Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2021)
Vol.03/ No.03
Pages: 150-163
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2021.3.001

A Review on Data Securing Techniques using Internet of Medical Things

P. P. Joby

Professor, Department of Computer Science and Engineering, St. Joseph's College of Engineering and Technology, Kerala

E-mail: jobypcse@gmail.com

Abstract

At present, the traditional healthcare system is completely replaced by the revolutionary technique, the Internet of Medical Things (IoMT). Internet of Medical Things is the IoT hub that comprises of medical devices and applications which are interconnected through online computer networks. The basic principle of IoMT is machine-to-machine communication that takes place online. The major goal of IoMT is to reduce frequent or unwanted visits to the hospitals which makes it comfortable and is also highly preferred by the older people. Another advantage of this methodology is that the interpreted or collected data is stored in cloud modules unlike amazon and Mhealth, making it accessible remotely. Although there are countless advantages in IoMT, the critical factor lies in data security or encryption. A surplus number of threat related to devices, connectivity, and cloud might occur under unforeseen or threatening circumstances which makes the person in the situation helpless. Yet, with the help of data security techniques designed especially for Internet of Medical Things, it is possible to address these challenges. In this paper, a review on data securing techniques for the internet of medical things is made along with a discussion on related concepts.

Keywords: Internet of Medical Things, Medical Devices, Data Securing Technique, Privacy, Security Threat, Medical Applications

ISSN: 2582-337X
Submitted: 21.07.2021
Revised: 29.08.2021
Accepted: 15.09.2021
Published: 27.09.2021

1. Introduction

Internet of Medical Things (IoMT) is a progressive version [1] of IoT which plays an important role in health care. It contains multiple nodes which are systematized into a set of IoT medical devices. It increases the quality of the patient’s treatment and the responses time of the treatment. IoMT devices are used to curtain the patients in their homes [2]. It also provides many services like improving health care services, data analysis, low-cost services [3], diseases management [4], and patient experience. Table-1 shows us the category and features of medical devices used in the IoMT system:

Table 1. Category and Features of medical devices used in IoMT system

Device type	**Placement**	**Example**	**Risk value**
Implantable	Within the human tissues	Deep brain implants [5], heart pacemaker, and insulin pump [6]	High
Wearable	On the human body	Smart watches [7], fitness devices	Low
Ambient	Outside the human body	Elderly monitoring devices in smart home [8]	Low
Stationary	Inside hospitals	Medical image processing devices of MRI [9] and CT- scan	Low

1.1 Architecture of IoMT Systems

IoMT systems are divided into sensor layer [10], gateway layer, cloud layer, and visualization layer that are given as a layered architecture in Figure 1.

1. **Sensor Layer**: This layer collects the patient’s biometrics in worn sensors or small implanted sensors [11].

2. **Gateway Layer**: In this layer, the processing operations such as data storage, analysis, and validations are done. The Patient's smartphone or an Access Point [12] is the devices in this layer.

3. **Cloud Layer**: This layer is responsible for getting the data from the gateway for secure access, analysis, and storage. The (KGS) key generation server [13] is answerable for creating id's of various patients.

4. **Visualization or Action Layer:** The data of the patients are presented to the physicians to track their health [14]. This layer contains the actions suggested by the physicians based on the patients' health conditions.

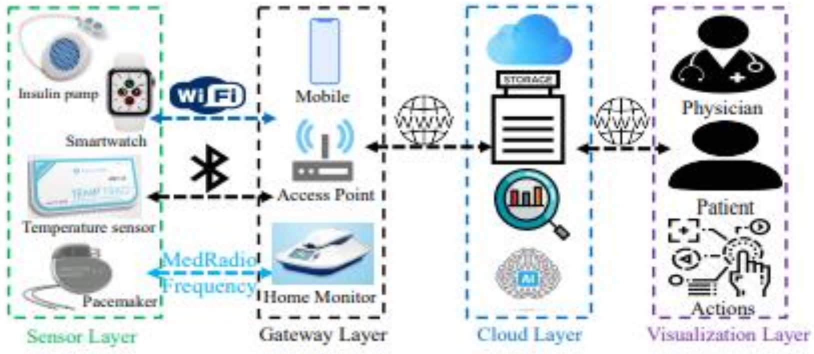

Figure 1. IoMT system architecture

1.2 IoMT Threats

The data collected through the IoMT of the patients [15] should be protected in all the stages such as collection [16], storage, and transmission. It can be clearly explained using the four architectures [17] of the IoMT.

