International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Privacy Preserving Mechanism for IoT Based Mobile Healthcare Emergency Services

Jagadeesh Kandanuru, V. N. Rajavarman

Abstract: ***The upcoming decade will observe a hazardous development in the frameworks that screen a patient through a body-worn inexpensive individual monitoring devices.In any case, m-Healthcare still faces many difficulties including data security and protection conservation. So we propose a protected and security safe guarding framework called Medical Cyber Physical Systems (MCPS) for m-Healthcare emergency. The obtained information is transmitting to public or private cloud by MCPS for storage and handling.Then the decision is facilitated on acquired data by applying critical system and predicts the health condition.The extensiveness of smart phones and the development of remote body sensor systems (BSNs), and the mobile Healthcare (m-Healthcare), which broadens the task of healthcare supplier into an unavoidable situation for better health screening, have pulled in significant attention recently. The present innovation advancement of the conventional medical model toward the participatory medication. It can help the Internet of Things (IoT) worldview including sensors (environmental, wearable and embedded) spread inside domestic situations with the reason to screen the patient's health and initiate remote support.***

Keywords : Medical Cyber Physical Systems, IOT (Internet of Things),Medical Data Privacy, Body sensor Networks, Mobile Healthcare.

I. INTRODUCTION

The upcoming decade will observer hazardous developments that screen a patient via body-worn inexpensive individual monitoring device in the frameworks that record numerous physiological signals for example ECG and pulse rate [1] [2], or progressively modern devices which measure the physiological markers for example body temperature, EMG and skin resistance [3] [4].The rise of these devices joined with the client alertness for their significance in the personal health monitoring even risen patterns to make such devices trendy [5]. The progress of the patient health monitoring frameworks can be clinically utilised in the improvement of these devices. The details of the patient is acquired by the distributed sensor network and then transmitted to a private cloud or public cloud. The integration of monitoring, obtaining and sharing of data like location and facilities of the hospitals through secure administration layer is characterised as IOT. In basic terms, IOT can be characterized as remote system of devices which conveys through Embedded System devices that can sense and interact within internal states or with external environment without human-machine interaction through internet enabled devices. This technology not only enables the devices to be associated yet in addition robust and comfortable. In order to provide ease to medical users and the doctors IOT plays a very important role. These enormous amounts of shared information and data have to be recorded and analysed in future also and it is a major test. The structure of Internet of Things Analytics (IOTA) is executed to solve such problems. The data is converted to useful medical information using data extraction and data analytics. Getting continuous information from different sources for this situation, area and boundless administrations offered by various emergency clinics for an expansive timeframe has turned out to be simple and quick utilizing the capability of IOT [20]. The crisis healthcare administrations are showing signs of improvement and less exorbitant. Its efficiency is getting improved.

Proposed system goes for the security and protection issues, and builds up a user driven security get to control of opportunistic registering in m-healthcare crisis. The application records several physiological signs for example heart rate, blood sugar, body temperature and blood pressure of the patient. We propose a protected and security safeguarding framework called Medical Cyber Physical Systems (MCPS) for m-Healthcare emergency [5].

The advancement of devices empowered the improvement of these devices that is clinically utilized. The patient's health information is obtained and transmitted over cloud. Patient medical data is encrypted by using AES schemes to provide data privacy during transmission. Results will be provides from the encrypted data by the doctor. Move from a clinically oriented, brought together medicinal services framework to a patient situated, appropriated human services framework.

Manuscript published on January 30, 2020.
* Correspondence Author
Jagadeesh Kandanuru*, Research Scholar, Department of Computer Science & Engineering, Dr. M. G. R. Educational and Research Institute University, Chennai, India. E-mail:drkandanuru@gmail.com
Dr. V. N. Rajavarman, Professor & Deputy Dean, Department of Computer Science & Engineering, Dr. M. G. R. Educational and Research Institute University, Chennai, India. E-mail:nrajavarman2003@gmail.com

Diminish healthcare costs through more productive utilization of clinical assets and prior recognition of medicinal conditions challenges [4]. While the traditional encryption plans were giving just secure storage option, emerging encryption plans also provides secure information sharing and computation.

