Maintaining Confidentiality when Sharing Health Information with Cloudlet

Dr. J. Vanitha Vani[1], Dr. M. Chandra Naik[2], A. Vennala[3], K. keerthi[4], Shravya Chidurala[5]
[1, 2, 3, 4]Department of Computer Science and Engineering,
[5]Software Engineer
[1,2,3,4] QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India
[5]Accenture
[1] vanithavani.j@qiscet.edu.in, [2] chandranaik.m@accenture.com, [3]vennala.a@qiscet.edu.in
[4]keerthi.k@qiscet.edu.in,[5]shravya.chidurala@accenture.com,
Corresponding Author Mail: qispublications@qiscet.edu.in

Article Info
Page Number: 550 - 560
Publication Issue:
Vol 70 No. 2 (2021)

Abstract
As wearable devices and cloudlet technology gain momentum, there is a growing need for better healthcare. Among other things, the collection, storage and transfer of all the data drop within the area of the processing chain of medical data.The healthcarethat was followed traditionally often sends sensitive information about cloud patients, here a lot of energy is consumed and which showsits impact negatively on the environment. The important and difficult problem facing now a days is sharing the medical data. In this ,we can take the benefit of the versatility of cloudlets to invent a healthcare system newly. The features of Cloudlet involves sharing of data, protection of privacy, and intrusion detection. The Number Theory Research Unit (NTRU) approach is firstly used to encipher the customers physical data gathered from the wearable device. To save power, this data is efficiently sent to neighboring cloudlets. To help out users, to identify trustCloudlet associates, we offer a new conviction model that Cloudlets may utilise. This approach makes easier communication between patients with similar illnesses of others who are suffering. Third, back up the patient medical data saved in the hospitalpersonal cloud in three sections. Finally, aoriginalmutual intrusion detection system (IDS) A cloudlet mesh-base method for remote securing the big data cloud of healthcare systems. Experimental results show's that the suggested process is Impressive.

Article History
Article Received*: 05 September 2021*
Revised*: 09 October 2021*
Accepted*: 22 November 2021*
Publication*: 26 December 2021*

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

I. INTRODUCTION

With healthcare big data, and apparelknowledgein addition toutilising the cloud and transmission technology, cloud-based healthcare big data computeis becoming more prevalentlysignificant to meet the growing consumer demand for healthcare advice. [3–5]. A toughest problem is how to have professional health data available to a wider audience[6]. A preliminary study [7] suggested sharing social networks and healthcare services to allow patients to track their progress in treating their illnesses. One illustration of a healthcare social network is Patients-LikeMe [9] that allows you to collectdata gleaned from other patients .who have shared

personal medical information and who had similar experiences. Posting medical information on social media is helpful to both patients and physicians, but sharing personal information can lead to privacy and security issues if shared data is not properly protected [10].][11]. Medical data exchange may sometimes be slow and complicated, Therefore, balancing convenience and privacy protection is a major issue..Due to the massive amounts of data that can be stored in a range of clouds with big storage, from local clouds to distant clouds, people can now more easily transfer information and conduct difficult calculations[16, 17] as a result of the advent of cloud computing. But cloud-based data allocation is fraught with a number of serious issues.

How probable is it that user perception data will be preserved while being sent to a cloudlet? What can be done safely to ensure that data sharing in cloudlets doesn't lead to security concerns? Security concerns related to a distant cloud that includes large amounts of healthcare data must receive enormous attention as electronic medical records (EMR) and cloud-based apps become more common..Here the question is Why? In which way, we can preserve the far-away cloud storage of healthcare big data? Need to know how to protect the entire network from hostile attacks as a system administrator?To address the issues raised in this study, a cloudlet-based healthcare system is proposed. Wearable technology transmits information about your body to a neighbouring cloudlet while it is worn. Additionally, the data is sent to a faraway cloud so that medical professionals can use it to diagnose patients and design treatment plans. We categorise data security into three stages based on the order in which it is transferred. The data that the wearable gadget sends there is processed by the Cloudlet Gateway first. Data security is prioritised here. In the following step, user data is sent to a distant cloud via Cloudlet. Some mobile devices could need or want to exchange particular data with other "Cloudlets" in order to establish a "Cloudlet."This phase takes into account both data interchange and data protection. To decide whether users can exchange data with one another, a trust model is employed.

Because the user's medical information is stored in a remote cloud, we divide it into distinct categories and put in the appropriate security measures. In addition to the three methods already described, we are also considering a joint IDS based on Cloudlet Mesh to protect the cloud ecosystem. The main advantages of this study are generally:We have created a cloudlet-based healthcare system that transfers data using cloudlets for reasons of efficiency and privacy. Data is NTRU protected while transfer to Cloudlet.. • Utilize user affinities and reputation to increase user confidence in Cloudlet. Based on the user's level of trust, the system decides whether to share data. To protect diverse sorts of data on remote clouds, use encryption techniques. We recommend a collaborative IDS built on Cloudlet Mesh to safeguard the entire healthcare system from hostile intrusion.

