Securing Communication in the IoT- Based Power Constrained Devices in Health Care System

Sandhya Sarma. K. N, Hemraj Shobharam Lamkuche, E.Chandra Blessie

Abstract: ***One of the most appealing IoT application areas is medical care and health care. This promising technology is reshaping current health-care service that comply with treatment and mediation at home. The core part of IoT constitutes sensors and various devices for diagnosis and imaging. Now-a-days sensors are becoming smaller, allowing them to be worn without interfering with daily activities.. To make sensors wearable and wireless, it should be small in dimensions and also the energy, memory, and processing power available also matters. Health services dependent on the Internet of Things are supposed to minimise cost, enhance the user's experience and improve their quality of life. IoT has many hurdles in its implementation, security is the most important. This paper throws light on the different methods of securing the medical sensitive data through the network.***

Keywords: Internet of Things, Cloud Computing, Healthcare cloud, Security, Sensors.

I. INTRODUCTION

Recently, there is tremendous growth in usage of internet, and connecting things from real world to internet is nothing but Internet of Things. World is coming closer and completion of work has increased rapidly due to IoT. We can see many uses of IoT in different sectors like personal use, agriculture, smart irrigation, healthcare, education, home automation, environmental monitoring, smart cities, industrial automation, smart energy, etc. IoT is equally valuable in all areas. In healthcare it can save a life through fast detection of diseases and their immediate treatment . Agriculture has a major impact on economy of country and monitoring the health of the crops can help in producing good quality crops in a more faster way.

Information about natural calamities can be also be given to farmers prior through environmental monitoring which may help them to save crops. Industry plays another crucial role in a country's growth, so if industrial work goes in smart way through IoT, it can be more profitable with good quality.

Smart city involves a vast use of IoT. People can use services rapidly from anywhere in smart city, which can save their time. Although, we can say IoT is a boon but it can lead to risks, if proper security measures are not applied to IoT applications, data and devices. IoT needs continuous network access, so what if network failure or power failure occurs, for this, preventative measures are sharply needed.

Mobility is one of the factors important to be considering in IoT. Mobility and Cyber security might not be fully overlapping. Cyber security comes with adoption of new technology. Cyber security is needed for all types of devices on network and most of the devices in network can be mobile devices. For ex. smartphone. So, in IoT , the devices are connected to network and tasks are getting smarter. With mobility we are carrying technology in our pocket. We can say IoT involve mobility as in IoT applications smart approach is involved. For ex. Smart phone has sensors connected to applications which is the use of IoT and Smartphone itself is mobile, it moves along with us. We can say IoT and mobility are overlapping. Another example is connected car and there are many such implementations of IoT.

It is very important to set policies from security point of view for any device that connects to internet. The lack of frameworks would aid an organisation in identifying IoT-related threats and implementing appropriate controls. This is still a big problem in such areas, but that is changing and AT&T has established a four-part system for assessing IoT threats..

An organization's various stakeholders must be represented. The IT security team and business divisions, as well as the executive officers and board of directors, are among them. Determine whether or not there are any legal or regulatory concerns. Organization should use encryption, use latest hardwares and softwares, regular updates.

In initial phases of IoT adoption for small to medium business, it seems very easy and simple to implement and use it but as IoT hardware devices, software and users increases, the complexity grows and then businesses faces these challenges which might be through some bad experiences about security leakage. So businesses must have to implement strong security policies. IoT devices in the network produce a large amount of data. to tackle with such a huge amount of data is biggest challenge. Heterogeneity increases complexity in security.

Manuscript received on May 20, 2021.
Revised Manuscript received on May 26, 2021.
Manuscript published on May 30, 2021.
* Correspondence Author
Sandhya Sarma K N*, Department of Computer Science, Bharathiar University, Coimbatore, India. Email: sandhyasvivek@gmail.com
Dr. Hemraj Shobharam Lamkuche, Department of Computer Science, Symbiosis Centre for Information Technology, Pune, India. Email: hemraj@scit.edu
Dr. E Chandra Blessie, Department of Computing(AIML), Coimbatore Institute of Technology, Coimbatore, India. Email chandra_blessie@yahoo.co.in

Iot in simple words are things that sense data, process and share it to other things through internet. IoT systems consists of sensors or devices that send data to cloud, software processes it and has ability to send data over a network without requiring human-to-human or human-to-computer interaction .Wiki leaks in March-17 made to think how much the data stored in cloud server is safe and secure in the future. In the near future IoT is poised to play a strong role in all aspects of health care. With the aid of health-care data, researchers and physicians can access a wealth of information that can be used to assess a patient's health and well-being, confirm whether the patient is displaying any disease symptoms, and eventually predict which disease the patient will develop.

