Research Journal of Computer Systems and Engineering

ISSN: 2230-8571, 2230-8563

Volume 03 Issue 01 - 2022 (January to June)

Page 48:55

Secure Sensor Node-Based Fusion by Authentication Protocol Using Internet of Things and Rfid

Dr. Imran Qureshi
Computer Science & Communication Engineering
University of Technology and Applied Science Al Musanna
ORCHID ID-219772735
imranqureshi1210@gmail.com

Mrs. Sheetal S. Patil
Computer Science & Communication Engineering
BVDUCOE Pune
https://orcid.org/0000-0003-4381-1228
sspatil@bvucoep.edu.in

Article History

Received: 22 January 2022
Revised: 14 April 2022
Accepted: 19 May 2022

Abstract

Recently, there is a demand for systems based on Radio Frequency Identification (RFID) in several applications and are applied successfully in various areas. This paper proposes the novel integration of sensor nodes in IOT model with RFID authentication protocol (RAP) based smart monitoring system. Here the data has been collected from the wearable devices of a patient and transmitted through sensor node with security. The data has been segmented and their text and image features have been segmented. Then by using classification process by fast deep convolutional neural network (FDCNN), the normal and abnormal data has been classified. Based on the classified results, the accuracy, precision, recall, F-1 score has been calculated by the proposed simulation results. This proposed technique has been proved to be enhanced result through comparative analysis with existing technique.

Keywords: Radio Frequency Identification (RFID), Healthcare industry, internet of things (loT), RFID authentication protocol (RAP), smart monitoring system, classification, FDCNN.

1. Introduction:

Internet of Things (IoT) with the ability of self-configuration is a global dynamic network which operates based on the interoperable and standard communication protocols. Seamlessly, these things are combined with RFID (Radio Frequency Identification) information network which shapes to be the building block for IoT [1]. Generally, in hospitals, e-healthcare system helps in obtaining the patient's information [2]. Moreover, it has allowed smart appliances and gadgets which considers energy to exploit sensor nodes in wireless network [3]. Every device contains a RFID tag, sensors, actuators etc. [4]. Healthcare servers maintain medical records of the patients registered electronically and offers several services to medical advisors, patients, and familiar caretakers.

2. Related works:

Recently, numerous authentication protocols have been designed and implemented for RFID systems. Health monitoring system based on loT plays a significant role. In [5], a secure mobile RFID authentication protocol was developed based on elliptic curve signature. In [6], developed a protocol which provided solutions for security challenges. This protocol provided mobility, scalability and privacy, Moreover, it was suitable for multi-server environment. In [7], Aa novel hash based lightweight RFID mutual authentication protocol was developed for health-care applications. In [8], developed a protocol which gave anonymity for both the reader and tag and also provided forward–backward untrace ability. In [9],[10]a lightweight mutual authentication protocol was introduced to satisfy the security properties required by a RFID system.

3. Research methodology:

Initially the data has been sensed from wearable device of a patient which has RFID authentication protocol (RAP). The role of RAP is to avoid malicious users to access the data. Only the hospital can access the data which has been collected by the wearable device. Since wearable devices are linked with the patient mobile phones, anomaly attacks can occur. RAP can avoid the malicious attacks. Then data has been transmitted by secured sensor nodes in the IoT module. Here the sensor nodes have been clustered and cluster head collect the data which is needed to be transmitted. This module consists of base station for data transmission and here secured routing has been carried out. The data has been collected with security and created as the dataset. This dataset comprises of both text medical data of the patient and the scans based on the pre-historic medical data. Then for cleaning the data pre-processing has been carried out. In segmentation process, the data and image has been segmented and based on decision tree algorithm their features have been extracted. These extracted features have been classified using Fast deep convolutional neural network (FDCNN). Finally, the normal and abnormal data has been classified. Once the abnormal data has been detected the alert message is sent for fast diagnosis and treatment. The overall architecture of this research is given in figure-1.

