusion detection. In the stage of data collection, we first utilize Number Theory Research Unit (NTRU) method to encrypt user's body data collected by wearable devices. Those data will be transmitted to nearby cloudlet in an energy efficient fashion. Secondly, we present a new trust model to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps similar patients to communicate with each other about their diseases. Thirdly, we divide users' medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect the healthcare system from malicious attacks, we develop a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks. Our experiments demonstrate the effectiveness of the proposed scheme.

Keywords: Privacy Protection, Data Sharing, Collaborative Intrusion Detection System (IDS), Healthcare.

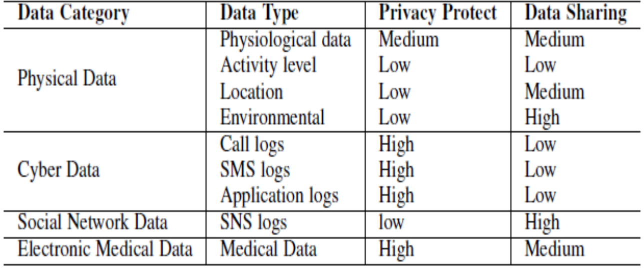
I. INTRODUCTION

With the development of healthcare big data and wearable technology [1], as well as cloud computing and communication technologies [2], cloud-assisted healthcare big data computing becomes critical to meet users' ever growing demands on health consultation [3]–[5]. However, it is challenging issue to personalize specific healthcare data for various users in a convenient fashion [6]. Previous work suggested the combination of social networks and healthcare service to facilitate [7] the trace of the disease treatment process for the retrieval of real time disease information [8]. Healthcare social platform, such as Patients-LikeMe [9], can obtain information from other similar patients through data sharing in terms of user's own findings. Though sharing medical data on the social network is beneficial to both patients and doctors, the sensitive data might be leaked or stolen, which causes privacy and security problems [10] [11] without efficient protection for the shared data [12]. Therefore, how to balance privacy protection with the convenience of medical data sharing becomes a challenging issue. With the advances in cloud computing, a large amount of data can be stored in various clouds [13], including cloudlets [14] and remote clouds [15], facilitating data sharing and intensive computations [16] [17]. However, cloud-based data sharing entails the following fundamental problems:

- How to protect the security of user's body data during its delivery to a cloudlet?
- How to make sure the data sharing in cloudlet will not cause privacy problem?
- As can be predicted, with the proliferation of electronic medical records (EMR) and cloud-assisted applications, more and more attentions should be paid to the security problems regarding to a remote cloud containing healthcare big data. How to secure the healthcare big data stored in a remote cloud?
- How to effectively protect the whole system from malicious attacks?

In terms of the above problems, this paper proposes a cloudlet based healthcare system. The body data collected by wearable devices are transmitted to the nearby cloudlet. Those data are further delivered to the remote cloud where doctors can access for disease diagnosis. According to data delivery chain, we separate the privacy protection into three stages. In the first stage, user's vital signs collected by wearable devices are delivered to a closet gateway of cloudlet. During this stage, data privacy is the main concern. In the second stage, user's data will be further delivered toward remote cloud through cloudlets. A cloudlet is formed by a certain number of mobile devices whose owners may require and/or share some specific data contents. Thus, both privacy protection and data sharing are considered in this stage. Especially, we use trust model to evaluate trust level between users to determine sharing data or not. Considering the users' medical data are stored in remote cloud, we classify these medical data into different kinds and take the corresponding security policy. In addition to above three stages based data privacy protection, we also consider collaborative IDS based on cloudlet mesh to protect the cloud ecosystem.

TABLE I: Feature Table According To Data Style



Data Category	Data Type	Privacy Protect	Data Sharing
Physical Data	Physiological data Activity level Location Environmental	Medium Low Low Low	Medium Low Medium High
Cyber Data	Call logs SMS logs Application logs	High High High	Low Low Low
Social Network Data	SNS logs	low	High
Electronic Medical Data	Medical Data	High	Medium

In summary, the main contributions of this paper include:

- A cloudlet based healthcare system is presented, where the privacy of users' physiological data and the efficiency of data transmissions are our main concern. We use NTRU for data protection during data transmissions to the cloudlet.
- In order to share data in the cloudlet, we use users' similarity and reputation to build up trust model. Based on the measured users' trust level, the system determines whether data sharing is performed.
- We divide data in remote cloud into different kinds and utilize encryption mechanism to protect them respectively.
- We propose collaborative IDS based on cloudlet mesh to protect the whole healthcare system against malicious attacks.

The remainder of this article is organized as follows. In Section II, we introduce the related work. For the healthcare data in the remote cloud and users' private health data, we propose a security system and introduce the framework of the entire system in Section III. In Section IV, system analysis. Section 5 describes implementation.

