International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 06, Volume 5 (June 2018) www.ijirae.com

# A PRIVACY PROTECTION SCHEME TO TRANSMIT MEDICAL DATA FROM WEARABLE DEVICES TO CLOUDS THROUGH CLOUDLETS

**Garima Dadheech**
Scholar, Computer Science, and Engineering, Pacific Institute of Technology,
Pacific University, Udaipur, Rajasthan, India
garry.dadheech@gmail.com

**Manuscript History**
Number: **IJIRAE/RS/Vol.05/Issue06/JNAE10081**
Received: 02, June 2018
Final Correction: 09, June 2018
Final Accepted: 18, June 2018
Published: **June 2018**
**Citation:** Dadheech (2018). A PRIVACY PROTECTION SCHEME TO TRANSMIT MEDICAL DATA FROM WEARABLE DEVICES TO CLOUDS THROUGH CLOUDLETS. IJIRAE::International Journal of Innovative Research in Advanced Engineering, Volume V, 210-217. **doi://10.26562/IJIRAE.2018.JNAE10081**
**Editor:** Dr.A.Arul L.S, Chief Editor, IJIRAE, AM Publications, India


**Abstract** - In the current scenarios, there was a huge demand for the wearable devices due to the development of clouds and cloudlet technology. So there has been wide essential to offer a better medical care to the people. For processing the patient medical information from one system to another includes various phases such as data collection, data storage, data sharing, etc. In the case of traditional healthcare system, it needs medical data transformation to cloud which includes user's sensitive data and further cause's communication energy consumption. Basically, medical data sharing referred as a most challenging issue. So, this research provides an apt solution to the medical data sharing. Here, a novel healthcare system is being developed by making use of flexibility of cloudlet. The cloudlet mainly functions to provide privacy protection, data sharing and intrusion detection. NTRU (Number Theory Research Unit) method is being initially used here to encrypt the user's information that is being gathered through wearable devices. This information will be further transmitted to the nearest cloudlet in an energy efficient way. Apart from this method, this research also proposes a new trust model to assist the users to choose trustable partners whoever wishes to share the information stored in cloudlet. This model mainly helps the patients who are suffering from some health problems by communicating with each other. The user's medical information which is being stored in remote cloud of hospital is classified into three parts and further secures them. For securing the healthcare system from malicious attacks this research developed a novel collaborative IDS (Intrusion Detection System) method through cloudlet mesh. As this can secure the remote healthcare big data cloud from various attacks. Finally, NTRU and AES-Rijndael algorithm are being used in order to attain more robust functionality. For implementation, Java technologies have been used to prove that proposed scheme remains effective.

**Keyword** – Cloud Computing: Wearable Devices;, NTRU, Cloudlet;

## I. INTRODUCTION

### Introduction to Cloudlet

From the past few decades, cloud computing technology has been developed greatly. This technology provides flexibility and high cost-efficiency through consolidation in which storage, network management functions, and computing work in a centralized manner.


 

Due to the rapid development of mobile internet and its related applications, the current cloud computing architecture is facing numerous challenges(Ai, Peng, & Zhang, 2017a). With powerful mobile devices and modern smartphones, the mobile apps offer many benefits to society. However, it has increased the demand for the online accessibility and availability. Cloud computing is introduced in the market to be widely adopted by the people for numerous applications specifically in mobile devices. Yet, there are many benefits and limitations while making use of cloud computing and mobile applications. The main drawback of cloud servers is the distance from the device. So, in order to overcome from this drawback Cloudlets have been introduced. The aim of cloudlets is to bring the cloud server closer to the mobile devices as it assists to use many disadvantages of cloud server for the mobile industry. Currently, there is numerous cloudlet architecture which is being developed by various researchers in their research work(Jaiswal, Thakare, & Sherekar S.S, 2015). In simple terms, cloudlet is defined as a small scale of computers which are designed to quickly offer cloud computing services to the mobile devices like smart phones, wearable devices, and tablets within the close geographical proximity(Rouse, 2016). Once they enter the cloudlet, a new middle-tier architectural element is located among cloud providers and mobile devices which decrease end-to-end latency which brings the services of cloud computing to the edge. At the time of application execution, the mobile device will act as a client which offloads significant computations to the nearest cloudlet. So, now the real-time response will be met by one-hop, low-latency, wireless access to cloudlet rather than connecting to the remote cloud provider. If no cloudlets are available, then the mobile devices can still depend on the distant cloud provider or can make use of their own resources(Vargas Vargas, 2016). Hence, it can be stated that the cloudlet systems attracting interests from various industries and also the research institutions.

