EFFICIENT MANAGEMENT OF SECURITY AND PRIVACY AND INTRUSION DETECTION SYSTEM FOR CLOUDLET-BASED HEALTHCARE SECTOR

A.Chaitanya Sravanthi, Assoc. Prof., Department of MCA, QIS College of Engineering and Technology, Ongole,
K.Chinna Vengamma, Final Year Student of Master of Computer Applications, QIS College of Engineering and Technology, Ongole

Abstract-- With the prominence of wearable gadgets, alongside the improvement of clouds and cloudlet innovation, there has been an expanding need to give better medical consideration. The handling chain of medical data for the most part incorporates data gathering, data stockpiling, and data sharing, and so on. Conventional healthcare system regularly requires the conveyance of medical data to the cloud, which includes clients' delicate data and causes correspondence vitality utilization. Essentially, medical data sharing is a basic and testing issue. Along these lines in this paper, we develop a novel healthcare system by using the adaptability of cloudlet. The elements of cloudlet incorporate privacy protection, data sharing, and intrusion detection. In the phase of data gathering, we initially use the Number Theory Research Unit (NTRU) strategy to scramble client's body data gathered by wearable gadgets. Those data will be transmitted to close-by cloudlet in a vitality productive manner. Furthermore, we present another trust model to assist clients with selecting trustable accomplices who need to share put away data in the cloudlet. The trust display additionally causes comparative patients to speak with one another about their ailments. Thirdly, we partition clients' medical data put away in the remote cloud of an emergency clinic into three sections and give them legitimate protection. At last, so as to shield the healthcare system from malevolent assaults, we build up a novel collaborative intrusion detection system (IDS) technique dependent on cloudlet work, which can successfully keep the remote healthcare enormous data cloud from assaults. Our analyses show the viability of the proposed plan.

Index Terms-- privacy protection, data sharing, a collaborative intrusion detection system (IDS), healthcare.

I. INTRODUCTION

This with the advancement of healthcare enormous data and wearable innovation [1], just as cloud computing and correspondence advances [2], cloud-helped healthcare huge data computing winds up basic to fulfill clients' consistently developing needs on wellbeing discussion [3]– [4]. Be that as it may, it is a testing issue to customize explicit healthcare data for different clients in a helpful style [5]. Past work recommended the mix of interpersonal organizations and healthcare administration to encourage [6] the hint of the sickness treatment process for the recovery of constant ailment data [7]. Healthcare social stage, for example, Patients Like Me [8],[9] can get data from other comparable patients through data sharing as far as client's own discoveries. In spite of the fact that sharing medical data on the informal organization is advantageous to the two patients and specialists, the delicate data may be spilled or stolen, which causes privacy and security issues [10] [11] without proficient protection for the mutual data [12]. In this manner, how to offset privacy protection with the accommodation of medical data sharing turns into a testing issue.

With the advances in cloud computing, a lot of data can be put away in different clouds [13], including cloudlets [14] and remote clouds [15], encouraging data sharing and escalated calculations [16] [17]. Notwithstanding, cloud-based data sharing involves the accompanying crucial issues:

• How to ensure the security of the client's body data amid its conveyance to a cloudlet?

• How to ensure the data sharing in cloudlet won't cause a privacy issue?

• As can be anticipated, with the multiplication of electronic medical records (EMR) and cloud-helped applications, increasingly more consideration ought to be paid to the security issues in regards to a remote cloud containing human services enormous data. How to verify the healthcare huge data put away in a remote cloud?

• How to viably shield the entire system from malevolent attacks?

