Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 3s (2025)

An Efficient Algorithm to Enhance Confidentiality, Security and Quality of Service(QoS) for Internet of Things(IoT) Communication Network

Voore Subrahmanyam[1], N. Sateesh Kumar[2], Nagurla Mahender[3], Jyothi Devaraj[4], Indraneel K[5], Sriram Parabrahmachari[6]

[1]Associate Professor, Department of IT, Guru Nanak Institute of Technology, Hyderabad.

[2]Associate Professor, Department of CSE, Mall Reddy Institute of Technology, Hyderabad

[3]Assistant Professor, Department of CS&AI, SR University, Warangal.

[4]Assistant Professor, Department of IT, Kakatiya Institute of Technology&Science, Warangal.

[5]Assistant Professor, Department of IT, Guru Nanak Institute of Technology, Hyderabad.

[6]Assistant Professor, Department of CSE, Guru Nanak Institute Technical Campus, Hyderabad.

Email: [1]subrahmanyam.voore@gmail.com, [2]adepurajeshadepu@gmail.com, [3]mahi.nagurla@gmail.com, [4]jpingali14@gmail.com, [5]indraneelk@gmail.com, [6]sriram.p@gniindi.org

Article History:

Received: *18-09-2024*

Revised: *03-11-2024*

Accepted: *15-11-2024*

Abstract:

The communication between physical devices and Internet environment provides a flexible and more secure by Internet of Things(IoT) enable Cyber Physical Systems. The cyber physical systems are providing a bridge between physical systems platform to virtual system platform for better usage of communication technology. The IoT devices are less battery life, less processing capability and small in size. These sensor devices are constrained devices are suitable for constrained network where network is un-reliable and require low bandwidth. It is essential to provide security for these sensor devices for securely data transfer is a challenging task. To solve this task as well as to fulfill various performance metrics like minimum time consumption, enhance secure communication between these IoT devices, memory usage, confidentiality rate etc. The proposed paper applying a Cryptography based Secure Encrypted & Decryption Algorithm(CSEDA) algorithm to provide security and also to minimize attacks for IoT device in a secure network communication. In the first step, the IoT sensor devices are sensed and collected real-time analog data from outer environment. This collected data will be analyzed in hidden layer with jackknife regression function. In the second step, these classified data to be forward to further hidden layer to encrypt the data will be perform by Schmidt Samoa (SS) Encryption Algorithm after that the data will transform to cloud for store & further process. In the third step, The decryption is performed by Schmidt Samo (SS) Decryption Algorithm. In the cloud the finally the original data is stored in the database for further processing. This method is providing the security of data communication and processing with less time. The real-time data is being sensed and collected by sensor devices and perform classification, processing time and memory usage. The proposed CSEDA method providing high confidentiality of the data and minimize processing time and well utility of memory space when compare with existing algorithms GRBFNN, Deep learning model, JRSSC-DASL.

Keywords: Internet of Things, Cyber Physical Systems, Secure Communication, Cryptography methods, Encryption and Decryption algorithm.

1. Introduction

Integration of Cyber Physical Systems (CPSs) combined with Internet of Things(IoT) are providing the security features to enhance better communication. The development of real-time application by IoT devices are uses wireless communication for transmission of real-time data frequently cause attacks. It is essential to provide a secure way of communication for data transfer by these sensor devices is a challenging task. The neural network algorithm is proposed to minimize the data transmission through a shared communication of devices in a IoT network. This algorithm enabled with cryptographic method provides confidentiality[1,2,3,4].

The contribution of proposed CSEDA algorithm solving the secure data communication between sensor devices in IoT networks as follows...A novel CSEDA algorithm is perform secure communication of IoT with CPS with various targeted processing like data analysis, classification, encryption, memory utilization and security. Jackknife regression(JR) function is within CSEDA algorithm is essential to data is to be classify first, before data transmission. The analysis of regression function features to improve classification accuracy. The CSEDA algorithm reduces the execution time to perform secure communication. For enhancing the confidentiality of the data using the cryptosystem ie Schmidt-Samoa to generate public and private key are treated as temporary keys to communication only once. For that reasons CSEDA algorithm avoids un-authorized users to illegally access the data. To improve the confidentiality rate, CSEDA algorithm uses Schmidt-Samoa cryptography algorithm. In the procedure of transmit the data, these data will be classified later on changed by Schmidt-Samoa encryption process into cipher text. To avoiding illegal data access. These encrypted cipher text has been transmitted to the remote cloud via wireless network.

