Cloudlet Based Medical Data Sharing with Privacy Protection

Anita Harsoor, Revanasidda, PrakashPattan

***Abstract:** This modern society expects sophisticated modern health care services to enhance the healthy living conditions. The world's ageing population and prevalence of chronic diseases has lead to high demand for medical data monitoring. The modern technology is supporting in all the way to realize the sophisticated health services. Specialized doctors are generally very rare and they may be geographically far away from needy patient. Without the support of technology, they cannot provide health services from remote places. In most of the cases, patients are immovable to doctor's place due to their critical health conditions. But, the technology is a coming to help in such situations in a great way. The modern technology is helping in providing health services remotely with same quality as a local doctor can provide. The key concept behind this technology is collecting health data with highest possible accuracy and sharing it with remotely present health specialists. The wearable devices can collect body data most accurately and can send data to cloud for sharing it with remotely present health specialists. But, we know, sharing medical information is very critical and challenging issue because medical information contains patient's important and highly confidential information. On the other hand, medical ethics says that doctors cannot share patient's health records with others without the consent of patient. Such data will be shared between only authentic persons in cloud. The chain of processing mainly includes data collection, data storage, and data sharing. In this work a protected cloudlet based medical data sharing is proposed. In this paper, three major issues pertaining to medical data sharing are addressed. Firstly, a method for secured medical data sharing using cloudlet is proposed. During data collection, Number Theory Research Unit (NTRU) method used to encrypt user's body data collected by wearable devices, then transmitted to nearby cloudlet. Secondly, a new trust model to help users to select trustable partners for sharing stored data in the cloudlet is presented. This model is to help similar patients to communicate with each other. Thirdly, a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh is proposed, which can effectively prevent the remote healthcare big data cloud from attacks. Finally, an analysis of security to the information is presented and the results are quite encouraging.*

***Index Terms:** Index Terms: NTRU, IDS, Cloudlet and Healthcare.*

I. INTRODUCTION

This medical data on the relational association is useful to the two patients and masters, the fragile data might be spilled or stolen, which causes privacy and security issues without powerful protection for the basic data In Cao et al, a MRSE (multi-watchword situated investigate encoded data in distributed computing) privacy confirmation structure was shown, which intends to give customers a multi-catchphrase strategy for the cloud's mixed data [1]. Disregarding the way that this methodology can give come about situating, in which people are interested, the proportion of estimation could be blundering. A need based health data accumulation (PHDA) plot was acquainted with guarantee and complete particular sorts of healthcare date in cloud helped remote body region organize (WBANs). The article inspects security and privacy issues in convenient healthcare frameworks, including the privacy-protection for healthcare data combination, the security for data taking care of and inconvenience making [2]. Depicts a versatile security exhibit especially for data driven applications in distributed computing based circumstance to guarantee data privacy, data trustworthiness and fine grained access control to the application data. It gives an exact composition review of privacy-confirmation in cloud-helped health mind structure.

By making usage of the assorted headways, for instance, wearable contraptions, health mind huge data, distributed computing, etc. the customer can send his health data to the adjoining master and an association can be worked among pro and a patient as showed up in the underneath figure 1. Regardless, the delicate data can be discharged or accepted control by the third individual or the intruder and in this way this causes security issue. By methods for the distributed computing an incredible piece of the data can be held in the mists that join cloudlets and the protected mists.

The genuine inconvenience here is the security and privacy from furious ambushes. Taking idea of above issue, this paper proposes a cloudlet based health mind system (reference K. Hung).

The assembled data from wearable devices are transmitted to the nearby cloudlets from where it is also transmitted to the sheltered mists from where masters will get to the data and examine the sickness.