As far as the above issues, this paper proposes a cloudlet based healthcare system. The body data gathered by wearable gadgets are transmitted to the adjacent cloudlet. Those data are additionally conveyed to the remote cloud where specialists can access for sickness finding. As per data conveyance chain, we separate the privacy protection into three phases. In the primary stage, the client's crucial signs gathered by wearable gadgets are conveyed to a storage room portal of cloudlet. Amid this stage, data privacy is the principle concern. In the second stage, the client's data will be additionally conveyed toward a remote cloud through cloudlets. A cloudlet is shaped by a specific number of cell phones whose proprietors may require or potentially share some particular data substance. In this way, both privacy protection and data sharing are considered in this stage. Particularly, we utilize a trust model to assess the trust level between clients to decide sharing data

or not. Considering the clients' medical data are put away in a remote cloud, we characterize these medical data into various types and take the comparing security approach. Notwithstanding the over three phases dependent on data privacy protection, we likewise consider collaborative IDS dependent on cloudlet work to ensure the cloud ecosystem. In outline, the fundamental commitments of this paper include:

• A cloudlet based healthcare system is introduced, where the privacy of clients' physiological data and the proficiency of data transmissions are our primary concern. We use NTRU for data protection amid data transmissions to the cloudlet.

• In request to share data in the cloudlet, we utilize clients' likeness and notoriety to develop a trust demonstrate. In view of the deliberate clients' trust level, the system decides if data sharing is performed.

• We separate data in a remote cloud into various types and use encryption system to ensure them individually.

• We propose collaborative IDS dependent on cloudlet work to secure the entire healthcare system against malevolent attacks.

II. Related Work

Our work is firmly identified with cloud-based privacy protecting and cloudlet work based collaborative IDS. We will give a concise survey of the works in these angles.

2.1 Cloud-based Privacy Preservation

In spite of the improvement of cloud innovation and the rise of increasingly more cloud data sharing stages, the clouds have not been broadly used for healthcare data sharing because of privacy concerns [18]. There exist different deals with customary privacy protection of healthcare data [11], [19]–[25]. In Lu et al. [19], a system called SPOC, which represents the safe and privacy-safeguarding astute computing structure, was proposed to treat the capacity issue of healthcare data in a cloud domain and tended to the issue of security and privacy protection under such a situation. The article [21] proposed a compound goals which applies various consolidated innovations for the privacy protection of healthcare data sharing in the cloud condition. In Cao et al. [11], a MRSE (multi-watchword positioned look over encoded data in cloud computing) privacy protection system was exhibited, which means to furnish clients with a multi-catchphrase technique for the cloud's scrambled data. In spite of the fact that this strategy can give result positioning, in which individuals are intrigued, the measure of estimation could be bulky. In Zhang et al. [24], a need based wellbeing data accumulation (PHDA) conspire was displayed to secure and total distinctive sorts of healthcare data in cloud helped remote body region organize (WBANs). The article [25] researches security and privacy issues in versatile healthcare systems, including the privacy-protection for healthcare data total, the security for data handling and bad conduct. [26] depicts an adaptable security demonstrate particularly for data-driven applications in cloud computing based situation to ensure data secrecy, data respectability and fine-grained get to control to the application data. [27] give a systematic writing audit of privacy-protection in the cloud-helped healthcare system.

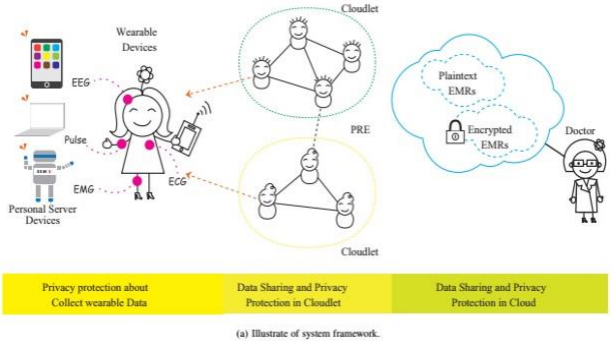
2.2 Collaborative IDS dependent on cloudlet work

Various earlier works [28] have examined diverse intrusion detection systems with very a few advances. For instance, [29] proposed a conduct rule particular based system for intrusion detection. The primary commitment is the execution outflanks different strategies for peculiarity based procedures. [30] proposed a collaborative model for the cloud condition dependent on dispersed IDS and IPS (intrusion avoidance system). This model makes utilization of a half and half detection procedure to identify and take relating measures for any sorts of intrusion which hurt the system, particularly disseminated intrusion. Notwithstanding, collaborative IDS dependent on the cloudlet work structure is another sort of intrusion detection strategy, which was first proposed in Shi et al. [31]. The creators exhibited that the detection rate of the intrusion detection system built up based on a cloudlet work is moderately high. [32] depicts configuration space, attacks that sidestep CIDSs and attacks on the accessibility of the CIDSs, and presents a correlation of explicit CIDS approaches. [33] depicts the IDS for a private cloud. The creators give a diagram of intrusion detection of cloud computing and give another plan to privacy cloud protection.