Analyzing and forecasting a patient's health and well-being would necessitate a significant amount of storage and computation. Cloud computing has solved the issue of data storage and computation, allowing us to focus on other things. When such a large volume of private data is obtained from various patients, we must ensure that the data is maintained in its integrity. The data collected through the body sensors should be transmitted to the central medical server of the hospital and should be accessible to only the specified doctors, as the patient's body data is sensitive data. Here in this paper we discuss the various security methods proposed to protect this sensitive data.

II. IOT IN HEALTH CARE

It is a heterogeneous computing, communicating system of apps that connect patients and health providers. Few examples are headsets that measure brainwaves, Clothes with sensing devices, BP/Glucose/ECG/Pulse/ monitors and any wearable technology device. IoT has major impact in health care by reducing the cost and improving the treatment. IoT technologies in healthcare benefit patients, families, physicians, hospitals, and insurance providers.

Patients – Patients have access to personalized attention through wearable devices such as blood pressure and heart rate monitoring cuffs, glucometers, and other wirelessly linked devices. These devices can be set to remind you of some things like calorie counting, exercise, appointments, blood pressure changes, and much more.

The Internet of Things has changed people's lives, especially the lives of elderly patients, by allowing them to track their health in real time. This has a major effect on lonely people and their families. Family members and concerned health practitioners receive alerts from a warning system, if a person's normal activities are disrupted or changed.

Physicians – Wearables and other IoT-enabled home monitoring equipment will help physicians keep better track of their patients' health. Data from IoT devices can assist clinicians in determining the appropriate treatment process for their patients and achieving the desired results.

Hospitals - Hospitals can benefit from IoT devices in a variety of ways, in addition to monitoring patients' health. Wheelchairs, defibrillators, nebulizers, oxygen pumps, and other monitoring devices are all monitored in real time using IoT devices with sensors.

Health Insurance Companies – There are numerous opportunities for health insurers with IoT-connected intelligent devices. Insurance companies can leverage data captured through health monitoring devices for their underwriting and claims operations. This data will enable them to detect fraud claims and identify prospects for underwriting.

Sensors are used in IoT are for/in video surveillance and lightning systems, intelligent devices for monitor environmental conditions, cameras, traffic lights, connected cars and many other smart devices in cities. Connected ambulance, intelligent medical devices, traffic flow optimization-connected traffic cameras, smart factory, smart roads, pet tracking, Smoke detectors, water metres, garbage cans, vending machines, and gas monitoring health of Buildings- periodically send a radio signal of suitable amplitude and phase characteristic to inform about the structure's state/health, water level for lakes, streams, sewages, gas concentration in the air for cities, laboratories, and deposits, soil humidity and other characteristics, inclination for static structures (e.g., bridges, dams),position changes (e.g., for landslides),lighting conditions either as part of combined sensing or standalone, to detect intrusions in dark places, infrared radiation for heat (fire) or animal detection, waste management, smart parking - Radio Frequency Identification (RFID) is useful for vehicle identification systems, smart health.

III. RELATED WORKS

Patients always want the doctors and hospitals to assist them with high efficiency without revealing their identities to the cloud server For wearable devices such as bracelets, ornamentation, patches, caps, t-shirts, bands, glasses, wearable processes can be tailored to the "real body." This equipment has been used to contact the person who monitors the disease and personal health of patients. The information gathered is then been sent to the central and internal research centre. Three elements used to monitor are wearable devices such as cameras, machine buildings and exhibits. Wearable devices may provide natural statistics, including calories, steps, heart rate, blood pressure; time spent exercising, and so on. The effect of these devices is enormous and of course very strong, which has a good focus on monitoring the physical health of our users.

Various wearable devices as given below:

A. Pulse Oximetry:

This device measures the difference in skin blood flow associated with the cardiac cycle and checks the human body's oxygen saturation level. The pump oximeter, containing an image detector and light-emitting diodes (LEDs), is connected to the finger or ear. The red light sent or carried back into the human body tests infrastructure. The distinction between the level of the installation and the amount of deoxygenated hemoglobin helped to measure oxygen saturation. It is used to calculate the heart rate as Photo Plethysmo Graph (PPG).

B. Electrocardiography (ECG):

A waveform that monitors the heart continues to function and provides time information.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

There is also restricted readiness for automation for ECG calculation based on wireless sensor devices.