The research paper is organized in various sections. They are In Section2 provides Related work. The Section3 provides in detail about description of CSEDA algorithm as well as system framework. The Section4 provides proposed work with experimental setup, Result analysis and comparison with existing algorithms. In Section5 provides Conclusion.

2. Literature Survey

In[5] authors proposed a multi-layered technique for Cyber Physical Systems for collectiveness by safety and security risk system using IoT devices. In this paper provides the CPSs is integrating with widely information technologies, physical components are co-operate, co-ordinate integrate to operate automation of functions and also provide on security. But authors not providing information about safety from risks.

In[6] authors proposed a security as well as privacy method communication. The authors focusing on Cyber Physical System threats and providing security about privacy and security. Author proposed a detect scheme for Sybil attack for safe communication of CPS. By Sybil attack in CPS cause data loss, route loss, change the time synchronization etc. Author proposed sybil attack mitigation deduction and mitigation algorithm for improve throughput, energy and delay. But it is a failure for applying a digital signature method for cryptographic methods for accurate detection the data that are attack in CPS.

In[7] authors proposed a computation method for process of heterogeneous data to manage IoT enabled cyber applications. Authors introduce solutions for cyber technology security and safe methods. But

authors not proposed any application.

In[8] authors proposed a monitoring human based activities but it is failed to gather the information from IoT . proposed a design a computational framework for smart devices for sharing health monitoring of applications.

[9] authors proposed higher data security and confidentiality. Authors consider to take upto 1000 sensor data only. To improve the data security the existing paper apply cryptographic method for encryption and decryption. The existing algorithm achieve low processing time as well as low memory usage.

3. Proposed Work

Proposed Cryptography based Secure Encrypted & Decryption Algorithm(CSEDA) is introduce to perform securely perform for various tasks data analysis for IoT enabled with CPS for the process of classification and encryption. The CSEDA having advantages for the process of classify the data before transmission. The performance of classification will be improved by regression function. For that reasons CSEDA algorithm avoids the data accession illegally from un-authorized users by converting the data encryption. The authorized user can will apply description and receives original data.

The feature of Cyber Physical Systems are connect, communicate the physical outer world environment and providing the automation strategy. The CPS enabled with IoT is emerging technology to enhance the quality for remote monitoring, sensing from remotely connected real-time objects and access real-time data very securely. Due to users connected the devices remotely the attacks is concerned the CPS are being critical. In this proposed paper we providing a secure communication of IoT enabled Cyber Physical Systems protect against cyber attacks by applying Encryption algorithm[10,11].

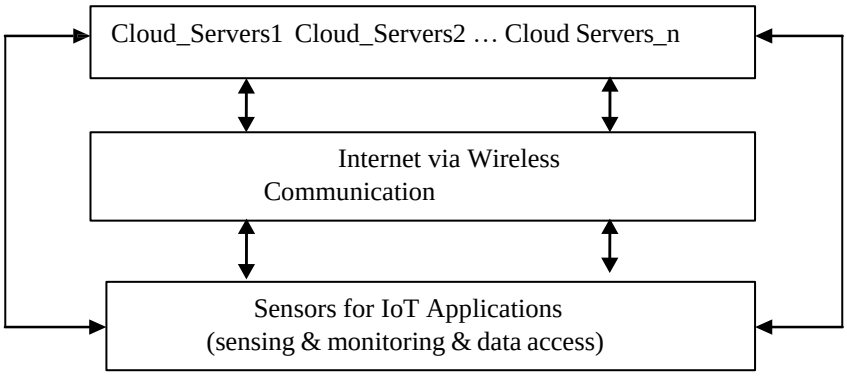

Figure 1. An architecture structure of Internet of Things(IoT) enabled CPS

The Figure.1 shows the structure of IoT enabled Cyber Physical System. It perform in two stages are physical stage and cyber state. Mainly in Physical stage the Internet of Things(IoT) devices are deployed in a threshold are for smart applications. Ex: smart temperature, smart health, smart vehicles, smart industry and smart city application etc. IoT devices are inbuilt with sensing, actuation, tiny devices are implement with electronics, embedded environment. IoT devices are mainly enabled the objects to sense and monitor the data. The IoT devices collected data will be analyzed and stored in cloud server in a secure manner by Internet. During these communication, the un-authorized and

vulnerable are corrupt the data and communication.