II. RELATED WORK

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

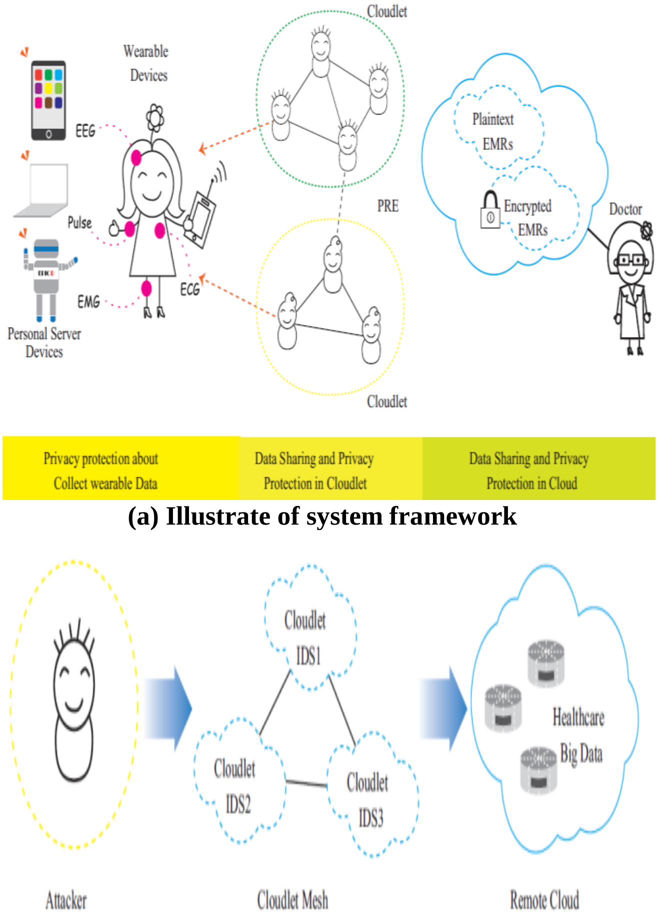
Despite the development of the cloud technology and emergence of more and more cloud data sharing platforms, the clouds have not been widely utilized for healthcare data sharing due to privacy concerns [8]. There exist various works on conventional privacy protection of healthcare data [11]. In Lu et al. [9], 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 [21] 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. [24], a priority based health data aggregation (PHDA) scheme was presented to protect and aggregate different types of healthcare date in cloud assisted wireless boby area network (WBANs). The article [25] investigates security and privacy issues in mobile healthcare networks, including the privacy-protection for healthcare data aggregation, the security for data processing and misbehavior. [26] 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. [27] 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 [28] have studied different intrusion detection systems with quite some advances. For example, [29] proposed a behavior-rule specification-based technique for intrusion detection. The main contribution is the performance outperforms other methods of anomaly-based techniques. [30] 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. [31]. The authors demonstrated that the detection rate of the intrusion detection system established on the basis of a cloudlet mesh is relatively high. [32] describes design space, attacks that evade CIDSs and attacks on the availability of the CIDSs, and introduces comparison of specific CIDS approaches. [33] 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. SYSTEM FRAMEWORK

The framework of the proposed cloudlet-based healthcare system is shown in Fig. 1. The client's physiological data are first collected by wearable devices such as smart clothing [34]. Then, those data are delivered to cloudlet. The following two important problems for healthcare data protection is considered. The first problem is healthcare data privacy protection and sharing data, as shown in Fig. 1(a). The second problem is to develop effective countermeasures to prevent the healthcare database from being intruded from outside, which is shown in Fig. 1(b). We address the first problem on healthcare data encryption and sharing as follows.



(a) Illustrate of system framework

(b) Collaborative IDS of remote cloud

Fig.1. Illustration of the system architecture: (a) Privacy protection; (b) Collaborative IDS.

- **Client Data Encryption:** We utilize the model presented in [23], and take the advantage of NTRU [35] to protect the client's physiological data from being leaked or abused. This scheme is to protect the user's privacy when transmitting the data from the smartphone to the cloudlet.
- **Cloudlet Based Data Sharing:** Typically, users geographically close to each other connect to the same cloudlet. It's likely for them to share common aspects, for example, patients suffer from similar kind of disease exchange information of treatment and share related data. For this purpose, we use users' similarity and reputation as input data. After we obtain users' trust levels, a certain threshold is set for the comparison. Once reaching or exceeding the threshold, it is considered that the trust between the users is enough for data sharing. Otherwise, the data will not shared with low trust level.
- **Remote Cloud Data Privacy Protection:** Compared to user's daily data in cloudlet, the data stored in remote contain larger scale medical data, e.g., EMR, which will be stored for a long term. We use the methods presented in [36] [21] to divide EMR into explicit identifier (EID), quasi-identifier (QID) and medical information (MI), which will be discussed in 4.3. After classifying, proper protection is given for the data containing users' sensitive information.
- **Collaborative IDS based on Cloudlet Mesh:** There is a vast volume of medical data stored in the remote cloud, it is critical to apply security mechanism to protect the database from malicious intrusions. In this paper, we develop specific countermeasures to establish a defense system for the large medical database in the remote cloud storage. Specifically, collaborative IDS based on the cloudlet mesh structure is used to screen any visit to the database as a protection border. If the detection shows a malicious intrusion in advance, the collaborative IDS will fire an alarm and block the visit, and vice-versa. The collaborative IDS, as a guard of the cloud database, can protect a vast number of medical data and make sure of the security of the database.

IV. SYSTEM ANALYSIS

A. Existing System

- There has been a great interest in developing attribute based encryption due to its fine-grained access control property.
- Goyal et al. designed the first key policy attribute-based encryption scheme, where ciphertext can be decrypted only if the attributes that are used for encryption satisfy the access structure on the user private key. Under the reverse situation, CP-ABE allows user private key to be associated with a set of attributes and ciphertext associated with an access structure. CP-ABE is a preferred choice when designing an access control mechanism in a broadcast environment.
- Cheung and Newport proposed a selectively secure CP-ABE construction in the standard model using the simple Boolean function, i.e., AND gate. By adopting proxy re-encryption and lazy re-encryption techniques, Yu et al. also devised a selectively secure CP-ABE scheme with the ability of attribute revocation, which is perfectly suitable for the data-outsourced cloud model.

Disadvantages Of Existing System:

- The encrypted data can be effectively utilized then becomes another new challenge.
- Significant attention has been given and much effort has been made to address this issue, from secure search over encrypted data, secure function evaluation, to fully homomorphic encryption systems that provide generic solution to the problem in theory but are still too far from being practical due to the extremely high complexity.
- Symmetric cryptography based schemes are clearly not suitable for this setting due to the high complexity of secret key management.

- Extending user list approach to the multi-owner setting and on a per file basis is not trivial as it would impose significant scalability issue considering a potential large number of users and files supported by the system.
- Additional challenges include how to handle the updates of the user lists in the case of user enrollment, revocation, etc., under the dynamic cloud environment.