Assuring the privacy of patient's health details during the transmission from mobile application to server and from server to doctor's web application. Decision support is facilitated in cloud for healthcare experts by applying critical system to the procured information and anticipating patient health condition [2].Definite security examination demonstrates that the proposed system can effectively accomplish user driven protection get to control in m-Healthcare crisis. Also, execution assessments by means of broad recreations demonstrate the practicality of giving high dependable individual information process of the health and transmission though constraining the assurance divulgence in the midst of m-Healthcare crisis[6].

Designing MCPS requires upcoming technological obstacles in establishing the architectural parts of the MCPS and assuring the privacy of patient's health details during the transmission from mobile application to server and from server to doctor's web application. This also involves encryption scheme such as AES to give secure capacity, secure information sharing and computation.

As indicated by the Health Insurance Portability and Accountability Act (HIPAA), within each layer of MCPS information privacy needs to be ensured. Some of the encryption plans guarantee that medicinal information is assessed only by approved users, in this manner giving information protection on confined information squares. Guaranteeing framework level security needs laying out a crypto-outline for the MCPS all things considered. Because of the distinctions in hardware and communication capacities of every layer, assorted encryption plans should be utilized to ensure information protection inside that layer in perspective of their capacity to give secure capacity, information sharing and computation in a MCPS.

II. LITERATURE REVIEW

N. Powers et al (2015) exhibited a platform for executing face acknowledgement on a mobile device. This application is executed in three steps: Face detection can be done on mobile device, projection done on cloudlet and searching on cloud.

A.F. Hani, I. V. Paputungan, M. (2014), introduced private cloud storage plan and model advancement inside an association to illuminate such issues. Utilizing on the capacity of cloud computing is indicated meet to the system requirements. The model is actualized on Own Cloud distributed storage system. The total usefulness of Own Cloud made it a perfect stage to create and send this sort of cloud-based framework. Own Cloud can keep pictures in various file formats and offer such pictures to other.

S. X. et al (2014)depicted test and hypothetical methodologies for utilizing thoughts in soft micro fluidics, controlled mechanical clasping, and organized adhesive surfaces to accomplish ultralow modulus, very stretchable frameworks that fuse gatherings of high-modulus, firm, best in class useful components. The result is a thin, similar device innovation that can delicately cover onto the surface of the skin to empower progressed, multifunctional process for physiological checking in a remote mode.

A. Page et al (2014), proposed a framework that combines health monitoring procedures with scientific techniques to allow the extraction of important data form patient information without trading off protection. The proposition depends on the idea of fully homomorphic encryption (FHE). As the system is known to be source heavy, the papers build up a proof-of-idea to evaluate its reasonableness. Outcomes are displayed from proposed model framework, which copies live QT monitoring and recognition of medication instigated QT prolongation. A.Benharref and M. A. Serhani [2014],proposed a structure to gather patients' information continuously, perform proper non-intrusive observing, and propose medicinal as well as way of commitment at whatever point needed and appropriate. The framework depends on the cloud and the Service Oriented Architecture (SOA), permits a consistent combination of various applications, developments, and organisations. It additionally incorporates adaptable innovations to easily gather and convey key information from wearable Biosensors of the patient while considering the cell phones restricted abilities and power drainage. By then information is secured in the cloud and made accessible by methods for SOA to permit straightforward access by specialists, paramedics or some other allowed component.

S. Babu et al (2013), proposed Open Geo-Spatial Consortium (OGO) standard based remote wellbeing observing framework that permits coordination of sensor and wed utilizing standard electronic interface. The point is to give the information in an open and interoperable way, and diminish information excess. Settled detail is utilized for trade of sensor information all inclusive for all sensor systems. OGC SWE is material to various sensor frameworks including medicinal sensor systems. A standard organization is ported on to cloud which gives scalability, centralised user access, and no Foundation upkeep taken a toll for overwhelming volumes of delicate health information.

