Cryptography-based deep artificial structure for secure communication using IoT-enabled cyber-physical system

Chakrapani Kannan1 | Muralidharan Dakshinamoorthy1 | Manikandan Ramachandran1 | Rizwan Patan2 | Hariharan Kalyanaraman1 | Ambeshwar Kumar1

1 School of Computing, SASTRA Deemed University, Thanjavur, Tamil Nadu, India
2 Department of Computer Science and Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India

Correspondence
Rizwan Patan, Department of Computer Science and Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India.
Email: prizwan5@gmail.com, rizwan@vrsiddhartha.ac.in

Abstract
Internet of things (IoTs) enabled cyber-physical systems is a system that provides communication between physical devices and cyber environment. They run independently without any user interaction. Because the IoT devices are vulnerable to a variety of attacks, security is a noteworthy factor in the development process during communication. To improve secure communication with minimum time consumption, a novel technique called jackknife regressive Schmidt Samoa cryptography-based deep artificial structure learning (JRSSC-DASL) is introduced. Initially, the data is monitored by IoT devices and is collected from the dataset. The proposed deep artificial structure learning technique trains the gathered data with multiple layers. Then, the collected data is analysed in the first hidden layer with the help of the jackknife regression function by learning the feature and it classifies the data with higher accuracy. The classified data is sent to the next hidden layer where encryption is performed using Schmidt Samoa (SS) encryption algorithm. Then, the encrypted data is sent to the cloud server where the decryption is performed using the SS decryption algorithm. The cloud server obtains the original data and it is stored in their database for further processing. This process enhances the security of data communication and achieves high data confidentiality with less processing time. Experimental estimation is performed on the factors such as classification accuracy, confidentiality rate, processing time and memory usage to the number of data sensed from IoT device. Conferred results reveal that the proposed JRSSC-DASL technique has high confidentiality rate and minimum processing time as well as memory usage when compared to state-of-the-art methods.

1 INTRODUCTION

In recent days, cyber-physical systems (CPSs) and internet of things (IoTs) deal with the physical world under a combined view of safety and security characteristics. IoT devices utilise a wireless medium to transmit data which affects several attacks. With the rapid growth of sensing information, security of transmission is very important. To enhance the security of data communication, a deep neural learning scheme based on a cryptographic algorithm is proposed.

A Gaussian radial basis function neural network (GRBFNN) was presented in [1] for attack estimation to improve the data transmission via shared communication networks. The designed GRBFNN failed to implement deep learning (DL) with cryptographic technique for achieving a higher confidentiality rate. A dual DL model was presented in [2] for effectively learning the system behaviours and to detect the variety of attacks to improve security. But the learning model failed to analyse the performance of the processing time of attack detection. A certificateless encryption scheme was introduced in [3] to perform the security analysis. However, the higher security of anonymous communication in the cyber-physical-social system was not achieved.

A novel approach was introduced in [4] to guarantee the security of a cloud-based CPS using an authentication scheme. However, the performance of security parameters was not
considered. A new computing architecture in CPS was introduced in [5] for transferring the information using independent devices and smart systems. A privacy-preserving data integrity verification method was presented in [6] with streaming of data for health-CPS. The designed model used the encryption, but it failed to provide more security. A machine learning quorum decider was developed in [7] for large-scale IoT employments to perform anomaly detection with the learned features. The method failed to improve the performance accuracy of anomaly detection.

A secure password-based authentication method was designed in [8] for communicating data with higher security. The designed method has less computation time but the data confidentiality rate was not improved. An IoT-enabled adaptive context-aware and the playful CPS was developed in [9] to improve users’ experience for flexibly controllable remote applications. A software-defined CPS was introduced in [10] to improve the scalable and flexible way of cyber security and to enhance the quality of service.

The major contributions of the proposed jackknife regressive Schmidt Samoa cryptography-based deep artificial structure learning (JRSSC-DASL) technique are summarized as follows:

- A novel JRSSC-DASL technique is introduced to perform secure communication in IoT-enabled CPS with various processes, namely data analysis, classification and encryption with multiple layers.
- Jackknife regression (JR) function is employed in JRSSC-DASL technique to learn the features and classify the data before data transmission. The regression function accurately analyses the feature and improves classification accuracy. Therefore, the classification process of JRSSC-DASL technique minimises the time taken to perform secure communication.
- To improve the data confidentiality by applying Schmidt–Samoa cryptosystem which employs temporary keys (public and private keys). These keys allow the communication session only once. Therefore, JRSSC-DASL technique avoids illegal accessing of data from unauthorised users.
- To improve the data confidentiality rate, JRSSC-DASL technique uses the Schmidt–Samoa cryptography technique. During data transmission, the classified sensed data are converted into cipher text by applying Schmidt–Samoa encryption process. The cipher text is transmitted to the cloud server over the wireless network to avoid illegal data access. Then, the authorised cloud server performs decryption and receives the original data.
- Finally, experimental analyses are carried out with various methods to find that the JRSSC-DASL technique outperforms the standard and other related approaches.