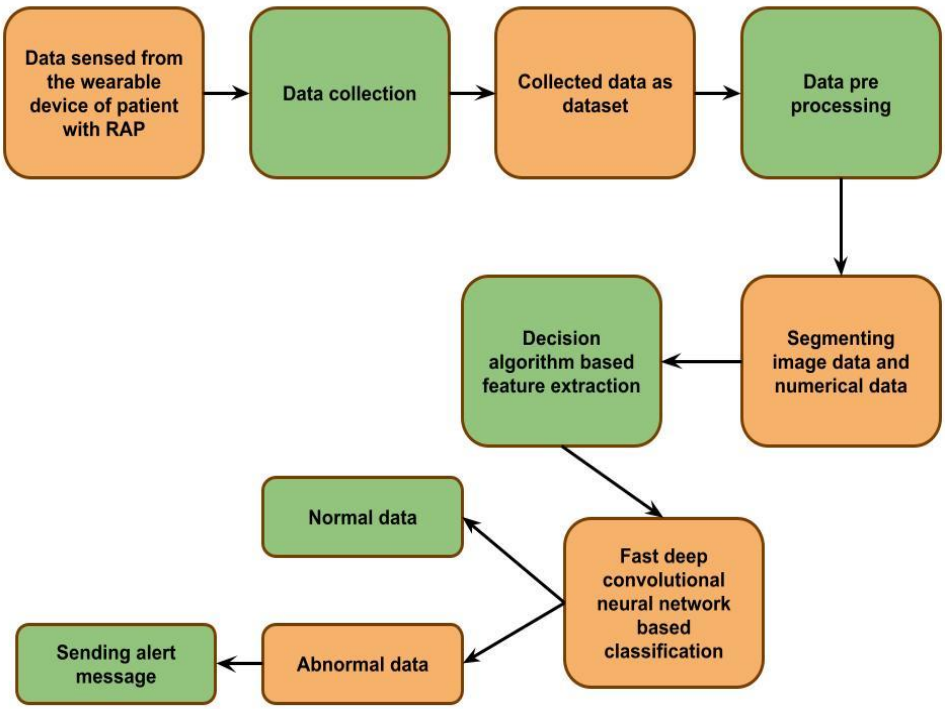


Figure 1: Overall Architecture

3.1 Wearable device with RFID Authentication Protocol:

A novel wearable device with RFID authentication protocol (RAP)which uses a secret-session key sharing strategy is developed. This model secures the way the patient and back-end (hospital server) database servercommunicate. These phases solve challenges of existing protocols namely privacy, security, and counterfeit. To deal with security issues, thesignificant feature used in this paperisa secret-session key. Additionally, these keys are generated subsequently at back-end database server SSk→SSk−1 so that session key output valuesof the tag are updated. By this method the data has been collected by the sensor nodes with security.

3.2 Decision tree-based feature extraction:

Model shown is a Decision Tree Classifier,the input instances are considered as Nodes.The node is divided into pairs by using if-else clause on the basis of labelled variable. On the basis of randomness of instance, the input is routed to a specific leaf node and this process continues till the randomness of the cluster value is zero and then determine the final prediction. There are three types of nodes,

1. Root Node: It doesn't have any parent node,then it divide the nodes into two child nodes based on the application.

2. Internal Node:It will have a parent node and conquer into two children nodes.

3. Leaf Node:if the randomness of the instances is zero and does not have any children nodes.

Grossberg Decision Tree Detector Algorithm:

Input Training set $\{(x_1, y_1, \ldots., (x_n, y_n)\}$

1. Let a single unlabeled nodeis denoted by T.
2. **While** unlabeled leaves v in *T* **do**
3. Navigate data samples to their corresponding leaves.
4. **for** every*v*in *T* **do**
5. **if** *v* satisfies the terminating condition **or** no samples reach*v***then**
6. *v* is labelled with the most frequent label among the samples that reach *v*
7. **else**
8. Select candidate splits for *v* and estimate D for each of them.
9. Using the highest estimation of D, v is split.
10. **end if**
11. **end for**
12. **end while**

The extracted features have to be classified for detecting the abnormal data with improved accuracy.