This proposed method is for data collection, analysis and encryption for providing secure communication of the data towards process. The data collection is performed via Deep Learn(DL). This structure contains input layer and multiple hidden layers and one output layer. The gathered data from IoT devices is considered as input for these DL process. These data is classified and analyzed by JR function in hidden layer. These data will be classified and converted into encrypted form and send to the cloud platform. The encryption process perform by second hidden layer by applying SS algorithm. Again for the further processing the available data will be decrypted via SS algorithms[12,13,14,15].

3.1 Data Collection

The Deep learning(DL) method is perform for data collection. The DL network contains single input layer and multiple hidden layers and one output layer. The Deep learning communicate with IoT devices and collect the data and process it and given output. In a first hidden layer, the data analyzed and classified using JR function. These data to be encrypted and transmit to cloud server. In the second hidden layer, the encryption process is being perform using Schmidt-Samoa algorithm. For further processing, the SS decryption algorithm received data will be decrypted.

The Data collection phase is a process of data being collected data from open source data set created by virtual environment of Internet of Things. These collected is analyzed by applying machine learning algorithms. Through the Internet the final data will be transmit completely to remote cloud. Here the by cryptographic algorithms the data security will be applied[16].

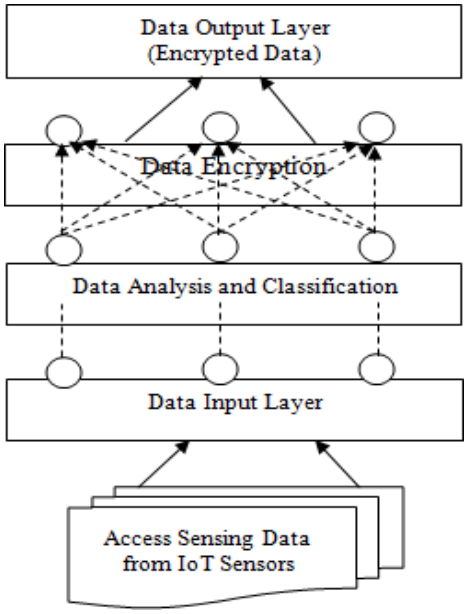

Figure 2. Neural structure for data output

The Figure2 describes about deep artificial learning structure which contains a network system of multiple layers. It receives the real-time data from IoT sensor already automated by enabled applications. These type of data access from sensor devices as taken as input sensor data like data d1,d2,d3...dn access from IoT sensor devices and transform to input to IoT device and transform to

input layer. The Deep learning(DL) processing various neurons to form neural network. The neuron's process identify by 't' is the time that specify in the following equation..

$$\Phi_t = \sum_{i=1}^{n} d_i * \omega 1 + b \quad (1)$$

In Eq.(1) the input layers are collect the real-time sensor data as 'di', the weight consider as $\omega 1$ between the hidden layer 1, b is consider as bias.

4.The Data Analysis And Classification

While receiving the output, the data procedure of data analysis and data classification are taken to consider after receiving output. The regression function applying in premier hidden layer. The Regression analysis is the method for applying to the data to analyze & estimate various data for finding the core-relation between dependent as well as independent data.

$$\mu = 1/n = \sum_{i=1}^{n} d_i \quad (2)$$

In equation 2 , μ denotes as mean for class, 'n' denotes the number of input. d_i denotes as data.$\sigma_{jackknife} = |\mu - d_i \quad (3)$

In Eq.(3), $\sigma_{jackknife}$ denotes as Jackknife variance, μ denotes as class, d_i denotes as data.

The next step is analysis of the data, for further process is treated as classified input is send to the cloud for encryption. In second hidden layer, the encryption process is performed. The SS cryptosystems for asymmetric cryptograph in that the private as well as public key used to extend to performance for the purpose of data communication security. Almost these keys are used as temporary used once at a time in the process of data encryption and data decryption. SS act as cryptosystem to perform various features like encrypt the data, decrypt the data and also key generate. The prime number x and y will generate private key and public key by following Eq.(4).

$$R = x^2\ y \quad (4)$$

R is treated as publication in equation(4). The private key is generated by following equation(5)

$$P = R^{-1}\ mod\ LCM\ (x - 1, y - 1) \quad (5)$$

In above equation(5), P denotes as private key. The encryption is perform after key generation and obtain the ciphertext.