The rest of the article is organised into different sections. Section 2 provides a literature survey. Section 3 details the description of JRSSC-DASL technique and system frameworks. Section 4 explains the experimental setup, result analysis and comparison with other state-of-the-art methods. Finally, the conclusion is presented in Section 5.

## 2 | LITERATURE SURVEY

A behaviour rule specification-based misbehaviour identification method was introduced in [11] for IoT-enabled CPS to detect the misbehaving device. The design rule-based detection method failed to minimise memory and computation overhead. In [12], multi-layered architecture was introduced to the precision agriculture area for solving security and privacy issues in this dynamic cyber-physical environment.

In [13], several research works were presented to analyse and classify the security of cyber-physical systems against cyberattacks. The designed work analyses the performance of confidentiality and integrity, but estimation of time was not solved. The various cyber-physical threat was analysed in [14] with the application of smart home. But the cryptographic technique was not employed to improve the security of the system.

A generic tamper-resistant commitment method was designed in [15] for securing resource-efficient mobile healthcare systems and to provide security through attribute-based encryption scheme. But the performance of data confidentiality of the mobile healthcare system was not improved.

A multi-layered diagrammatic illustration of CPSs was described in [16] for collective safety and security risk analysis with the help of IoT devices. A novel Sybil attack detection method was developed in [17] to improve the security and privacy of communication. However, the designed method failed to apply a digital signature-based cryptographic scheme to accurately detect the Sybil attack in CPS.

Computation techniques and advanced algorithms were developed in [18] for processing heterogeneous data and managing the IoT with cyber-enabled applications. But the quantitative analysis of various performance metrics remains unaddressed. A distributed method based on the IoT model was introduced in [19] for monitoring human activities. The designed model failed to apply classifier for processing the information gathered from the IoT device. In [20], a battery-free wireless sensor was deployed in CPS for health monitoring applications and was sent to the communicating node. But the secure communication of healthcare data remains unaddressed.

## 3 | JACKKNIFE REGRESSIVE SCHMIDT–SAMOA CRYPTOGRAPHY-BASED DEEP ARTIFICIAL STRUCTURE LEARNING TECHNIQUE

CPSs are consciously structured physical systems for the ability to capture a variety of information and interact with the physical world in a fully automatic manner. Deployment of IoT is responsible for the emerging CPS to monitor the information
from various remote objects. Besides, an IoT provides online services to the users through long-distance remote devices (e.g., mobile and sensors). But, the IoT devices are vulnerable to both cyber and physical attacks and hence CPS remains critical. This paper examines the concentration is on secure communication against various attacks using JRSSC-DASL technique. The basic structure of IoT-enabled CPS is depicted in Figure 1.

Figure 1 depicts the basic structure of IoT-enabled CPS. The CPS system comprises two spaces, namely physical and cyberspace. In physical space, IoT devices are deployed for diverse smart applications, such as smart vehicles, smart healthcare, and smart industrial, smart city and so on. IoT is a physical device that is implemented with electronics, software and sensors. It enables the objects for monitoring and sensing the data. Then, the collected data are transferred into cyberspace through wireless communication network (i.e., internet). In cyberspace, the data is analysed and stored in the cloud server for further processing. During communication, security needs to ensure that the different types of attacks are prevented. The proposed JRSSC-DASL technique comprises different process, namely, data collection, analysis and encryption.

The process of data collection is performed through DL. The DL network consists of one input layer, multiple hidden layers and one output layer. Here, two hidden layers are considered. The data gathered from various IoT devices is given as inputs to the deep learning network. Then, the received data is analysed and classified by using JR function in the first hidden layer. Then, the classified data is sent to the cloud server in encrypted form. Encryption is performed in the second hidden layer by using Schmidt–Samoa encryption algorithm. The obtained data is further decrypted through SS decryption algorithm for further processing.