C. Blood Pressure:

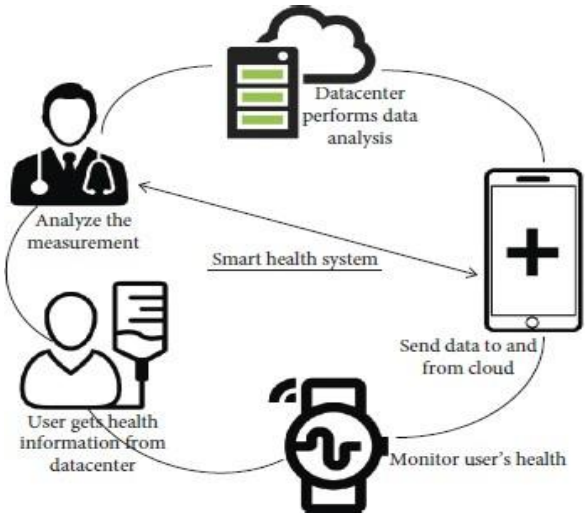
The energy used by blood pumping into the blood vessels helps to quantify it. The oscillometric approach is used to calculate these types of sensors for the hand frame and systolic readings.

D. Electromyography (EMG):

The muscle research works by looking at the muscle's electrical signals. For all electric signals EMG is the spatio-temporal DRM. The EMG signal therefore provides an efficient way to monitor human muscles' activities.

E. Electroencephalography (EEG):

The electroencephalogram (EEG) is a description of human brain functions. The Wireless Intelligent Sensor (WISE) is a low-frequency control system with EEG data acquisition, wireless connectivity, analogue signal synchronisation, and low-level real-time signal processing capabilities.



Implantable Devices

Artificial Implants are implanted under the jar of the human body to help improve a component or structure. Implants are more widely used for multiple applications including neural prosthesis, orthopedics, heart stent, artificial pacemakers, etc. Any organic material such as apatite, silicone, titanium can be extracted from the outside layer of the implanted equipment, and the contents must be chosen according to the human body's specifications. Ceramics, metals and polymers may be manufactured from materials used for artificial devices. The following are other equipment listed:

A. Glucose Monitoring:

A mixed membrane in the tumor tissue is the competent procedure for the implantation of the sensor. During the 30s, body sugar levels can be tracked and data transmission occurs approximately every 5 minutes. When the sensors are in place and the level of glucose can be regulated, an alternative to the insulin level is given.

B. Implantable Neural Stimulators:

These types of electrical stimulation trigger electric impulses to relieve chronic pain in the human spinal cord or brain.

Applications of IoT in Healthcare

Patients and adults can live independently with the help of healthcare apps. IoT sensors are used during this period for diagnosing and re-evaluation of their wellbeing and sending alerts in unlawful circumstances. The IoT device itself will advise the patient appropriately when other minor problems are detected". "The sections below cover the different IoT uses in healthcare.

They are split into two general types of health applications made for IoT: single step and mixed mode.

A. Single status applications: such applications designed for a specific disease.

- **Glucose Sensitivity:** Diabetes is a metabolic condition if the sugar level at a long-term period is above average. The blood sugar control system generates blood glucose of some kind and helps to prescribe a healthy diet, appropriate tests and medications. It is currently proposed an m-IoT configuration process that is not permitted based on glucose.To this end, different sensors are linked in patients through the correct provider of IPv6 connectivity. In the operating system, it creates an IoT-based communication unit that transmits the information gathered to the level of blood sugar. A collector of glucose, a computer or a smart phone and the processor is included in this package. A standard IoT- based detector for glucose levels is also proposed.
- **Blood Pressure Monitoring System:** High blood pressure shows the heart pumping through the body powerfully. The method of IoT promotes the diagnosis and treatment of health problems, including blood pressure (BP), hemoglobin (HB), levels of blood sugar and abnormal cell growth. An IoT system for blood pressure, diabetes and obesity treatment.
- **Body Temperature Monitoring:** Body temperature control and tracking is an essential component in health applications. The homeostasis change depends on the temperature of the body, based on the m-IoT principle. Telos Bmote software body-sensor sensors have clear and efficient internal performance. On the top of an IoT unit, the body temperature control device is centered on the home port. It supports the control and calculation of the temperature infrared detection and RFID module.
- **Oxygen Saturation Monitoring System:** The Pulse oximeter is used to measure oxygen in the blood continuously. The use of IoT with pulse oximetry is useful for technical applications. The benefit of IoT-based pulse oximetry is addressed by coAP-based health care system studies. Ninin shows the function of the Wrist OX2 oximeter machine.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