## II. LITERATURE SURVEY

**Chen, Min, et al. (2016).** In the present scenarios, traditional wearable devices have many shortcomings like insufficient accuracy, long-term wearing, etc. So, carrying out a health monitoring with traditional wearable devices is very difficult to be sustainable. This research designed a Smart Clothing in order to acquire healthcare huge information by sustainable health monitoring. This proposed design will facilitate the unobtrusive gathering of numerous physiological indicators of the human body. Here, the smart clothing was built by using cloud computing, big data analytics, and mobile internet. Particularly, the collection of electrocardiograph signals by smart clothing is mainly used for emotion detection and mood monitoring.

**Sajjad, Syed, Muhammad, et al. (2015).** For a smooth working of the internet, the timely identification of anomalous activity in WSN (Wireless Sensor Networks) is very important. This research proposed an intrusion detection technique depending on the computation of trust of the neighboring node. Here in this IDS, each of the nodes will observe the neighboring node trust level. Depending on these trust values, the neighbouring nodes will be declared as risky, malicious and trustworthy. It's highly recommended to use the trustworthy nodes to forwarding engine for packet forwarding purposes. The introduced scheme will successfully identify the jamming attack, selective forwarding attack and hello flood attack by assessing the malicious node behaviour and network statistics.

**Raj, Arjun,and Rani, Suja MS (2015).** In the current scenarios, the demand for MCPS (medical cyber-physical systems) is increasing day by day. Each and every healthcare firm are making use of MCPS in order to ease the complicated tasks. These systems will assess the status of the patient by making use of physical sensors and employ the corresponding reaction by making use of actuators. The sensor devices are attached to the patient that states the real-time data. Currently, CPS (cyber-physical systems) is being used as a tool for the cyber-attacks. So these attacks will definitely have an effect on the patient either directly or indirectly on their life. So, here the researcher deployed intrusion detection system where it makes use of behavioural rule specification that is efficient in order to identify the unknown attack.

**Vasilomanolakis, Emmanouil, et al. (2015).**Nowadays, the society depends more on the networked computers. For instance, the digital networks are turned to drivers, computer networks as a central nervous system in the physical world, etc. However, the continuous functioning of the networked computers has more threatens when compare to other systems. Since the number of attacks on the IT systems has increased significantly, IDS are an important component of defence measure which is utilized and studied extensively in past. In this means, CIDS (Collaborative IDSs) emerge where includes numerous monitoring components which gather and exchange the information. This results in providing alerts which are correlated with the multiple monitors to create a view of the monitored network.

**Rajendran, Praveen Kumar, et al. (2015)**. Prevention and detection of intrusion is a very tedious process in the cloud environment. Here, they introduced a hybrid intrusion detection algorithm specifically for the private cloud environment. This algorithm is more efficient in terms of performance and security.


 

An in-depth research has been carried out on the existed intrusion detection systems since the current system till now did not identify the intrusion effectively. In this research work, artificial intelligence (AI) has been incorporated in order to identify any type of intrusion which occurs in private cloud environment. Incorporating the AI technique will lead toself-adaptive intrusion detection system that has been tested by making use of real-time data gathered with network speed.

**Rajendran, Praveen Kumar et al. (2015).**In the IT (Information Technology) sector, cloud computing is one of the emerging and latest areas where it gave various dimension to the firms. Security and performance concerns are the two main issues which need to be addressed in cloud computing particularly with respect to private and public cloud. One more security issues in cloud computing arean intrusion. Here the researcher discussed the whole idea related to cloud computing, types of intrusion detection systems, and related works. Finally, they build a Hybrid intrusion detection system in such a way that it would recognize the intrusion present in the cloud.

**Sajid, Anam et al. (2015).** In the real-time environment, the utility and deployment of a WBANs need new technologies like cloud computing and IoT (Internet of Things). These technologies are requiring in order to deal with the processing and storage limitations of WBANs. This rise of the system to cloud-based healthcare systems increased the privacy concerns regarding the healthcare data. Thus, there is a necessity for the effective mitigation and proactive identification mechanisms for the patient's data privacy concerns which pose continuous threats to stability and integrity of healthcare environment. Here, the researcher conducted a literature review where it clearly illustrated the patient's data privacy concerns regarding the cloud-assisted healthcare systems and assessed the mechanisms which are being proposed recently.