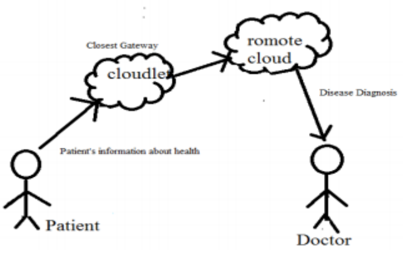


Fig 1: Encrypted data through cloudlet sent to doctor

In Figure 1 the privacy insurance is dispersed into three phase's .In the main stage the data of client's health gathered through wearable gadgets is transmitted to the close-by cloudlets. Transmission of this health data should be secured a ton. Next, the data from the cloudlet is transmitted to the safe cloud where the third stage the data is isolated into various sorts and comparing security is given. With a

Revised Manuscript Received on july 09 , 2019.

Revanasidda, Computer Science and Engineering, PDACE, Kalaburgi, India.

Dr.Anita Harsoor, Computer Science and Engineering, PDACE,Kalaburgi, India..

Dr.PrakashPattan, Computer Science and Engineering, PDACE, Kalaburgi, India.

specific end goal to give the above stages we consider combinative In DS to ensure cloud resound framework.

II. LITERATURE REVIEW

In paper [1] maker build up a novel healthcare structure by utilizing the flexibility of cloudlet. The components of cloudlet include privacy protection, data sharing and interference recognizable proof. In the period of data gathering, directly off the bat utilize Number Theory Research Unit (NTRU) procedure to encode customer as body data accumulated by wearable devices. Those data will be end to close-by cloudlet in an imperativeness gainful structure. Additionally, show another trust model to assist customers with choosing trustable associates who need to share set away data in the cloudlet. The trust show in like manner makes unclear patients talk with one another about their diseases. Thirdly, parcel customer's medical data set away in remote haze of specialist's office into three areas, and give them proper protection. Finally, remembering the ultimate objective to shield the healthcare structure from harmful strikes, layout a novel helpful intrusion ID system (IDS) strategy depend upon cloudlet work, which can reasonably keep the remote healthcare gigantic data cloud from attacks.

In this paper [2], out of nowhere, portray and light up the testing issue of privacy saving multi-catchphrase positioned seek over encoded cloud data (MRSE). They set up a game plan of severe privacy essentials for such a sheltered cloud data use system. Among various multi-watchword semantics, they pick the capable closeness proportion of "encourage organizing", i.e., whatever number matches as would be reasonable, to get the significance of data reports to the inquiry question. They moreover use "inside thing likeness" to quantitatively survey such equivalence measure. To begin with propose a major idea for the MRSE in light of secure inside thing estimation, and thereafter give two basically upgraded MRSE plans to achieve distinctive stringent privacy necessities in two different peril models. Escalated examination of surveying privacy and profitability affirmations of proposed plans is given.

In this paper [3], maker developed a safe and privacy-saving spearheading processing framework, called SPOC, for m-Healthcare emergency. With SPOC, propelled cell resources including figuring power and essentialness can be innovatively accumulated to process the registering genuine individual health data (PHI) in the midst of m-Healthcare emergency with unimportant privacy disclosure. Specifically, to utilize the PHI privacy disclosure and the high trustworthiness of PHI procedure and transmission in mHealthcare emergency, They present a capable customer driven privacy get to control in SPOC structure, which is depend upon a characteristic based access control and another privacy protecting scalar thing estimation (PPSPC) framework, and stipends a medical customer to pick who can share in the cunning processing to help with setting up his staggering PHI data. Separated security ponder demonstrate that the proposed SPOC framework can profitably achieve customer driven privacy get to control in mHealthcare emergency.

This paper [4] first introduces the guideline purpose of this unprecedented issue and gives a short principle. By then, the present condition of the apportionment of EMRs is inspected. Starting there forward, the creating data progresses are presented which extraordinarily influence the healthcare course of action. These join health identifying for medical data gathering, medical data study and utilization for exact recognizable proof and desire. Next, distributed computing is discussed, as it may offer versatile and monetarily keen transport of healthcare administrations.

III. PROPOSED WORKS

Regardless of the improvement of numerous stages for sharing the data's by means of cloud, cloudlets and so on, and these innovations are utilized much in health mind data sharing since it requires bunches of privacy and security.