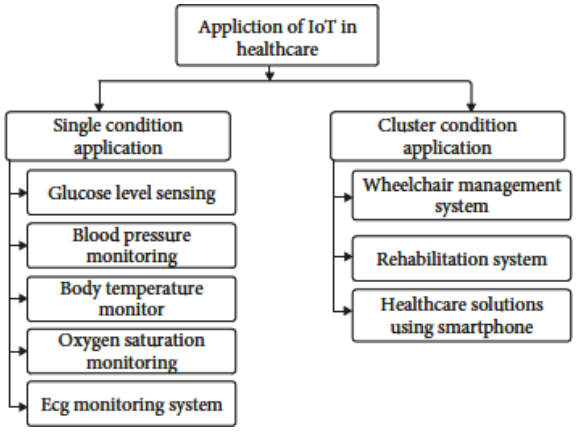
This system is wired to Bluetooth and links the sensor directly to Monere. To track remote patients, an IoT-based norm and low-pulse oximeter is used. The IoT network allows this system to continuously monitor the health of patients.

- **ECG (Electrocardiogram) Monitoring System:** The ECG monitoring unit has the option of displaying the user / patient ECG waves. A patient's medical report is published by gathering ECG signals and uploading data to the cloud network. Provides user input on the basis of the collected information. With a traditional analogue to digital transformer, the IIo-OTG microcontroller transforms ECG signals and downloads a binary file output from the cloud network for analysis and identification of irregular conditions for human health. The full advantage of these machines decreases waiting times and decreases facilities in hospitals and emergency departments.

B. Consolidated status requests: These applications can treat certain diseases together.

- **Wheelchair Management System:** Comfortable wheelchairs are suggested by experts to save the lives of the elderly and individuals with disabilities. IoT plays a significant role in speeding up this process in this region. Smart wheelchairs are fitted with different sensors to track seat movement and also to display the status of patient / user.
- **Rehabilitation System:** The process of regenerating population growth issues and a lack of life skills can be improved by IoT. The capabilities of physically disabled people can be strengthened. In order to strengthen the recovery mechanism, the Body Sensor Network was introduced. Ontology-based automation architecture reveals that IoT can be a great way to manage information in real time. The Early Childhood Education programmed, the intelligent city medical recovery programmed and the integrated goal technology programmed are many of the services that IoT has created.

Healthcare Solutions Using Smartphone: The electronic device control system with sensors has so far been seen on the Smartphone. Specific mobile applications are offered in the healthcare sector to support patients, provide medical training and provide initial training. A range of software and hardware products that portray the Smartphone as a useful tool in healthcare are being developed.



This can be achieved through anonymous authentication discussed by Abid Mehmood.et.al[4].The proposed scheme uses rotating group signature scheme based on Elliptic curve cryptography to provide anonymity to the patients.

Mohamed Elhoseny et al. [5], proposed steganography techniques and hybrid encryption algorithms to hide digital information in an medical image. The encryption scheme is formed by combining Advanced Encryption Standard-AES, and Rivest,Shamir and Adleman – RSA algorithms. The paper also aims in improving the security of medical data transmission by integrating steganography and hybrid encryption techniques.

In the paper proposed by Haiping Huang et al. [1] an health care system is designed that proposes secured medical data transmission from Wireless Body Area Networks(WBAN) to Wireless Personal Area Networks(WPAN). Homomorphic encryption based on matrix scheme is used to ensure privacy. It also enacts privacy-protecting policies in order to improve connectivity between users' smartphones and embedded medical devices.

Signal Scrambling is another powerful method used in modern data communication schemes to secure data and provide synchronization between transmitter and the receiver. In the paper proposed by Shu-Di Bao et al.[2], sensitive health care data is secured and for added security, a small piece of data is used to partition and scramble the health care data. The scrambled data is stored in the cloud, while the tiny data is held locally for retrieval.

The term "cloud of things" refers to the combination of cloud computing and the Internet of Things. Mukhtar M E Mahmoud et.al „s literature[6] analyses CoT architectures and platforms and alsoimplementation of CoT in smart health care. Different energy efficiency methods in CoT that can be applied in health care is analyzed deeply in the paper.

IoMT is a new term introduced in the paper [7] by Ankur Limaye et al . The paper paves a way for researches on new optimization techniques that enable efficient execution of emerging IoMT. Edge computing is used to solve bandwidth bottlenecks. A benchmark suite HERMIT which comprises of applications spanning various domains in health care is introduced for IoMT.

Hadeal Abdulaziz Al Hamad et al.[3] in their paper focused on fog computing facility to secure health care private data in cloud. A tri-party one-round authenticated key agreement protocol was proposed based on bilinear pairing cryptography. Decoy technique is used to store and access private heath care data.

Attribute Based signature (ABS) is a very useful technique for the privacy protection of users and suitable for anonymous authentication and privacy access control . LPPMSA scheme proposed by Jingwei Liu et al [8]is based on multi authority ABS to ensure that the sensitive information of users is not disclosed.