II. RELATEDWORKS

N. Cao et al. Al. the author [1,] contend that they characterise and mysteriously resolve MRSE security protection test difficulties. Secure cloud information utilisation design calls for stringent security measures. The benefit of information archiving for tracking queries based on expert similarity measures was eventually best captured by "organisational coordination," one of many various multi-subject semantics that were investigated. The concept of "internal closeness of articles" can also be used to generate this comparability statistic. We present two of MRS's MRS

plans that have been drastically modified to satisfy two separate and demanding protection criteria with two distinct risk models, starting with the fundamental principle of safe internal item computations. We carefully examined the proposed plan's assurances of productivity and safety.

The developer is said to have created a safeguard character framework dubbed his SPOC in anticipation of potential m-Healthcare problems [2]. In the middle of a low security risk m-healthcare crisis, SPOC permits the use of PDA assets, involves processing capacity, and involves strength to process crucial personal health information (PHI) registrations. These illustrate efficient client-driven safeguards that the SPOC system can manage. To explicitly handle PHI security issues and PHI big trust, the SPOC system supports function-based access control and another Privacy Preserving Dot Product Computation (PPSPC) approach..Healthcare customers can choose who can participate in artwork to help patients become alert for boiling point, supporting mHealthcare crisis protocols and communication. Yang and others. explains how the authors of this case started off by outlining the nature of this particular situation and providing a straightforward rule of thumb. The evaluation of his current EMR selection status is ongoing. When you get to this point, you'll realise how quickly information changes and how it significantly affects how human services are set up. For precise location and prediction, these systems combine the detection of medical conditions with the gathering and processing of medical data. Let's move on to discussing cloud computing. This is due to the promise for more flexible and affordable delivery of human services.

Healthcare customers can choose who can participate in artwork to help patients become alert for boiling point, supporting mHealthcare crisis protocols and communication. Yang and others. explains how the authors of this case started off by outlining the nature of this particular situation and providing a straightforward rule of thumb. The evaluation of his current EMR selection status is ongoing. When you get to this point, you'll realise how quickly information changes and how it significantly affects how human services are set up. For precise location and prediction, these systems combine the detection of medical conditions with the gathering and processing of medical data. Let's move on to discussing cloud computing. This is due to the promise for more flexible and affordable delivery of human services.

Disadvantages

(1) The lack of a joint intrusion detection system makes the security of outsourced data lessened (IDS).

(2) There isn't currently a method in place to protect the privacy of remote cloud data.