3.1 Data collection

In this phase, the data is collected from the open-source dataset that is created by a virtual IoT environment. After collecting the sensing data from various IoT applications, the data is analysed using machine learning techniques. Finally, the data is transmitted to the cloud server through the internet in a secure manner. The security is achieved by applying the cryptographic technique.

Figure 2 displays the structure of the deep artificial learning which comprises many layers for learning the input. Deep structure receives the input data from the IoT devices which are implemented in various applications. The input data $d_1, d_2, d_3, \ldots, d_n$ is gathered from the IoT device and is given to the input layer. The DL architecture includes several neurons like the nodes which are connected from one layer to consecutive layer in a forward manner with dissimilar regulating weights and it creates the whole neural network. The neurons’ activity at the input layer with time ‘$t$’ is specified as the following expression:

$$\phi_t = \sum_{i=1}^{n} d_i \ast \omega_1 + b$$  \hspace{1cm} (1)

From Equation (1), input layers collect the numerous data, ‘$d_i$’ with regulating weight, ‘$\omega_1$’ between the input and hidden layer 1 and ‘$b$’ symbolizes the bias.
3.2 Jackknife regression function-based data analysis and classification

After receiving the input, the data analysis and classification are carried out by applying the JR function in the first hidden layer. Regression analysis is the statistical method for estimating and analysing various data to find the correlation between one or more independent data and dependent data.

Figure 3 represents the JR function that is applied to analyse the input data and dependent data for identifying which set of categories it belongs to. The classes and the jackknife mean are estimated as follows:

\[ \mu = \frac{1}{n} \sum_{i=1}^{n} d_i \]  
\[ \sigma_{jack} = |\mu - d_i| \]

From Equation (2), \( \mu \) indicates mean of the class, '\( n \)' indicates the number of input samples and \( d_i \) indicates data. Jackknife estimates the variance from its mean to find different classes of data:

From Equation (3), \( \sigma_{jack} \) represents Jackknife variance, \( \mu \) denotes mean of class and \( d_i \) indicates data.

3.3 Schmidt–Samoa cryptosystem

After the analysis of data, the input classified data is sent to the cloud server in the form of encryption. The encryption is performed in the second hidden layer. The SS cryptosystem is an asymmetric cryptograph where the private key and public key are employed to improve the security of data communication. Both these keys are temporary keys which are used only once at a time for data encryption and decryption. This in turn helps in avoiding illegal data access and further improves the data confidentiality. The public keys are distributed broadly and the private key is kept secretly and is identified only to the owner. The SS cryptosystem comprises three processes, namely key generation, encryption and decryption.

Let us consider two largest dissimilar prime numbers \( x \) and \( y \) that generates the private and public key as follows:

\[ R = x^2 \times y \]  
\[ P = R^{-1} \mod \text{LCM}(x-1, y-1) \]

From Equation (4), \( R \) is the public key. The private key is generated as given below:

From Equation (5), \( P \) denotes private key. After the key generation, the encryption is performed to obtain the ciphertext. Figure 4 illustrates SS data encryption. Let us consider the classified data \( d_1, d_2, d_3, \ldots, d_n \) for encryption. The encryption is performed with the help of the public key of the receiver. To encrypt the input data \( 'd' \) and then compute the ciphertext as given below:

\[ D = d^R \mod R \]

In Equation (6), \( D \) denotes the cipher text, \( d \) indicates data and \( R \) denotes the public key of the receiver. Then, the cipher text is sent to the cloud server in cyberspace through the wireless network, that is, the internet. This helps to improve the privacy level of data during communication. The output of the hidden layer is obtained as follows:

\[ G(t) = \sum_{i=1}^{n} d_i \beta_1 + \beta_2 G(t-1) \]
output of the hidden layer is transferred into the output layer as given below:

\[ H(t) = \beta_3 \ast G(t) \]  

(8)

From Equation (8), \( H(t) \) indicates the output from the output layer \( \beta_3 \) designates regulating weight between the hidden and output layer and \( G(t) \) is the output from the hidden layer. The encrypted data is sent to the cloud server through the internet. The cloud server receives the encrypted data and then performs decryption to obtain original data for further processing.