D. Kim et al (2012), Advances in materials, mechanics, and assembling now permit development of excellent hardware and optoelectronics in structures that can promptly incorporate with the time-dynamic, delicate, and curvilinear surface of the human body the subsequent capacities make new chances for examining disease states checking health, enhancing surgical techniques, setting up human–machine interface, and accomplishment of different capacities. Above survey compresses these advancements and represents their utilization in structures coordinated with the brain, the skin and the heart.

T. Soyata et al [2012],designed and executed. The MOCHA architecture; cell phones interface with the cloudlet and the cloud by means of numerous associations and utilize dynamic partitioning to accomplish their QoS objectives. Y. Mao et al [2011],

exhibited an early cautioning framework (EWS) projected to detect the indications of clinical disintegration and offer early cautioning to genuine clinical occasions. EWS is intended to give solid early alerts to patients at the general medical clinic wards (GHWs). EWS naturally distinguishes patients in danger of clinical crumbling dependent on their current electronic medicinal record. The fundamental assignment of EWS is a testing characterization issue on high dimensional stream information with unpredictable, multi-scale information holes, estimation blunders, anomalies, and class awkwardness. This paper also describes a novel information digging system for examining such medicinal information streams. The system tends to the above difficulties and speaks to a down to earth approach for early expectation and counteractive action dependent on information that would practically be accessible at GHWs.

III. METHODOLOGY

Innovative uses of IoT technology in healthcare not only bring benefits to doctors and managers to access wide ranges of data sources but also challenges in accessing heterogeneous IoT data, especially in mobile environment of real-time IoT application systems. The big data accumulated by IoT devices creates the problem for the IoT data accessing. Our study provided three main results.

1) It is concluded that IoT is useful in data-intensive industrial applications because it provides a platform to access large scales of data sources in mobile application environment [37]–[41]. With IoT, users can collect more data, which are important to industrial applications such as medical services. Using the data picked up by the IoT devices, managers and analysts can conduct better business analytics.
2) Methodologically, we demonstrate how the heterogeneous IoT data can be accessed ubiquitously. In many IoT applications, smart objects are manifold and moving, so that ubiquitous data accessing is critical to IoT data analysis. Resource-based data model can support accessing data cross-platform by URI through Web for IoT applications.
3) We highlight the use of UDA-IoT in emergency medical services. In emergency medical services, data of patients, doctors, nurses, and ambulances can be collected by IoT notes and transferred to cloud computing platform. In UDA-IoT model, heterogeneous IoT data are encapsulated in unified format of resources with unique URI so as to be accessed ubiquitously. The UDA-IoT is significant to support decision-making in emergency medical services.

In this paper, we focus on unified data model and semantic data explanation by ontology in data storage and accessing. New challenges may exist in industrial sectors involved with long supply chain [42]–[47]; as in these sectors, large numbers of companies are involved and the industry ecology becomes complex. As such it is difficult to apply an unified data model to the entire supply chain. The proposed UDA-IoT method is suitable for information-intensive industries, such as healthcare, in which relatively short value chains are involved that are suitable for applying standard data models through the entire business process.

IV. IOT TECHNOLOGIES IN HEALTH CARE

Wireless Body Area Network (WBAN) comprises of the wireless device which is implanted over the human body to monitoring vital parameter in the remote location [11]. Wireless Personal Area Network (WPAN) comprises of small devices which is accessible by computer wirelessly these devices are a video camera, pressure humidity and so on situated on the body to sense the critical parameters and the data will be transmitted over the internet. Sensors like opto chemical transducer are used for its diverse class of sensing [12]. The gateway connects WBAN and WPAN to World Wide Web which plays sharps and flat role in connecting ad hoc devices with themachine. A gateway can be anything like Personal Digital Assistant (PDA), router, server,a mobile phone, or complete machine [13, 14]. IoT-based ambient assisted living ensures the action of well-being in life and safeguards to the senior people which include an application such as services, products, and so on. One of the principal goals of the ambient helped living is it has the benefits to isolate the economy which has increased efficiency to fortuitous resources for society [15,16].