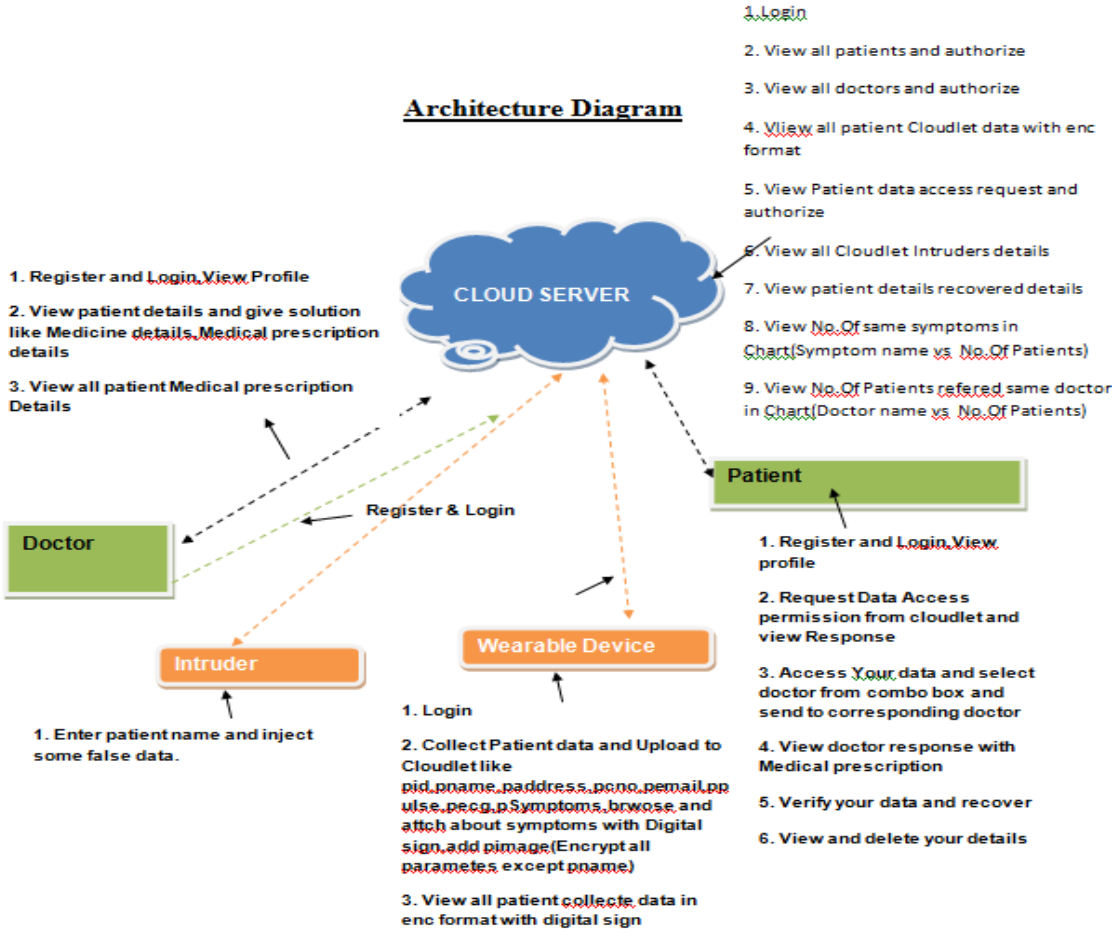
PROPOSED SYSTEM ARCHITECTURE

Our main goal is to maintain the effectiveness of data exchange and the confidentiality of users' physiological data in the developed cloudlet-based healthcare system. NTRU protects cloudlets when moving data. To create trust models and facilitate data flow in Cloudlets, employ user affinities and reputations. After determining the user's level of trust, the system decides whether to give data. The suggested approach separates the data from the remote cloud into numerous categories and uses cryptographic methods to protect each. A cloudlet mesh-based joint IDS is suggested as the preferred method to protect the entire medical system from hostile intrusions.

Advantages

Due in part to a cooperative intrusion detection mechanism, cloudlet-based data sharing is utilised to increase the security of offloaded cloud data.

Wearable technology is the main topic of this section. Show all patient data collected in digitally signed enc format and add pimage (encrypt all parameters except pname).. Cloudlet is used to upload patient data, which is then stored there in an encrypted fashion. You can watch all patients on cloud servers and even approve doctors, providing a data storage service for wearable technology. You can access all of the patient data in cloudlet in enc format. Requests for access to patient data can be seen and approved. You may read more about Cloudlet intrusions and the patient data retrieved here. Patients with the same condition are shown in the table together with the number of patients with that condition (patient number and symptom name) (doctor name and patient number). Logging is part of this module. Logging in, viewing responses, looking through profiles, and asking Cloudlets for data access permissions are all part of this module. Send the medical record to the doctor of your choice by using the combo box in the top right corner of the page. Review and recover your information, view and delete, and look at how doctors react to prescriptions. It is the doctor's responsibility to register, log in, view patient data, peruse profiles, and offer services like prescription information and medication details. Check out the whole list of drugs each patient has been prescribed.



.