The IoT_d1, IoT_d2, IoT_d3….IoT_dn denotes as classified sensor data for encryption. It is performed by receiver's public key. In this process first, encrypt the Input data 'd' than next process to compute the cypertext by following equation

$$D = d^R mod\ R \quad (6)$$

In equation(6), D is noted as cipher text, d noted as concerned data, R denote is act as receiver public key. To improve the privacy and secure way of data communication via wireless network the cipher text has been set the cloud. Generate output via hidden layer is obtained by equation7

$$G(t) = \sum_{i=0}^{n} d_i * \beta_1 + \beta_2 * G(T-1)$$

As per above Eq.(7), G(t) is consider as data, β_1 consider as weight between input as well as hidden layer β_2.

This process is the consider for output for these hidden layers. G(t-1) consider first hidden layer's output is generated. These process treated as here hidden layer's output will be transmitted to output layer performed by following Eq.(8).

$$H(t) = \beta_3 * G(t) \qquad (8)$$

As per above equation(8), H(t) consider as output of β_3 for considering weight of G(t). Through the Internet the data will be encrypted and has been sent to remote cloud. The servers residing in the remote cloud will receive the data will be perform data decryption process for further processing for getting the original form of the data The encrypted data is received by cloud use private key to decryption. This decryption is denoted by equation(9).

$$d = D^p \ mod \ xy \qquad (9)$$

As per above Eq.(9), d is represent as the original data. D is represent as the cipher text. P is represent as private key. The parameters x and y are represents as prime number. The remote cloud having real-time original data. The algorithms encrypt the data as well decrypt the data for providing secure communication to avoiding un-authorized data access. The process of decryption of the data is as follows.

5. Proposed Cryptography Based Secure Encrypted Algorithm(CSEA) For Authentication

The proposed algorithm is providing data communication with secure communication. The real-time data has been collected by various connected and communication devices. The same data will be considered for input layer. The data analysis and classification is being performed at the foremost hidden layer contain input data. The dependent as well as independent data analysis has been performed by JR function. The data has been sent to the cloud for decryption process to acquire the data. The proposed algorithm minimize the process and maximize data communication performance within short period of time.

Input: The real time data is being accessed from IoT devices are IoT_d1, IoT_d2, IoT_d3 … .IoT_dn
Output : Now starts the securely data communication

Start

The real time accessing sensing data IoT_d1, IoT_d2, IoT_d3 … .IoT_dn

Analysis of data is being operated

Initialization of the classes Class_C1, Class_C2 …Class n

Every data

'μ' consider for mean to compute

σjack consider for purpose of calculation of variance

Data classification

End for

Execute the encryption process

To generate P, R as keys

'd ' is consider for every data classification

'D' is consider to convert original data into cipher text

'Ci' used to cipher text to server

Each encrypted data

Decrypts the data by the server

'd' is data obtain as the original data

End

6. Experimental Analysis

The experimental analysis for performing using IoT enabled Cyber Physical Systems to secure data communication for the real-time smart healthcare applications. The data sets are taken from mobile heath datasets. The dataset is taken to experiment from MHEALTH ± Dataset. To monitoring of human behavior and health status via body sensing use the MHEALTH dataset. For measuring the motion of the various parts of the human body like chest, right wrist, left & right angle parts. The human parts motions like acceleration, rate of turn etc.

The IoT device for monitor human body parts motion and the data is generated and stored in various log file. The activity identify these activities by these attributes and labels. The classification is the association task perform by the dataset. These datasets contains of motion of the body, vital signs recording while performs number of physical activities. These physical exercises and activities like sitting, standing, lying down, climbing stairs, walking, forward & backward walking, knees bending, cycling, jogging, front and back running and jumping etc.

The motion test of various body parts for acceleration. The motion body activities performing various physical activities like standing, sitting, relaxing, walking, climbing, knees bending, cycling, jumping and running etc. These human activities taken from the sensor devices.

6.1 Comparative Analysis and Evaluation metrics

Various evaluation metrics are taken for testing and analyse the performance of the proposed method over the used techniques are GRBFNN as well as Dual Deep Learning and JRSSC-DASL method.

6.2 Data accuracy using Classification methodology

The data accuracy by classification technique is one of the metric consider for calculate the IoT devices generate the no. of classified data to the no. of generated data. Following Eq(10) measure the accuracy...

$$A_{ca} = [N_{dacl} / N * 100] \quad (10)$$

In Eq.(10), A_{ca} is represents as classification accuracy, N is represents as no. of generated data from devices of IoT network, N_{dacl} is represents no. of accuracy is being classified in the form of

percentage%. In Experimental evaluation in figure using proposed method better than existing methods GRBFNN, Dual deep learning technique and JRSSC-DASL. The proposed method uses DL technique is implemented a proposed method of JR function to analyse the classify the input health data from devices of IoT network. The performance of the proposed method is shows better results improvement by 10% than existing methods.