B. Proposed System

- This paper focuses on the problem of search over encrypted data, which is an important enabling technique for the encryption-before-outsourcing privacy protection paradigm in cloud computing, or in general in any networked information system where servers are not fully trusted.
- In this paper, we address these open issues and present an authorized keyword search scheme over encrypted cloud data with efficient user revocation in the multi-user multi-data-contributor scenario.
- We realize fine-grained owner-enforced search authorization by exploiting ciphertext policy attribute-based encryption (CP-ABE) technique.
- Specifically, the data owner encrypts the index of each file with an access policy created by him, which defines what type of users can search this index as shown in Fig.2. The data user generates the trapdoor independently without relying on an always online trusted authority (TA). The cloud server can search over the encrypted indexes with the trapdoor on a user's behalf, and then returns matching result if and only if the user's attributes associated with the trapdoor satisfy the access policies embedded in the encrypted indexes. We differentiate attributes and keywords in our design.
- Keywords are actual content of the files while attributes refer to the properties of users. The system only maintains a limited number of attributes for search authorization purpose. Data owners create the index consisting of all keywords in the file but encrypt the index with an access structure only based on the attributes of authorized users, which makes the proposed scheme more scalable and suitable for the large scale file sharing system. In order to further release the data owner from the burdensome user membership management, we use proxy re-encryption and lazy re-encryption techniques to shift the workload as much as possible to the CS, by which our proposed scheme enjoys efficient user revocation.

Advantages Of Proposed System:

- Formal security analysis shows that the proposed scheme is provably secure and meets various search privacy requirements.
- Furthermore, we design a search result verification scheme and make the entire search process verifiable. Performance evaluation demonstrates the efficiency and practicality of the ABKS-UR.
- We design a novel and scalable authorized keyword search over encrypted data scheme supporting multiple data users and multiple data contributors.
- Compared with existing works, our scheme supports fine-grained owner-enforced search authorization at the file level with better scalability for large scale system in that the search complexity is linear to the number of attributes in the system, instead of the number of authorized users.
- Data owner can delegate most of computationally intensive tasks to the CS, which makes the user revocation process efficient and is more suitable for cloud outsourcing model.
- We formally prove our proposed scheme selectively secure against chosen-keyword attack.
- We propose a scheme to enable authenticity check over the returned search result in the multi-user multi-data-contributor search scenario.

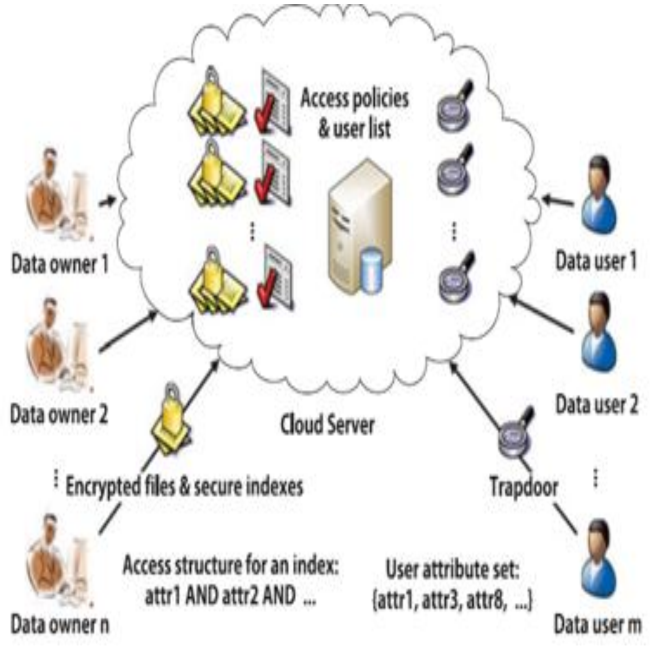


Fig.2. cloud data system design.

V. IMPLEMENTATION

A. Modules

- Authorized Keyword Search
- Efficient User Revocation
- Trapdoor Unlinkability
- Authenticated Search Result

Authorized Keyword Search: The CP-ABE technique to achieve scalable fine-grained authorized keyword search over encrypted cloud data supporting multiple data owners and data users. Specifically, for each file, the data owner generates an access-policy-protected secure index, where the access structure is expressed as a series of AND gates. The secure search system should enable data-owner-enforced search authorization, i.e., only users that meet the owner-defined access policy can obtain the valid search result. Besides achieving fine grained authorization, another challenge is to make the scheme scalable for dynamic cloud environment.

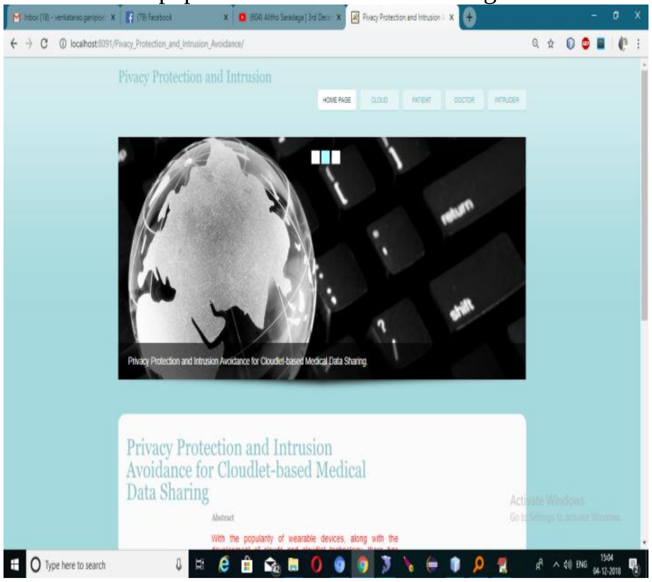
Efficient User Revocation: The design goal is to efficiently revoke users from the current system while minimizing the impact on the remaining legitimate users. The server can efficiently eliminate the revoked user’s identity information from the corresponding user lists.

Trapdoor Unlinkability: This security property makes the CS unable to visually distinguish two or more trapdoors even containing the same keyword. Note that the attacker may launch dictionary attack by using public key to generate arbitrary number of indexes with keyword of his choice, and then search these indexes with a particular trapdoor to deduce the underlying keyword in the trapdoor, which is referred to as predicate privacy and it cannot be protected inherently in the PKC-based search scenario. To generate a trapdoor, the data user chooses a different random number u to obfuscate the trapdoor such that the CS is visually unable to differentiate two or more trapdoors even produced with the same keyword. Thus, the ABKS-UR can provide trapdoor unlinkability property.