Fig.1 system architecture

III. RESULTS AND DISCUSSION

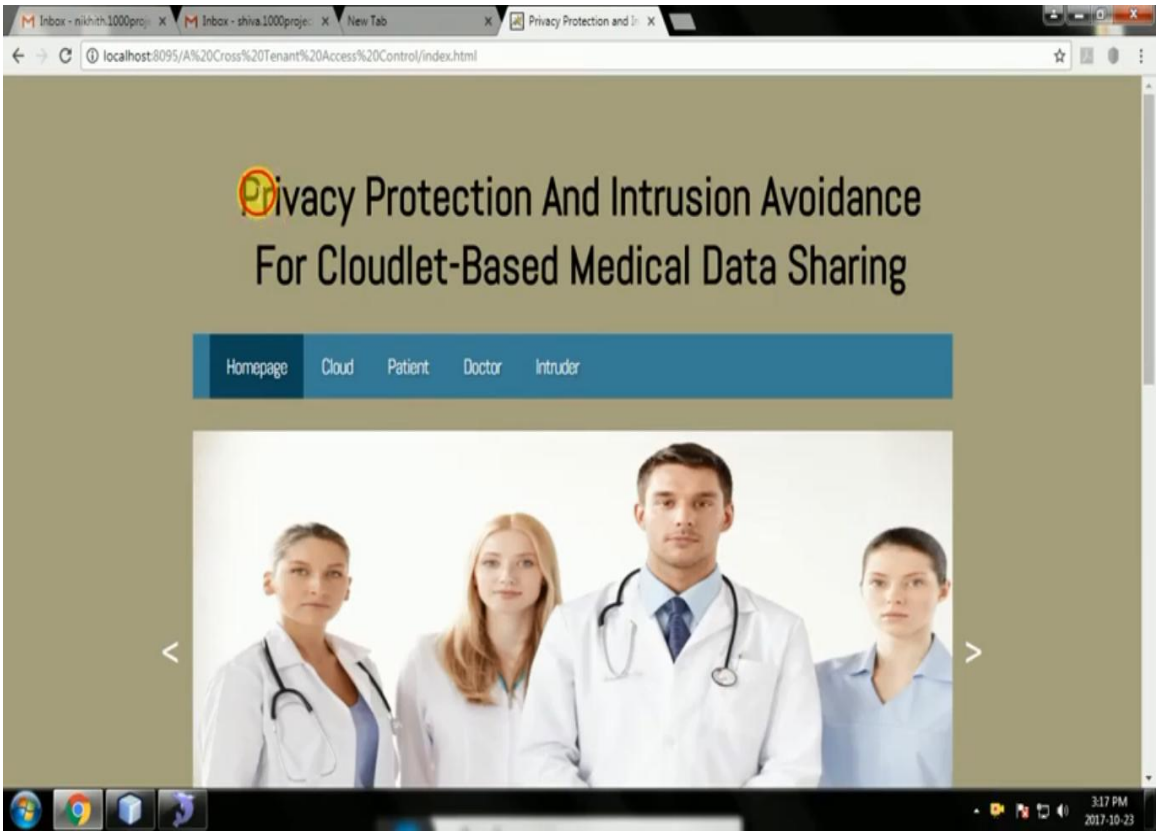


Fig. 2 main page

