European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume09, Issue 03, 2022

PRIVACY PROTECTION AND INTRUSION AVOIDANCE FOR CLOUDLET-BASED MEDICAL DATA SHARING

P.Firoze khan,[1]
[1]Asst. Professor, Department of Computer Science and Engineering
QIS College Of Engineering And Technology
K.sirisha[2], T.KrishnaLasya[3], B.Swapna[4]
Student, Department of Computer Science and Engineering

Abstract*-*Better medical care is becoming more necessary as wearable gadgets and cloudlet technologies become in prominence. Data collection, storage, and dissemination, among other things, all fall within the purview of the medical data processing chain. In the traditional healthcare system, sensitive information about patients is often sent to the cloud, which consumes a great deal of energy and has a negative impact on the environment. In the real world, medical data exchange is a crucial and difficult subject. The versatility of the cloudlet is used to create a new healthcare system in this article. Cloudlet's features include data sharing, privacy protection, and intrusion detection. To encrypt user's body data collected by wearable devices, we use the Number Theory Research Unit (NTRU) method first. In order to save energy, this data will be sent to a neighbouring cloudlet in an efficient manner. To assist users, identify trustworthy cloudlet partners, we provide a novel trust model that can be applied to the cloudlet. The trust model also facilitates communication between patients with similar illnesses. Third, we separate the medical data of patients stored in the hospital's remote cloud into three sections and safeguard them. At long last, we've developed a novel, collaborative intrusion detection system (IDS) method based on cloudlet mesh to safeguard the healthcare system's big data cloud remotely. The results of our experiments show that the proposed method is effective.

Keywords— Intrusion, Privacy, Protection, Medical Data, Data Sharing.

I. INTRODUCTION

Health care big data and wearable technology, as well as cloud computing and communication technologies, have made cloud-assisted healthcare big data computing more important to satisfy consumers' ever-growing needs for health consultation [3–5]. A more difficult problem is how to make specialised healthcare data useful to a wide range of people [6]. Preliminary research [7] revealed that social networks and healthcare services might be used together to help patients track the progress of their illness treatment. Patients-LikeMe [9] is an example of a healthcare social network that may get information from other patients who have had similar experiences via the exchange of personal medical data. It is helpful to both patients and clinicians for medical information to be shared on social media, however the sharing of sensitive information might lead to privacy and security issues [10] [11] without adequate protection for the shared data. Medical data exchange may be cumbersome, so how to combine privacy protection and ease is an important problem.As cloud computing progresses, massive

amounts of data may be stored in a variety of clouds, from local clouds to faraway clouds, making it easier for people to share information and do complex calculations [16, 17]. There are, however, a number of basic issues with cloud-based data sharing:

Is it possible to safeguard sensitive user data when it is being sent to a cloudlet? To ensure that data sharing in cloudlets does not result in privacy issues, how can this be ensured?Since electronic medical records (EMR) and cloud-based applications are becoming more common, greater attention should be given to the security issues associated with a distant cloud that contains healthcare big data. Why How can we safeguard the distant cloud storage of healthcare big data? As a system administrator, how can you keep your whole network safe from hostile attacks?This study suggests a cloudlet-based healthcare system in response to the issues outlined in this research. When you wear a wearable gadget, it sends information about your body to a cloudlet nearby. In addition, the data is sent to a distant cloud, where clinicians may use it for illness diagnosis and treatment plans. We categorise privacy protection into three phases based on the order in which the data is sent. To begin with, wearable devices send their data to a cloudlet closet gateway, where it is processed. Data security is the primary issue at this point. Cloudlets will be used in the second step to transport user data to a distant cloud. Some mobile devices may need and/or want to exchange particular data with other cloudlets, forming a "cloudlet." In this stage, both privacy and data sharing are taken into consideration. The trust model is used to establish whether or not users may share data with one other.

Because the medical data of our users is kept in a distant cloud, we've separated it into several types and implemented a security strategy to match. To safeguard the cloud ecosystem, we are also considering collaborative IDS based on cloudlet mesh in addition to the three steps outlined above. Overall, this paper's main contributions are as follows: For the sake of privacy and efficiency, we've developed a cloudlet-based healthcare system that uses cloudlets to transmit data. Data transfers to the cloudlet are protected using NTRU. • To create confidence in the cloudlet, we exploit users' similarity and reputation. If a user's trust level is assessed, the system decides whether or not to share their data. We use encryption mechanisms to safeguard various types of data in the distant cloud. To safeguard the whole healthcare system from harmful intrusions, we propose a collaborative IDS based on cloudlet mesh.