Table1-Classification Accuracy

No. of data	GRBFNN	Deep learning model	JRSSC-DASL	Proposed (CSEDA)
1000	83	78	91	95
2000	84	80	92	96
3000	87	82	93	97
4000	85	80	91	95
5000	88	82	94	97
6000	87	83	93	97
7000	86	80	92	96
8000	85	81	90	94
9000	87	83	92	94
10000	85	82	91	95
11000	86	82	93	97
12000	85	81	92	96
13000	87	83	95	98
14000	86	83	96	99
15000	88	85	97	100

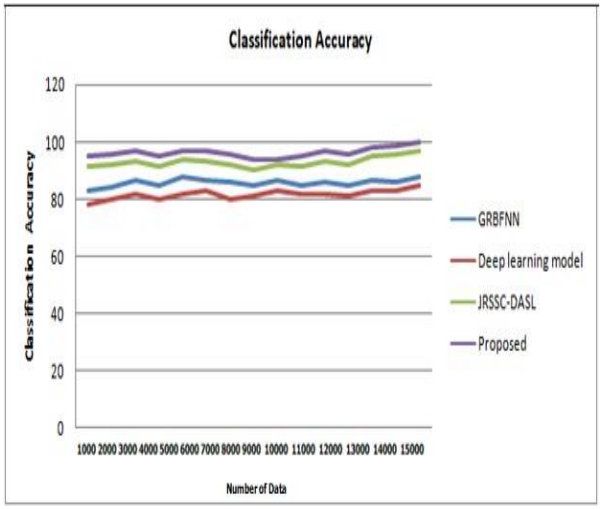

Figure 3. Classification of Accuracy of Data

The proposed CSEA algorithm uses DL method implement JR function perform to analyze healthcare real-time data accessing by sensor devices. Regression analysis function analyse the dataset collected from health datasets. The regression function of ML algorithm classifies various organs of human body as per the mean variance. The recommended datasets taken for experimental analysis from 1000 to 15000 sensor datasets. For every round of running the program the results of various classification accuracy results displayed by various techniques. In existing JRSSC-DASL algorithm apply with less quantity of sensor data. With this limited datasets shows low performance. In proposed CSEDA algorithm taken to consider 1000 to 15000 datasets. It improves the performance of algorithm capacity level of supports for heavy size data sets of sensor data for classification accuracy. In Fig3 is graphical representation of proposed method for accuracy of classification using sensor data is taken 1000 to 15000. For every run the performance results shows sensor sensing data consider as input data for accurately calculate of classification data. The results is show in the Y axis of graph. As per the classification results of GRBFNN, Deep learning model, JRSSC-DASL and proposed CSEDA are showing the colours display orderly in colours namely blue, red, green, violet. The overall performance of proposed method improve the classification of accuracy of sensor data performance when compare with the existing methods.

6.3 Processing Time

The processing time is noted that amount of time will be taken by algorithm to perform the secure data communication on IoT enabled Cyber Physical System. To calculate the processing time data communications is performing by Equation.

$$P\_Time = N\_IO * Time\ [d_S] \quad (11)$$

In above Eq.(11), P_Time is noted as processing time, N_IO is noted input, Time [d_s] noted as the time to process algorithm for processing the data. It is measure by ms. The figure shows processing time will be increased for three methods as per the large data generates by sensor devices. All these 3 methods the minimum processing time taken by proposed method. The process minimize the data transmission for secure transfer from sender system to receiver system. The proposed method taken less time for data transfer when compare with existing methods. Its shows better performance of proposed method.

