Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

Review on Data Securing Techniques for Internet of Medical Things

R. Kanthavel

Department of Computer Engineering, King Khalid University, Abha, Kingdom of Saudi Arabia

E-mail: kanthavel2005@gmail.com

Abstract

In recent days Internet of Things (IOT) has grown up dramatically. It has wide range of applications. One of its applications is Health care system. IOT helps in managing and optimizing of healthcare system. Though it helps in all ways it also brings security problem in account. There is lot of privacy issues aroused due to IOT. In some cases it leads to risk the patient's life. To overcome this issue we need an architecture named Internet of Medical Things (IOMT). In this paper we have discussed the problems faced by healthcare system and the authentication approaches used by Internet of Medical Things. Machine learning approaches are used to improvise the system performance.

Keywords: Internet of Things (IOT), healthcare system, Internet of Medical Things (IOMT), authentication, machine learning

1. Introduction

The medical field has been growing each and every day with the advancement in current trends. The Internet of things plays vital role in health care system [1]. These are categorized under Internet of Healthcare system and a special attention is given to Internet of Medication things. This is due to the security threats developed in medical field. We use sensors to predict the patient's health condition and these are stored in clouds [2-5]. The privacy issue and security threads occur there. This is very handy embedded device which is smart wearable one. Eavesdropping and denial of service (DoS) makes IoMT inefficient. These authentication

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

problems must be rectified to improve the system performance. We have to concentrate more on authentication, privacy, encryption, insecure interfaces and insecure software [3]. The device must be only operated by authenticated users. To preserve the systems security we have to ensure the authentication between user and device. This helps to maintain patient's medical history and defend their privacy [4]. The network and system can be maintained with the help of public key cryptography. Since the IoT devices are small and wearable they are designed with low battery conception this restricts few of cryptographic methods. It requires very high security mechanism compare to IoT [5].

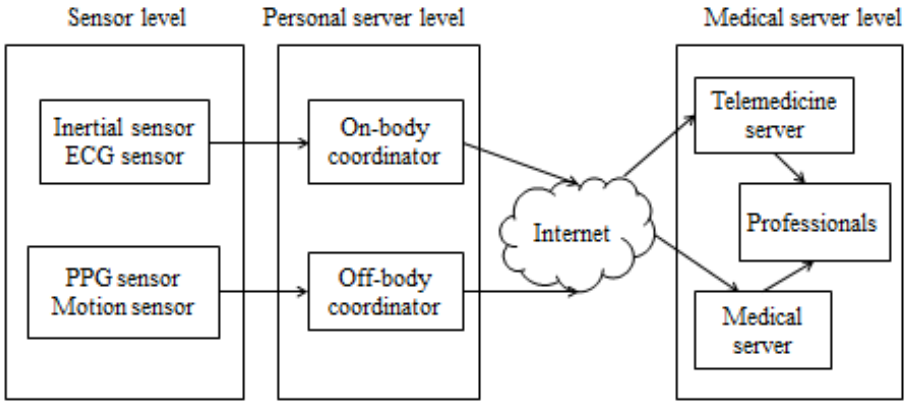

Figure 1. General architecture of IoMT-based Healthcare system

2. Related Work

Authentication plays major role in providing security. The main challenge is also present in this stage. There are various challenges in providing accurate authentication [6]. The remote authentication challenge requires authentication for every action. It monitors the authentication regularly and checks for the mismatch. User has to provide proper authentication key each and every time and the system checks for the match and provide authorization [7]. The security depends on the system verification method. To provide privacy and trust factor SVM verification method is used. It provides security by using classifiers [8]. The server notifies the user regularly to give a key to get access. It maintains trust factor by establishing a

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

network where it can be completely demonstrated by the user. It performs as per the wish of user's demonstration [9]. The feature classification is made as user's demonstration. The decision making authority is given to the user. The server generates token with real and non-real SVM classifier [10]. The user has to differentiate it and it is considered as the authentication key [11]. Here the user only decides the feature so while differentiation a attacker has no knowledge about the SVM so it provides security and privacy. It is based on machine learning approach [12].

3. Internet Of Medical Things (IOMT)

The general architecture of Internet of medical things (IoMT) comprises of three stages [13]. This is implemented in many recent devices. They are namely,

Sensor level

Personal level

Medical server level

The sensor level is occupied with the medical devices and sensors. This customs a local network called Body Sensor network (BSN) [14]. For wireless communication Radio-frequency Identification (RFID) [15], Near-field communication (NFC) [16], Bluetooth low energy (BLE) [17] is imposed in sensor and personal level. Among this BLE can operate in all topologies whereas NFC and RFID can operate in ultra-low energy [18]. Such elements are required for our device.