3.3 Fast deep convolutional neural networks (FDCNN):

A FDCN Nuses weighted soft max cross entropy loss and Adam Optimizer, while CNNs use ReLU activation and dropout which follows the convolution layer at the training phase. Here, seven frames are provided as input to the FDCNN modelwith size 60 * 40. Initially, a set of hardwired kernels are applied for generatingseveral information channels from input frames.

$$I_i^{(m)} = f_{ReLu}(b^{(m,i)} + \sum_j I_j^{(m-1)} W_j^{(m,i)}) \quad (1)$$

The common output function for classifying the problems with K classes is the softmax function which is given by:

$$f_i = \frac{\exp\,(I_i^{(o)})}{\sum_j \exp\,(I_j^{(o)})} \tag{2}$$

$$I_i^{(o)} = b^{(o,i)} + \sum_{k=1}^{k} W_k^{(o,i)}\, I_k^{(N)} \tag{3}$$

$$f = a + (b - a)(1 + \exp\,(b^{(o)} + \sum_j W_j^{(o)}\, I_j^{(N)})^{-1} \tag{4}$$

Whena ranking-type multi-class classification problem is considered like malignancy level prediction, output function defined here may perform more efficiently.

4. Performance Analysis:

This section provides the comparative analysis of data sensing rate with RAP, computation cost, data transmission rate with security, data classification accuracy, precision, recall, F-1 score, true positive, false positive value for detection the normal data and abnormal data during the authentication phase, data transmission phase and classification. The comparative analysis has been made between existing and proposed techniques.

Table-1 Data transmission rate with security

Number of Sensor Nodes	SMRAP	HLRMAP	HLP	TSP	EPC	WRAP-DA-FDCNN
50	15	19	25	29	31	49
75	21	22	29	32	35	52
100	25	26	33	36	39	56
125	28	29	35	39	42	59
150	32	35	39	41	45	62

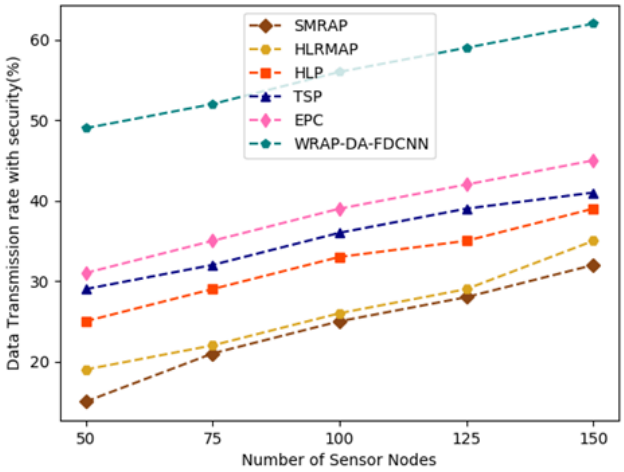


Figure-2 Data transmission rate with security

The above table-1 shows data transmission rate with security for number of sensor nodes and figure-2 shows the graphical representation for data transmission

Table-2 Comparison of Precision

Number of Sensor Nodes	SMRAP	HLRMAP	HLP	TSP	EPC	WRAP-DA-FDCNN
50	14	15	19	19	21	39
75	20	19	23	22	25	42
100	24	23	27	26	29	46
125	26	25	30	29	32	49
150	30	29	36	31	35	52