Block chain technology has strong potential to improve the management of medical data, as it does not suffer from issues like single point of failure, centralized data stewardship and system vulnerability found in traditional client – server and loud based health care data management system.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

[9] authored by Leila.et.al proposed light weight bock chain architecture for health care data management reduces the computational and communication overhead compared to Bitcoin network.

Fengwei Wang.et.al proposed a new scheme PCML[10] to address the security issues and improve the accuracy of online medical diagnosis service. Based on Paillier cryptosystem with threshold decryption and distributed skyline computation, health care centers can securely learn a global diagnosis model with their local diagnosis models in the assistance of cloud. LIST[11] is proposed by Yang et.al in which patient data are encrypted end-to-end from a patient's mobile device to data users and it also enables efficient keyword search. Attribute based encryption is opted to provide fine grained access on encrypted data.

IV. REVIEW OF PAPERS

Table 1 summarizes the contributions and concepts explained in each paper along with the author name and year of publishing.

Ref. No	Title of Paper	Author and Year	Contribution	Concept Used /Remarks
1	Private and secured MedicalData Transmission and Analysisfor wireless Sensing Health careSystem	Haiping Huang et al. (2017)	Proposes a secured medical datatransmission from Wireless Body Area Networks(WBAN)to Wireless Personal Area Networks(WPAN).	Homomorphic encryptionbased on matrix scheme isused to ensure privacy.
2	A Method of Signal Scrambling to Secure Data storage for Healthcare Applications.	Shu-Di Bao et al. (2017)	The data is scrambled beforestoring in cloud.	Signal Scrambling.
3	A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing Based Cryptography	Hadeal Abdulaziz Al Hamad et al (2017)	Fog computing facility is used to secure health care private data in cloud.	Fog computing, Bilinear pairing cryptography,Decoy technique.
4	Anonymous Authentication Scheme for Smart Cloud Based Healthcare Application	Abid Mehmoodet al. (2018)	Provides anonymousauthentication to patients whodo not want to reveal their identity	Rotating Group signaturescheme based on Ellipticcurve cryptography
5	Secure Medical DataTransmission Model for IoT – Based Healthcare Systems	Mohamed Elhoseny et al.(2018)	Provides a method to hide digital information in medicaldata	Steganography technique .Combination of AES and RSA algorithms to encryptthe secret data before hiding.
6	Enabling Technologies onCloud of Things for Smart Healthcare	Mukhtar M. E. Mahmoud et al. (2018)	Analyses CoT architectures andplatforms and also implementation of CoT in context of smart health care	Survey paper on Cot architectures in healthcare
7	HERMIT: A Benchmark Suitefor the Internet of Medical things.	Ankur Limaye etal. (2018)	Optimization techniques that enable efficient execution of emerging IoMT	Edge computing.
8	Ligtweight and Privacy – Preserving Medical ServiceAccess for Healthare Cloud . LPP-MSA.	Jingwei Liu et al . (2019)	Privacy protection of users and anonymous authentication of users and privacy access control .It ensures that the sensitive information of users is not disclosed.	Multi authority AttributeBase Signature.
9	Lightweight Blockchain	Leila.et.al.(2019)	Proposed light weight bock chain architecture for healthcare data management to improve the management ofmedical data, reduces the computational and Communication overhead compared to Bitcoin network.	Block chain.
10	Privacy-Preserving Collaborative Model LearningScheme for E-Healthcare	Fengwei Wang.et.al. (2019)	A new scheme [PCML] to address the security issues and improve the accuracy of online medical diagnosis service.	Based on Paillier cryptosystem withthreshold decryption and distributed skyline computation
11	Light weight Shareable and Traceable Secure Mobile Heath System	Yang Yg et al.(2020)	End-to-end encryption of data from a patient's mobile device to data users and it also enables efficient keyword search.	Attribute Based Encryption (ABE) .

V. CONCLUSION

In this paper we have reviewed the IoT technologies with cloud computing in health care system. We have noted that there is a large scope in research to study and develop applications, devices and platforms that rely on cloud computing and IoT. In the coming years, there will be a lot of research into the protection of confidential medical data stored in the cloud.