II. RELATEDWORKS

The author, N. Cao et. al. [1,] claims that the testing problem of security protecting MRSE is characterised and settled out of the blue by them. Such a secure cloud information use architecture required strong security measures to be put in place. Many various multicatchphrase semantics were considered, but ultimately, they settled on "organise coordinating" as the best way to capture the value of information archives to the pursue query because of its professional likeness measurement. This metric of comparability may also be quantified using the term "internal item closeness." Starting with a basic idea for the MRS in view of safe internal item computation, we provide two fundamentally improved MRS plans to meet various rigorous protection requirements in two unique risk models. We've done a lot of digging into the proposed plans' security and productivity guarantees.

It's been reported that in preparation for the impending m-Healthcare problem [2], creators have constructed a secure and protective figure framework known as SPOC. SPOC enables PDA assets, including calculating force and vitality, to be used to handle the registration of important personal health information (PHI) in the midst of the m-Healthcare crisis with little exposure to security risks. They present an effective client-driven protection get to control in

SPOC system, which relies on a characteristic-based access control and another privacy-preserving scalar product computation (PPSPC) procedure, in particular to use the PHI security exposure and high dependability of PHI process and transmission in mHealthcare crisis, and permits a medical client to choose who can participate in the artistic figuring to help prepare hi An examination of security considerations shows that the suggested SPOC structure is capable of achieving client-driven protection control in the event of healthcare crisis. Yang et al [3] describe how the author of this study begins by outlining the essence of this unique problem and offering a brief rule of thumb. The current EMR selection situation is evaluated at this moment. Once we get to that stage, we can see how rapidly information is evolving and how it has a significant impact on the way human services are organised. For exact location and anticipation, these systems combine well-being detection with medical data collection and analysis. Next, cloud computing is mentioned because it may be able to provide more flexible and cost-effective delivery of human services.

It was shown that an MRSE (multi-keyword ranked search over encrypted data in cloud computing) privacy protection system can offer users with a multi-keyword technique for cloud-encrypted data in the already existing system, in Cao et al. It is possible that the quantity of calculations required to provide a useful result ranking might be prohibitive for this strategy.

Zhuo Zhang and his colleagues proposed the use of the Priority-Based Health Data Aggregation (PHDA) method to safeguard and combine various forms of healthcare data inside a WBAN (WBANs). The article under the current system examines security and privacy challenges in mobile healthcare networks, including privacy protection for healthcare data aggregation, security for data processing, and misbehaviour.

To ensure the confidentiality, integrity and fine-grained access control of application data, the system provides a customizable security paradigm for cloud-based data-centric applications. Privacy-protection in cloud-based healthcare systems is examined in a thorough literature study provided by the system.

Disadvantages

(1) Due to a lack of a joint intrusion detection system, outsourced data is less secure (IDS).
(2) A remote cloud data privacy security scheme does not exist at this time.

III. PROPOSED SYSTEM ARCHITECTURE

It is our primary goal to protect both the privacy of users' physiological data and the efficiency of data exchanges in the cloudlet-based healthcare system we've developed. The cloudlet is protected by NTRU during data transfers. We leverage users' similarity and reputation to develop a trust model in order to exchange data in the cloudlet. If a user's trust level is assessed, the system decides whether or not to share their data. The suggested method separates data on a distant cloud into multiple types and uses encryption mechanisms to safeguard each one. In order to safeguard the healthcare system as a whole against harmful assaults, a cloudlet mesh-based collaborative IDS is proposed in the proposed system.

Advantages

Cloudlet-based data sharing has been used to increase the security of outsourced cloud data, thanks in part to the Collaboration Intrusion and Detection system.