Authenticated Search Result: Data users may desire the authenticated search result to boost their confidence in the entire ABKS-UR search process, especially when the result contains errors that may come from the possible storage corruption, software malfunction, and intention to save computational resources by the server, etc. we are able to assure data user of the authenticity of the returned search result by checking its correctness (the returned search result indeed exist in the dataset and remain intact), completeness (no qualified files are omitted from the search result), and freshness (the returned result is obtained from the latest version of the dataset). The main idea of the verification scheme is to allow the CS to return the auxiliary information containing the authenticated data structure other than the final search result, upon which the data user is capable of doing result authenticity check.

VI. RESULT

Results of this paper is as shown in bellow Figs.3 to 16.

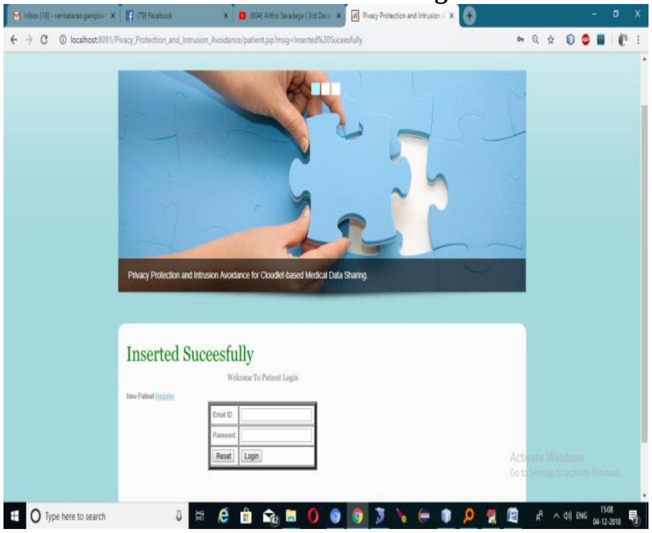

localhost:8091/Pivacy_Protection_and_Intrusion_Avoidance/
Pivacy Protection and Intrusion
HOME PAGE
CLOUD
PATIENT
DOCTOR
INTRUDER
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing.
Type here to search

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

Abstract

With the popularity of wearable devices, along with the

Fig.3. Home page.


localhost:8091/Pivacy_Protection_and_Intrusion_Avoidance/patient.jsp?msg=Inserted%20Sucessfully
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing.
Type here to search

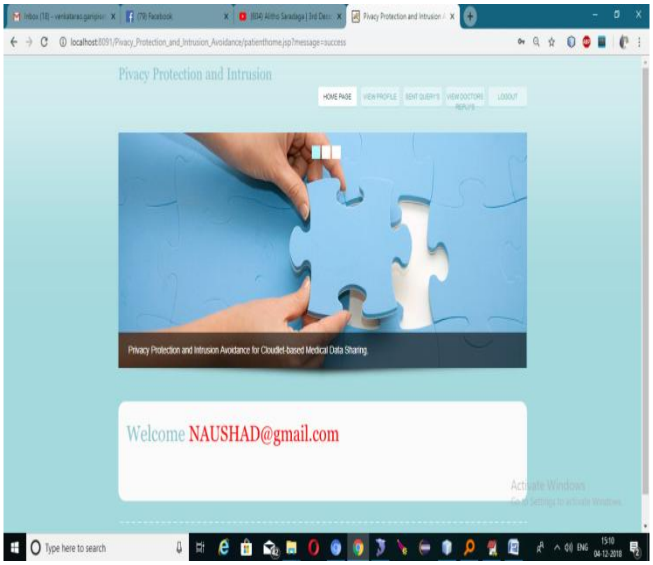
Inserted Suceesfully

Welcome To Patient Login

New Patient Register

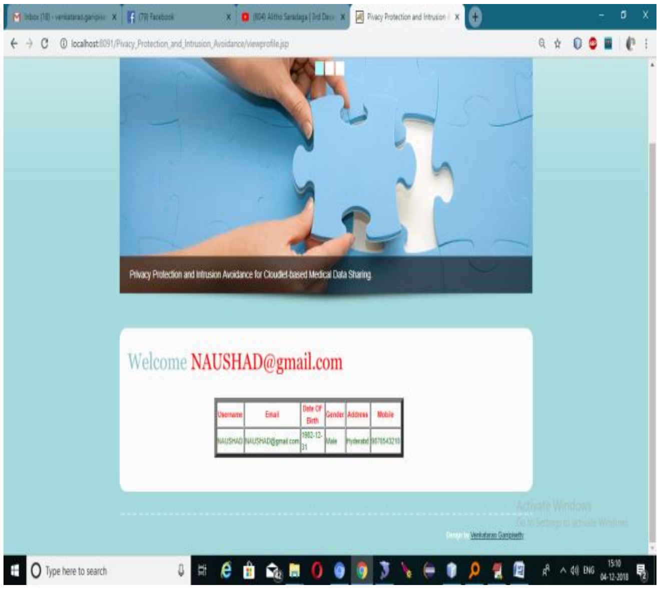
Email ID	
Password	
Reset	Login

Fig.4. Patient Home Page.


localhost:8091/Pivacy_Protection_and_Intrusion_Avoidance/patienthome.jsp?message=success
Pivacy Protection and Intrusion
HOME PAGE
VIEW PROFILE
SENT QUERY'S
VIEW DOCTORS REPLYS
LOGOUT
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing.
Type here to search