V. MEDICAL CYBER PHYSICAL SYSTEMS

The progress of remote body sensor systems and mobile healthcare (m-healthcare)develops the operation of healthcare provider into an unavoidable situation for betterhealth monitoring. In any case, m-Healthcare still faces more difficulties containing datasecurity and protection conservation. We propose a protected and security safeguardingframework called Medical Cyber Physical Systems (MCPS) for m-Healthcare emergency.The obtained information is transmitting to public or private cloud by MCPS for storageand handling.

As indicated by the Health Insurance Portability and Accountability Act (HIPAA), within each layer of MCPS information privacy needs to be ensured. Some of the encryption plans guarantee that medicinal information is assessed only by approved users, in this manner giving information protection on confined information squares. Guaranteeing framework level security needs laying out a crypto-outline for the MCPS all things considered.

The architecture of MCPS is shown in Fig 1.The medical user or patient will send the encrypted data through smartphone and that data will be stored on the server. Encryption scheme provides secure computation on server. Then the decision is facilitated on acquired data by applying critical system and predicts the health condition. The results of this will be given to trusted authority.

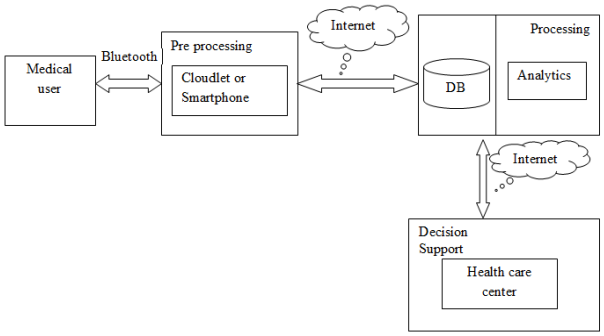

Fig. 1. Architecture of MCPS

The following are the four layers of the MCPS:

A.Data Acquisition Layer

This layer typically consists of wireless wearable sensors i.e., Body Area Network (BAN) [6] which collects the information of the patient and forwards it to the cloudlet or smart phones through Bluetooth or ZigBee protocols.

B.Data Concentration/Aggregation Layer

A cloudlet or smart phone is needed as sensors which makes up BAN has very low computational intensity. Then the sensors transmits the accumulated from the patient to a gateway server, here it acts as cloudlet through Bluetooth. The most vital building block of IOT based design is cloudlet and it aggregates the data from more powerful devices such as smart phone.

C.Cloud Processing and Storage Layer

The most important function of the cloud is to ensure secure storage since exact determination needs long-term monitoring of the patient health information. Also, the government health controls needs the storage of therapeutic records for an all-inclusive measure of time.

Most of the cloud administrators store medical information by consenting to a Business Associate Arrangement (BAA). In theprivate cloud (i.e., data centre) medicinal foundations run their applications, hence utilizing the cloud for the second essential reason: processing.The third main role of the cloud is data analytics the decision is facilitated on acquired data by applying critical system and predicts the health condition. In remote health monitoring systems these procedures have recently gained considerations.

D.Action Layer

This layer consists of either “active” action or “passive” action. In active action, to turn the outcomes of algorithms an actuator is utilised that keep running in the cloud into the enactment of the actuator, for example a robotic arm. Instances of this sort of action are robot assisted surgery.

In passive action, no physical action is really made. To provide decision support the results of the analytics are given to the trusted authority.