III. METHODOLOGY

System Framework

This structure of the proposed cloudlet-based healthcare system is appeared in Fig. 1. The customer's physiological data are first gathered by wearable gadgets, for example, brilliant apparel [34]. At that point, those data are conveyed to cloudlet. The accompanying two imperative issues for healthcare data protection is considered. The primary issue is healthcare data privacy protection and sharing data, as appeared in Fig. 1(a). The second issue is to create successful countermeasures to keep the healthcare database from being barged in from outside, which is appeared in Fig. 1(b).



(a) Illustrate of system framework.

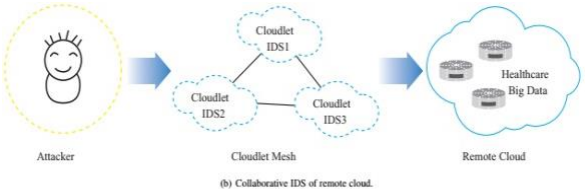


Fig. 1. Illustration of the system architecture: (a) Privacy protection; (b) Collaborative IDS

We address the primary issue on healthcare data encryption and sharing as pursues.

• Client data encryption. We use the model presentedin [23], and exploit NTRU [35] to shield them customer's physiological data from being spilled or mishandled.

This plan is to secure the client's privacy when transmitting the data from the cell phone to the cloudlet.

• Cloudlet based data sharing. Regularly, clients topographically near one another interface with the equivalent cloudlet. It's presumable for them to share normal perspectives, for instance, patients experience the ill effects of comparative sort of infection trade data of treatment and offer related data. For this reason, we utilize clients' closeness and notoriety as info data. After we acquire clients' trust levels, a specific limit is set for the correlation. When coming to or surpassing the edge, it is viewed as that the trust between the clients is sufficient for data sharing. Something else, the data won't be imparted to a low trust level.

• Remote cloud data privacy protection. Contrasted with the client's every day data in cloudlet, the data put away in remote contain bigger scale medical data, e.g., EMR, which will be put away as long as possible. We utilize the strategies presented in [36] [21] to separate EMR into an unequivocal identifier (EID), semi identifier (QID) and medical data (MI), which will be talked about in 4.3. In the wake of ordering, appropriate protection is given for the data containing clients' delicate data.

• Collaborative IDS dependent on cloudlet work. There is a tremendous volume of medical data put away in the remote cloud,it is basic to apply a security component to ensure the database from vindictive intrusions. In this paper, we create explicit countermeasures to set up a resistance system for the expansive medical database in the remote cloud stockpiling. In particular, collaborative IDS dependent on the cloudlet work structure is utilized to screen any visit to the database as a protection fringe. On the off chance that the detection appears vindictive intrusion ahead of time, the collaborative IDS will fire an alert and square the visit, and the other way around. The collaborative IDS, as a gatekeeper of the cloud database, can secure countless data and ensure the security of the database.

IV. PROPOSITION METHODOLOGY

4.1 CONTENT SHARING AND PRIVACY PROTECTION

In this area, we address the issue of protection and data sharing. To start with, we present the encryption procedure for clients' privacy data, which keeps the spillage or pernicious utilization of clients' private data amid transmissions. Next, we present the personality the board of clients who need to get to the emergency clinic's healthcare data. In this way, we can dole out various clients with various dimensions of authorizations for data get to, while maintaining a strategic distance from data access past their consent levels. At long last, we give an utilization of utilizing clients' private data, which is valuable to the two clients and specialists. In view of the healthcare enormous data put away in the remote cloud, a sickness expectation demonstrate is fabricated dependent on a choice tree. The expectations will be accounted for to the clients and specialists on interest.