## III. OBJECTIVE OF STUDY

The main objectives of the present research paper are listed below:

- To research on the concepts related to cloudlet and relation with the cloud computing.
- To propose privacy protection scheme for transmitting health records from wearable devices to clouds via cloudlets.
- To evaluate the proposed scheme outcome for analyzing its effectiveness.

## IV. PROPOSED WORK

A new public key cryptographic algorithm is being introduced by considering shortest vector problem in a lattice by Jeffrey Hoffstein, Jill Pipher,and Joseph H. Silverman. One of the main benefits of this algorithm is that it runs much faster with a very low memory requirement when compared to conventional public key algorithms like RSA. The NTRU cryptosystem security will come from the interaction of polynomial mixing system with the independence of reduction modulo two relatively prime integers p and q (Hoffstein, Pipher, & Silverman, 1998). NTRU is a gathering of mathematical algorithms depending on manipulating lists of very small integers and polynomials. This permits NTRU to attain high speeds with the use of minimal computing power. Apart from RSA cryptosystem, being a very popular public key system, it needs more computing power when compared to other public key systems like NTRU and ECC. Majority of the smart cards are not able to process RSA 1024 key lengths because of the high computing power. Hence, there is a huge demand for another public key system where it should have an ability to offer the same level of security with a less computing power at the same time. So, one of the most appropriate ones is NTRU cryptosystem because of its low requirement of computing power and the ability to offer an equivalent level of security which is being provided by RSA 1024 (Challa, Narasimham, 2007). In the year 2007, both Challa and Pradhan made an experimental study on the comparison of NTRU and RSA. The results of this study show that NTRU needs only one-third time that RSA is in need for encryption process and one-seventh RSA time for decryption process. In all means, the selected NTRU is 217 times much after when compared to RSA in the encryption process and 31 times faster when compared to RSA in the decryption process.

Even if the NTRU algorithm provides various benefits (faster, less computing power, etc.) when compared to other algorithms such as ECC and RSA. Still, even this algorithm has few limitations which are listed below:

- The NTRU have an encryption algorithm known as NTRU Encrypt where it is being used for encryption, decryption and a signature algorithm. Here, NTRU Sign will be used for digital signature. Now, the researcher must use NTRU Encrypt key for both encryptions and decryption. Moreover, NTRU Sign key pair for digital signature processes. Here, the NTRU keys are not interchangeable.
- One can encrypt the data only with the public key and decrypt with the only private key. So, the NTRU user must make use of two pair keys. One pair key for encryption or decryption and second for digital signature.
- The asymmetric cryptography algorithms security level will not only depend on problem difficulty but also on padded of plain text in order to overcome attacks.


 

On the mobile phone devices, NTRU algorithm is fast enough to attain all cryptographic operations however, it has one disadvantage which is ciphertext size. The ciphertext of NTRU is large, and moreover, the encrypted SMS size with NTRU results in the large output. In this research, NTRU keys are used with strength 251 that offer a high level of security as offered by RSA 1024 key strength. In this research, NTRU 251 key strength with SVES-3 padding mode will generate a ciphertext with size 251 byte for every block with a size of 20 bytes. In simple terms, it can be said that SMS with 140-byte size will be broken down into seven blocks to encrypt and now ciphertext value will be 1757 byte (251 multiplied by 7). Hence, in this research along with NTRU, AES-Rijndael is being used. Here, NTRU used for securing the key-exchange sessions. The aes-rijndael symmetric algorithm is being used to secure the ordinary messages. In this process, initially, the Diffie-Heman algorithm is being used in order to make an agreement on the temporary key where this will be used only for one time in order to encrypt the NTRU public keys by making use of the AES-Rijndael algorithm. Now the NTRU algorithm is being used for encrypting and signing the secret keys during the key exchange session. Finally, AES-Rijndael algorithm is being used for encrypting the secret messages and these messages are further signed with NTRU private keys.