Welcome NAUSHAD@gmail.com

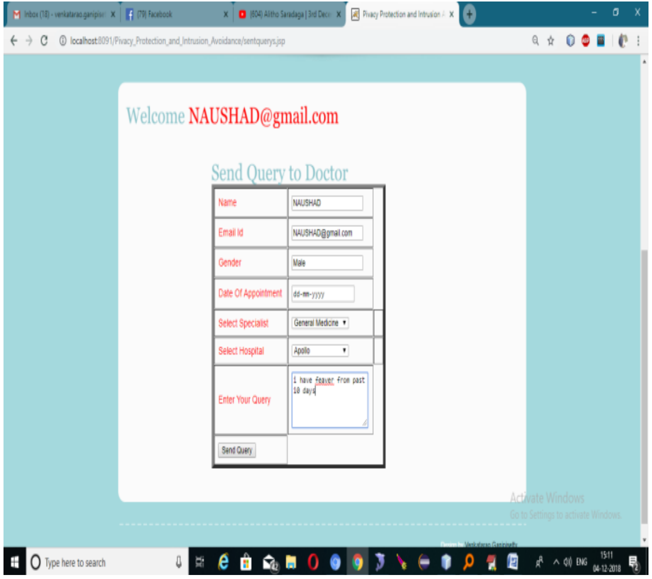
Fig.5. View profile.


localhost:8091/Pivacy_Protection_and_Intrusion_Avoidance/viewprofile.jsp
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing.
Design by Venkataran Ganipsetty
Type here to search

Welcome NAUSHAD@gmail.com

Username	Email	Date OF Birth	Gender	Address	Mobile
NAUSHAD	NAUSHAD@gmail.com	1982-12-31	Male	Hyderabd	9876543210

Fig.6. Send Query To Doctor.

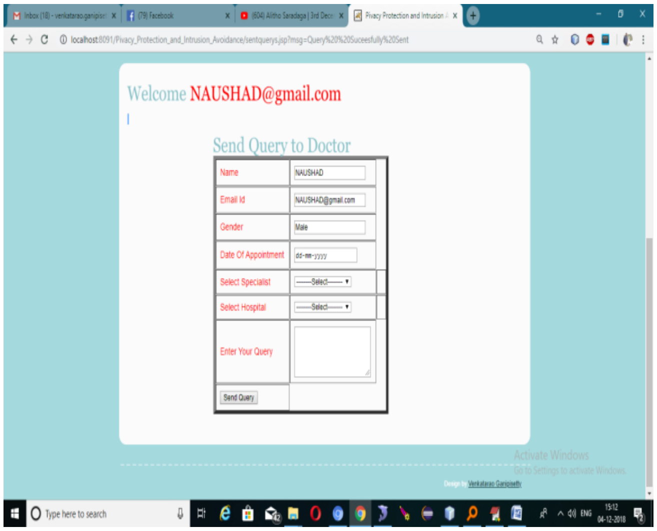

localhost:8091/Pivacy_Protection_and_Intrusion_Avoidance/sentquerys.jsp
Pivacy Protection and Intrusion
Activate Windows
Go to Settings to activate Windows.
Design by Venkatarao Ganipisetty
Type here to search

Welcome NAUSHAD@gmail.com

Send Query to Doctor

Name	NAUSHAD
Email Id	NAUSHAD@gmail.com
Gender	Male
Date Of Appointment	dd-mm-yyyy
Select Specialist	General Medicine ▾
Select Hospital	Apollo ▾
Enter Your Query	i have feaver from past 10 days
Send Query	

Fig.7. View Doctor's Replay.

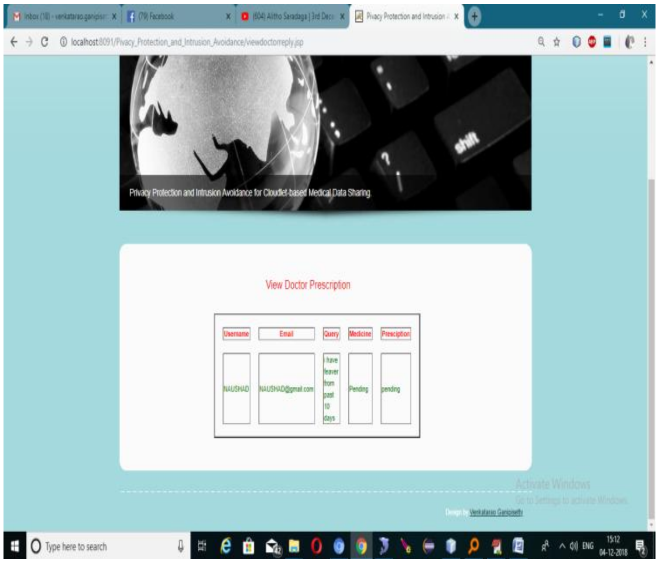

localhost:8091/Pivacy_Protection_and_Intrusion_Avoidance/sentquerys.jsp?msg=Query%20%20Suceesfully%20Sent
Pivacy Protection and Intrusion
Activate Windows
Go to Settings to activate Windows.
Design by Venkatarao Ganipisetty
Type here to search

Welcome NAUSHAD@gmail.com

Send Query to Doctor

Name	NAUSHAD
Email Id	NAUSHAD@gmail.com
Gender	Male
Date Of Appointment	dd-mm-yyyy
Select Specialist	--------Select-------- ▾
Select Hospital	--------Select-------- ▾
Enter Your Query	
Send Query	

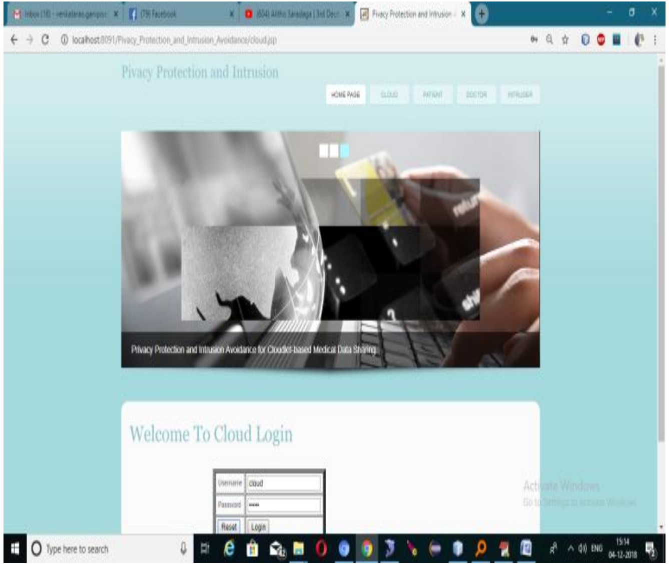
Fig.8. Cloud login.