REFERENCES

1. Haiping Huang,Tianhe Gong,Ning Ye, Ruchuan Wang, Yi Dou," Private and secured Medical Data Transmission and Analysis for wireless Sensing Health care System" , *IEEE Trans.Industrial Informatics*.,vol 13, No 3, June 2017.
2. Shu-Di Bao, Meng Chen, Guang-Zhong,"A Method of Signal Scrambling to Secure Data storage for Healthcare Applications." *IEEE Trans.Biomed. Health Informatics*., vol.21,No.6,Nov 2017

3. Hadeal Abdulaziz Al Hamid, Sk Md Mianur Rahman, M. Shamim Hossain, Ahmad almogren, Atif Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Usinga Fog Computing Facility With Pairing Based Cryptography." , *IEEE Access*.,vol 5, 2017.
4. Abid Mehmood, Iynkaran Natgunanathan, Yog Xiang, Howard Poston, Yushu Zhang, "Anonymous Authentication Scheme for Smart Cloud Based Healthcare Application", *IEEE Access*.,vol 6, 2018.
5. Mohamed Elhoseny, Gustavo Ramirez-Gonzalez, Osama M, Abu-Elnasr, Shihab A Shawkat, ArunKumar N, Ahmed Farouk, "Secure Medical Data Transmission Model for IoT – Based Healthcare Systems", *IEEE Access Information Security,Telecommunication Applications*.,vol 6, 2018.
6. Mukhtar M e Mahmoud, Joel J P C Rodrigues, Syed Hassan Ahmed, Sayed Chhattan Shah, Jalal F Al-Muhtadi "Enabling Technologies on Cloud of Things for Smart Healthcare", *IEEE Access cyber threats, Countermeasures in Healthcare sector*,vol 6, 2018.
7. Ankur Limaye, Tosiron Adegbija,"HERMIT: A Benchmark Suite for theInternet of Medical things.", *IEEE Trans, Internet of Things*,vol 5, October 2018.
8. Jingwei Liu, Huifang Tang, Rong Sun, Xiaojiang Du,Mohsen Guizani, "Ligtweight and Privacy – Preserving Medical Service Access for Healthare Cloud . LPP-MSA.", *IEEE Access*.,vol 7, August, 2019.
9. Leila Ismail, Huned Materwala, Sherali Zeadally,"Lightweight Blockchain for Healthcare", *IEEE Access*.,vol 7, October, 2019.
10. Engwei Wang, Hui Zhu, Ximeng Liu, Rongxing Lu, Jiafeng Hua, Hui Li,"Privacy-Preserving Collaborative Model Learning Scheme for E-Healthcare", *IEEE Access*.,vol 7, November, 2019.
11. Yang Yang, Ximeng Liu, Robert H. Deng, Yingjiu Li,"Light weight Shareable and Traceable Secure Mobile Heath System", *IEEE Trans, Dependable and Secure Computing*,vol 17, January 2020.
12. Y.Yin,Y. Zeng, X. Chen, andY. Fan, ``The Internet of Things in healthcare: An overview," *J. Ind. Inf. Integr.*, vol. 1, pp. 3_13, Mar. 2016.
13. Sandip Roy, Ashok Kumar Das, Santanu Chatterjee, Neeraj Kumar, Samiran Chattopadhyay, Joel J.P.C.Rodrigues, "Provably Secure Fine- Grained Data Access Control Over Multiple Cloud Servers I Mobile Cloud Computing Based Healthcare Applications", *IEEE Trans, Industrial Informatics*, vol 15, No 1, January 2019.
14. Huansheng Ning, Hong Liu, Laurence T . Yang, "Cybernity Security in the Internet of Things".
15. Owusu-Agyemang Kwabena, Zhen Qin, Tianming Zhuang, Zhiguang Qin, "MSCryptoNet: MultiScheme Privacy – Preserving Deep Learningin Cloud Computing", *IEEE Access*.,vol 7, March , 2019.
16. Hadi Habibzadeh, Karthik Dinesh, Omid Rajabi Shisvan, Andrew Boggio-Dandry, Gaurav Sharma, "A survey of Healthcare Internet of Things(HIoT): a Clinical Perspetive", *IEEE Trans, Internet of Things*,vol 17, January 2020.
17. S.M.Riazul Islam, Daehan Kwak, MD. Humaun Kabir, Mahmud Hossain, Kyung-SUP Kwak, "The Internet of Things for Health Care: A comprehensive Survey, *IEEE Access*,vol 13, January 2015Raman Dugyala, N Hanuman Reddy, N Chandra Sekhar Reddy, J Phani Prasad, "A Roadmap to Security in IoT", IJAE Reseach ISSN 0973-4562, vol 12,2017.
18. Anoma Abade ," Security in Internet of things Using Attribute Based Encryption", JASC, ISSN NO: 0076-5131, vol 5, July 2018.
19. Rodrigo Roman, Pablo ajera, Javier Lopez, "Securing the Internet of Things", *IEEE Computer society*, September 2011.
20. Stephanie B Baker, Wei Xiang, Ian Atikson, "Internet of things for Smart Healthcare: Technologies, Challenges, and Opportunities", *IEEE Access*,vol 5, 2017.
21. AbdulAziz Shebab, Mohamed Elhoseny, Khan Muhammad, Arun Kumar Sangaiah, Po Yang, Haojun Huang, Guolin Hou, "Secure and Robust Fragile Watermarking Scheme for Medical Images", *IEEE Access*,vol 6, 2018.
22. Hao Jin,, Yan Luo, eilong Li, Jomol Mathew, " A Review of Secure and Privacy-Preserving Medical Data Sharing", *IEEE Access*,vol 7, 2019.
23. Ashraf Darwish Aboul Ella Hassanien, Mohamed Elhoseny, Arun Kumar Sangiah, Khan Muhammad, "The impact of the hybrid platform of internet of things and cloud computing on healthcare system: opportunities, challenges, and open problems", Journal of Ambient Intelligence and Humanized Computing, December 2017.