The personal level server has two devices namely on-body device and off-body device. Gadgets such as smart phone, tablet and programmers are considered as on-body devices and gateway and routers are considered as off-body devices [19]. The data from sensory level are sent to the personal level. These are stored in cloud. This forms a network with medical level server. They can be remotely accessible and they should not break because of poor network

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

connection [20]. Doctors can easily monitor their patients remotely and assess them with proper medications and required measures.

3.1 Challenges

The Internet of medical things (IoMT) faces few challenges that affect the system performance they are

a) Postural body movement
b) Temperature rise
c) Energy efficiency
d) Transmission range
e) Heterogeneous environment
f) Quality of service

3.2 Security And Privacy Requirements Of Internet Of Medical Things (IOMT)

The Internet of medical things (IoMT) has more security concern than IoT [21]. Device localization is used for better security management. Since the Internet of medical things (IoMT) has multi-level the security system must be built for each and every level separately. The major considerations in each level are stated below

3.2.1 Data Level

The data level is the initial stage and it must be more précised. The following are the considerations in data level. Here the sensors collect the data of the patient [22]. This must be vulnerable and sensors are directly connected to individual. The following are the privacy requirements of data level server.

a) Confidentiality
b) Integrity

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

c) Availability

3.2.2 Sensor Level

The sensor level is followed by the data level. These collects the data from the data level server and process it in this stage [23]. The data must be finely processed and stored. Here we focus on next level of consideration such as

a) Tamper-proof hardware
b) Localization
c) Self-healing
d) Over-the-air programming
e) Forward and backward compatibility

3.2.3 Personal Level

The patient's data will be stored here so we require additional security. Two types of authentication are followed here [24]. This is connected in a network which can be remotely accessed by the authorised persons. The data must be in correct form because the doctors use these data for the treatment of their patients.

a) Device authentication
b) User authentication

3.2.4 Medical Server Level

The patient's reports are examined here so we have to take major considerations on this level. It must be accessed only by the authorised users [25]. All the medical history, currently monitored data will be present here. The altered data can even risk the life of patient.

a) Access control
b) Key management

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

c) Trust management

d) Resistance of DoS attack

Table 1. DOS attack on each layer

Layers	DOS Attack
Physical layer	Jamming, Node tempering
MAC layer	Collision & unfairness, Denial of sleep
Network layer	Spoofing, replying and wormhole, Homing, Hello flood
Transport layer	Flooding, De-synchronization
Application layer	Overwhelming sensor, Reprogramming attack, Route based DOS

3.3 Security Schemes For Internet Of Medical Things

The security scheme of Internet of Medical things is based on the cryptographic design, security analysis and application. Random number generator (RNG) is one of the important factors of security scheme. It comes under cryptography and biometric authentication is also discussed below.

3.3.1 State-Of-Art

A cryptographic algorithm is classified into two types namely, symmetric and asymmetric method. The asymmetric method is also called as public key authentication. Among these two, Asymmetric method works well but it requires high computational levels. Though IoMT's sensor level is capable of low battery level we cannot dump huge calculations on it. The encryption and decryption method with minimal computation and less weight data

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

is applied to sensor level. On other hand the Transmission part requires high security levels. They are transmitted from personal level to medical level through public channels.

In sensor level we require less weight data so public key authentication such as cloud based authentication, data storage and access controlled are used. In transmission level we require high level of security so we use symmetric method with less data consumption. Elliptic curve cryptography (ECC) is used instead of Rivest-Shamir-Adleman (RSA). Access control and data transmission which are symmetric authentication with minimal data is utilized by IOMT. It is also been used as session key for hybrid security schemes. Mutual authentication, A&T, forward security and contextual privacy are used to avoid the attacks such as eavesdropping, chosen plain text attack, reply and man-in-the-middle attack.

The state-of-the-art uses RNG as security scheme. It is generated by pseudo-random number generator (PRNG). It is a simulation process done in computer software and the random seed is generated and with this random seed the RNGs are produced. The same seed will produce same sequence of data. True generators are required to avoid inhalation of attackers. Due to its computational capacity it is less used in IoMT.

3.3.2 Biometric Authentication

Many factors can be implemented to determine the identity of the authorised user. Most précised one is biometric authentication. But most of the IoMT devices uses numeric or alphanumeric passwords as authentication key. Implementation of the Biometric authentication in such small device is under research field. Biometric authentication performs two main operations such as identification and verification. Both does the same work matching. But they differ by matched data. The identification matches the input sample with all the samples in the database whereas verification matches the input sample with specified individual’s database.