localhost:8091/Pivacy_Protection_and_Intrusion_Avoidance/viewdoctorreply.jsp
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing
Activate Windows
Go to Settings to activate Windows.
Design by Venkatarao Ganipisetty
Type here to search

View Doctor Prescription

Username	Email	Query	Medicine	Presciption
NAUSHAD	NAUSHAD@gmail.com	i have feaver from past 10 days	Pending	pending

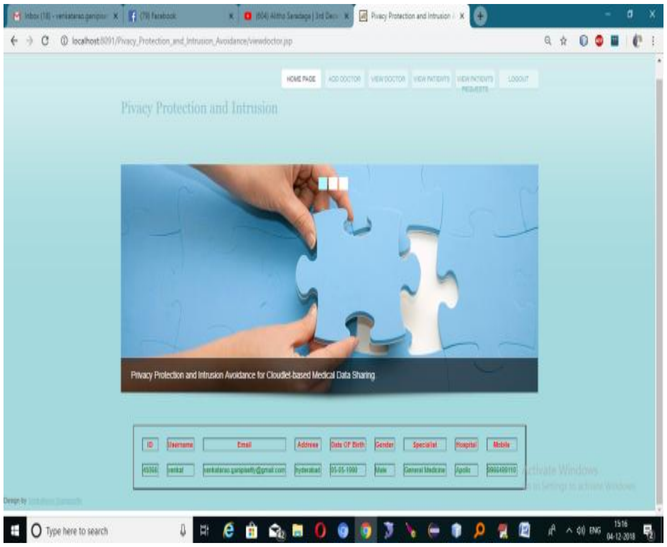
Fig.9. Add Doctor.


localhost:8091/Pivacy_Protection_and_Intrusion_Avoidance/cloud.jsp
Pivacy Protection and Intrusion
HOME PAGE
CLOUD
PATIENT
DOCTOR
INTRUDER
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing
Activate Windows
Go to Settings to activate Windows.
Type here to search

Welcome To Cloud Login

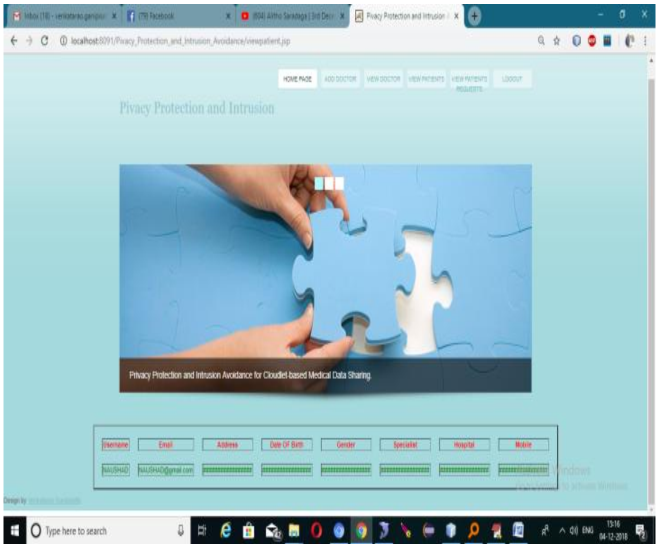
Username	cloud
Password	•••••
Reset	Login

Fig.10. View Patient's.


localhost:8091/Pivacy_Protection_and_Intrusion_Avoidance/viewdoctor.jsp
HOME PAGE
ADD DOCTOR
VIEW DOCTOR
VIEW PATIENTS
VIEW PATIENTS REQUESTS
LOGOUT
Pivacy Protection and Intrusion
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing
Activate Windows
Go to Settings to activate Windows.
Type here to search

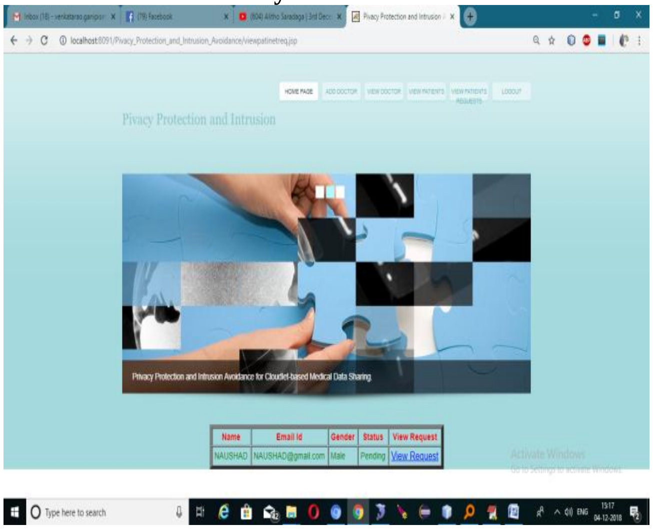
ID	Username	Email	Address	Date OF Birth	Gender	Specialist	Hospital	Mobile
45366	venkat	venkatarao.ganipisetty@gmail.com	hyderabad	05-05-1990	Male	General Medicine	Apollo	9966499110

Fig.11. View patient's Querys.


localhost:8091/Pivacy_Protection_and_Intrusion_Avoidance/viewpatient.jsp
HOME PAGE
ADD DOCTOR
VIEW DOCTOR
VIEW PATIENTS
VIEW PATIENTS REQUESTS
LOGOUT
Pivacy Protection and Intrusion
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing.
Activate Windows
Go to Settings to activate Windows.
Type here to search

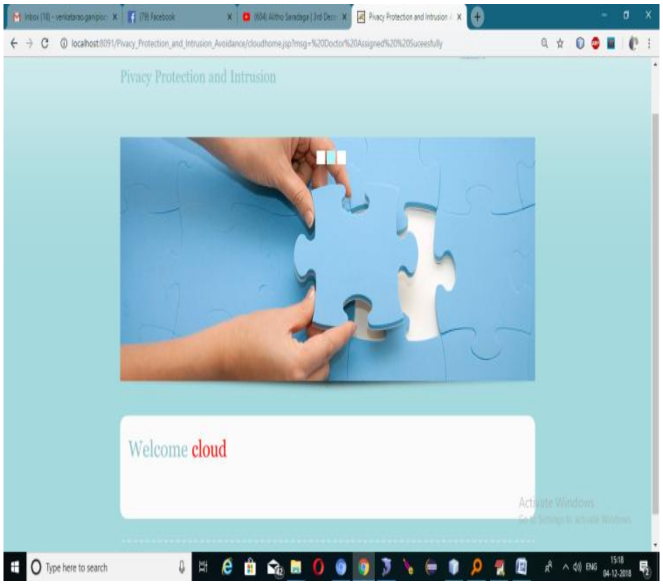
Username	Email	Address	Date OF Birth	Gender	Specialist	Hospital	Mobile
NAUSHAD	NAUSHAD@gmail.com	################	################	################	################	################	################

Fig.12. Assign Doctor.