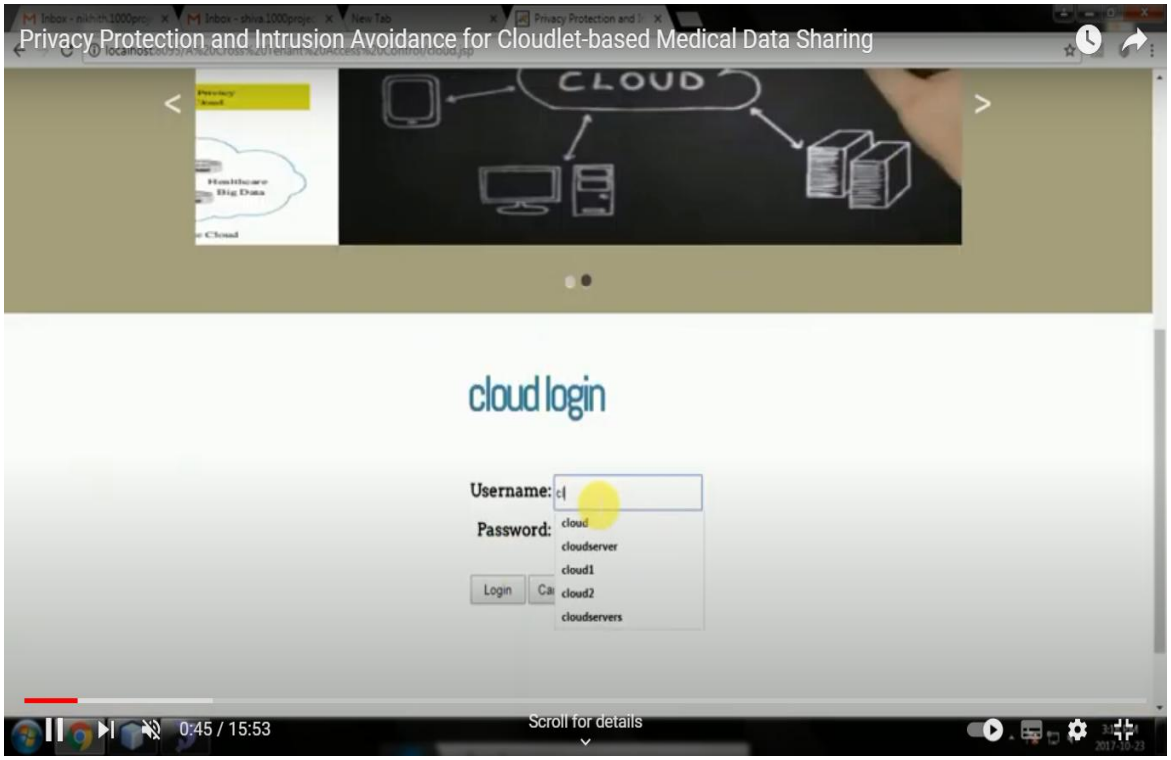


Fig.3 login page of cloud

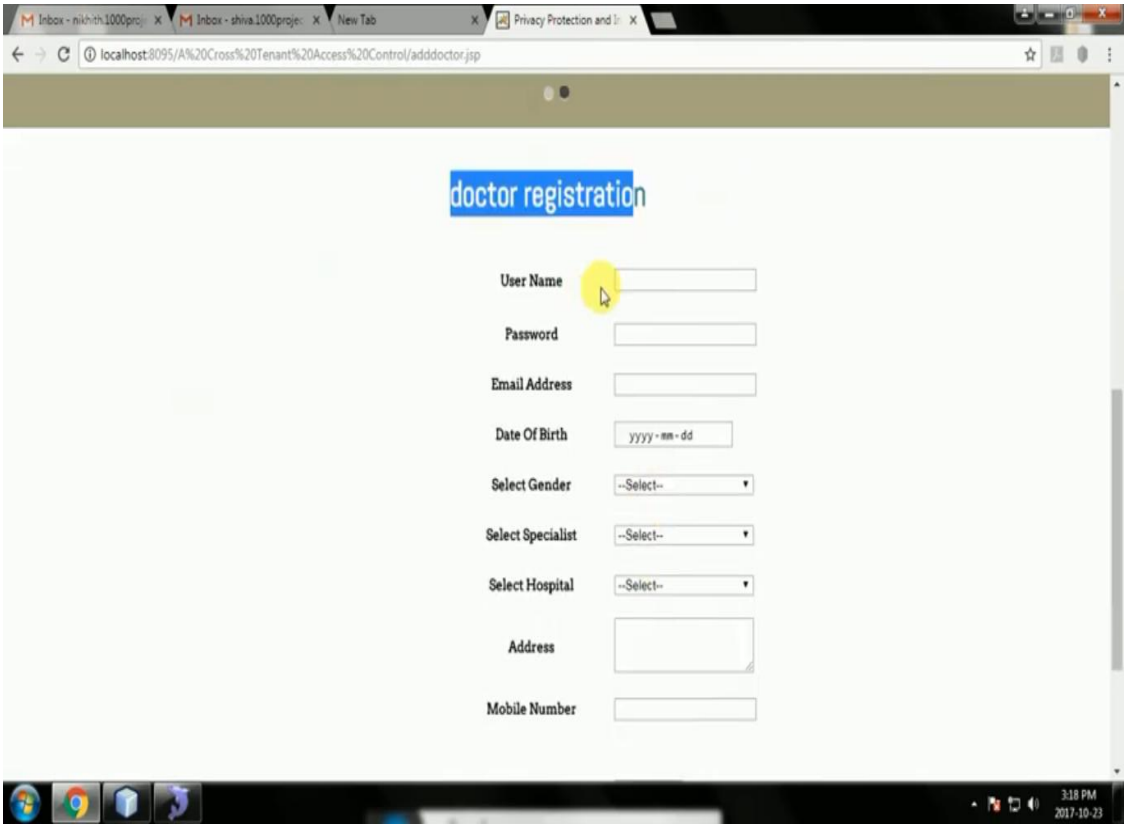
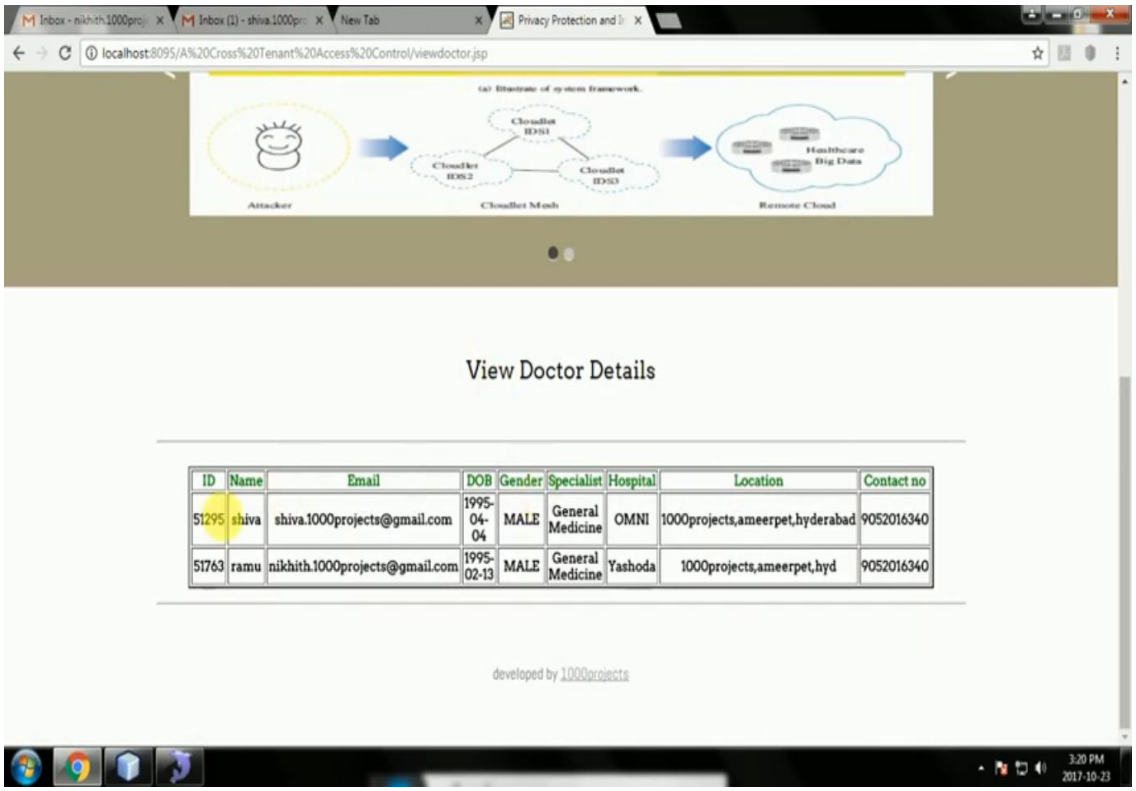