The wearable gadget is the focus of this section. Add a pimage (encrypt all parametes except for the pname) and see all patient collected data in enc format with digital sign. The patient data will be uploaded to the Cloudlet, which will store the data in encrypted form. Data storage service for

wearable devices is provided by the Cloud server, which can also see all patients and approve physicians. The enc format allows you to see all patient Cloudlet data. View and approve the access request for patient data. Cloudlet Intruders and retrieved patient data may be seen in full detail here. Number of patients with the same symptom on the chart (symptom name vs. number of patients) and the number of patients who were referred to the same physician (Doctor name vs No.Of Patients). View profile, Request Data Access permission from cloudlet and see response, and Login are all part of this module. Send your medical records to the doctor of your choice using the combo box in the upper right-hand corner of the page. Examine a medical professional's reaction with a prescription, Verify and restore your information, as well as see and delete it. It is the doctor's responsibility to register and log in, see the profile, view patient information, and provide solutions such as medication information and prescription data See a complete list of every patients' medical prescriptions.

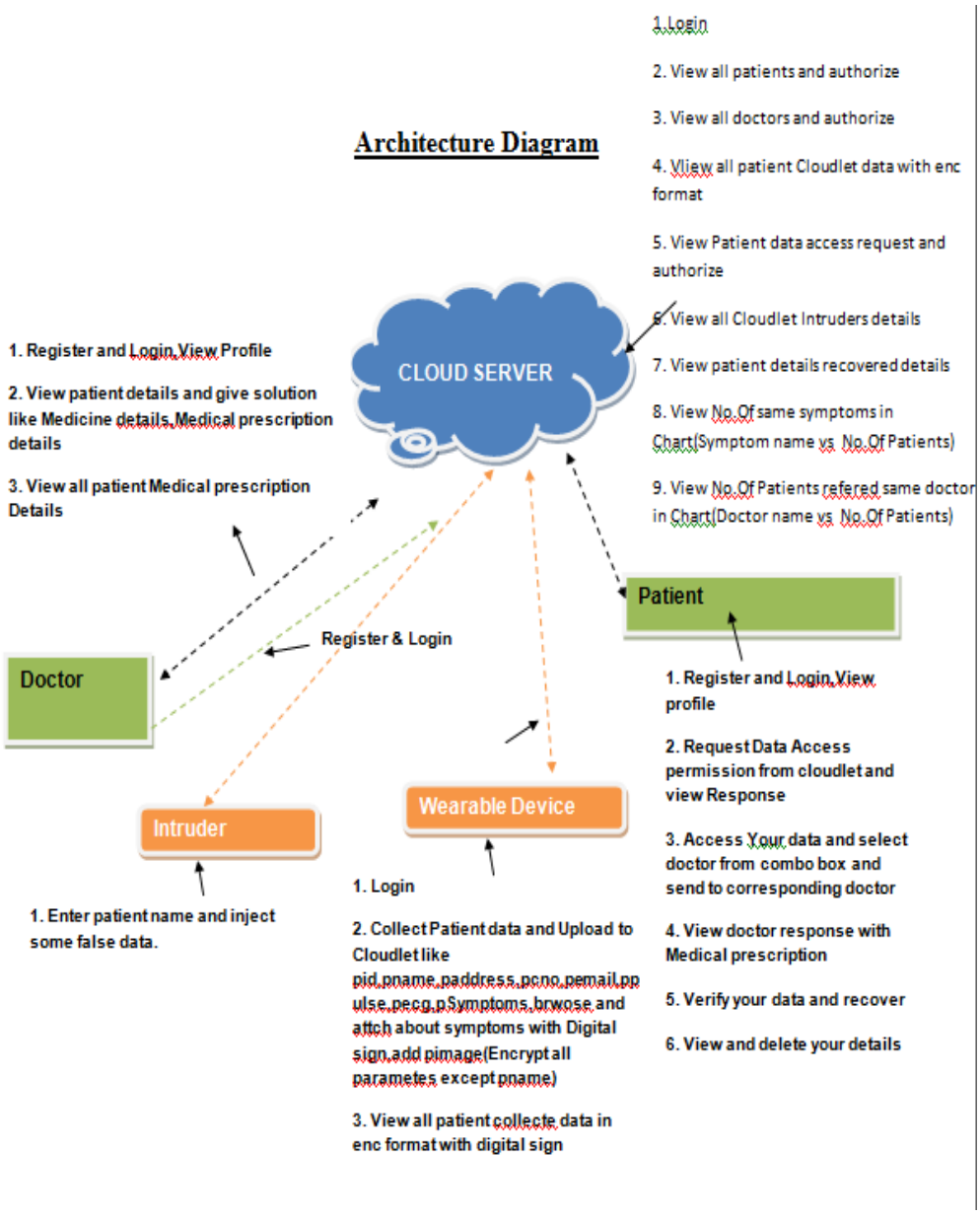


Fig.1 Architecture of suggested system

IV. RESULTS AND DISCUSSION

The results obtained after executing the implementation code is shown from Fig.2 to Fig.8.