Privacy Protection and Intrusion
HOME PAGE
ADD DOCTOR
VIEW DOCTOR
VIEW PATIENTS
VIEW PATIENTS REQUESTS
LOGOUT
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing

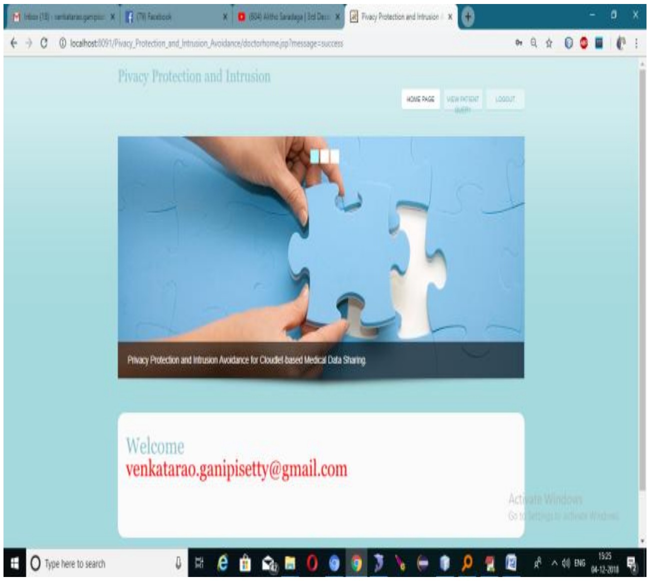
Name	Email Id	Gender	Status	View Request
NAUSHAD	NAUSHAD@gmail.com	Male	Pending	View Request

Fig.13. Doctor Login.



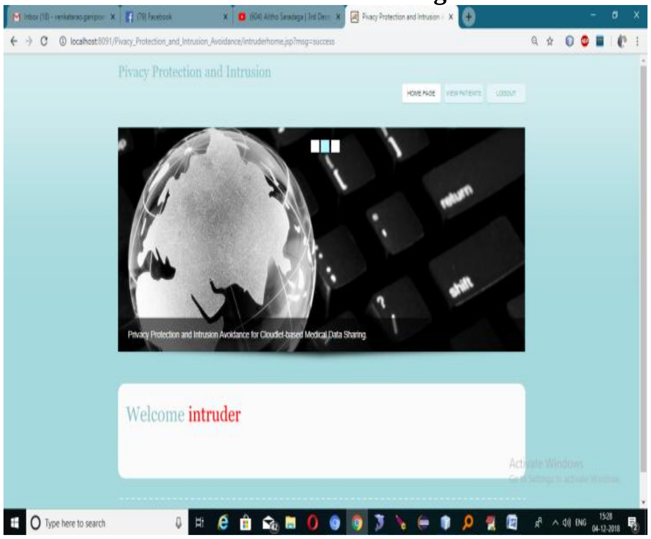
Welcome cloud

Fig.14. Reply.


Privacy Protection and Intrusion
HOME PAGE
VIEW PATIENT QUERY
LOGOUT
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing

Welcome venkatarao.ganipisetty@gmail.com

Fig.15. Intruder Login.


Privacy Protection and Intrusion
HOME PAGE
VIEW PATIENTS
LOGOUT
Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing

Welcome intruder

Fig.16. Intruder Home Page.

VII. CONCLUSION

In this paper, we investigated 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 Detection Rate Cost Detection Rate IDS Number Cost and detection rate of the entire IDS system. The optimal configuration is shown to use 4 IDS's with a 75% detection rate under a minimum system cost of 0:02. Only relative costs are shown here. 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.

VIII. REFERENCES

[1] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telehome healthcare," in Engineering in Medicine and Biology Society, 2004. IEMBS'04. 26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.

[2] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," 2015.

[3] J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej, A. Streit, and D. Georgakopoulos, "A security framework in g-hadoop for big data computing across distributed cloud data centres," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.

[4] M. S. Hossain and G. Muhammad, “Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring,” Computer Networks, vol. 101, pp. 192–202, 2016.

[5] R. Zhang and L. Liu, “Security models and requirements for healthcare application clouds,” in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010, pp. 268–275.

[6] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, “Deypos: Deduplicatable dynamic proof of storage for multi-user environments,” 2016.

[7] L. Griffin and E. De Leastar, “Social networking healthcare,” in Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on. IEEE, 2009, pp. 75–78.

[8] W. Xiang, G. Wang, M. Pickering, and Y. Zhang, “Big video data for light-field-based 3d telemedicine,” IEEE Network, vol. 30, no. 3, pp. 30– 38, 2016.

[9] “https://www.patientslikeme.com/.”

[10] C. Zhang, J. Sun, X. Zhu, and Y. Fang, “Privacy and security for online social networks: challenges and opportunities,” Network, IEEE, vol. 24, no. 4, pp. 13–18, 2010.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[12] K. T. Pickard and M. Swan, “Big desire to share big health data: A shift in consumer attitudes toward personal health information,” in 2014 AAAI Spring Symposium Series, 2014. 2168-7161 (c) 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_ standards/publications/rights/index.html for more information. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2016.2617382, IEEE Transactions on Cloud Computing 9.