When utilizing wearable gadgets to gather clients' data, the method definitely includes the client's delicate data. In this way, how to successfully gather and transmit clients' data under effective privacy protection is a basic issue [19]. In [24] a data accumulation technique, called PHDA, is proposed dependent on data need which can give legitimate expense and deferral to various needs data. In [37], Li et al. examine the procedure of data accumulation and uses entirety total to acquire data to ensure the security of clients' privacy within the sight of questionable sensors. In [38], Lu et al., think about 3V data privacy protection issue dependent on huge data of healthcare. In view of the model introduced in [23], this paper uses the benefits of the NTRU encryption plot [35]. NTRU can ensure the client's physiological data, for example, pulse, circulatory strain and Electrocardiography (ECG), and so on. Before transmitted to a cell phone, NTRU encryption plot executed. The encoded data will at that point be put away in the cloudlet through a cell system or Wi-Fi, as appeared in Fig. 2.

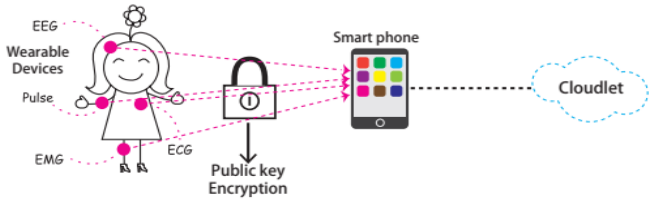


Fig. 2. Collection of encrypted data in the cloudlet

More often than not, the data gathered by brilliant attire are largely unsigned number vectors. For instance, for pulse data, the normal heart pulsates recognized every moment is meant by hr and the plain data will be [hr, 0, •, 0]. We have to characterize clear space and figure space for the encryption. As the meaning of the polynomial ring is R: = Z[x]/(xn + 1), on account of a discretionary positive number q, the meaning of the remainder ring is known as Rq = R/qR. We characterize the unmistakable space as Rp with the goal that the length is n and the whole number vector is modulus p, which is dependably among 2 and figure space is Rq, so the length is n and the number vector is modulus p. In light of transmission capacity, we by and large make the Rq pass utilizing the Chinese Remainder Transform (CRT) portrayal. For starting

security, we have n = 1024 and q = 32. We thus portray the procedures of encryption and translating in the accompanying.

KeyGen()→ (pk, sk): let f ∈ R, g ∈ R, while f, g pursues the discrete Gaussian conveyance, f = 1 mod q, and f is reversible. Along these lines, the mystery key is indicated by sk = f; the open key is signified by pk = h = g • f-1 mod q.

• Enc(pk = h, μ ∈ Rp)→ c ∈ Rq: let r ∈ R, m ∈

R, m = μ mod p. Both m′ and r pursue the discrete

Gaussian dissemination and we have m = p • m′ + μ, c =p • r • h + m mod q.

• Dec(sk = f, c ∈ Rq) → μ: ascertain ¯b = f • c mod q, and make it a whole number polynomial b, with variables inside

[-q/2, q/2). Accordingly, we have μ = b mod p.

The scrambled data will be transmitted to the cell phone with the homomorphism handling. We accept that the unmistakable data of heartbeat is [hr, 0, ..., 0] and the exhibit encryption is c1. In the same way, on the off chance that the circulatory strain is bp, at that point the reasonable data is signified as [0, bp, 0, ..., 0] and the enciphered data will be c2. Along these lines, we can get clear data and figure data all things considered. Since we utilize an open key encryption system and homomorphism encryption (HE), the cell phone can get data {c1, c2, . . . , cn} transmitted to c agg = c1 + ... + cn mod q. In this manner, after we process the data with homomorphism encryption, the transfer speed is decreased adequately before the data are transferred to the cloudlet, along these lines accomplishing vitality and transmission capacity reserve funds.

a) Medical Data Sharing in the Cloudlet

The motivation behind medical data sharing is to improve use of data between clients. The paper [39] proposed data sharing strategy among a few clouds, which utilized an encryption method based on a credit to acknowledge data sharing under a semi-confided in cloud condition. In any case, it didn't consider clients' social activities. In [40], Fabian et al., propose huge data sharing technique dependent on network cloud, yet it didn't go for medical data particularly. Based on the exchange above, we give the judgment amid data sharing as pursues.