1. **Data Collection:** In the sensor layer of the IoMT system the patient's data [18] is collected. Data tampering and sensor hardware manipulation attacks can take during this stage.

2. **Data in transit:** This stage tells about the communication between all four layers in IoMT devices. Outbreaks can manipulate [19] or block the data in this stage.

3. **Data in storage:** Once the patient's data are processed it is stored in the cloud layer. In this stage, the patient's data may be stolen [20].

1.3 IoMT Security Requirements

The patient's data should be safe and secured in IoMT systems. Hence the necessary parameters are gathered from CIANA [21].

1. **Integrity:** Integrity is connected to the competence of shielding the data from any unofficial damaging during the collection, transmission, and storage.

2. **Availability:** The data of every patient should be updated and monitored continuously in the IoMT system.

3. **Non-repudiation:** These prerequisite securities that any communication in the system cannot be deprived of. The Digital signature technique [22] can be applied here to avoid such threats.

4. **Authentication:** The authenticated user only has the right to execute the commands to which they are authorized. It can be achieved only through using proper data encryption and access techniques.

5. **Confidentiality or Privacy:** The data of every patient in the IoMT systems should be kept confidential [23]. The common technique is to attain this requirement is data encryption and access control lists.

6. **Obscurity:** The data of the patients and the physicians should be kept hidden from unauthorized users. The Smart card can fulfil this obligation [24].

ISSN: 2582-337X
Submitted: 21.07.2021
Revised: 29.08.2021
Accepted: 15.09.2021
Published: 27.09.2021

2. Related Works

The A module to secure data in the IoMT systems is demonstrated in [25]. Along, a set of techniques, an overview of IoMT systems, security model, or a framework is also designed for better understanding. The proposed framework can solve most of the privacy threats but yet the need for a more secured framework to overcome challenges persists [26]. According to the authors of [27], it is found that only a little importance is paid to data protection in IoMT systems. It is because of the complication and alteration difficulties of a huge amount of data. So, a review of 153 papers was done to cover the security issues and the possible solutions. In [28], the basic architecture of the IoMT system, present operations of I0MT in healthcare sectors, related case studies, and emerging techniques were outlined. The working pattern of platforms like blockchain, & AI and their associated challenges were given. In [29], the authors have investigated factors like privacy issues, security attacks and vulnerability. Further, an analytic network process is also proposed and implemented using ISO27002 standard to put a full stop to such threats. As most of the data are confined to IoMT devices are vulnerable to Ransomware there is a high need for privacy, suggests the authors of [30]. A study over the possible privacy issues, attacks are carried out throughout and some of the best practices to ensure end-to-end encryption and overall integrity is also discussed.

3. Data Securing Techniques in IoMT

In this session, a detailed review of security risks, different attacks on the layer, and different data security techniques associated with IoMT systems is given.

3.1 IoMT Security Requirements

As said before there are countless security threats possible in IoMT systems. Some of the risks associated with IoMT layers include: data exposure, financial loss and life risk. As data is a vital part of the medical field, there are times where an intruder exploits such medical devices and lead to data exposure. When a system or device encounters hacking methodology

ISSN: 2582-337X
Submitted: 21.07.2021
Revised: 29.08.2021
Accepted: 15.09.2021
Published: 27.09.2021

the recovery plan or backup needs to be secured this, in turn, raises the overall financial budget. If a data leakage occurs in the medical device that is directly associated with the patient, the destined functionality gets interrupted, and hence the life of the patient is put at risk.

3.2 Portrayals of threats of each layer in IoMT Environment

The attacks concerned with each layer of IoMT Architecture are given a detailed view in Figure 2.