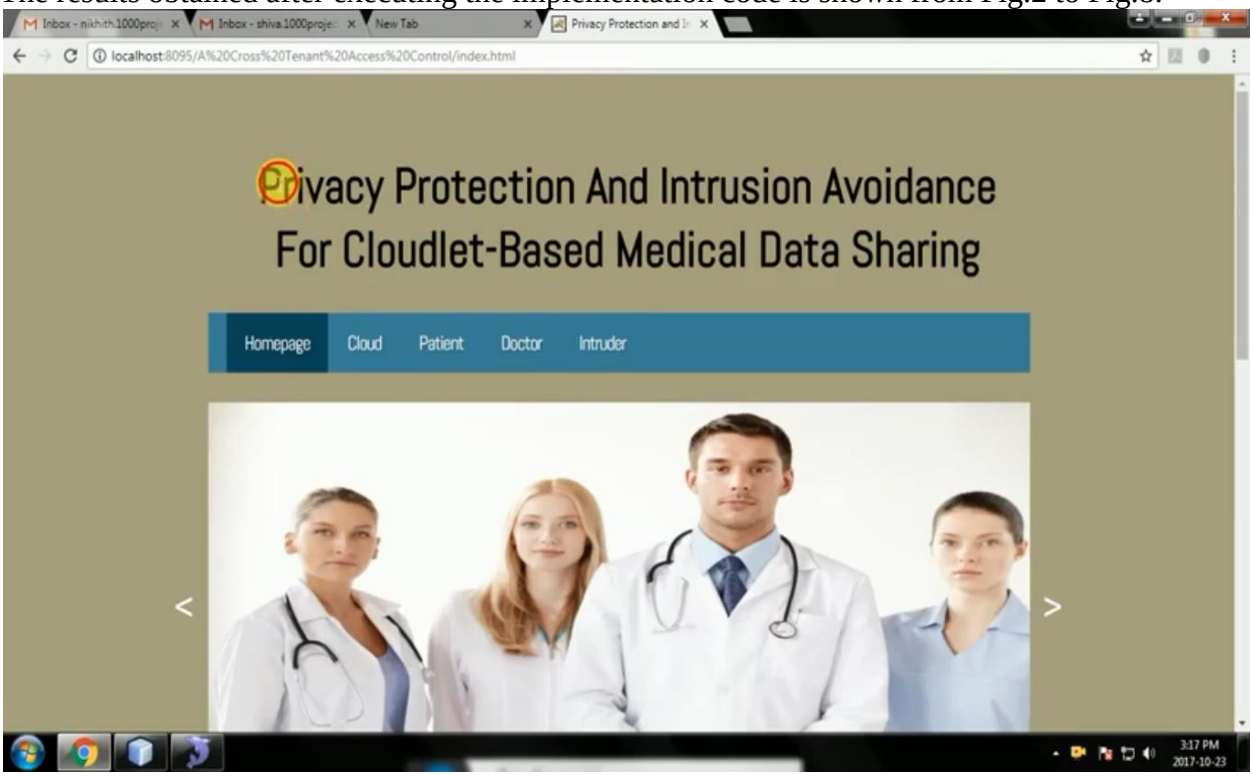


Fig. 2 Home Page

Fig.3 Cloud Login