24. Al-Dahhan, R. R., Shi, Q., Lee, G. M., & Kifayat, K. (2019). Survey on revocation in ciphertext-policy attribute-based encryption. In *Sensors (Switzerland)* (Vol. 19, Issue 7, pp. 1–22). https://doi.org/10.3390/s19071695
25. Ali, M., Sadeghi, M.-R., & Liu, X. (2020). Lightweight Revocable Hierarchical Attribute-Based Encryption for Internet of Things. *IEEE Access*, *8*, 23951–23964. https://doi.org/10.1109/access.2020.2969957
26. Bansal, S., & Kumar, Di. (2019). IoT Application Layer Protocols: Performance Analysis and Significance in Smart City. *2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019*, 1–6. https://doi.org/10.1109/ICCCNT45670.2019.8944807
27. Bellemou, A. M., García, A., Castillo, E., Benblidia, N., Anane, M., Álvarez-Bermejo, J. A., & Parrilla, L. (2019). Efficient implementation on low-cost SoC-FPGAs of TLSv1.2 protocol with ECC_AES support for secure IoT coordinators. *Electronics (Switzerland)*, *8*(11), 1–18. https://doi.org/10.3390/electronics8111238
28. Chen, X., Liu, Y., Chao, H. C., & Li, Y. (2020). Ciphertext-Policy Hierarchical Attribute-Based Encryption against Key-Delegation Abuse for IoT-Connected Healthcare System. *IEEE Access*, *8*, 86630–86650. https://doi.org/10.1109/ACCESS.2020.2986381
29. Fontaine, C. (2019). *About Homomorphic Encryption Implementation Progresses and Challenges*.
30. Goodman, N., Zwick, A., Spicer, Z., & Carlsen, N. (2020). Public engagement in smart city development: Lessons from communities in Canada's Smart City Challenge. *The Canadian Geographer / Le Géographe Canadien*, *June*. https://doi.org/10.1111/cag.12607
31. Hung, C. W., & Hsu, W. T. (2018). Power consumption and calculation requirement analysis of AES for WSN IoT. *Sensors (Switzerland)*, *18*(6). https://doi.org/10.3390/s18061675
32. Jaloudi, S. (2016). Open source software of smart city protocols current status and challenges. *2015 International Conference on Open Source Software Computing, OSSCOM 2015*. https://doi.org/10.1109/OSSCOM.2015.7372690
33. Jawhar, I., Mohamed, N., & Al-Jaroodi, J. (2018). Networking architectures and protocols for smart city systems. *Journal of Internet Services and Applications*, *9*(1). https://doi.org/10.1186/s13174-018-0097-0
34. Kalmeshwar, M., & K S, A. P. D. N. P. (2017). Internet Of Things: Architecture,Issues and Applications. *International Journal of Engineering Research and Applications*, *07*(06), 85–88. https://doi.org/10.9790/9622-0706048588
35. Khan, M. A., Sargento, S., & Luís, M. (2018). Data collection from smart-city sensors through large-scale urban vehicular networks. *IEEE Vehicular Technology Conference*, *2017-Septe*(August 2019), 1–6. https://doi.org/10.1109/VTCFall.2017.8288308
36. Kölsch, J., Heinz, C., Ratzke, A., & Grimm, C. (2019). Simulation-based performance validation of homomorphic encryption algorithms in the internet of things. *Future Internet*, *11*(10). https://doi.org/10.3390/FI11100218
37. Leveugle, R., Mkhinini, A., & Maistri, P. (2018). Hardware support for security in the internet of things: From lightweight countermeasures to accelerated homomorphic encryption. *Information (Switzerland)*, *9*(5). https://doi.org/10.3390/info9050114
38. Liao, T. L., Lin, H. R., Wan, P. Y., & Yan, J. J. (2019). Improved attribute-based encryption using chaos synchronization and its application to MQTT security. *Applied Sciences (Switzerland)*, *9*(20). https://doi.org/10.3390/app9204454
39. Narayanaswamy, S., & Kumar, A. V. (2019). Application layer security authentication protocols for the internet of things: A survey. *Advances in Science, Technology and Engineering Systems*, *4*(1), 317–328. https://doi.org/10.25046/aj040131
40. Peralta, G., Cid-Fuentes, R. G., Bilbao, J., & Crespo, P. M. (2019). Homomorphic encryption and network coding in IoT architectures: Advantages and future challenges. *Electronics (Switzerland)*, *8*(8), 1–14. https://doi.org/10.3390/electronics8080827
41. Rasori, M., Perazzo, P., & Dini, G. (2020). A lightweight and scalable attribute-based encryption system for smart cities. *Computer Communications*, *149*(May 2019), 78–89. https://doi.org/10.1016/j.comcom.2019.10.005
42. Shahrokni, H., & Brandt, N. (2013). Making sense of smart city sensors. *Urban and Regional Data Management, UDMS Annual 2013 - Proceedings of the Urban Data Management Society Symposium 2013*, *May 2013*, 117–127. https://doi.org/10.1201/b14914-15
43. Suryadevara, N. K., & Biswal, G. R. (2019). Smart plugs: Paradigms and applications in the smart city-and-smart grid. In *Energies* (Vol. 12, Issue 10, pp. 1–20). https://doi.org/10.3390/en12101957