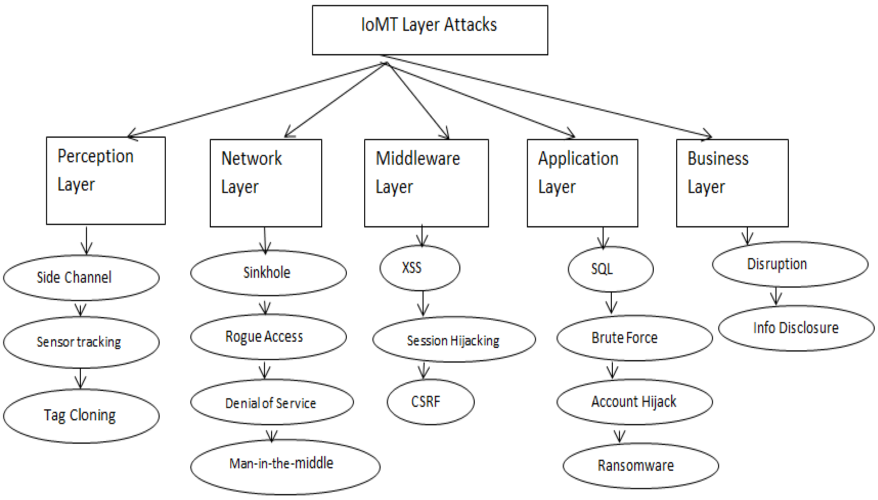

Figure 2. Extortions of attacks in IoMT Environment

3.3 Portrayals of threats of each layer in IoMT Environment

The different security techniques to protect the IoMT medical devices can be easily understood by viewing the below figure 3.

Symmetric Cryptography includes the algorithm based on an undisclosed and collective key between two or further nodes which need to be communicated. Without any prior setup, one can secure patient data in IoMT systems using hierarchical access which is a branch in symmetric cryptography. With the help of hierarchy access, one can take control of data security stored in the cloud layer. In this technique, a hierarchy model is developed where based on authorized access encryption and decryption is performed.

a. *Wireless signal characteristics*: This technique operates by making keys without the help of any previous networks. This technique has the capability to produce its own keys and operate on them.

b. *Gait*-based *Technique*: When it comes to the case of gait patterns related to patients, these walking designs are used to generate symmetric keys which are used in the future to safeguard the communications between the IoMT sensors. One of the popular models of this technology is recognized to be the one crafted by sun and lo.

c. *Facial Recognition:* Facial recognition is the one-way mode of data securing technique where authentication fully relies on the facial recognition of the patient.

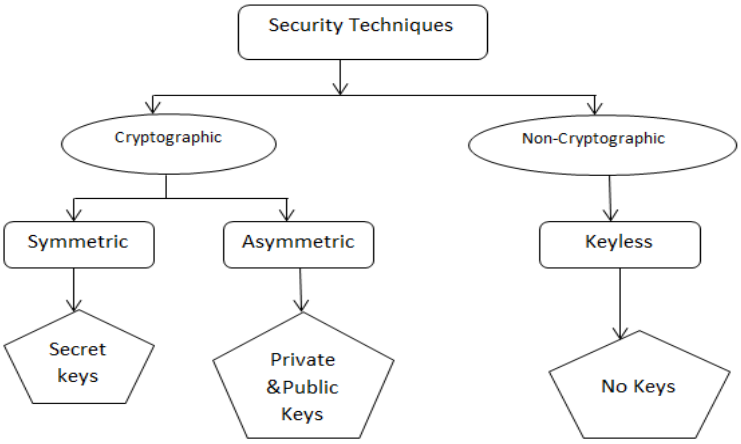

Figure 3. Security Techniques in IoMT Environment

Asymmetric Cryptograph: In the case of asymmetric cryptograph two keys are used, likely: public and private keys. As its name suggests, the public key is known by everyone,

ISSN: 2582-337X
Submitted: 21.07.2021
Revised: 29.08.2021
Accepted: 15.09.2021
Published: 27.09.2021

whereas, the private key is kept secret with the owner. This mode of cryptography is used in smart cards, Digital Signatures, and in ways of implementing two-step authentications.

a. *Homomorphic Encryption*: It is the easiest mode of asymmetric cryptography that includes limited mathematical interpretation for encryption/decryption, but yet offers a high degree of privacy. Homomorphic Encryption is found in a smartwatch where data is encrypted end-to-end making it accessible only by the patient and not even the medical staff except in case of emergency.

b. *Digital Signatures*: Implemented digitally, Digital Signature finds application even in small IoMT systems. Carried out entirely with the help of the sender's asymmetric keys the overall process like encryption verification, decryption is done. With additional software, Digital Signature can be integrated into a sensor network as well.

Keyless Non-Cryptographs: While the above-mentioned data securing techniques are based on key usage, this sort of non-cryptographic methodology is used in biometrics. Some of the sub-related tactics include:

a. *AI and Blockchain Technology:* Due to the successful record in the field of finance, Blockchain and AI are now implemented in IoMT Environment. As a mixture, both are used in security management and anonymous detection.

b. *Biometrics:* In order to enhance additional security in IoMT devices Biometric mode of operation that involves the patient's fingerprint or ECG sensors are now implemented.