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

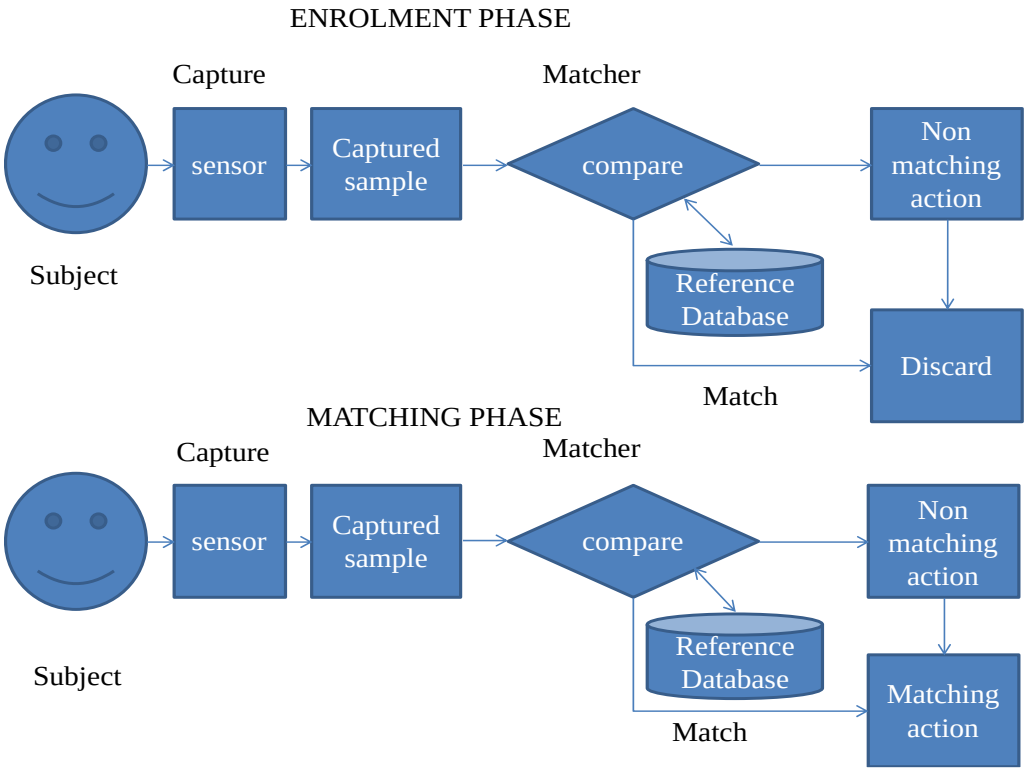

Figure2. Block diagram of Biometric authentication system

Enrolment phase and matching phase are the two main phases of the Biometric authentication. The user's uncooked samples are recorded in the enrolment phase and they are processed by templates and features vectors and stored in the database. Matching phase will verify the given sample with the samples of database and get accessed only if it is matched. Physical biometric traits are used widely. They perform differently for each and every type of physical biometric traits. By combining these techniques we can achieve better results.

3.4 Security Schemes for Implantable IOMT Devices

The implantable IoMT device is specially designed to perform surgery in patient. This must be designed with proper restrictions to attackers, power consumption, communication and

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

emergency situations. It must maintain high security because a small error can risk the life of the patient.

3.4.1 Proxy Based Protection

The proxy based security system has a proxy device placed between the implanted device and external device. This secondary device will provide security by producing a noise factor. It can be accessed only if the decoded data matches with the noise. It is known shortly as IMD and the above mentioned technique is called as IMD-shield. Shielding protects the device by producing noise. Other technique is IMD-Guard. Here the ECG signal is taken as shared key. It can be accessed only by the guardian and user.

3.4.2 Distance Bounding

Distance bounding is also called as proximity based access control. The security system is enhanced by limiting the distance between the implant and the external device. It is suitable for device with low bandwidth and it is applicable for charging and programming of IoMT. It reduces the wireless communication distance. It is technically called as inductive coupling. It is been used in medical implant communication system (MICS). Whose spectral bandwidth is around 402 Hz and 405 Hz, Its distance is reduced to 2m. For more accuracy it can be reduced less than 1m.

3.4.3 ECG Based Encryption

The implant device can capture ECG signals. so we can use the ECG signal as entropy source to encrypt a message. For an instance of security device with one time pad (OTP) uses inter-pulse as keyword and provide access to the system. Individual does not require remembering the password all the time. Though it has lot of merits and highly secure, it has few limitations which are stated below.