A. Combinative indsNetwork:

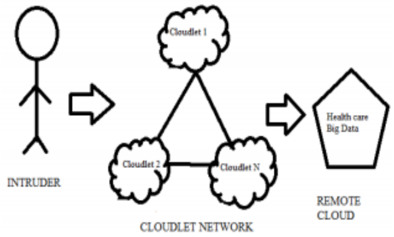


Fig 2: Combinative InDS of the secure cloud.

When an attack by an intruder is detected, an alarm is fired. The finding rate of a Combinative InDS is better than a single InDS which ensures the security.

B. Inter-network communication

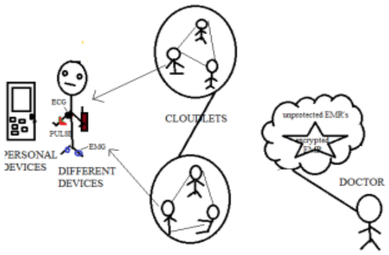


Fig 3: Inter-NetworkCommunication

Framework of the healthcare system is shown in the above figure. The user’s data that is collected is delivered to the nearby cloudlet. During this transmission we suffer from two problems:

1. Privacy Protection.
2. To develop counter measures to prevent data from being stolen from outsiders. Privacy Protection of health care can be encrypted and shared as follows:

a. Client data encryption.
b. Cloudlet based data sharing.
c. Secure cloud privacy protection.
d.CombinativeInDS based on cloudlet mesh.

C. Sharing of Data and Security

Here, we depict the issues that happen amid transmission of the substance from customer to the specialist. We can give every client distinctive Authority to access the data where the client can just access the data inside his/her level and can't go past the access rights.

We can give an application to utilize the private data that is helpful to both customer and in addition specialists, by making utilization of the healthcare huge data.

Enormous data is available in some protected cloud, in light of the subtle elements gave by the client; a sickness expectation display is setup which depends on the idea of choice tree that is utilized to reason the infection the client is experiencing and in light of which specialist propose the right prescription. The expectations acquired are sent to both customer and Doctor. Encryption at Client Edge And sharing Information on Network.

The data's which are acquired from the different detecting gadgets that are connected to persistent are sent to the closest cloudlet guaranteeing its security. For example, the normal heart beat rate that is gathered by means of the gadgets is passed on to the cloudlet in a secured way, keeping in mind the end goal to build up the collaboration between customers. The paper [7] proposed data sharing procedure among a few clouds, contingent upon the trait, the security strategy is utilized. It doesn't think about clients' social exercises.

In [5], Fabian et al., Based on the discourse, amid data sharing we give judgment that is as per the following.

We set clinic for put stock in specialist (TA).Let us consider a case, Since Abhi needs to impart the data to Akash, so he solicits TA to check the data's from Akash. At that point the TA work is partitioned into the accompanying two phases:

1. We need to check for the data which is comparable amongst Abhi and Akash this should be possible utilizing the data exhibit in the TA. For instance ECG's of two customers. Familiarities can be of three phases low, medium and high.

2. Examine the put stock in level amongst Abhi and Akash. We ought to likewise consider the generosity of the customers that comprises of awful, normal and great. We need to consider familiarities got in the past advance as an information data.

The data in the protected cloud is gotten from patients who are dealt with in doctor's facility. The data of treatment and bills of patients are kept up as records, and spared in cloud that can limit cost and accommodating to Doctors to give treatment and research on the infections. The secured condition is made which guarantee that the medical data sharing should be possible with no interference. We must be watchful will sharing such private data of customers.

As indicated by [7] [6], we can isolate EMR table into the accompanying three composes:

(1)UID: The properties which can recognize the user's personal information. E.g.name, contact number,mail id, home address and so on.

(2)PID: The property which enables us to identify the user's in the cloudlet. E.g., zip code, DOB and gender.

(3)The medical details of the patients are shared in a secured manner so that the doctor and the patients suffering from similar disease can access the information provided UID and PID are encrypted.