VI. SPOC FRAMEWORK (SECURE AND PRIVACY-PRESERVING OPPORTUNISTIC COMPUTING)

In m-healthcare emergency SPOC framework [19] aims at privacy and security problems. It advances a user-centric protection access control of opportunistic computing.With SPOC, the assets which are accessible on other opportunistically reached patients smart phones assembled to manage with the registering PHI process in crisis condition.Since the PHI will be uncovered amid the procedure in opportunistic computing, to limit the PHI security disclosure, SPOC presents a client driven two–stage protection get to control to just permit the medical users who have same symptom and also it introduce an effective client driven privacy access in *this* framework. Definite security examination demonstrates that the proposed system can effectively accomplish user driven protection get to control in m-Healthcare crisis. Moreover, performance assessments by means of broad simulations exhibit the SPOC’s viability in term of giving high reliable PHI process and transmission while limiting the security discovery amid m-Healthcare crisis.

Patient’s personal health information (PHI) like blood sugar level, heartbeat,blood pressure and body temperature can be collected first from the BSN then via Bluetooth all the information are collected by smart phone. Finally, via 3G networks all the information is further transmitted to the health care centre. At healthcare centre based on the collected information from the patients can continuously monitor the health condition of the patients and rapidly respond to the patient’s conditions and dispatch the ambulance to save their lives to an emergency location in a timely manner [21].

The SPOC framework for healthcare emergency is shown in Fig 2.

Advantages:

- Shift from hospital oriented, centralised healthcare system to a patient oriented, distributed healthcare system.
- Performance, Reliability, Scalability, QoS, Privacy, Security.
- Diminish the healthcare prices via further efficient utilise of clinical assets and earlier detection of medical conditions challenge.

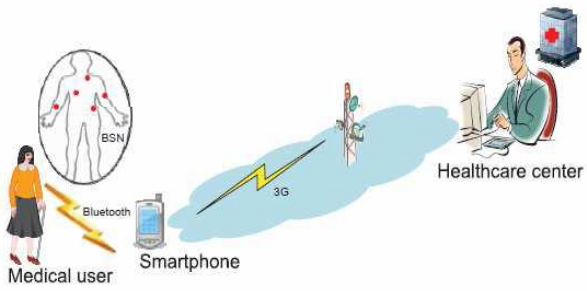

Fig. 2. SPOC framework for mobile healthcare emergency

VII. DATA PRIVACY USING CONVENTIONAL ENCRYPTION SCHEME

Here we use AES encryption scheme to provide security to the m–healthcare services and it has been majorly used because of its lower resource requirements co pared to other encryption schemes.

Advanced Encryption Standard (AES)

This is an encryption algorithm which is accepted as government application standard. AES is a symmetric key encryption algorithm. AES allows running on the 8-bit microcontroller to high end desktops and servers due to its low resource intensity.

Algorithm: AES Encryption

input : Plaintext Block ptxtb, Secret Key sk
output: AES state state
state = InitState(ptxtb, sk)
AddKey(state, sk0)
for i = 1 **to** nr _ 1 **do**
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddKey(state, keyi)
SubBytes(state)
ShiftRows(state)
AddKey(state, keynr_1)

VIII. RESULTS

We compared our research work with several other inter-organizational group decision support systems (GDSSs), as shown in Table I.

In Table I, the comparison result shows that various types of methods are adopted in the development of the DSSs, including Model-Driven Architecture, knowledge-centered[26]–[35], activ- ity-centered and user-centered, to support inter-organizational cooperation. With the use of smart devices, mobile computing is an important feature in today's decision support systems [36]. Datamodels,whichcansupportdataaccessefficientlyandconv e- niently, play critical roles in the architecture of the mobile DSSs.