We set the emergency clinic for confided in power (TA). Expect the client p solicits TA to check the data from client q, i.e., client p needs to impart data to client q. At that point the TA work is partitioned into the accompanying two stages:

Stage 1: Compare the comparability of client p and client q. For precedent, we can use the model comparative as [41] and utilize clients' data put away in TA, for example, EMR, to quantify the closeness of client p and client q. Likeness can be separated into three dimensions, in particular Low, moderate and high

Stage 2: Describe the trust level between client p and client q. We utilize the notoriety of client p which incorporates terrible, normal and great, and the comparability of client p and client q which got through step1, as info data. We can use a trust model to acquire a trust level as pursues.

• Determine the info and yield. The info comprises of notoriety and comparability and yield comprises of the relating trust level. So as to speak to these factors, we evaluate every one of them as a scalar somewhere in the range of 0 and 1. Select a Gaussian capacity as the relating capacity, which will outline an incentive in the gathering into a trust level
• Formulate the applicable rules and have the specialists set up the trust-related rules with the related information also, experience.

• Build a model that can decide the noteworthiness as per the character, credit, and likeness.

In the wake of acquiring clients' trust level, we can pass judgment on whether to believe client p dependent on the limit esteem set by client q. On the off chance that the trust level is equivalent to or more prominent than the edge esteem, at that point the client p can be trusted, so TA will share client q data to client p. In the event that the trust level is not exactly the edge esteem, at that point the client p can't be trusted, so TA will decline the demand of the client p.

b) Medical Data Privacy Protection in the Cloud

Data in a remote cloud are produced from the patients treated in the emergency clinic. As the records of determination and installments will be kept in numerous individual documents having a place with countless, sparing such data in the cloud can diminish costs and be helpful for specialists to analyze and examine ailments. In this way, we will make a protected situation to guarantee that medical data sharing happens without danger of spillage. Subsequently, we will focus on the protection of privacy in such data sharing.

As per [36] [21], we can isolate the EMR table into the accompanying three sorts: (I) EID: the properties which can recognize the client evidently, e.g., name, telephone number, email, place of residence, etc; (ii) QID: the property which can distinguish the client roughly, e.g., a client might be distinguished by qualities, for example, postal division, date of birth, and sexual orientation [42]; (iii) MI, or some clinical appearance and sickness types. So as to ensure the privacy of data and make it helpful for specialists or different patients with a comparable illness to get to the data, we will encode EID and QID yet share MI. Allude to the method for articulation in [21], we part the EMR data table An into two autonomous tables, i.e., a ciphertext table Te and a plaintext table Tp. The ciphertext table contains primarily auxiliary data including the encryption table of EID and QID property; while the plaintext table contains mostly basic and semi-basic data including a reasonable content table of MI property.

We have to ensure the mutual data and some physiological lists gathered by checking the particular illnesses. Assume

there are M kinds of ailments, set apart as {D1, D2, . . . , DM }. For every malady Di, there are relating qualities {Ci;1, Ci;2, . . . Ci;in }, I = 1, . . . , M. So as to quantize dis-ease attributes, we characterize an inquiry Qi;j for each characteristic Ci;j , I = 1, . . . , M, j = 1, . . . , in. For instance, coronary illness displays attributes of dyspnea, palpitation, pectoralgia, and so on. For the normal for palpitation, we can structure the inquiry, for example, "Do you have palpitation?". In the event that the inquiry result is '1', at that point it implies indeed, else, it implies no with the sign of '0'. In other words, there are comparing test questions {Qi;1, Qi;2, . . . , Qi;in } for every trademark in {Ci;1, Ci;2, . . . Ci; in } of the relating maladies Di, = 1, 2, . . . , M. For straightforwardness, we accept that the response to each question is 0 or 1. Along these lines, every infection Di can gain its testing results {ei;1, ei;2, . . . , ei;in }, I = 1, . . . , M, with each ei;j = 0 or ei;j = 1.