Fig.4. registration page



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 details of docter

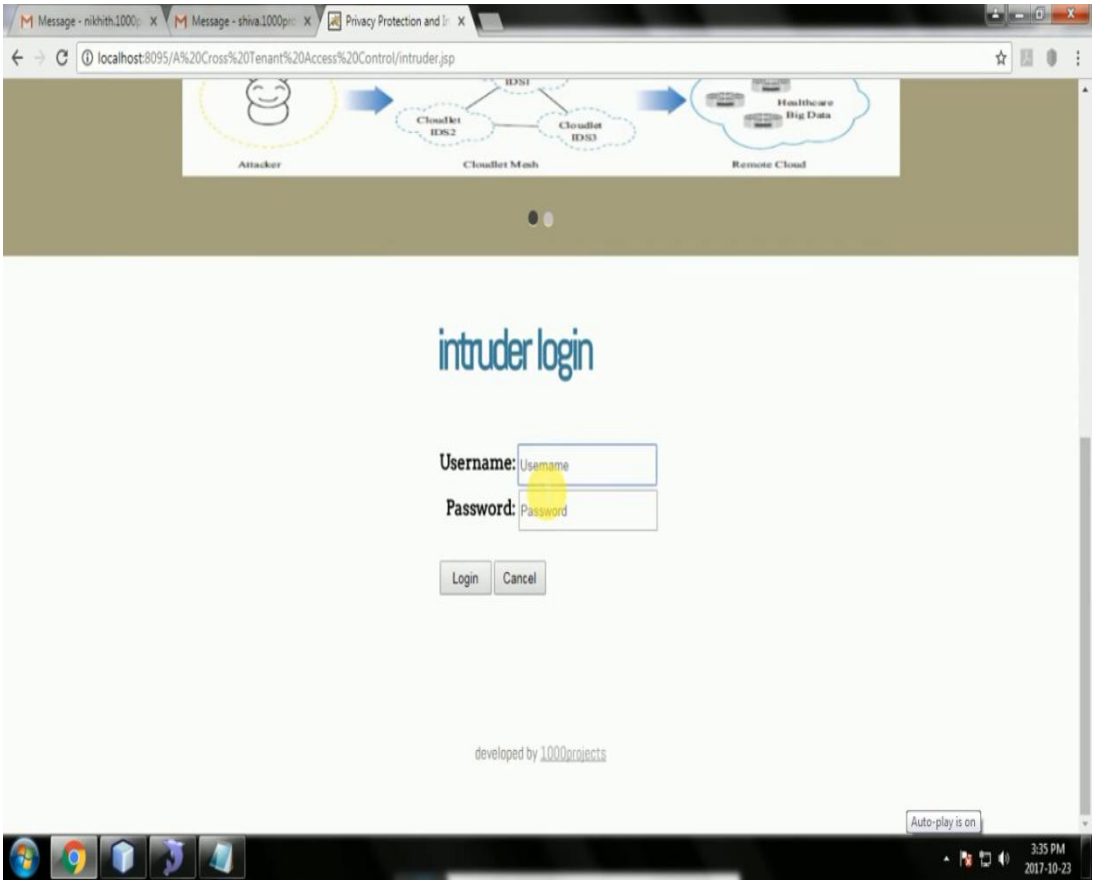


Fig.6 login page of intruder

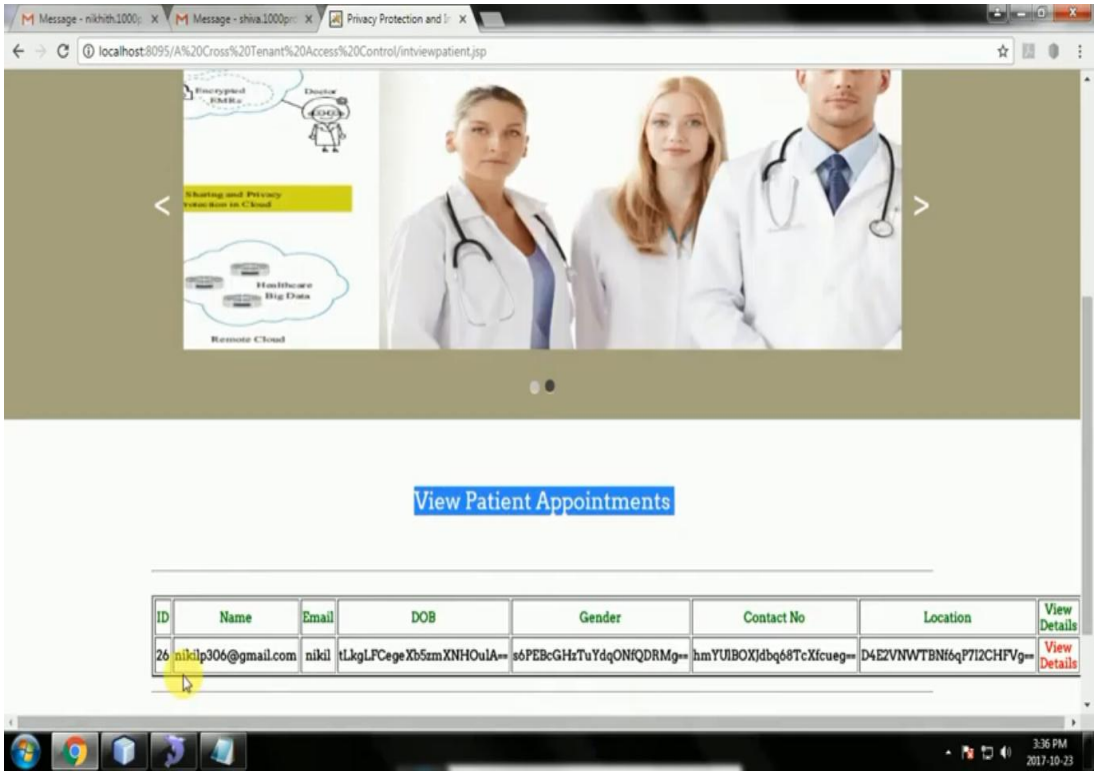


Fig. 7 details of patient

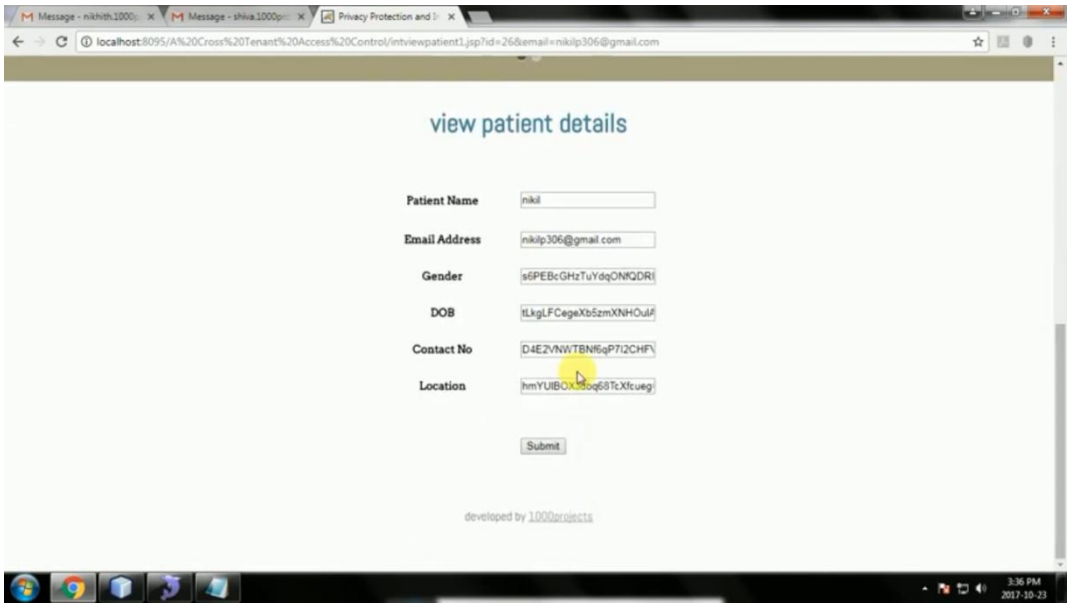


Fig. 8 Details of patient in the form of encryption

FUTURE OUTLOOKAND CONCLUSION

In this article, we discussed cloudlets and remote clouds to protect and share critical healthcare data. We created a mechanism to stop users from transferring information to distant clouds, guaranteeing that collected data is secure and reducing connection costs.Data sharing issues could arise for users migrating data to Cloudlet. To protect user privacy, we use the NTRU approach to securely encrypt the data transmission to Cloudlets. Based on the user's level of trust, we apply a trust model to decide whether to publish data in Cloudlet. It also distributes and encrypts remote cloud data in a number of ways while boosting transmission efficiency in order to safeguard data privacy. The next item on the agenda is a Cloudlet mesh-based joint IDS to protect the entire network.

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.

[21] K. A. Khan, Q. Wang, C. Luo, X. Wang, and C. Grecos, "Comparative Study of internet cloud and cloudlet over wireless mesh networks for realtime Applications," in SPIE Photonics Europe. International Society for Optics and Photonics, 2014, pp. 91 390K.