Features	UDA-IoT	Emergency DSS [22]	MECDSS[23]	Mobile DSS [24]
Data model	Resource model	MySQL	Data warehouse	Fuzzy preference relations
Business process management	√	×	√	×
Heterogeneous data integrating	√	×	√	×
Development methodology	MDA	Knowledge-centered	Activity-centered	User-centered
Mobile computing	√	×	×	√
Software architecture	Restful	Java EE	SOA	M-Internet

Table I: comparison of our method with several other GDSSS

IX. CONCLUSION

The purpose of this discussion is to save the life of critical stage patients and the authorized user can able to monitor the details of the patient and their health condition continuously. Secure computation and storage requirements provided using AES encryption.Then the decision is facilitated on acquired data by applying critical system and predicts the health condition. In this paper, we presented a Medical Cyber Physical Systems (MCPS) which is equipped for transmitting the obtained patient information to a private or public cloud for capacity and processing. For m- Healthcare crisis, we also presented a Secure and Privacy Preserving Opportunistic Computing (SPOC) structure, which basically exploits how to utilisethe opportunistic computing to accomplisha high reliability quality of PHI process and transmission in emergency while restricting the insurance exposure amid the opportunistic computing.IoT has broad application and uses throughout several areas still growth of internet of things in healthcare domain is preeminent hence this comprehensive review discusses in detail about attacks in healthcare systems and its similar IoT technologies. IoT helps both doctor and patients simultaneously because the patients are monitored all the time by other hand doctors also receives all the necessary information thereby this becomes a notice requirement in the medical field. The future work would be placing the nanosensors with minimum power consumption and minimum maintainers along the secured architecture were security challenges to be considered as the significant part of the work.

REFERENCES

1. N. Powers, A. Alling, K. Osolinsky, T. Soyata, M. Zhu, H. Wang, H. Ba, W. Heinzelman, J. Shi, and M. Kwon, "The cloudlet accelerator: Bringing mobile-cloud face recognition into realtime," in Globecom Workshops (GC Wkshps), Dec 2015
2. A. F. Hani, I. V. Paputungan, M. F. Hassan, V. S. Asirvadam, and M. Daharus, "Development of private cloud storage for medical image research data," in Int. Conf. on Computer and Inf. Sciences (ICCOINS), June 2014, pp. 1–6.
3. S. X. et al., "Soft microfluidic assemblies of sensors, circuits, and radios for the skin," Science, vol. 344, pp. 70–74, 2014.
4. A. Page, O. Kocabas, T. Soyata, M. K. Aktas, and J. Couderc, "Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance," Annals of NoninvasiveElectrocardiology (ANEC), vol. 20, no. 4, pp. 328–337, 2014.
5. A. Benharref and M. A. Serhani, "Novel cloud and SOA-based framework for E-Health monitoring using wireless biosensors," IEEE Journal of Biomed. and Health Inf., vol. 18, no. 1, pp. 46–55, Jan 2014.
6. S. Babu, M. Chandini, P. Lavanya, K. Ganapathy, and V. Vaidehi, "Cloud-enabled remote health monitoring system," in Int. Conf. on Recent Trends in Inform. Tech. (ICRTIT), July 2013, pp. 702–707.
7. D. Kim, R. Ghaffari, N. Lu, and J. A. Rogers, "Flexible and stretchable electronics for biointegrated devices," Annual Review of Biomedical Engineering, pp. 113–128, 2012.
8. T. Soyata, R. Muraleedharan,C. Funai, M. Kwon, and W. Heinzelman, "Cloud-Vision: Real-Time Face Recognition Using a Mobile-Cloudlet-Cloud Acceleration Architecture," in IEEE Symposium on Computers and Communications, Jul 2012, pp. 59–66.
9. Y. Mao, Y. Chen, G. Hackmann, M. Chen, C. Lu, M. Kollef, and T. C. Bailey, "Medical data mining for early deterioration warning in general hospital wards," in IEEE 11th Int. Conf. on Data Mining Workshops (ICDMW), Dec 2011, pp. 1042–1049.
10. A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systemsfor health monitoring and prognosis," IEEE Trans. Sys., Man, and Cybernetics, Part C: Applic, and Reviews, vol. 40, no. 1, pp. 1–12, Jan 2010.
11. Wang, C., Wang, Q. and Shi, S., 2012, May. A distributed wireless body area network for medical supervision. In Instrumentation and Measurement Technology Conference (I2MTC), 2012 IEEE International (pp. 2612-2616). IEEE.
12. Vaidiyanathan. R, B. Anand. Opto chemical Transducers of GaInN Quantum glowing structure of Biosensor and Chemical Sensors for Health Care System. Research J. Pharm. and Tech 2017; 10(12): pp. 4362-4364.