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

a) It cannot be used in emergency situation because it takes some time to prepare the data calculation.
b) It produces distortion and attenuation easily with small movement and poor skin contact with the patient.
c) It fails to eliminate false rejection rate.
d) The measurements varies from original data and the data captured by IMD in different location.

3.4.4 Analogue Shielding

Adequate sensor robustness leads to analogue attack. The sensor is the important factor that causes this attack. This has very small amplitude and analogue in nature. So it produces false injected data. It makes noisy environment and these can be ignored by proper design architecture such as cable shielding in data transmission.

3.4.5 Zero Power Consumption

The zero power consumption is introduced to avoid power drawing issue. This depletes the battery of the implant. It always requires the communicational device to initialize with non-power such as piezoelectric RF harvest. It can be even achieved by radio frequency energy harvest. It notifies a signal during initialization. It is suitable for devices which are connected closer and that are the drawback of the scheme.

3.4.6 Anomaly Detection

The battery of the IMD is reduced by resource depletion attack. They are identified and altered by changing the pattern of the architecture. It examines both the physical and behavioural characteristics of the IMD. It provides integrity alone. So there is a need for further security scheme to increase the performance.

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

4. Discussion

The IoMT devices are best alternative for hospitalized treatment. Here the equipment is directly implanted on patient's body and it provides continuous monitoring and prompt treatment can be availed at current time. It is cost effective and can be easily maintained. Security level must be in high level to enhance the performance of the system and provide secure healthcare to the patient. It is directly connected to the patient, for treating major problems such as cardiac, nerve and insulin. When the data is hacked it will reflect directly on patient's life. Enhanced security scheme is required to avoid such malicious attack.

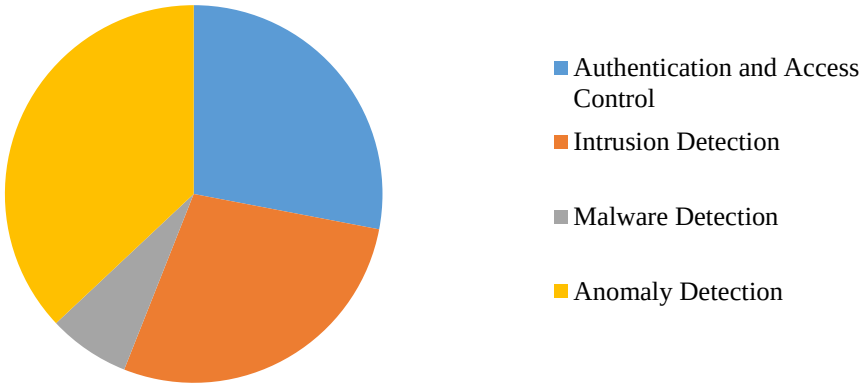

Figure 3. Graphical Representation of Accuracy

The hacking methodologies are faster than the security schemes. Every day they come up with new hacking methods and the administrator has to check each and every patch and has to update the anti-virus in the system. In healthcare system the device are implanted directly to patient's body so we can wait till next update and wait for someone to repair the system. The security updates must be on air and such schemes are under research. Out of the schemes state-of-the-art works well. It provides the needed security to the healthcare system. Biometric scheme is more accurate and provide high security level but due to the limitations of IMD, implementing biometric method is quite risky.

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

5. Conclusion

In the recent decade, a massive growth is observed in the IoMT technology. It is one of the applications of IoT that faces similar issues as seen in other resource. It is similar to IoT but it is specially designed for medical use and for patients. It has proven well in the healthcare system. Due to size, design and wearable model it is attracted by the patients. It is also helpful to the healthcare professionals to look after the current status of the patient's health. It will be very much useful in pandemic situations. It follows the architecture of IoT and it faces similar issues faced by IoT. To avoid this various methodologies are applied. Out of that state of the art works well and meets all the requirements. Biometric method works well and highly accurate but due to its limitations we cannot implement it right now. This ensures the safety, privacy, cyber and physical elements of the patient's data.

Reference

[1] Yingnan sun, et al., "Security and Privacy for The Internet of Medical Things Enabled Healthcare Systems: A Survey", Digital object identifier IEEE Access 2960617 2019

[2] Vijayakumar, T. "Synthesis of Palm Print in Feature Fusion Techniques for Multimodal Biometric Recognition System Online Signature." Journal of Innovative Image Processing (JIIP) 3, no. 02 (2021): 131-143.