The underlying privacy data of clients are obtained by finishing a review. So as to be advantageous for encryption, we receive the strategies as examined above to change over these attributes into numerical data, in particular the blend of 0's and 1's. We choose triple {a, b, c} fulfilling |a2 | < |b| < |c| . At that point we pick three irregular numbers {pi, qi, wi} fulfilling the accompanying conditions.

$$p_i + q_i = bw_i, \quad \frac{bw_i}{2} < q_i < bw_i, \quad a^2 buw_i < c, \qquad (1)$$

where *u* is an integer.

After the parameters of *a*, p_i, q_i is obtained, encrypted data can be calculated. Then we have

$$v_i = ae_i + p_i, \quad v_i' = s \cdot q_i \bmod c, \quad v_0' = s \cdot q_0 \bmod c. \quad (2)$$

, ,

$v_i = ae_i + p_i$, $v_i = s \cdot q_i \bmod c$, $v_0 = s \cdot q_0 \bmod c$. (2)

In this way, we get (a, c, v, v′) as the encoded data, which is difficult to be unscrambled without the mystery keys (as a result of the obscure estimation of α. Consequently, the encryption procedure of clients' private data is finished.

4.2 COLLABORATIVE INTRUSION DETECTION

So as to ensure medical data, we additionally build up an intrusion detection system in this paper. When a malevolent assault is identified, the system will fire an alert. This area introduces a novel plan to assemble a collaborative IDS system to hinder interlopers. In the accompanying, we initially think about what occurs if the system is experiencing distinctive attacks, while detection rates for individual IDS differ with the cloudlet servers. We will plot the detection rate and false alert rate as the beneficiary working trademark (ROC) bends.

Next, we assess the collaborative detection rate and gauge the normal expense of execution in the cloudlet work. We apply a choice tree to pick the ideal number of IDS to be sent on the work. The objective is to accomplish an endorsed detection exactness against the bogus alert rate under the reason of limiting the system cost.

(a) Collaborative IDS

In this segment, collaborative IDS is planned among m IDS, e.t., S1, S2, •, Sm, so as to get a higher detection rate and lower false caution rate. The m IDS are expected to distinguish freely. There exist K distinctive kinds of intrusion. So as indicated by derive in the accompanying, we can get the detection rate and false alert rate of collaborative IDS. So as to assess it, we give the ROC bend.

Prior to transmitting data to the remote cloud, we set up the collaborative IDS dependent on the cloudlet work to finish the intrusion detection errand. We use {S1, S2, . . . , Sm} to speak to the arrangement of IDS in the collaborative IDS (CIDS) system. Assume that every id can distinguish intrusion freely. For straightforwardness, we use I to show that there is intrusion conduct in this system and NI to demonstrate that there is no intrusion. Besides, An implies that IDS raises an alert while NA implies no caution. We use 1-β to show the detection rate and α as the bogus caution rate. In the event that there exist K diverse kinds of intrusion, indicated as I1, I2, . . . , IK, at that point we have I = I1∪I2 • •∪IK. Expect that the likelihood of Ij is pj, j = 1, 2, . . . , K. Consequently, the likelihood of intrusion conduct in this system is p(I) = ∑K i=1 pi, while the likelihood of no intrusion conduct is P (NI) = 1 - p(I). We in this way have p(A|I) = 1 - β and p(A|NI) = α.

(b) Evaluation of collaborative IDS

We next think about the cost issue of collaborative IDS, with its expense being isolated into three sections:

- when the intrusion conduct isn't identified by the system, yet IDS creates a caution, the system will keep the transmission of this current client's data, which will influence the typical utilization of the healthcare system by the client, and may prompt an abatement of the system's unwavering quality. The expense right now is signified as C ;

- when the system experiences intrusion Ii, 1 ≤i≤ K, yet the IDS does not create an alert, the system will permit this nosy conduct, which will break the healthcare enormous data; the healthcare data in the remote cloud is assaulted and may most likely reason spillage of patients' data. The expense of this situation is indicated as Ci, 1 ≤ I ≤ K;

- the cost in different situations is set apart as 0 .