13. Meingast, M., Roosta, T. and Sastry, S., 2006, August. Security and privacy issues with healthcare information technology. In Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE (pp. 5453-5458). IEEE.
14. Barakah, D.M. and Ammad-Uddin, M., 2012, February. A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture. In Intelligent Systems, Modelling and Simulation (ISMS), 2012 Third International Conference on (pp. 214-219). IEEE.
15. Georgieff, P., 2008. Ambient assisted living. Marktpotenziale IT-unterstützterPflegefüreinselbstbestimmtesAltern, FAZIT Forschungsbericht, 17, pp.9-10.
16. Takács, B. and Hanák, D., 2007. A mobile system for assisted living with ambient facial interfaces. IADIS Int. J. Comput. Sci. Inf. Syst, 2, pp.33-50.
17. Shuichi, W., Peijie, J., Chunlan, Y., Haomin, L. and Yanping, B., 2010. The development of a telemonitoring system for physiological parameters based on the B/S model. Computers in biology and medicine, 40(11), pp.883-888.
18. Fei, D.Y., Zhao, X., Bianca, C., Hughes, E., Bai, O., Merrell, R. and Rafiq, A., 2010. A biomedical sensor system for real-time monitoring of astronauts' physiological parameters during extra-vehicular activities.Computers in biology and medicine, 40(7), pp.635-642.
19. M. Conti, S. Giordano, M. May, and A. Passarella, "From opportunistic networks to opportunistic computing," IEEE Communications Magazine, vol. 48, pp. 126–139, September 2010
20. Suriya Begum and venugopal, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.3, March- 2016, pg. 59-66
21. Rongxing Lu, Xiaodong Lin, and Xuemin (Sherman) Shen, "SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare
22. Emergency" IEEE transactions on parallel and distributed systems, 2012.
23. P Krishna Kishore, "An Authentication of Significant security for accessing Password through Network System" volume.12, pages.3130-3133, publisher: http://www.ripublication.com, International Journal of Applied Engineering Research, 2017.
24. P Krishna Kishore, "An efficient probability of detection model for wireless sensor networks" pages. 585-593, book. Proceedings of the First International Conference on Computational Intelligence and Informatics, publication date:2017, publisher: Springer, Singapore.
25. P Krishna Kishore, "DITFEC: Drift Identification in Traffic-Flow Streams for DDoS Attack Defense Through Ensemble Classifier" book: Computing and Network Sustainability, pages. 299-307, publisher: Springer, Singapore, 2019.
26. P Krishna Kishore, "Detection, Defensive and Mitigation of DDoS Attacks through Machine learning Techniques: A Literature" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, pages. 2719-2725, November 2019.

AUTHORS PROFILE

Jagadeesh Kandanuru, Research Scholar, Department of Computer Science & Engineering, Dr.M.G.R Educational and Research Institute University, Chennai. drkandanuru@gmail.com

Dr. V.N Rajavarman, Professor & Deputy Dean in Dr. M.G.R Educational and Research Institute,chennai, Ph.D, Computer Science, Dr. M.G.R Educational and Research Institute, Chennai, India.M.E, Information Technology, VMRF University, salem, India.M.Sc, Computer Science, Bharathidasan University, India. Published more than 30 research articles in various scopus journals, Published more than 30 articles in International Conferences, research Supervisor for nearly 10 Research Scholors, Life time Member of The Computer Society of India (CSI), IAENG: Member Number: 173582, SDIWC Member, Microsoft Certified Technical Analyst (MCTA) – Software Development Fundamentals.