Figure 5 demonstrates the block diagram of the SS data decryption to obtain the original data. The cloud server receives the encrypted data and performs the decryption with its private key. The decryption process is expressed as follows:

\[ d = D^P \mod \gamma \]  

(9)

From Equation (9), \( d \) indicates original data, \( D \) represents the ciphertext and \( P \) denotes private key where \( x \) and \( y \) are the two prime numbers. Then, the cloud server contains the original data. This process increases secure communication by avoiding unauthorised access. The algorithmic description of encryption and decryption is given below:

Algorithm 1 describes data communication with higher security. Initially, the input data is collected from several IoT devices and this data is taken as input at the input layer. The input data is then transferred into the first hidden layer where the data analysis and classification is performed. The JR function is applied to analyse the dependent and independent data. Followed by this, the data with different classes is obtained. Then, the data is sent to the cloud server through the internet. After receiving the data, the cloud server performs the decryption to obtain the original data. This process enhances the security of data communication with minimum time.

4 | EXPERIMENTAL EVALUATION AND PARAMETER DESCRIPTION

Experimental evaluation of the proposed JRSSC-DASL technique and existing methods, namely GRBFNN [1] and dual deep learning model [2] are implemented in Java language with cloud simulator. In order to perform secure data communication in IoT enabled CPS systems, the smart healthcare application is considered in this article using the MHEALTH (Mobile Health) dataset. The dataset is taken from the UCI machine learning repository https://archive.ics.uci.edu/ml/datasets/MHEALTH+Dataset. The MHEALTH dataset is used for monitoring human behaviour through multimodal body sensing. Here, the sensor is used as an IoT device which is placed on the subject’s chest, right wrist and left ankle to measure the motion experienced by various body parts, namely acceleration, rate of turn and magnetic field orientation. The dataset uses 10 subjects to place the IoT device for monitoring their activities. For each subject, the thousands of the data are generated and the data are stored in a different log file. Each file comprises the attributes (by rows) recorded data for all sensors (by columns).

The dataset comprises 23 attributes and one label attribute for identifying the activities. The association task performed by the dataset is a classification. The dataset consists of body
motion and vital signs recordings while performing 12 physical activities such as standing still, sitting and relaxing, lying down, walking, climbing stairs, waist bends forward, frontal elevation of arms, knees bending (crouching), cycling, jogging, running and jumping front and back.

### 4.1 Evaluations metrics and comparative analysis

Different evaluation metrics are used for analysing the performance of the JRSSC-DASL technique over the existing methods, namely GRBFNN [1] and dual deep learning model [2]. These metrics are described and the results are discussed in this section.

#### 4.1.1 Classification accuracy versus data

Classification accuracy is the metric used to measure the number of data that is correctly classified to the number of data generated from the sensor devices. The accuracy is measured using the following expression:

\[
A_{\text{ac}} = \left[ \frac{N_{\text{acl}}}{N} \right] \times 100
\]

From Equation (10), \(A_{\text{ac}}\) denotes classification accuracy, \(N\) denotes the number of data generated from the IoT devices and \(N_{\text{acl}}\) represents the number of data accurately classified. The accuracy is measured in terms of percentage (%). The accuracy of various methods using different data is depicted in Table 1.

An experimental evaluation of classification accuracy using JRSSC-DASL, GRBFNN [1] and dual DL model [2] is shown in Table 1. The recorded value indicates that the accuracy of JRSSC-DASL technique is higher when compared to

| Number of data | GRBFNN | Dual deep learning model system | JRSSC-DASL |
|----------------|--------|---------------------------------|------------|
| 1000           | 83     | 78                              | 91         |
| 2000           | 84     | 80                              | 92         |
| 3000           | 87     | 82                              | 93         |
| 4000           | 85     | 80                              | 91         |
| 5000           | 88     | 82                              | 94         |
| 6000           | 87     | 83                              | 93         |
| 7000           | 86     | 80                              | 92         |
| 8000           | 85     | 81                              | 90         |
| 9000           | 87     | 83                              | 92         |
| 10,000         | 85     | 82                              | 91         |

The graphical illustration of classification accuracy from Figure 6 demonstrates the graphical illustration of classification accuracy recorded in the range of 1000 to 10,000. The input sensed data is taken as input for calculating the accuracy. The various accuracy results are obtained at the vertical axis of the two-dimensional graph. As shown in Figure 6, the accuracy of JRSSC-DASL, GRBFNN [1] and dual DL model [2] is represented by three different colours, namely green, violet and red, respectively. The graphical plots inferred that the accuracy is found to be comparatively better using the JRSSC-DASL technique when compared to refs [1] and [2]. The overall performance of the JRSSC-DASL technique is improved by 7% and 13% than the existing methods.