D. Combination of Interruption

Detection Interruption detection system is used to protect medical data. On the off chance that there is any suspicious assault, the framework consequently cautions by an alert. It helps in simple assurance of the interrupters .Next advance is to decide the identification standard in combinative InDS. We can take care of that cloudlet system can be actualized with the assessed taken a toll .The quantity of InDS to be to be available in the system is controlled by discretion structure. The primary point is to accomplish a higher location rate of the phony alert likewise guaranteeing that it is taken a toll limiting framework.

E. Combinative inds

In Combinative InDS let us consider n InDS I1, I2………, in which enhance detection level and reduce the fake alarm. Before moving the data to a secured cloud we have to perform combinative interruption detection on cloudlet network in order to complete the task of interruption detection where each of InDS can determine interruption of individually.

IV. ALGORITHMS

In this paper proposes a cloudlet based human services system. The body data assembled by wearable gadget is transmitted to for the proposed system, we have used two algorithms, first is Number Theory Research Unit algorithm which is used to encrypt the user's body information for privacy protection and second is MKE system algorithm for the provision of trustworthy answers to the patients.

Algorithm 1: Number Theory Research Unit

Input: u, v, Message (m).

Output: encrypted and decrypted message.

Step 1: Two small polynomial u and v.
Step 2:The large modulo j and modulo k.
Step 3: The inverse of u modulo k and the inverse of u modulo j.
Step 4: u * uk = 1 (mod k) and u * uj= 1 (mod j)
Step 5: Creating uj = u-1 (mod j) and uk = u-1 (mod k).
Step 6: Using j, uk and v, calculate the private key pair and the public key h.
Step 7: h = juk * v (mod k).
Step 8: Encrypted message e is created using m, r and h as follows: e = r * h + m (mod k).
Step 9: The private key u is used to calculate: x = u * e (mod k).
Step 10: z = uj * y (mod j)

The polynomial z will be equal to the original message, if decryption procedure has been successfully finished.

NTRU Key generation:

The private and public key pair is created using the NTRU key generation scheme. The key generation method starts by selecting two small polynomials u and v, where small is well-defined as having coefficients smaller than the large modulo j and modulo k. The user must calculate the inverse of u modulo k and the inverse of u modulo j such that u * uk = 1 (mod k) and u * uj = 1 (mod j). The inverse of u is calculated both modulo j and modulo k, creating uj = u-1 (mod j) and uk = u-1 (mod k). The values of u and uj are taken as the private key pair and the public key h is calculated. The public key is calculated as follows:

h = juk * v (mod k)…………… (1)

NTRU Encryption:

The encryption procedure begins by creating a polynomial message m whose coefficients lie in an interval of length k. A small polynomial, r, is then created and used to obscure the message The final encryption uses m, r and the public key h to create encrypted message e as follows:

e = r * h + m (mod k)………… (2)

NTRU Decryption:

The decryption procedure uses the private key u to calculate:

x = u * e (mod

k)…………………… (3)

The coefficients of x must be selected in appropriate interval of length k to guarantee the highest probability that the decryption procedure will be successful. Once the coefficients of x are selected on the appropriate interval, x is reduced modulo j and the second private key is used to calculate:

$y = x \pmod{j}$…………………. (4)

$z = uj * y \pmod{j}$……………… (5)

The polynomial z will be equal to the original message, if decryption procedure has been successfully finished.

V. RESULTS AND PERFORMANCE ANALYSIS

A. Simulation study

To start with we portray the exchange proportion to contrast client data encryption technique and encryption strategy for secure cloud we demonstrate the connection between InDSids, sum spent and level of discovery.

B. Enforcement level of data encryption

Keeping in mind the end goal to secure the data about the client, we make utilization of encryption algorithm for the data encryption. We additionally need to quantify the viability of the algorithm .We draw chart by considering the variety in exchange proportion of client data encryption technique with encryption strategy for secure cloud with expanding interims. As indicated by the diagram it would seem that both the bends give a decent exchange proportion yet encoded data sent by the safe cloud appears to have great authorization than scrambled data sent by the client.