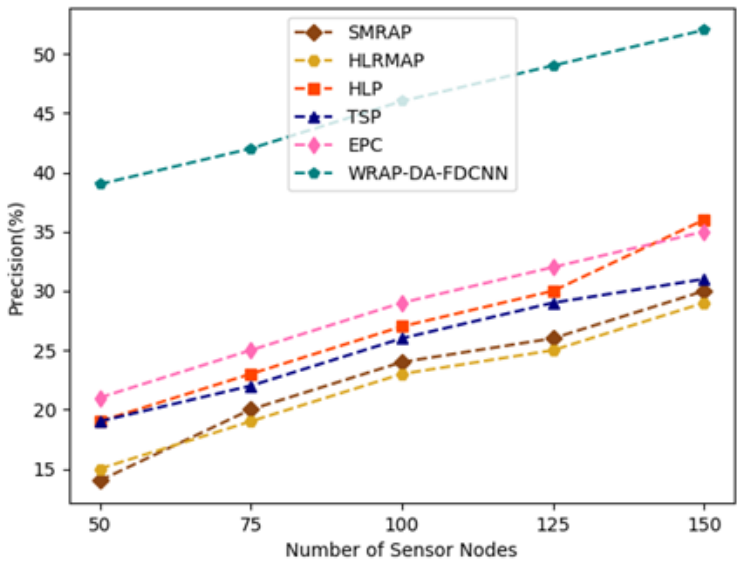
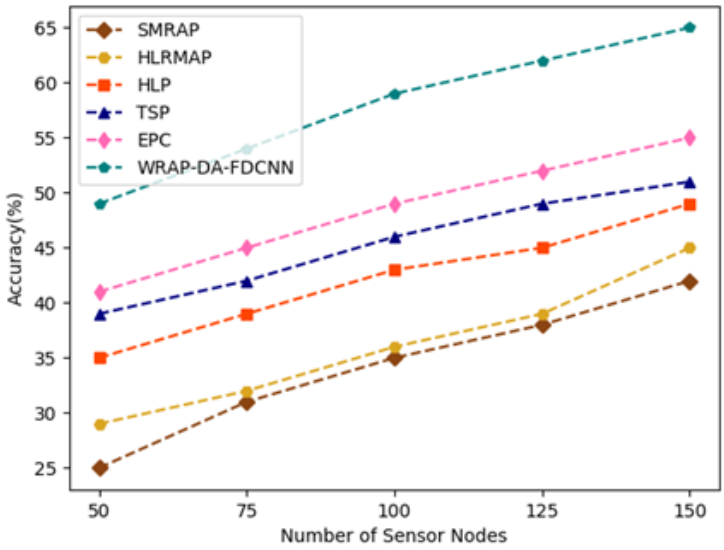


Figure 3 Comparison of Precision

Table-3 Comparison of Accuracy

Number of Sensor Nodes	SMRAP	HLRMAP	HLP	TSP	EPC	WRAP-DA-FDCNN
50	25	29	35	39	41	49
75	31	32	39	42	45	54
100	35	36	43	46	49	59
125	38	39	45	49	52	62
150	42	45	49	51	55	65



Figire-4 Comparison of Accuracy

Table-4 Comparison of Recall

Number of Sensor Nodes	SMRAP	HLRMAP	HLP	TSP	EPC	WRAP-DA-FDCNN
50	29	33	39	42	44	52
75	33	35	42	49	49	56
100	38	39	45	52	52	59
125	42	42	49	53	55	63
150	45	48	51	56	59	69

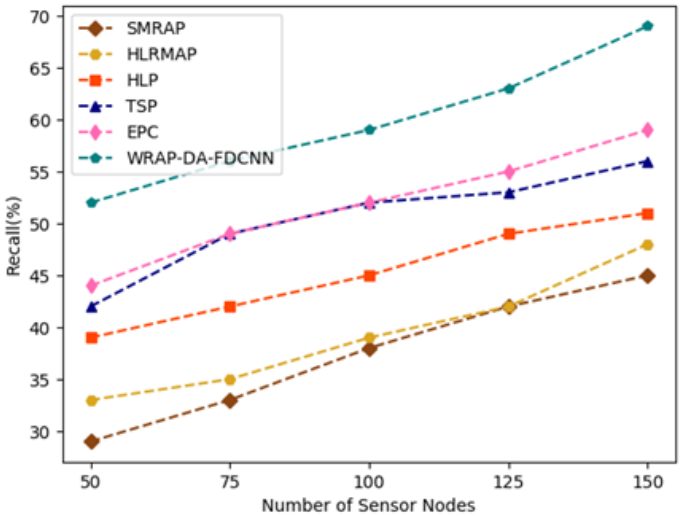


Figure-5 Comparison of Recall

Table-5 Comparison of True positive and False Positive Rate

True positive and False Positive Rate	HLRMAP	HLP	TSP	EPC	WRAP-DA-FDCNN
0.2	0.15	0.29	0.25	0.32	0.45
0.4	0.25	0.39	0.36	0.49	0.58
0.6	0.61	0.65	0.42	0.52	0.69
0.8	0.81	0.79	0.99	0.82	0.95
1	1	1	1	1	1