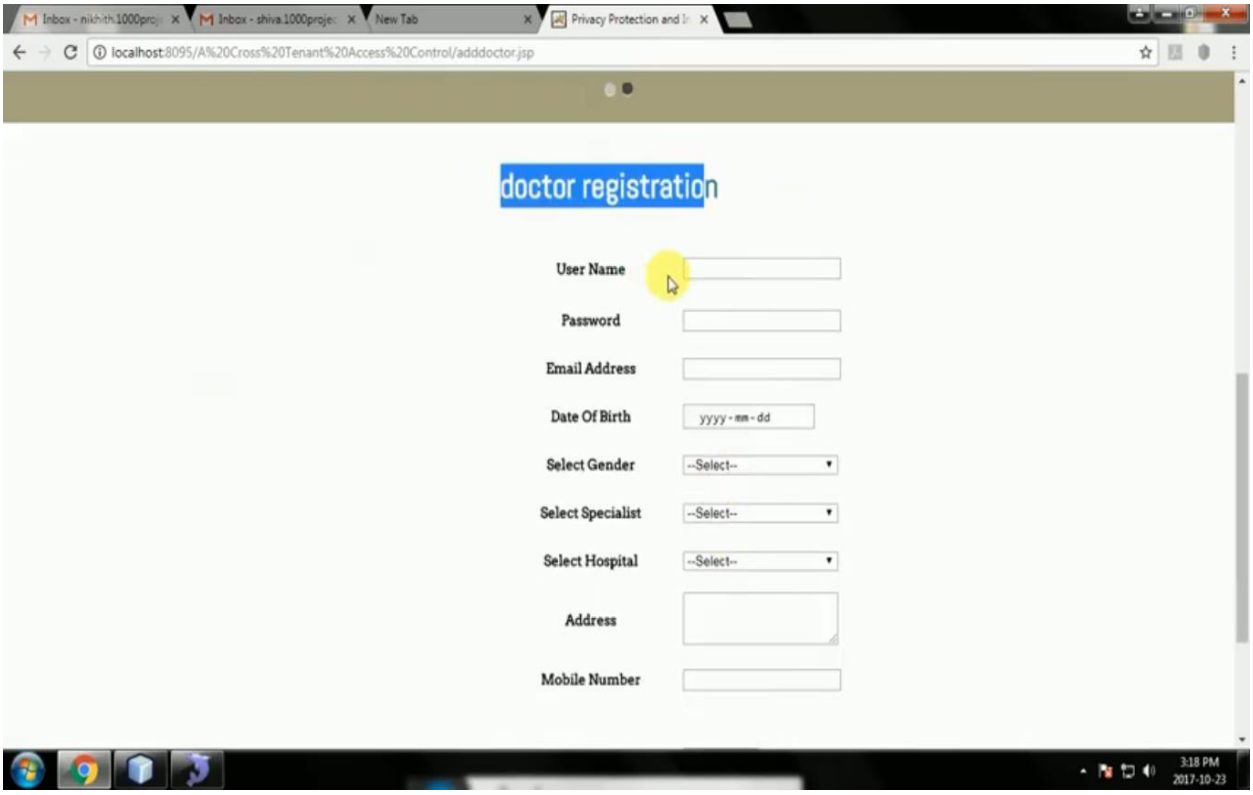
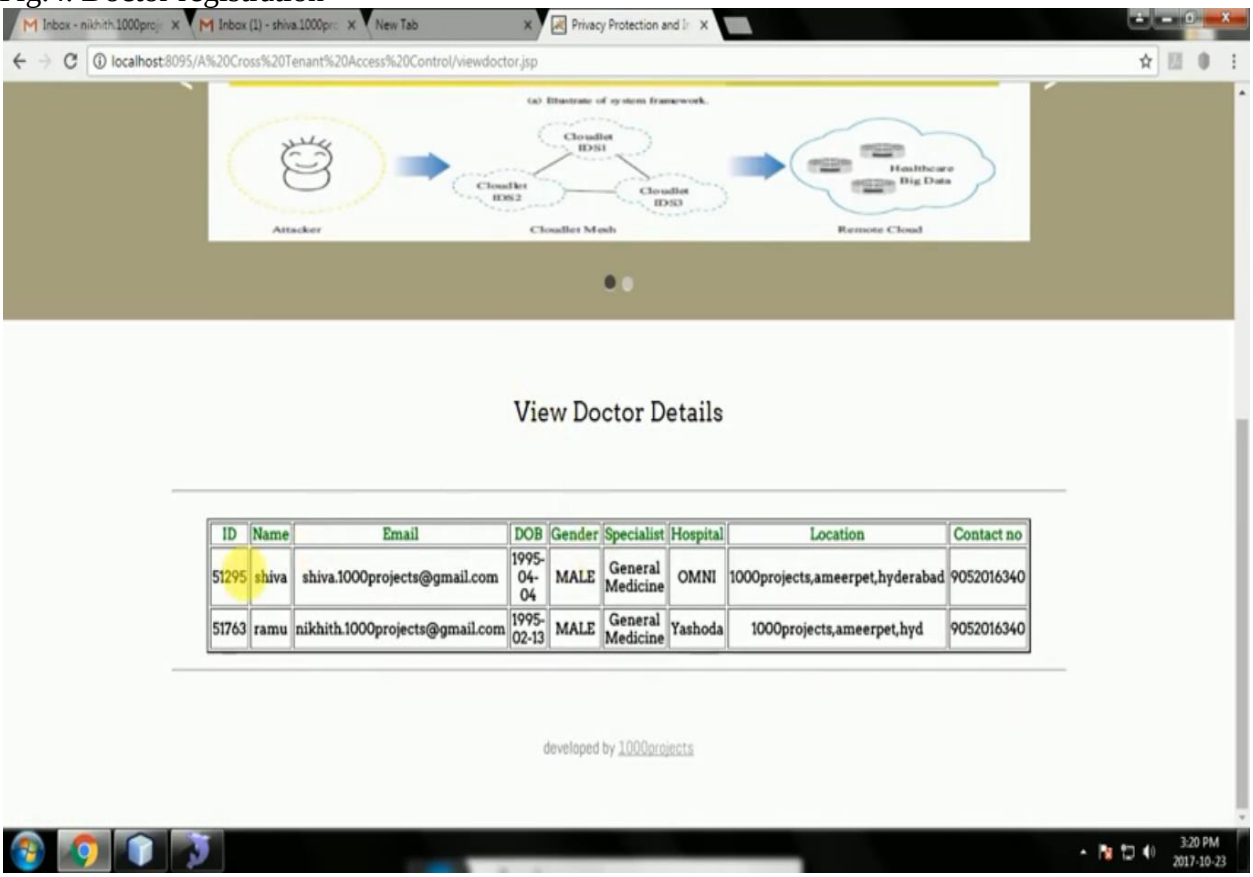