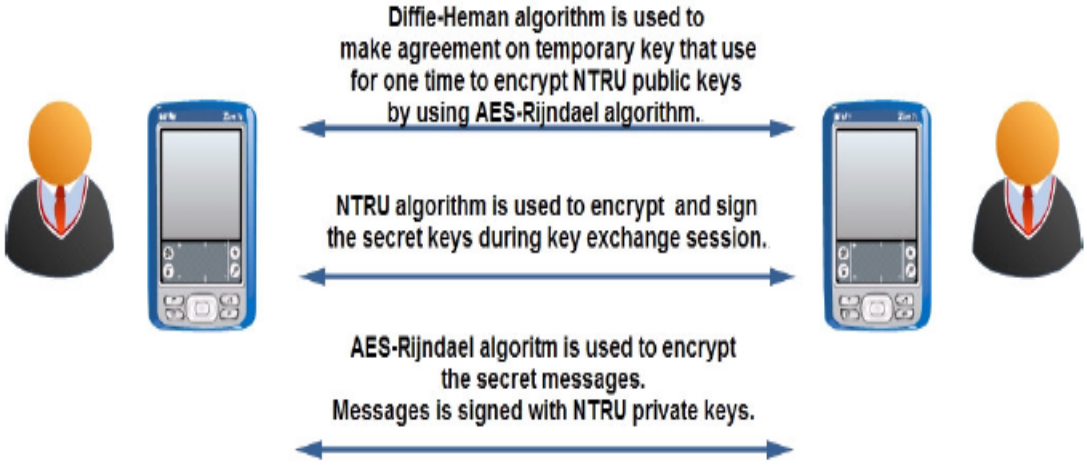


Figure 7: Shows the AES and NTRU usage in the system ((Hoostein, Pipher, & Silverman, 2001), p.3460).

Hence, in this way, the data that is being transferred from the wearable device to doctor through cloudlet and cloud is secured.

## V. CLOUDLET-BASED HEALTHCARE SYSTEM

A cloudlet based healthcare system was being proposed in this study. Initially, the patient's data was collected through wearable devices and further transmitted the nearest cloudlet. Now from this cloudlet the data is sent to the remote cloud where the doctors will have the authenticity to access the patient's information and give suggestions to them. Here in the data delivery chain, the privacy is provided to the whole process where protection is classified into three phases. In the initial phase, the patient's information gathered through wearable devices are transferred to the nearest gateway of cloudlet. In this stage, the main concern is on data privacy. In the second phase, the patient's information from cloudlets are further transferred to the remote cloud. Here, cloudlet is formed with only a few mobile devices and the owners have authority either to share particular data contents with other people. So, in this stage, both data sharing and securing privacy are considered as the main task.

A trust model is being used in this phase in order to compute the trust level among the different patients either to share the information with them or not. Now, in the third phase, the medical information stored in the cloud is categorized into different kinds and accordingly security policies are applied. Apart from all these three phases security, further this study used collaborative IDS based on cloudlet mesh in order to secure the cloud ecosystem. Until now the secured process is carried out between the wearable device and doctor in a secured manner. Here, the reply to the patient query will take some time. But, there are some scenarios where the patient needs doctor suggestions spontaneously. So, this research further proposed a hybrid cryptographic scheme where it merges both NTRU and AES. This scheme will allow the server to send SMS (Short Message Service) directly to the patient from doctors during the critical conditions. Hence, in this way, the proposed scheme provides security to the patient's health records.


 

### Advantages of Proposed System

When compared to the existing methods, the current proposed system provides numerous benefits to the firms whichever implement this system. Few of the main benefits that can be acquired through this system are listed below:

- NTRU will secure the whole information that is being transferred to cloudlet from wearable devices.
- Patients can share their information or queries with other people who also suffer from a same health problem. Security is provided to users through trust model where it identifies whether the data sharing can be performed or not.
- Patient's health records are highly secured by classifying them and making use of encryption mechanism.

For this research, a cloudlet-based health care system is being proposed and the framework of this system is shown in the below figure.