No. of data	GRBFNN	Deep learning model	JRSSC- DASL	Proposed
1000	32	35	28	25
2000	34	36	30	27
3000	37	39	33	30
4000	40	44	36	33
5000	45	48	40	37
6000	47	49	42	39
7000	49	51	46	43
8000	53	56	50	47
9000	57	59	54	50
10000	60	62	56	53
11000	63	65	58	55
12000	66	68	61	58
13000	69	71	65	62
14000	72	74	68	65
15000	75	77	71	68

Table2-Processing Time

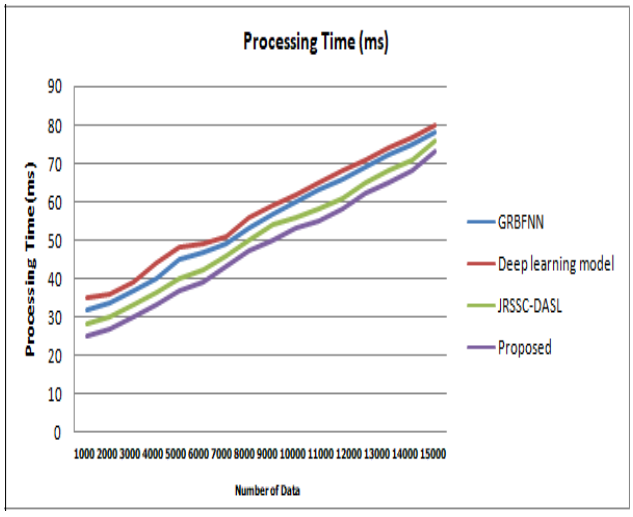

Figure 4. Processing Time

In Fig4 shows the experimental results in graphical manner. The results shows the processing time (in Y axis) as per the number of data(X axis). As per the generating the data by sensor devices and while increasing the input data automatically the processing time increased The processing time is increased with three available methods. The reason is the sensor devices generate large amount of data. While comparing with existing methods, in proposed CSEDA algorithm the processing time is minimized to transmit data to receiver securely. First partitioned into number of classes after only the data will be send. Data should be classified and transform to encryption with minimal time consumption. The

overall performance of proposed method improves the performance with the existing methods. The proposed algorithm apply classification based encryption method. In this technique, the data classified as well as analyzed. This algorithm reduce the secure data transmission sender to receiver. At first, the data analyzed and partitioned into no.of classes. Without sending the whole data at the same time. The proposed cryptographic method efficiently processes the encryption method within minimum time. The proposed algorithm taken very lesser time for data encryption When comparing the time taken for data encryption of existing methods. The time taken by proposed method for secure communication taken 20ms, JRSSC- DASL method taken 28ms, Dual deep learning model taken 32 ms, and GRBFNN method taken35ms respectively. These proposed algorithm with 14 runs are performed with sensed datasets of 1000 to 15000.The proposed CSEDA algorithm showed better performance than existing methods.

6. 4. Confidentiality Rate

Another performance related important metrics for the secure data transmission in Internet of Things(IoT) enabled Cyber physical systems(CPS) is Confidentiality rate. The authorized entity can be accessed and viewed the sensed data to improve the confidentiality. While distribute the data to estimating the confidentiality rate measured by formula is ....

$$Conf\_rate_{data} = N_{aa} / N * 100 \quad (12)$$

In Eq.(12) Conf_rate data is denoted as no. of data N_{aa} will be accessed by an authorized entity and considered as input N. The graph shows the accurate results of success rate of the data will be transmit to cloud server. The sensor related data collected from the sensors range in between 1000-15000. The performance of proposed method is providing better results while compare with existing methods. Because the proposed algorithm apply cryptographic method achieves for data transmission to the remote cloud through communication link using encrypted data & authentication mechanisms. While performing communication the cryptographic technique to encrypts data. As per the communication, the real data is transmission to remote cloud takes place through a secure communication channel. While data transmission through communication channel various attacks will be faced to secure protection of the data by SS cryptographic method. In this process, the input data will be converted in to cipher text and it will be send to cloud server. To decrypt process starts in server to convert original data. With this process, the proposed method shows more confidentiality rate when compare with existing methods.

Table3-Confidentiality Rate

No. of data	GRBFNN	Deep learning model	JRSSC- DASL	Proposed
1000	81	77	90	91
2000	82	78	91	93
3000	84	81	92	93
4000	82	79	90	92
5000	85	81	92	94
6000	84	82	90	92
7000	85	79	91	93
8000	83	80	89	90
9000	85	82	91	93

10000	84	81	90	92
11000	85	82	91	93
12000	86	83	92	94
13000	84	81	90	92
14000	85	82	91	93
15000	84	81	90	92