[13] T. Xu, W. Xiang, Q. Guo, and L. Mo, “Mining cloud 3d video data for interactive video services,” Mobile Networks and Applications, vol. 20, no. 3, pp. 320–327, 2015.

[14] M. Quwaider and Y. Jararweh, “Cloudlet-based efficient data collection in wireless body area networks,” Simulation Modelling Practice and Theory, vol. 50, pp. 57–71, 2015.

[15] K. Dongre, R. S. Thakur, A. Abraham et al., “Secure cloud storage of data,” in Computer Communication and Informatics (ICCCI), 2014 International Conference on. IEEE, 2014, pp. 1–5.

[16] M. S. Hossain, G. Muhammad, M. F. Alhamid, B. Song, and K. Al- Mutib, “Audio-visual emotion recognition using big data towards 5g,” Mobile Networks and Applications, pp. 1–11, 2016.

[17] J. Chen, K. He, R. Du, M. Zheng, Y. Xiang, and Q. Yuan, “Dominating set and network coding-based routing in wireless mesh networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 2, pp. 423–433, 2015.

[18] L. M. Kaufman, “Data security in the world of cloud computing,” Security & Privacy, IEEE, vol. 7, no. 4, pp. 61–64, 2009.

[19] R. Lu, X. Lin, and X. Shen, “Spoc: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency,” Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 3, pp. 614–624, 2013.

[20] J.-J. Yang, J. Li, J. Mulder, Y. Wang, S. Chen, H. Wu, Q. Wang, and H. Pan, “Emerging information technologies for enhanced healthcare,” Computers in Industry, vol. 69, pp. 3–11, 2015.

[21] J.-J. Yang, J.-Q. Li, and Y. Niu, “A hybrid solution for privacy preserving medical data sharing in the cloud environment,” Future Generation Computer Systems, vol. 43, pp. 74–86, 2015.

[22] A. Andersen, K. Y. Yigzaw, and R. Karlsen, “Privacy preserving health data processing,” in e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on. IEEE, 2014, pp. 225–230.

[23] K. Rohloff and D. B. Cousins, “A scalable implementation of fully homomorphic encryption built on ntru,” in Financial Cryptography and Data Security. Springer, 2014, pp. 221–234.

[24] K. Zhang, X. Liang, M. Baura, R. Lu, and X. S. Shen, “Phda: A priority based health data aggregation with privacy preservation for cloud assisted wbans,” Information Sciences, vol. 284, pp. 130–141, 2014.

[25] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. H. Luo, “Security and privacy for mobile healthcare networks: from a quality of protection perspective,” Wireless Communications, IEEE, vol. 22, no. 4, pp. 104–112, 2015.

[26] S. Saha, R. Das, S. Datta, and S. Neogy, “A cloud security framework for a data centric wsn application,” in Proceedings of the 17th International Conference on Distributed Computing and Networking. ACM, 2016, p. 39.

[27] A. Sajid and H. Abbas, “Data privacy in cloud-assisted healthcare systems: State of the art and future challenges,” Journal of Medical Systems, vol. 40, no. 6, pp. 1–16, 2016.

[28] S. M. Sajjad, S. H. Bouk, and M. Yousaf, “Neighbor node trust based intrusion detection system for wsn,” Procedia Computer Science, vol. 63, pp. 183–188, 2015.

[29] R. Mitchell and I.-R. Chen, “Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems,” Dependable and Secure Computing, IEEE Transactions on, vol. 12, no. 1, pp. 16–30,2015.

[30] H. Mohamed, L. Adil, T. Saida, and M. Hicham, “A collaborative intrusion detection and prevention system in cloud computing,” in AFRICON, 2013. IEEE, 2013, pp. 1–5.

[31] Y. Shi, S. Abhilash, and K. Hwang, “Cloudlet mesh for securing mobile clouds from intrusions and network attacks,” in The Third IEEE International Conference on Mobile Cloud Computing, Services, and Engineering,(Mobile Cloud 2015). IEEE, 2015.

[32] E. Vasilomanolakis, S. Karuppayah, M. M¨uhlh¨auser, and M. Fischer, “Taxonomy and survey of collaborative

intrusion detection," ACM Computing Surveys (CSUR), vol. 47, no. 4, p. 55, 2015.

[33] P. K. Rajendran, B. Muthukumar, and G. Nagarajan, "Hybrid intrusion detection system for private cloud: a systematic approach," Procedia Computer Science, vol. 48, pp. 325–329, 2015.

[34] M. Chen, Y. Ma, J. Song, C.-F. Lai, and B. Hu, "Smart clothing: Connecting human with clouds and big data for sustainable health monitoring," ACM/Springer Mobile Networks and Applications.

[35] D. Nu˜nez, I. Agudo, and J. Lopez, "Ntrureencrypt: An efficient proxy re-encryption scheme based on ntru," in Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. ACM, 2015, pp. 179–189.

Author's Profile:

Patan Naushad Khan, PG Scholar, Department of CSE with St. Mary's Group of Institutions, Chebrolu, Guntur, AP, India,
Email: naushad.khan1212@gmail.com.

Mr. Subhanis Haik M.Tech, (Ph.D), received the Master of Technology degree in Computer Science & Engineering From Nalanda Institute Of Engineering And Technology -Jntuk, He Received The Bachelor Of Technology Degree From Loyola Institute Of Technology & Management JNTUH. He is currently working as Associate Professor and a Head of the Department of CSE with St. Mary's Group of Institutions, Chebrolu, Guntur, AP, India, Email: subhanicsehod@stmarysgroup.com.

Mr. Jalaiah Saikam, received the Master of Technology degree in CSE from the QIS College of Engineering & Technology, Ongole, affiliated to JNTU Kakinada in 2011. He received the Bachelor Of Engineering degree in CSE from VRS & YRN college of engineering & technology, chirala affiliated to JNTU Hyderabad in 2008.He has 9 years of teaching experience. He is currently working as assistant Professor of CSE with St. Mary's Group of Institutions, Chebrolu, Guntur. He published international journal on Robustly Detecting and Eliminating the Conflicts in Firewall Policies, Email: jalaiahcse@gmail.com.