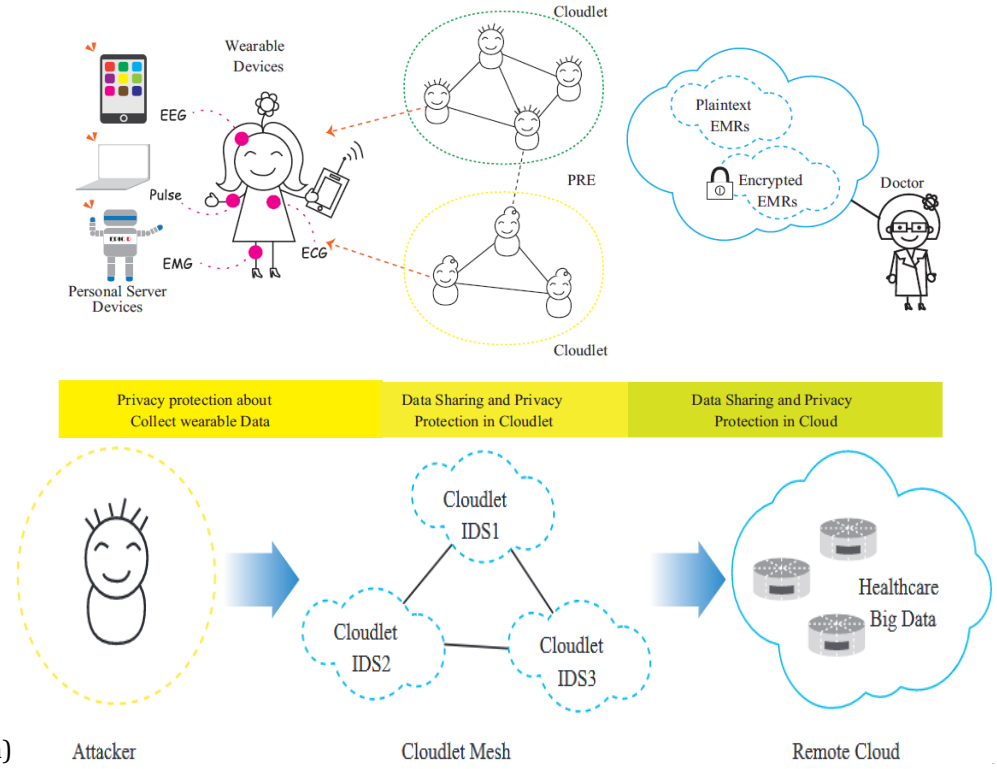


Figure 1: Illustrate the proposed system architecture (a) Privacy Protection system framework (b) Collaborative IDS of the remote cloud.

Initially, the psychological data of clients are gathered through wearable devices like smart clothing(Chen, Ma, Song, Lai, & Hu, 2016). Now, this collected information is delivered to cloudlet. In this research, two important issues are being considered for healthcare data protection. The first issue is about the healthcare data privacy protection and sharing the information which is shown in figure 5(a). The second difficulty is in developing an effective countermeasure to secure the healthcare database from being intruded from outside as shown in figure 5(b).

The first issue of healthcare data encryption and sharing are discussed below:

1. **Encryption of Client's Data -** Here, the researcher used the model that is being introduced by(Rohloff & Cousins, 2014) and further taken the advantage of NTRU(Nunez, Agudo, & Lopez, 2015) in order to secure the physiological information of the client's from abused. This scheme is mainly designed to secure the privacy of users while transmitting the information from smart phone to cloudlet.
2. **Cloudlet based data sharing –** generally, in the geographical aspect the user's will always be close to each other and will connect to the same cloudlet. So now it's a likely for these people to share the common aspects, for instance, the patients who suffer from the same disease will wish to share the data related to their treatment and other similar information. So, for data sharing the researchers make use of user's reputation and similarity as the input data.


 

3. After researcher acquires the trust levels of user's, a particular threshold is set for judgment. So, if it reaches or exceeds the threshold value then it is preferred that the trust level among the users is enough for sharing the data. Or else the user's data will not be shared if it has low trust level.
4. **Privacy protection for Remote cloud data –** when compared to the user's daily information stored in the cloudlet, the data that is being stored in the remote cloud will have more medical data. For instance, EMR where it will be stored in the cloud for more time. Here, the researcher makes use of the methods that are being presented in (Yang, Li, & Niu, 2015)(Yang et al., 2015)in order to classify EMR into EID, MI,and QID.
5. **Collaborative IDS based on cloudlet mesh –** in the remote cloud there is a huge amount of data stored in it. So it's very difficult to apply security mechanism for securing the database from malicious intrusions. In this research paper, the researcher will develop a particular countermeasure to establish a defense system for the large medical database in remote cloud storage. Precisely, collaborative IDS based on the cloudlet mesh structure is mainly utilized to screen any visit to the database as a protection border. If the detection system displays a malicious intrusion in advance, then the collaborative IDS will give an alarm and further restricts the visit and vice-versa. The collaborative IDS will acts as a protector of cloud database by securing numerous medical data and ensure in providing security to the database.