Figure 5. Confidentiality Rate

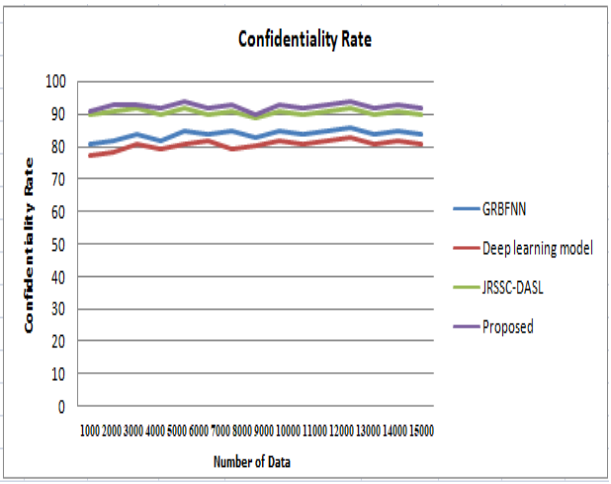

Figure 5. Confidentiality Rate

The Fig5 shows the confidentiality(in Y axis) versus no. of data(in X axis). As per the results its shows that the proposed method showing better performance than the existing methods. Cryptographic technique encrypts data as per performing communication. Cryptographic technique & authentication mechanism achieves for sensor data transmission to the remote cloud through communication link using encrypted data & authentication mechanisms. The results shows that the proposed method is better when comparing with existing methods for the performance of confidentiality.

6.5 Memory Usage

The memory usage is one of the performance metric is an quantity of amount of memory consumed for secure way communicate. Usage of memory will be calculate as follows.

Memory_usage = N_data* Mem_Cons[data] (13)

Eq.(13) Memory_usage is denoted as memory usage. N_data is denoted as number of data[d] and mem_cons is denoted as memory consumption for the processing the data. The measurement of usage of memory is megabytes(MB.). The real-tie results shows usage of memory and no. of usage of data. To calculate the memory consumption by data transmission securely. The memory consumption performance results and vary these two existing methods with proposed method. The proposed method consumes less memory space for communication the data in a secure manner. The reason is proposed method perform encryption process before transmit the data. And data taken in proposed algorithm is maximize upto 15000. As per encryption process the data size will be reduced and consumption of memory will be minimized. While comparing with existing methods i.e. GRBFNN, Deep learning model, JRSSC- DASL the proposed CSEDA model performing lower memory consuming for data

transmission.

Table4-Confidentiality Rate

No. of data	GRBFNN	Deep learning model	JRSSC- DASL	Proposed
1000	21	24	17	16
2000	26	30	22	20
3000	30	33	24	21
4000	34	36	28	26
5000	36	40	32	30
6000	39	42	36	33
7000	42	44	39	37
8000	46	48	42	40
9000	49	50	45	43
10000	52	55	47	45
11000	55	58	53	51
12000	58	61	55	52
13000	61	64	59	57
14000	64	67	62	60
15000	67	70	65	63

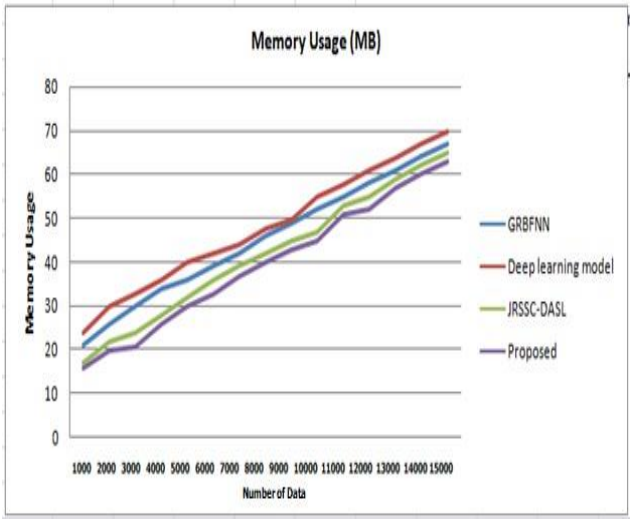

Figure 6. Memory usage for data communication

In Fig6 shows performance of memory usage experimental results (Y axis) and number of sensor data (X axis). The method shows to calculate to minimize the consumption of memory for the transmission secure of sensor related data. The Figure 6 shows the consumption of memory with various methods. The proposed CSEDA method consumes very less usage of memory for data processing, data transmission securely when comparing with existing methods GRBFNN, Deep learning model and JRSSC-DASL existing methods. The proposed method is consider to take input large sensor datasets upto 15000. For apply a method of data encryption, reduce the data size in this process energy consumption also minimized. Because the performance of the proposed method reach high performance results with less memory usage by reduce the size of the input data for the transmission. The proposed method apply cryptographic method achieves for data transmission to remote cloud through communication link using encrypted data & authentication mechanism. The proposed