IV. RESULT ANAYSIS

The system is built using Java framework on Windows platform. The Net beans IDE are used as a development tool. The system doesn't require any specific hardware to run; any standard machine is capable of running the application.

Expected Result

Table I. Time Efficiency Comparison

	Without KDC	With KDC
Time in ms	1200	800

Table I describes the time required in ms with KDC and without KDC. With KDC consume less time for key distribution than the without KDC.
Figure 2 represent the graphical comparison of time efficiency of with KDC and without KDC respectively. X axis represent the methods and y axis represent the time required in ms.

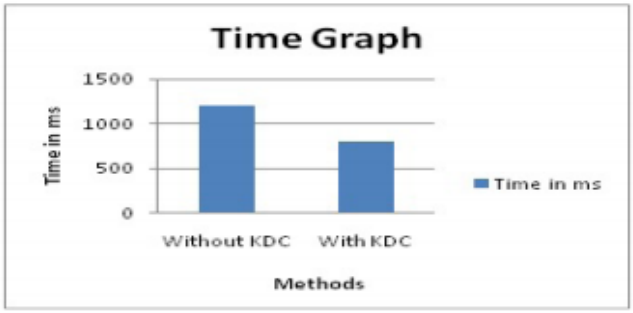


Figure 2: Time Graph

Figure 2: Time Graph

Table II. Memory Comparison

	Without KDC	With KDC
Memory in kb	1400	900

Table II describes the memory required in bytes for with KDC and without KDC methods. With KDC consume less memory to store the keys than the without KDC and improve the classification result.

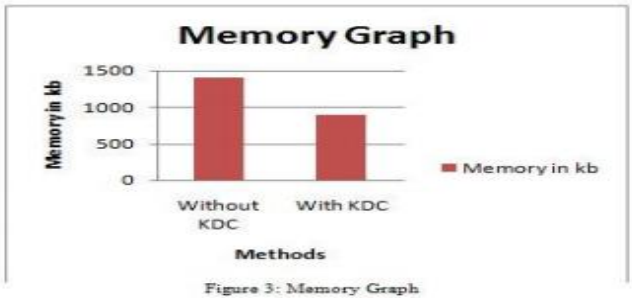


Figure 3: Memory Graph

Figure 3 represent the graphical comparison of memory consumption in with KDC and without KDC respectively. X axis represent the methods and y axis represent the memory consumed in bytes. Without KDC requires 1400 kb memory and With KDC requires 900 kb memory for classification.

V. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we explored the issue of privacy protection and sharing extensive medical data in cloudlets and the remote cloud. We built up a system which does not enable clients to transmit data to the remote cloud in light of secure gathering of data, just as low correspondence cost. Be that as it may, it allows clients to transmit data to a cloudlet, which triggers the data sharing issue in the cloudlet.

Initially, we can use wearable gadgets to gather clients' data, and so as to ensure clients privacy, we utilize a NTRU system to ensure the transmission of clients' data to cloudlet frailty.

Furthermore, to share data in the cloudlet, we utilize a trust model to quantify clients' trust level to pass judgment on whether to share data or not. Thirdly, for privacy-safeguarding of remote cloud data, we segment the data put away in the remote cloud and scramble the data in various ways, in order to guarantee data protection as well as quicken the adequacy of transmission. At long last, we propose collaborative IDS dependent on cloudlet work to secure the entire system.

VI. REFERENCES

[1] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for tele-home 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 centers," *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)–an 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. 3,614–624, 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, 2014,225–230.

[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, 2016,39.

[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. 63,183–188, 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 a 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] **First A.Chaitanya Sravanthi** currently working as an Associate Professor in Department of Master of Computer Applications in QIS College of Engineering & Technology with the Qualification MCA.

Second K. Chinna Vengamma pursuing MCA 3rd year in Qis College and Engineering and Technology in Department of Master of Computer Applications, Ongole.