4. Data Securing Techniques in IoMT

From the overall review and interpretation of data securing techniques for IoMT techniques and their related concepts, we can arrive at some results. It is found that the basic need is a security requirement of an IoMT system that comes under four factors like: Malware Deduction, Intrusion detection, Authentication and Access Control, and Anomaly detection. The discrimination in the form of a chart is given in Figure 4.

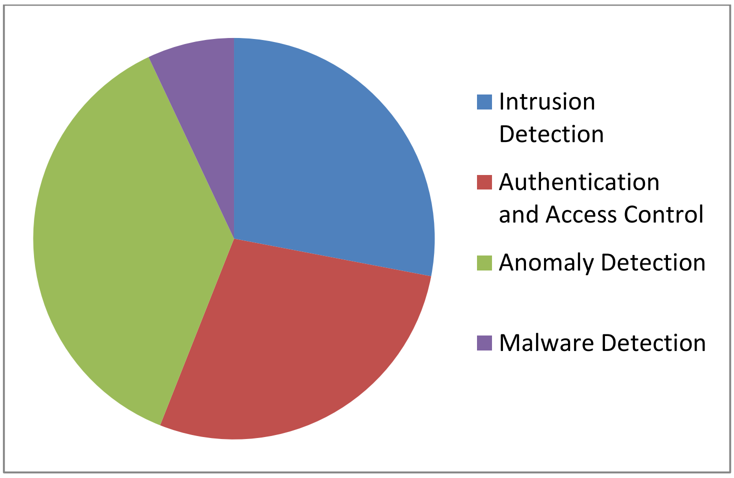

Figure 4. Security Requirements of IoMT System

When it comes to Architecture implementation or model design there are countless hardware choices among which are Arduino, Raspberry, FPGA, Smart Watch, Insulin Pump, Palm PDA. The percentage or level of practice is given in Figure 5.

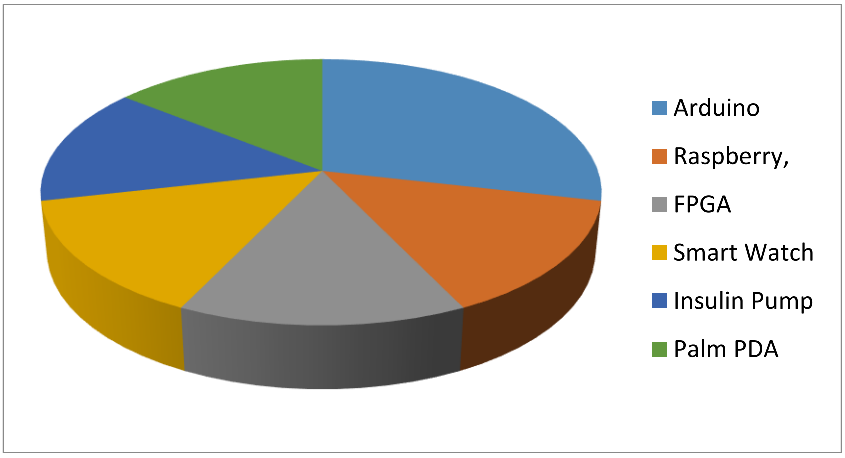

Figure 5. Different Hardware Implementation of IoMT Systems

ISSN: 2582-337X
Submitted: 21.07.2021
Revised: 29.08.2021
Accepted: 15.09.2021
Published: 27.09.2021

Finally, when a comparison or interpretation is made on the data securing techniques for IoMT devices it can be found from Figure 6 that all three sub divisions unlike Symmetric, Asymmetric, and keyless methodologies find equal importance irrespective of the field of implementation like Gait, Digital Signature, and Biometric.