CSEDA method improves the better results prove that consumption of memory will be minimized by 10% compared with existing methods like JRSSC-DASL (12%) and other existing (19%). It is conclude that as per above experiments analysis of various evaluation of performance metrics like are Classification accuracy data, processing time, confidential rate, and Memory usage are taken for testing and analyse the performance of the proposed method over the existing methods like GRBFNN, Dual Deep Learning and JRSSC-DASL model. It is proved that, the proposed CSEDA method is showing better performance and ability to consider high datasets when compare with existing methods.

Conclusion

The proposed paper shows performance of IoT Enabled Cyber Physical Systems for providing secure way of communication for IoT related sensor data to sense and to access by IoT smart sensor devices. The aim of our proposed method providing minimize the time to process of IoT sensor data and also providing the accuracy of the data. The aim of proposed method is to provide security to reach confidentiality rate with minimum time consumption. In this paper, data analysis is to perform as per JR function. The classification data perform by SS cryptographic algorithm, the security of sensor data is perform by encryption and decryption methods. For secure data communication the remote cloud will made data decryption. As per the results obtained, the efficiency of proposed CSEDA method is achieved better results for the better communication, confidentiality of data, processing of time will minimized and minimize less memory usage when compare with existing methods like GRBFNN, Deep learning model, JRSSC-DASL.

References

[1] Yaacoub, Jean-Paul A., et al. "Cyber-physical systems security: Limitations, issues and future trends." *Microprocessors and microsystems* 77 (2020): 103201.

[2] Khujamatov, Khalim, et al. "Networking and computing in internet of things and cyber-physical systems." *2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT)*. IEEE, 2020.

[3] Khujamatov, Halim, et al. "IoT, IIoT, and cyber-physical systems integration." *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation*. Cham: Springer International Publishing, 2021. 31-50.

[4] Salau, Babajide A., Atul Rawal, and Danda B. Rawat. "Recent advances in artificial intelligence for wireless internet of things and cyber–physical systems: A comprehensive survey." *IEEE Internet of Things Journal* 9.15 (2022): 12916-12930.

[5] Carreras, N.H., et al.: Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. Syst. Eng. Wiley, 23(2), 189–210 (2020)

[6] Kumaria, D., Singha, K., Manjul, M., Performance evaluation of Sybil attack in cyber physical system. Procedia Comput. Sci. Elsevier, 167, 1013– 1027 (2020)

[7] Zhou, X., et al.: Scalable platforms and advanced algorithms for IoT and cyber-enabled applications. J. Parallel Distrib. Comput. Elsevier, 118(Part 1), 1–4 (2018)

[8] Mora, H., et al.: An IoT-based computational framework for healthcare monitoring in mobile environments. Sensors 17, 1–25 (2017)

[9] Kannan, Chakrapani, et al. "Cryptography-based deep artificial structure for secure communication using IoT-enabled cyber-physical system." *IET Communications* 15.6 (2021): 771-779.

[10] Marwedel, Peter. *Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things*. Springer Nature, 2021.

[11] Maleh, Yassine. "Machine learning techniques for IoT intrusions detection in aerospace cyber-physical systems." *Machine Learning and Data Mining in Aerospace Technology* (2020): 205-232.

[12] Tertytchny, Georgios, Nicolas Nicolaou, and Maria K. Michael. "Classifying network abnormalities into faults and attacks in IoT- based cyber physical systems using machine learning." *Microprocessors and Microsystems* 77 (2020): 103121.

[13] Mishra, Ayaskanta, et al. "Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective." *International Journal of System Assurance Engineering and Management* 14.Suppl 3 (2023): 699-721.

[14] Tyagi, Amit Kumar, and N. Sreenath. "Cyber Physical Systems: Analyses, challenges and possible solutions." *Internet of Things and Cyber-Physical Systems* 1 (2021): 22-33.

[15] Mishra, Ayaskanta, et al. "Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective." *International Journal of System Assurance Engineering and Management* 14.Suppl 3 (2023): 699-721.

[16] Garg, Deepak, et al. "Hybrid technique for cyber-physical security in cloud-based smart industries." *Sensors* 22.12 (2022): 4630.