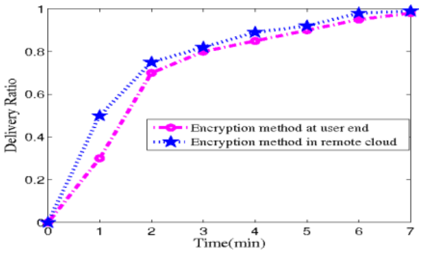
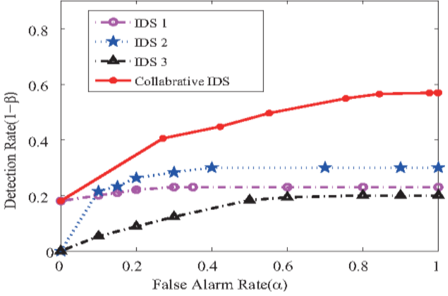


Fig 4: Compare the transfer ratio of the encryption method of secure cloud and client end.

We have to first determine the trust level before sharing the information on the cloudlet for this purpose it is necessary to know the good-will of the user on the network which can be ranged between [0,1] has specified.

If the good wiliness of clients seems to be low, a likeness of the user is poor. The resulting model is not so trustworthy. In these conditions the users hesitate to share the data on such model as it is not safe. As there is increase in good-will and alikeness the model becomes more trusted and encourages sharing their data on the network.



.

Fig 5: Comparison between detection rate of a single INDS and combinative INDS.

VI. CONCLUSION

In this endeavor, we examined the issue of privacy security and sharing broad medical data in cloudlets and the remote cloud. We developed a system which does not empower customers to transmit data to the remote cloud with respect to verify accumulation of data, and also low correspondence cost. In any case, it enables customers to send data to a cloudlet, which triggers the data sharing issue in the cloudlet. Directly off the bat, we can utilize wearable contraptions to assemble customers' data, and with a particular true objective to guarantee customers privacy, we use NTRU segment to guarantee the transmission of customers' data to cloudlet in security. Likewise, to share data in the cloudlet, we use trust model to measure customers' taken confidence in level to pass judgment on whether to share data or not. Thirdly, for privacy-protecting of remote cloud data, we section the data set away in the remote cloud and encode the data in different courses, to ensure data security just as animate the ampleness of transmission. Finally, we propose network situated IDS in light of cloudlet work to guarantee the whole structure. Customer makes the request to the master on the web and authorities give the reaction to customer.

REFERENCES

1. 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.
2. 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.
3. 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.
4. 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.
5. Y. Wu, M. Su, W. Zheng, K. Hwang, and A. Y. Zomaya, “Associative big data sharing in community clouds: The meepo approach,” IEEE Cloud Computing, vol. 2, no. 6, pp. 64–73, 2015.
6. 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.
7. 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).
8. 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.
9. 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).
10. 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).
11. Vasilomanolakis, E., Karuppayah, S., Mühlhäuser, M., & Fischer, M. "Taxonomy and Survey of Collaborative Intrusion Detection". ACM Computing Surveys, 47(4), pp.1–33. (2015).

AUTHORS PROFILE

thor-1 Photo

Revanasiddais currently pursuing M.tech in computer Network Engineering from Dept of CSE at PDACE Kalaburagi

Dr. Anita Harsoor M.Tech, Ph.D, Associate Professor, Computer Science and Engineering Department have teaching experience of 10 years. Areas of research are Digital Image Processing, Computer Vision, Cloud Computing and pattern Recognition. More than 25 technical papers in national and international Journals and in proceedings of international conference proceedings. One of the publication has been printed as book chapter in SPRINGER Journal.

Dr. Prakash PattanM.Tech, Ph.D
System Manager (Prof), Computer Science and Engineering Department. His area of research is Digital Image Processing and Computer Vision, Computer Networks, IoT, Big Data Analysis etc. He has published more than 35 technical papers in national and international journals and proceedings of international conferences. Two of his papers are included in the book entitled, “Measuring Shape” authored by Neil Brent and Dr. John C. Russ (CRC Publication).