[22] Rajendran, P. K., Muthukumar, B., &Nagarajan, G. "Hybrid Intrusion Detection System for Private Cloud": A Systematic Approach. Procedia Computer Science, 48,pp.325–329, (2015).

[23] Raj Scholar, A. P., & Rani Assistant professor, S. M. "Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems : A Review. International Journal of Computer Applications.

[24] Shi, Y., Abhilash, S., & Hwang, K. "Cloudlet Mesh for Securing Mobile Clouds from Intrusions and Network Attacks". In 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (pp. 109–118).(2015).

[25] Sajjad, S. M., Bouk, S. H., &Yousaf, M. Neighbor Node Trust based Intrusion Detection System for WSN. Procedia Computer Science, 63, pp.183–188, (2015).

[26] Vasilomanolakis, E., Karuppayah, S., Mühlhäuser, M., & Fischer, M. "Taxonomy and Survey of Collaborative Intrusion Detection". ACM Computing Surveys, 47(4), pp.1–33. (2015).

[27] P Ramprakash, M Sakthivadivel, N Krishnaraj, J Ramprasath. ”Host-based Intrusion Detection System using Sequence of System Calls” International Journal of Engineering and Management Research, Vandana Publications, Volume 4, Issue 2, 241-247, 2014

[28] N Krishnaraj, S Smys.”A multihoming ACO-MDV routing for maximum power efficiency in an IoT environment” Wireless Personal Communications 109 (1), 243-256, 2019.

[29] N Krishnaraj, R Bhuvanesh Kumar, D Rajeshwar, T Sanjay Kumar, Implementation of energy aware modified distance vector routing protocol for energy efficiency in wireless sensor networks, 2020 International Conference on Inventive Computation Technologies (ICICT),201-204