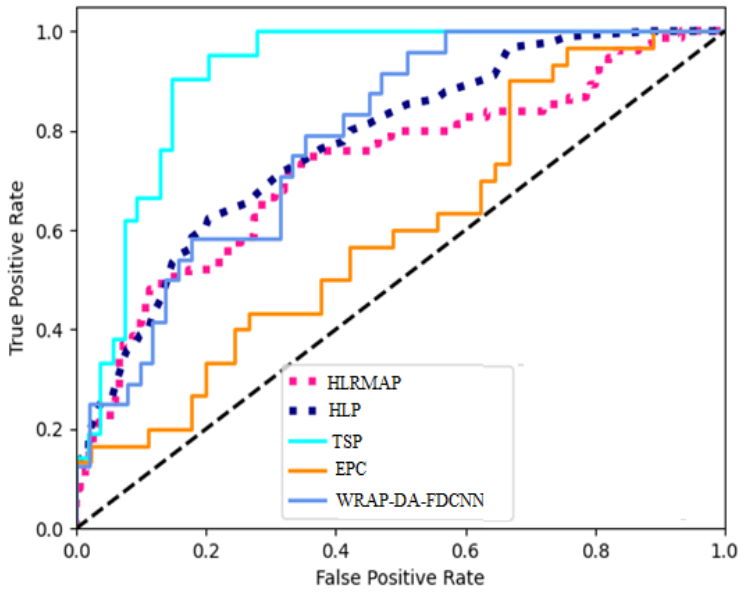


Figure 5- Comparison of True positive and False Positive Rate

The above table 2,3,4,5 shows the comparison of accuracy, precision, recall and true positive and false positive rate. The figure 2,3,4,5 shows the graphical representation in comparison with existing techniques.

5. Conclusion:

This paper elaborated the integrationofWSN with RFID technology applied in the IoT applications. Here the proposed architecture has 3 phases in which the wearable device with RFID authentication protocol senses the patient data and in phase 2 the IoT module with sensor nodes has been implemented for data transmission with security. The phase 3 carried out with extracting the feature of collected and created data, the finally the data classification is done for classifying the abnormal data and normal data. For abnormal data the alert message will be sent. The simulation results show that the proposed design show improved accuracy by fusion of RFID in WSN with IoT. The comparative analysis shows the optimized results achieved by the proposed design.

References:

[1] Wang, King-Hang, et al. "On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags." The Journal of Supercomputing 74.1 (2018): 65-70.

[2] Safkhani, Masoumeh, and NasourBagheri. "Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things." The Journal of Supercomputing 73.8 (2017): 3579-3585.

[3] Mansoor, Khwaja, et al. "Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography." Sensors 19.21 (2019): 4752.

[4] Alamr, Amjad Ali, et al. "A secure ECC-based RFID mutual authentication protocol for internet of things." The Journal of Supercomputing 74.9 (2018): 4281-4294.

[5] Aghili, SeyedFarhad, et al. "Seclap: Secure and lightweight rfid authentication protocol for medical iot." Future Generation Computer Systems 101 (2019): 621-634.

[6] Challa, Sravani, et al. "Authentication protocols for implantable medical devices: taxonomy, analysis and future directions." IEEE Consumer Electronics Magazine 7.1 (2017): 57-65.

[7] Li, X., Peng, J., Obaidat, M. S., Wu, F., Khan, M. K., & Chen, C. (2019). A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. IEEE Systems Journal, 14(1), 39-50.

[8] Feng, Q., He, D., Zeadally, S., Kumar, N., & Liang, K. (2018). Ideal lattice-based anonymous authentication protocol for mobile devices. IEEE Systems Journal, 13(3), 2775-2785.

[9] Galdi, C., Nappi, M., Dugelay, J. L., & Yu, Y. (2018). Exploring new authentication protocols for sensitive data protection on smartphones. IEEE Communications Magazine, 56(1), 136-142.

[10] Li, X., Peng, J., Obaidat, M. S., Wu, F., Khan, M. K., & Chen, C. (2019). A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. IEEE Systems Journal, 14(1), 39-50.