[3] Li, X., Dai, H. N., Wang, Q., Imran, M., Li, D., & Imran, M. A. (2020). Securing internet of medical things with friendly-jamming schemes. Computer Communications, 160, 431-442.

[4] Jambhale, Tejas, and M. Sudha. "A Privacy Preserving Hybrid Neural-Crypto Computing-Based Image Steganography for Medical Images." In Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2020, pp. 277-290. Springer Singapore, 2021.

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

[5] Adam, Edriss Eisa Babikir. "Survey on Medical Imaging of Electrical Impedance Tomography (EIT) by Variable Current Pattern Methods." Journal of ISMAC 3, no. 02 (2021): 82-95.

[6] Mahendran, R. K., & Velusamy, P. (2020). A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. Computer Communications, 153, 545-552.

[7] Doraipandian, Manivannan, and Sujarani Rajendran. "Design of Medical Image Cryptosystem Triggered by Fusional Chaotic Map." In Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2020, pp. 395-409. Springer Singapore, 2021.

[8] Karunakaran, P., and Yasir Babiker Hamdan. "Early Prediction of Autism Spectrum Disorder by Computational Approaches to fMRI Analysis with Early Learning Technique." Journal of Artificial Intelligence 2, no. 04 (2020): 207-216.

[9] 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.

[10] Karthikeyan, C., J. Ramkumar, B. Devendar Rao, and J. Manikandan. "Medical Image Fusion Using Otsu's Cluster Based Thresholding Relation." In International Conference on Innovative Data Communication Technologies and Application, pp. 297-305. Springer, Cham, 2019.

[11] Vijayakumar, T., Mr R. Vinothkanna, and M. Duraipandian. "Fusion based Feature Extraction Analysis of ECG Signal Interpretation–A Systematic Approach." Journal of Artificial Intelligence 3, no. 01 (2021): 1-16.

[12] 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.

[13] Kumar, KN Mohan, S. Sampath, and Mohammed Imran. "Robust Methods Using Graph and PCA for Detection of Anomalies in Medical Records." In International Conference

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

on Innovative Data Communication Technologies and Application, pp. 342-352. Springer, Cham, 2019.

[14] Chen, Joy Iong Zong, and P. Hengjinda. "Early Prediction of Coronary Artery Disease (CAD) by Machine Learning Method-A Comparative Study." Journal of Artificial Intelligence 3, no. 01 (2021): 17-33.

[15] Abouzakhar, N. S., Jones, A., & Angelopoulou, O. (2017, June). Internet of things security: A review of risks and threats to healthcare sector. In 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 373-378). IEEE.

[16] Pavithra, B. S., and KA Radhakrishna Rao. "BS6 Violation Monitoring Based on Exhaust Characteristics Using IoT." In Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2020, pp. 77-88. Springer Singapore, 2021.

[17] Manoharan, Samuel. "Early diagnosis of Lung Cancer with Probability of Malignancy Calculation and Automatic Segmentation of Lung CT scan Images." Journal of Innovative Image Processing (JIIP) 2, no. 04 (2020): 175-186.

[18] Fernández-Caramés, T. M. (2019). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. IEEE Internet of Things Journal, 7(7), 6457-6480.

[19] Singh, Akhilesh Kumar, and Manish Raj. "Automated Intelligent IoT-Based Traffic Lights in Transport Management System." In Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2020, pp. 261-266. Springer Singapore, 2021.

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

[21] Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., ... & Hassan, M. A. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access, 9, 47731-47742.

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021

Journal of Soft Computing Paradigm (JSCP) (2021)
Vol.03/ No.03
Pages: 177-191
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2021.3.004

[22] Chen, J. I. Z., & Yeh, L. T. (2020). Data Forwarding in Wireless Body Area Networks. Journal of Electronics, 2(02), 80-87.

[23] 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.

[24] Hariharakrishnan, Jayaram, and N. Bhalaji. "Adaptability Analysis of 6LoWPAN and RPL for Healthcare applications of Internet-of-Things." Journal of ISMAC 3, no. 02 (2021): 69-81.

[25] Kumar, R., & Tripathi, R. (2021). Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology. The Journal of Supercomputing, 1-40.

Author's biography

R. Kanthavel is a professor in the Department of Computer Engineering, in King Khalid University, Abha, in the Kingdom of Saudi Arabia. His research is mainly focused on the emerging smart computing technologies that includes Distributed Computing, quantum computers, Computer Graphics,Computer Networks, and Web Technologies.

ISSN: 2582-2640 (online)
Submitted: 03.07.2021
Revised: 18.08.2021
Accepted: 02.09.2021
Published: 11.09.2021