Fig.4. Doctor registration



ID	Name	Email	DOB	Gender	Specialist	Hospital	Location	Contact no
51295	shiva	shiva.1000projects@gmail.com	1995-04-04	MALE	General Medicine	OMNI	1000projects,ameerpet,hyderabad	9052016340
51763	ramu	nikhith.1000projects@gmail.com	1995-02-13	MALE	General Medicine	Yashoda	1000projects,ameerpet,hyd	9052016340

Fig. 5 View Doctor Details

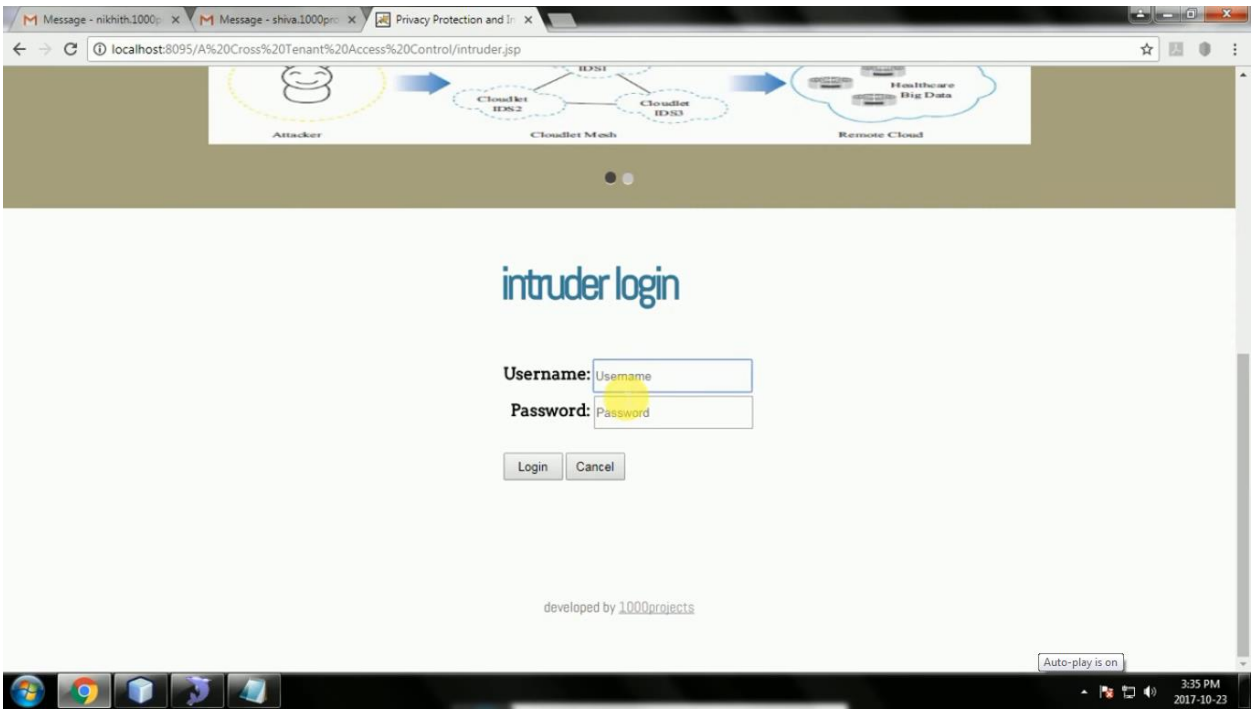


Fig.6 Intruder Login

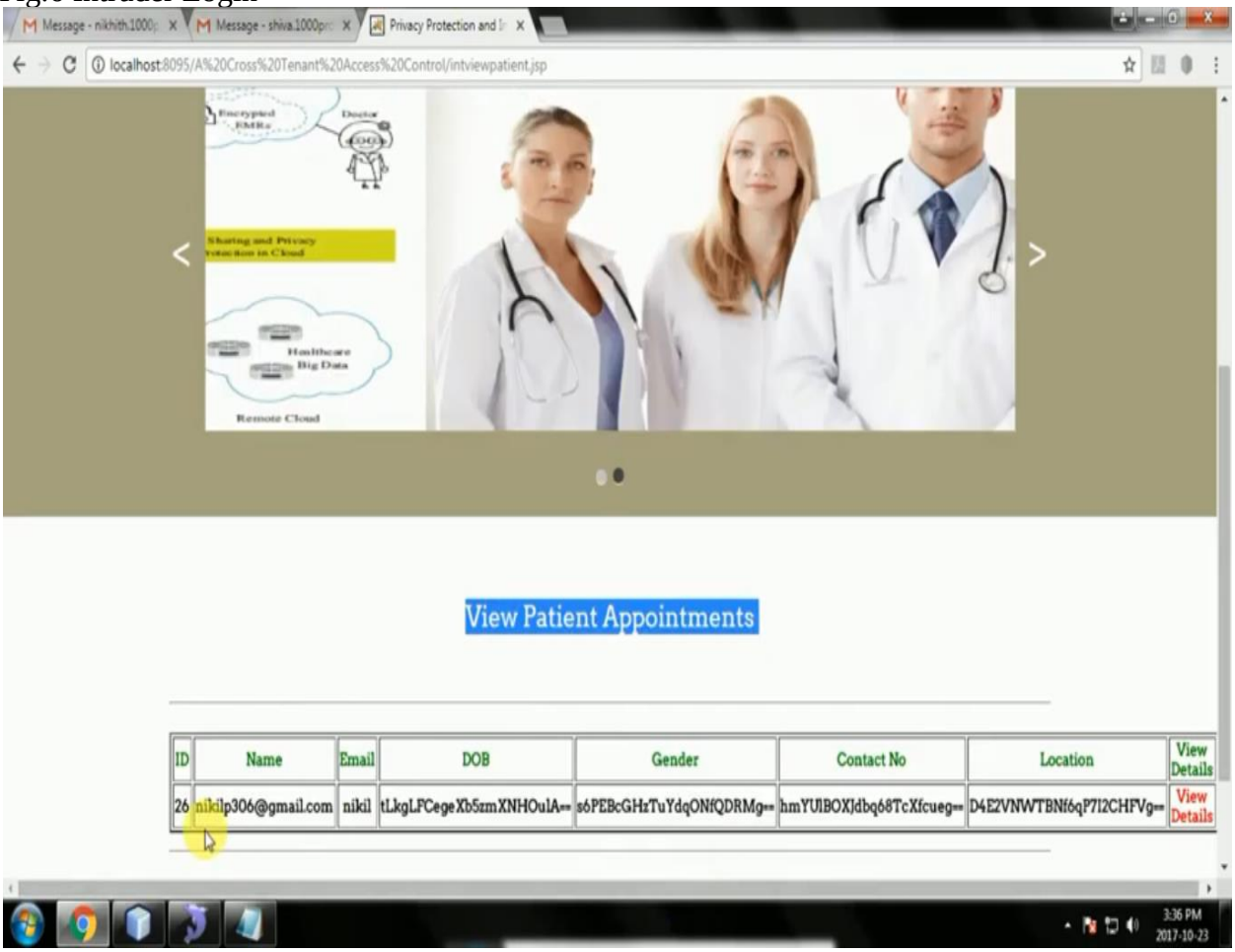


Fig. 7 View Patient Details

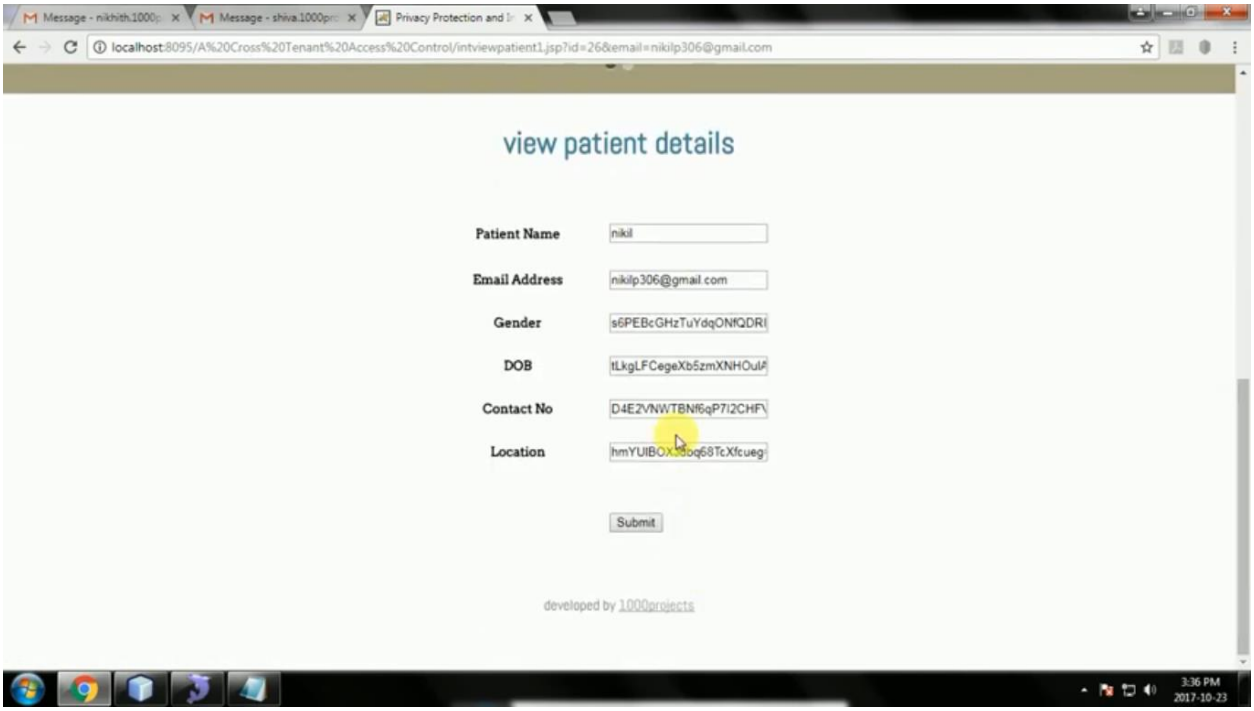


Fig. 8Patient Details in Encrypted form

v. FUTURE SCOPE AND CONCLUSION

Cloudlets and the distant cloud were studied in this article for the purpose of protecting and sharing significant medical data. We designed a system that prevents users from sending data to the distant cloud in order to ensure data collecting is safe and communication costs are kept to a minimum. The cloudlet data sharing issue might be triggered by users transmitting data to the cloudlet.In order to preserve the privacy of our users, we employ the NTRU mechanism, which encrypts the transfer of their data to the cloudlet, to ensure that their data is sent securely. For the purpose of sharing data in the cloudlet, we employ a trust model to determine whether or not to share data based on the trust level of the user. We also divide and encrypt distant cloud data in various ways to maintain data security while also speeding up transmission effectiveness in order to preserve remote cloud data privacy. A cloudlet mesh-based collaborative IDS is then proposed to secure the whole network. Simulations and tests are used to verify the presented plans.

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.
[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.