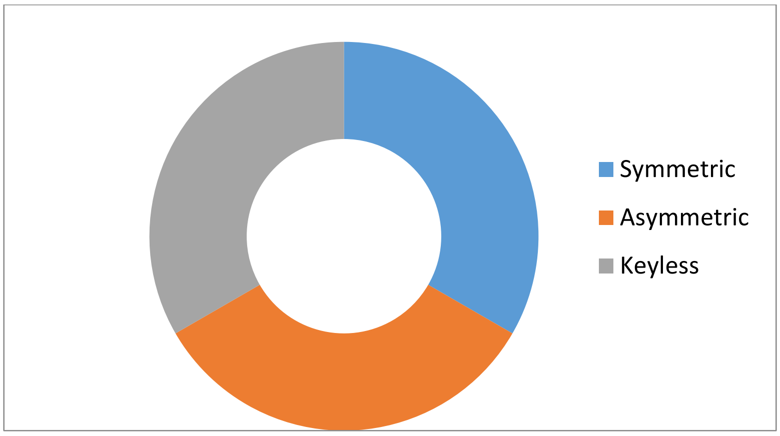

Figure 6. Comparison of Data Securing Techniques

5. Conclusion

When compared to the traditional medical systems IoMT devices, and applications are foremost appreciable in terms of high data integrity, privacy management and data management. With integration to cloud and modern devices like Smartwatch, Biometrics, Token System, Facial Recognition, Gait, Digital Signature and so on IoMT devices prove to the point that they are undoubtedly the best advancement in the field of medical application. In this paper, a review of different IoMT concepts like its associated privacy threats, basic architecture, and the Data Security Techniques that are in prevalence is carried out. Finally, a few results or comparisons on different factors and techniques were also made for better understanding. Although these techniques work better, there is still a need for a one-stop solution to work on the security issues and hence as future work, the existing platforms like Big Data and Deep Learning can also collaborate in IoMT applications.

ISSN: 2582-337X
Submitted: 21.07.2021
Revised: 29.08.2021
Accepted: 15.09.2021
Published: 27.09.2021

References

[1] Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A. K., & Jain, R. (2020). Recent advances in the internet of medical things (iomt) systems security. IEEE Internet of Things Journal.

[2] Vachhani, Hrishikesh, Mohammad S. Obiadat, Arkesh Thakkar, Vyom Shah, Raj Sojitra, Jitendra Bhatia, and Sudeep Tanwar. "Machine learning based stock market analysis: A short survey." In International Conference on Innovative Data Communication Technologies and Application, pp. 12-26. Springer, Cham, 2019.

[3] Hameed, S. S., Hassan, W. H., Latiff, L. A., & Ghabban, F. (2021). A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. PeerJ Computer Science, 7, e414.

[4] Sathye, Rohit, Sumedh Deshprabhu, Mandar Surve, and Deepak C. Karia. "Smart Medicine Distributing Tray." In International Conference on Innovative Data Communication Technologies and Application, pp. 57-66. Springer, Cham, 2019.

[5] Razdan, S., & Sharma, S. (2021). Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. IETE Technical Review, 1-14.

[6] Nene, Rajas, Pranay Narain, M. Mani Roja, and Medha Somalwar. "Fourier Descriptors Based Hand Gesture Recognition Using Neural Networks." In International Conference on Innovative Data Communication Technologies and Application, pp. 140-147. Springer, Cham, 2019.

[7] Smys, S., and Wang Haoxiang. "Data Elimination on Repetition using a Blockchain based Cyber Threat Intelligence." IRO Journal on Sustainable Wireless Systems 2, no. 4 (2021): 149-154.

[8] Raj, Jennifer S. "Security Enhanced Blockchain based Unmanned Aerial Vehicle Health Monitoring System." Journal of ISMAC 3, no. 02 (2021): 121-131.

[9] Huang, X., & Nazir, S. (2020). Evaluating security of internet of medical things using the analytic network process method. Security and Communication Networks, 2020.

[10] Hiremath, Shivarajkumar, and R. Sanjeev Kunte. "Public Auditing Scheme for Cloud Data Integrity Verification." In International Conference on Innovative Data Communication Technologies and Application, pp. 237-246. Springer, Cham, 2019.

[11] Manjunath, T. D., S. Samarth, Nesar Prafulla, and Jyothi S. Nayak. "Hopfield Network Based Approximation Engine for NP Complete Problems." In International Conference on Innovative Data Communication Technologies and Application, pp. 319-331. Springer, Cham, 2019.

[12] Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., & Tsatsoulis, C. (2019, May). Review of security and privacy for the Internet of Medical Things (IoMT). In 2019 15th international conference on distributed computing in sensor systems (DCOSS) (pp. 457-464). IEEE.

[13] Valanarasu, Mr R. "Comparative Analysis for Personality Prediction by Digital Footprints in Social Media." Journal of Information Technology 3, no. 02 (2021): 77-91.