[30] Ibrahim, S. Jafar Ali, and M. Thangamani. "Enhanced singular value decomposition for prediction of drugs and diseases with hepatocellular carcinoma based on multi-source bat algorithm based random walk." Measurement 141 (2019): 176-183. https://doi.org/10.1016/j.measurement.2019.02.056

[31] Ibrahim, Jafar Ali S., S. Rajasekar, Varsha, M. Karunakaran, K. Kasirajan, Kalyan NS Chakravarthy, V. Kumar, and K. J. Kaur. "Recent advances in performance and effect of Zr doping with ZnO thin film sensor in ammonia vapour sensing." GLOBAL NEST JOURNAL 23, no. 4 (2021): 526-531. https://doi.org/10.30955/gnj.004020 , https://journal.gnest.org/publication/gnest_04020

[32] N.S. KalyanChakravarthy, B. Karthikeyan, K. Alhaf Malik, D.BujjiBabbu,. K. NithyaS.Jafar Ali Ibrahim , Survey of Cooperative Routing Algorithms in Wireless Sensor Networks, Journal of Annals of the Romanian Society for Cell Biology ,5316-5320, 2021

[33] Rajmohan, G, Chinnappan, CV, John William, AD, ChandrakrishanBalakrishnan, S, AnandMuthu, B, Manogaran, G. Revamping land coverage analysis using aerial satellite image mapping. Trans Emerging Tel Tech. 2021; 32:e3927. https://doi.org/10.1002/ett.3927

[34] Vignesh, C.C., Sivaparthipan, C.B., Daniel, J.A. et al. Adjacent Node based Energetic Association Factor Routing Protocol in Wireless Sensor Networks. Wireless PersCommun 119, 3255–3270 (2021). https://doi.org/10.1007/s11277-021-08397-0.

[35] C ChandruVignesh, S Karthik, Predicting the position of adjacent nodes with QoS in mobile ad hoc networks, Journal of Multimedia Tools and Applications, Springer US,Vol 79, 8445-8457,2020