## VI. EVALUATION OF RESULT

In the proposed scheme, the patient's data (pulse, ECG, etc.) is collected from wearable devices and further it was encrypted. This encrypted information is further transmitted to a smartphone through homomorphic processing. Here in the research, it is assumed that the heartbeat information is [hr, 0, ……, 0], and array encryption is c1. Similarly, in all other cases like bp, ECG, etc. For bp, the clear data is represented as [0, bp, 0,……., 0] and its enciphered data will be c2. From these data, the researcher can acquire clear data and cipher data of all the sensors. This clear information was acquired with the public key encryption system and homomorphic encryption (HE). The data received by smart phone is {c1, c2, …..,cn} transmitted to cagg = c1 + c2 + ……+ can mod q. By processing the data with homomorphic encryption, it will decrease the bandwidth before the information is uploaded to cloudlet. Hence, in this way the bandwidth and energy are saved.

## VII. CONCLUSION

This study proposed a cloudlet based health care system and hybrid cryptographic scheme. Initially, the current research examined the issue of providing protection to the medical information that is being stored in cloudlets and remote cloud. Then it developed a system such that it permits the users to transfer the data to the remote cloud through cloudlets with a low communication cost. For carrying out this mechanism, the researcher used wearable devices in order to gather user's information. But to provide privacy to this information NTRU have been used to ensure the patient' health data to cloudlet in a secured manner. Further to share the information among the patients within the cloudlet, the trust model is being used to compute its trust level. This model will check out whether the data can be shared or not based on the trust level. Further to provide privacy-preserving if remote cloud data, this research classified the information which is being stored in the remote cloud and then encrypted the information in various ways. This process was carried out not only for ensuring the protection of data but also transmission efficacy. Collaborative IDS is also being introduced in this research depending on the cloudlet mesh in order to secure the entire system. This entire secured process is to allow the patient data from the wearable device to doctor through cloudlet and remote cloud. This whole process will take some time and doctor prescriptions given to the patients may take some time to reach the patient. So, in emergency cases, the doctor will directly send SMS to the patient so that the patient can take steps immediately to cure their diseases. Here, to attain this task the researcher used hybrid cryptographic scheme of merging both NTRU and AES-Rijndael algorithms. This scheme is being used as it allows to offer peer-to-peer SMS security solution where it can even be implementable in non-server architecture mobile security systems. This system offers all the essential services related to security such as integrity, confidentiality, non-repudiation, and authentication of the patients. This solution not only suggested in medical industry but it can also be used for every sector. Since this solution runs fast enough on mobile devices and there is no need for any hardware. The main benefit of this solution is that it entirely independent ofa third party or mobile network operator. However, this research failed to attain the result of the hybrid cryptographic scheme due to the short time period. So, this scheme is referred for future work.

## VIII.FUTURE WORK

In this project, two schemes are introduced for securing patients health record which is being transmitted to doctor from patients and vice-versa through cloudlet and clouds. The first scheme is cloudlet based healthcare system and other is a hybrid cryptographic scheme.


 

Here, in this current project the first scheme is successfully attained results in securing patient's health records from intruders and moreover, it even allows the patients to recover their data if in case it was corrupted. However, by making use of a hybrid cryptographic scheme of AES-Rijndael and NTRU the researcher failed to provide peer-to-peer SMS solution in non-server architecture mobile security systems. This scheme was mainly introduced in this research to send an SMS by a doctor to patients regarding the medical prescriptions in emergency cases. Yet, due to lack of time period, the researcher failed to attain this result. So, this scheme can be referred for the future work and the researcher can offer essential security services like confidentiality, authentication, non-repudiation, and integrity.