44. Talari, S., Shafie-Khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. P. S. (2017). A review of smart cities based on the internet of things concept. In *Energies* (Vol. 10, Issue 4, pp. 1–23). https://doi.org/10.3390/en10040421
45. Toma, C., Alexandru, A., Popa, M., & Zamfiroiu, A. (2019). IoT solution for smart cities' pollution monitoring and the security challenges. *Sensors (Switzerland)*, *19*(15). https://doi.org/10.3390/s19153401
46. Tsai, K. L., Huang, Y. L., Leu, F. Y., You, I., Huang, Y. L., & Tsai, C. H. (2018). AES-128 based secure low power communication for LoRaWAN IoT environments. *IEEE Access*, *6*, 45325–45334. https://doi.org/10.1109/ACCESS.2018.2852563
47. Tsai, K. L., Leu, F. Y., You, I., Chang, S. W., Hu, S. J., & Park, H. (2019). Low-Power AES Data Encryption Architecture for a LoRaWAN. *IEEE Access*, *7*, 146348–146357. https://doi.org/10.1109/ACCESS.2019.2941972
48. Wang, L., Li, J., & Ahmad, H. (2016). Challenges of fully homomorphic encryptions for the internet of things. *IEICE Transactions on Information and Systems*, *E99D*(8), 1982–1990. https://doi.org/10.1587/transinf.2015INI0003
49. Weize, Y., & Kose, S. (2017). A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *64*(11), 2934–2944. https://doi.org/10.1109/TCSI.2017.2702098

AUTHORS PROFILE

Ms. Sandhya Sarma K N, received her B.Sc degree in Computer Science from Mahatma Gandhi University, Kerala, India. MCA degree from Indira Gandhi National Open University ,Delhi, India and M.Phil from Bharathiar University. She is currently pursuing her Ph.d in Computer Science and working as Assistant Professor for the past 7years in Sahrdaya College of Advanced Studies, Kerala, India. Her core research interests include Cryptography, IoT and Network Security.

Dr. Hemraj Shobharam Lamkuche, is a full-time faculty at Symbiosis Centre for Information Technology, Pune, India. His research experience is around 7 years. His research area is Information Security, Cryptography, Network Security, Network Analysis, Web Security, Embedded System Security, IoT Security, Cryptanalysis of conventional block ciphers, and Data Analytics.

Dr. E.Chandra Blessie, received her MCA from Manonmaniam Sundaranar University, M.Phil from Alagappa University and Ph.D from Karunya University. She has an experience of 23 years in teaching and is currently working as Assistant Professor at Coimbatore Institute of Technology, Coimbatore, India. Her current research area include datamining and deep learning. She has published over 32 papers in peer reviewed journals and international conferences. She is an active member of International Journal of Research in Engineering and Management [Editorial Board Member], Computer Society of India, Coimbatore Chapter [Management Committee Membe]r, Institute of Advanced Scientific[Research .Member], IACSIT International Association of Computer Science & Information [Technology .member] .