[14] Yaacoub, J. P. A., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R., & Chehab, A. (2020). Securing internet of medical things systems: limitations, issues and recommendations. Future Generation Computer Systems, 105, 581-606.

[15] Smys, S., and Jennifer S. Raj. "Analysis of Deep Learning Techniques for Early Detection of Depression on Social Media Network-A Comparative Study." Journal of trends in Computer Science and Smart technology (TCSST) 3, no. 01 (2021): 24-39.

[16] Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: a review. Security and Communication Networks, 2018.

[17] Joe, Mr C. Vijesh, and Jennifer S. Raj. "Location-based Orientation Context Dependent Recommender System for Users." Journal of trends in Computer Science and Smart technology (TCSST) 3, no. 01 (2021): 14-23.

[18] Mawgoud, A. A., Karadawy, A. I., & Tawfik, B. S. (2019). A secure authentication technique in internet of medical things through machine learning. arXiv preprint arXiv:1912.12143.

[19] Haoxiang, Wang, and S. Smys. "Big Data Analysis and Perturbation using Data Mining Algorithm." Journal of Soft Computing Paradigm (JSCP) 3, no. 01 (2021): 19-28.

[20] Shirley, D. R. A., Ranjani, K., Arunachalam, G., & Janeera, D. A. (2021). Automatic Distributed Gardening System Using Object Recognition and Visual Servoing. In Inventive Communication and Computational Technologies (pp. 359-369). Springer, Singapore.

[21] Chakrabarty, Navoneel. "A Regression Approach to Distribution and Trend Analysis of Quarterly Foreign Tourist Arrivals in India." Journal of Soft Computing Paradigm (JSCP) 2, no. 01 (2020): 57-82.

[22] Shirley, D. R. A. (2014, July). Systematic diagnosis of power switches. In 2014 International Conference on Embedded Systems (ICES) (pp. 32-34). IEEE.

[23] Bhalaji, N. "Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks." Journal of ISMAC 2, no. 02 (2020): 106-117.

[24] Shirley, D., Sundari, V. K., Sheeba, T. B., & Rani, S. S. (2021). Analysis of IoT-Enabled Intelligent Detection and Prevention System for Drunken and Juvenile Drive Classification. In Automotive Embedded Systems (pp. 183-200). Springer, Cham.

[25] Valanarasu, Mr R. "Comparative Analysis for Personality Prediction by Digital Footprints in Social Media." Journal of Information Technology 3, no. 02 (2021): 77-91.

[26] Senthilkumar, M., Kavitha, V. R., Kumar, M. S., Raj, P. A. C., & Shirley, D. R. A. (2021, March). Routing in a Wireless Sensor Network using a Hybrid Algorithm to Improve the Lifetime of the Nodes. In IOP Conference Series: Materials Science and Engineering (Vol. 1084, No. 1, p. 012051). IOP Publishing.

[27] Smys, S., and Wang Haoxiang. "Naïve Bayes and Entropy based Analysis and Classification of Humans and Chat Bots." Journal of ISMAC 3, no. 01 (2021): 40-49.

[28] Dhaya, R. "Flawless Identification of Fusarium Oxysporum in Tomato Plant Leaves by Machine Learning Algorithm." Journal of Innovative Image Processing (JIIP) 2, no. 04 (2020): 194-201.

[29] Duraipandian, M. "Adaptive Algorithms for Signature Wavelet recognition in the Musical Sounds." Journal of Soft Computing Paradigm (JSCP) 2, no. 02 (2020): 120-129.

[30] Dash, Devidutta, Arun Agarwal, Kabita Agarwal, and Gourav Misra. "Post Catastrophe Fallouts and Challenges to Swim to Safety." Journal of Information Technology 3, no. 01 (2021): 12-17.

Author's biography

P. P. Joby is currently a Professor, in the Department of Computer Science and Engineering. St. Joseph's College of Engineering and Technology, Kerala. His research area includes Machine Perception, Robotics, Cyber-Physical Systems, Internet of Things, Complex Networks, Quantitative Network-based modelling, Complex and Intelligent Systems, Networks, Recommendation System, Human-Computer Interface, and Knowledge Representation.

ISSN: 2582-337X
Submitted: 21.07.2021
Revised: 29.08.2021
Accepted: 15.09.2021
Published: 27.09.2021