**PROTECTING PRIVACY AND PREVENTING INTRUDERS FOR CLOUDLET-BASED MEDICAL DATA SHARING**

*1M.Bhargavi, 2P. Rachana, 3K. Abhishek,4 J. Vamshi, 5Dr. P.Punnam Chandar*

##### *1,2,3,4Bachelor Degree, Cse,* Jayamukhi Institute Of Technological Sciences, *Narsampet ,Warangal.*

##### *5Dr P.Punnam Chandar, Associate Professor, Cse,* Jayamukhi Institute Of Technological Sciences, *Narsampet ,Warangal.*

**ABSTRACT:**

Better medical care is becoming more and more necessary as wearable technology gains prominence and cloud and cloudlet technology develops. The primary steps in the process chain for medical data include data gathering, data storage, and data exchange, among others. The transfer of medical data to the cloud is a common requirement in traditional healthcare systems, including private user data and using up communication energy. Practically speaking, exchanging health information is a crucial and difficult problem. Due to the flexibility of cloudlets, we construct a revolutionary healthcare system in this work.

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.

Data exchange, privacy protection, and intrusion detection are among the purposes of cloudlets. We initially apply the Number Theory Research Unit (NTRU) approach to encrypt user body data gathered by wearable devices during the data gathering stage. These information will be sent in an energy-efficient manner to a neighbouring cloudlet. In order to assist users in choosing reliable partners that want to exchange stored data in the cloudlet, we also propose a new trust model. The trust model facilitates communication amongst patients with comparable illnesses. Thirdly, we separate the users' medical information into three categories and properly safeguard it on the hospital's distant cloud.

Last but not least, we create a unique collaborative intrusion detection system (IDS) approach based on cloudlet mesh to safeguard the healthcare system from harmful assaults. This method can successfully shield the distant healthcare large data cloud from attacks. Our tests show that the suggested strategy is successful.

**INTRODUCTION:**

Internet-assisted healthcare big data computing is essential to address consumers' ever-increasing expectations for health consultation as wearable technology, care big data, cloud computing, and communication technologies evolve [1–2]. To conveniently personalise certain healthcare data for different consumers, meanwhile, is a difficult problem [6]. Previous research recommended using social networks with healthcare services to help [7] track the progression of illness treatment and retrieve real-time disease information [8]. Through the exchange of user-generated data, healthcare social platforms like Patients Like Me [9] may learn more about other patients who have similar conditions.

Although sharing medical information on social media is advantageous for both patients and clinicians, doing so increases the risk of privacy and security issues [10] [11] without effective data protection [12]. As a result, the difficult question of how to strike a balance between privacy protection and the practicality of exchanging medical data arises.

The development of cloud computing has allowed for the storage of vast amounts of data in a variety of clouds, including cloudlets and distant clouds, which has facilitated data sharing and heavy calculations [16] [17].

**RELETED DATA:**

Our work is strongly connected to cloud-based collaborative IDS and privacy-preserving cloudlet mesh technology. We'll provide a succinct overview of the works in these areas.

**Cloud-based Privacy Preservation:**

Despite the advancement of cloud computing technology and the growth of a growing number of cloud collaboration platforms, privacy concerns have prevented the cloud from being widely used for the exchange of healthcare data [18]. Various publications on the traditional privacy protection of healthcare data are available [11], [19]-[25]. A structure called SPOC, which stands for the secure and privacy-preserving opportunities computing framework, was proposed in Lu et al.'s study [19] to address the issue of safety and privacy within the cloud setting and to address the storage problem of healthcare data.

In the article [21], a compound solution was put up for the preservation of healthcare data sharing's privacy in the cloud environment. This solution combines a number of different technologies in combination. An MRSE (multi keyword ranked search over encrypted data in cloud computing) privacy protection system that intends to give users a multi-keyword technique for the cloud's encrypted data was introduced by Cao et al. in Cao et al. [11].

Despite the fact that this approach may produce the people-interesting result ranking, the quantity of calculation may be onerous.