## REFERENCES


1. Andersen, Anders, Yigzaw, Kassaye Yitbarek & Karlsen, Randi,„Privacy preserving health data processing", IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom),pp:225-230, DOI: 10.1109/HealthCom.2014.7001845,ISSN: 978-1-4799-6644-8 (2014).
2. Ai, Y., Peng, M., & Zhang, K., "Edge computing technologies for internet of things: a primer. Digital Communications and Networks", 4(2),pp:77–86, (2014a)
3. Badrul Anuar, N., Ngan Kuen, L., Zakaria, O., Gani, A., & Wahid Abdul Wahab, A., GSM Mobile SMS/MMS using Public Key Infrastructure: m-PKI. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.490.2773&rep=rep1&type=pdf.(2008).
4. Challa, N. and Pradhan, J. ,"Performance Analysis of Public key Cryptographic Systems RSA and NTRU". IJCSNS International Journal of Computer Science and Network Security, 7(8). Retrieved from http://paper.ijcsns.org/07_book/200708/20070812.pdf, (2007).
5. Chen, M., Ma, Y., Song, J., Lai, C.-F., & Hu, B. "Smart Clothing: Connecting Human with Clouds and Big Data for Sustainable Health Monitoring". Mobile Networks and Applications, 21(5), pp. 825–845, (2016).
6. Chen, M., Qian, Y., Chen, J., Hwang, K., Mao, S., & Hu, L."Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing". IEEE Transactions on Cloud Computing, XX(c), pp. 1–1, (2016).
7. Fabian, B., Ermakova, T., & Junghanns, P."Collaborative and secure sharing of healthcare data in multi-clouds". *Information Systems*, *48*, pp. 132–150 (2015).
8. Gao, Y., Hu, W., Ha, K., Amos, B., Pillai, P., & Satyanarayanan, M. Are Cloudlets Necessary? *Cmu-Cs-15-139*. Retrieved from http://reports-archive.adm.cs.cmu.edu/anon/anon/usr/ftp/usr0/ftp/2015/CMU-CS-15-139.pdf, (2015).
9. Ha, K., Abe, Y., Chen, Z., Hu, W., Amos, B., Pillai, P., & Satyanarayanan, M. "Adaptive VM Handoff Across Cloudlets", (June). Retrieved from http://ra.adm.cs.cmu.edu/anon/2015/CMU-CS-15-113.pdf, (2015).
10. Ha, K., Pillai, P., Richter, W., Abe, Y., & Satyanarayanan, M. Just-in-Time Provisioning for Cyber Foraging. Retrieved from https://www.cs.cmu.edu/~satya/docdir/ha-mobisys-vmsynthesis-2013.pdf. (2013).
11. Hassani Mohamed, Lebbat Adil, Tallal Saida, & Medromi Hicham. "A collaborative intrusion detection and Prevention System in Cloud Computing - Semantic Scholar" (2018).
12. Hoostein, J., Pipher, J., & Silverman, J. H. NTRU: A Ring-Based Public Key Cryptosystem. (2001).
13. Jaiswal, A. ., Thakare, V. ., & Sherekar S.S. (2015). Performance based Analysis of Cloudlet Architectures in Mobile Cloud Computing. International Journal of Computer Applications, pp.975–8887,(2015).
14. Li, J., Yang, J.-J., Zhao, Y., & Liu, B. A top-down approach for approximate data anonymisation. Enterprise Information Systems, 7(3), 272–302,(2013).
15. Li, Q., Cao, G., & Porta, T. F. La."Efficient and Privacy-Aware Data Aggregation in Mobile Sensing". IEEE Transactions on Dependable and Secure Computing, 11(2), pp. 115–129. (2014).
16. Lu, R., Lin, X., & Shen, X. SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency. IEEE Transactions on Parallel and Distributed Systems, 24(3), pp. 614–624.(2013).
17. Lu, R., Zhu, H., Liu, X., Liu, J. K., & Shao, J. "Toward efficient and privacy-preserving computing in big data era". IEEE Network, 28(4), pp. 46–50.(2014).
18. Nuñez, D., Agudo, I., & Lopez, J. "NTRUReEncrypt. In Proceedings of the 10th ACM Symposium on Information", Computer and Communications Security - ASIA CCS '15 (pp. 179–189), (2015).
19. Prasad, V. R., Sunanda, M., & Prasad, V. M. "Secure SMS with Identity Based Cryptography in Mobile Telecommunication Networks", 8491, pp.166–169. (2011).
20. Rohloff, K., & Cousins, D. B. A Scalable Implementation of Fully Homomorphic Encryption Built on NTRU (pp. 221–234),(2014).



 

21. 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).
22. Rajendran, P. K., Rajesh, M., Abhilash, R., & Associate, D. "Hybrid Intrusion Detection Algorithm for Private Cloud".(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, 131(16).(2015).
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).


 