. A priority-based health data aggregation (PHDA) strategy was introduced in Zhang et al.'s paper [24] to preserve and aggregate various forms of healthcare data in cloud-assisted wireless body area networks (WBANs). The paper [25] looks on security and privacy concerns in mobile healthcare networks, including healthcare data aggregation privacy protection, processing security, and misbehaviour security. In order to provide data confidentiality, data integrity, and fine-grained access control to the application data, [26] offers a flexible security architecture specifically for data-centric applications in a cloud computing-based environment. [27] present a thorough overview of the literature on the protection of privacy in the healthcare cloud.

**Collaborative IDS based on cloudlet mesh:**

Numerous earlier studies [28] have examined various intrusion detection systems with significant advancements. For instance, [29] suggested a behavior-rule specification-based intrusion detection approach. The performance outperforms existing anomaly-based algorithms, which is the key contribution. [30] presented a distributed IDS and IPS (intrusion prevention system)-based collaboration paradigm for the cloud environment. This model employs a hybrid detection method to identify and respond to any intrusion types that pose a threat for the system, particularly remote intrusion. However, a novel intrusion detection method that was initially presented by Shi et al. [31] is collaborative IDS based on the cloudlet mesh structure.

The authors showed that the intrusion detection system built on top of a cloudlet mesh had a pretty high detection rate. [32] provides comparison of several CIDS techniques and explains design space, evasion assaults, and attacks on the availability of the CIDSs. Described in [33] is the IDS for privacy cloud. The authors present a summary of cloud computing intrusion detection and a fresh concept for privacy cloud security.

**EXISTING SYSTEM:**

In the existing system, 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 body area network (WBANs). The article in the existing system investigates security and privacy issues in mobile healthcare networks, including the privacy- protection for healthcare data aggregation, the security for data processing and misbehavior.

The system 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. The system gives a systematic literature review of privacy-protection in cloud-assisted healthcare system.

###### **PROPOSED SYSTEM:**

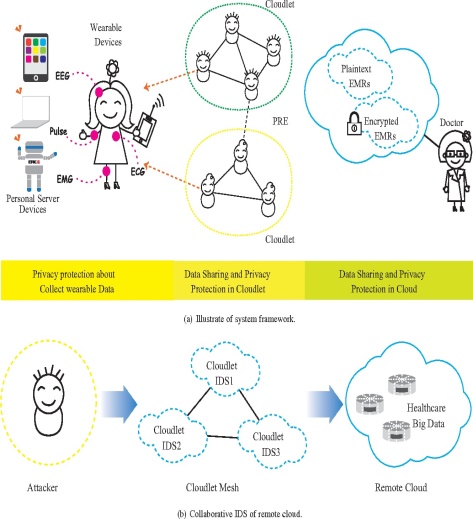
The proposed system, a cloudlet based health care system is presented, where the privacy of users’ physiological data and the efficiency of data transmissions are our main concern. The system uses NTRU for data protection during data transmissions to the cloudlet.

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.

The proposed system divides data in remote cloud into different kinds and utilizes encryption mechanism to protect them respectively.

The Proposed system proposes collaborative IDS based on cloudlet mesh to protect the whole healthcare system against malicious attacks.

**RESULT:**







**CONCLUTION:**

In this study, we looked at the issue of exchanging big medical data and protecting privacy in cloudlets and distant clouds.

In order to collect data securely and at a cheap cost, we designed a system that prevents users from sending information to a distant cloud. It does, however, let users to send data to a cloudlet, which causes the cloudlet's data sharing issue.

First, we may employ wearable technology to gather information from users and to safeguard users' privacy, Second, to determine whether or not users should share data in the cloudlet, we employ a trust model to gauge their level of trust. Thirdly, in order to safeguard the privacy of remote cloud data, we split the data stored there and encrypt the data using a variety of methods to both guarantee data security and boost the effectiveness of transmission. To defend the entire system, we suggest a collaborative IDS based on cloudlet mesh. Simulations and experiments are used to validate the proposed schemes.

**REFERENCE:**

[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. AlMutib, “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. Muhlh ¨ 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. Nunez, 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.

[36] J. Li, J.-J. Yang, Y. Zhao, and B. Liu, “A top-down approach for approximate data anonymisation,” Enterprise Information Systems, vol. 7, no. 3, pp. 272–302, 2013.