#### 4.1.2 Confidentiality rate

Confidentiality rate is another important metric of secure data transmission in IoT-enabled CPS system. The confidentiality rate is measured in terms of sensed data and is only accessed or viewed by the authorised entity. The mathematical formula for estimating the confidentiality rate while distributing the data is measured as follows:

\[
C_{\text{Data}} = \left( \frac{N_{\text{acl}}}{N} \right) \times 100
\]
TABLE 2  Confidentiality rate (%)

| Number of data | GRBFNN | Dual deep learning model system | JRSSC-DASL |
|---------------|--------|---------------------------------|------------|
| 1000          | 81     | 77                              | 90         |
| 2000          | 82     | 78                              | 91         |
| 3000          | 84     | 81                              | 92         |
| 4000          | 82     | 79                              | 90         |
| 5000          | 85     | 81                              | 92         |
| 6000          | 84     | 82                              | 90         |
| 7000          | 85     | 79                              | 91         |
| 8000          | 83     | 80                              | 89         |
| 9000          | 85     | 82                              | 91         |
| 10000         | 84     | 81                              | 90         |

FIGURE 7  Graphical illustration of confidentiality rate

The data confidentiality rate ($C_{Data}$) refers to the number of data ‘$N_{data}$’ only accessed or viewed by the authorized entity to the number of data taken as input ‘$N$’. It is measured in terms of percentage (%). The performance results of the confidentiality rate of data transmission from the physical world to the cloud server are reported in Table 2.

The experimental assessment of the confidentiality rate using three techniques JRSSC-DASL, GRBFNN [1] and dual DL model [2] is depicted in Table 2. The reported results prove that the JRSSC-DASL technique outperforms well in terms of higher data confidentiality rate. The observed confidentiality rates of three methods are illustrated in Figure 7.

The graphical representation of the confidentiality rate versus several data is depicted in Table 3 and Figure 7. To discuss the performance of the data confidentiality rate, the number of data obtained from the sensor device is taken in the range from 1000 to 10,000. The graphical plots demonstrate that the proposed JRSSC-DASL technique achieves improved performance compared to the other two state-of-the-art methods.

This improvement of the JRSSC-DASL technique is achieved by applying a SS cryptographic technique in the DL approach. The cryptographic technique encrypts the data while performing communication. During the communication, the data is transmitted to the cloud server via the communication channel. In this case, the communication suffers from various attacks in IoT-enabled CPS. Therefore, the proposed technique uses SS cryptographic technique to secure the data from the unauthorised entity and improves the security level of communication. By applying a SS cryptographic technique, the input data is converted into the cipher text form and sent to the cloud server. The authorised server receives the encrypted data and performs the decryption to obtain original data. This process of the JRSSC-DASL technique increases the data confidentiality rate. The overall comparison results indicate that the confidentiality rate is found to be increased by 9% using the JRSSC-DASL technique when compared to GRBFNN [1] and 13% when compared to Dual DL model [2].

4.1.3 Processing time

The third metric is the processing time which is referred as an amount of time taken by the algorithm to perform secure data communication in IoT-enabled CPS systems. The overall processing time data communication is measured using the following expression:

$$PT = N \times Time [d]$$ (12)

where $PT$ denotes the processing time, $N$ denotes the number of input data and $Time [d]$ denotes the time taken by the algorithm to process the single data. The time taken by the algorithm is measured in the unit of milliseconds (ms).

Table 3 and Figure 8 reports the experimental assessment results of processing time versus the number of data. As revealed in the graph, while increasing the count of input data,
processing time increased for all the three methods due to the large amount of data generated by the sensor device. Among the three methods, the processing time is found to be minimal by applying the JRSSC-DASL technique compared to the existing methods. The appropriate reason is that the classification-based encryption technique is applied. Before data transmission, the incoming sensed data is analysed and classified.

These processes minimise the secure data transmission from sender to receiver. Instead of sending the whole data to the server, the incoming data is analysed and partitioned into the number of classes. Then, the classified data is applied for encryption. Besides, the proposed SS cryptographic technique effectively executes the data encryption with lesser time consumption. This is proved by statistical evaluation by considering 1000 data to compute processing time. The amount of time taken by applying the JRSSC-DASL technique for secure communication is 28 ms and the processing time of the other two methods [1,2] are 32 and 35 ms, respectively. Likewise, the nine runs are performed with various counts of sensed data. The overall results of the proposed technique are evaluated with the results of existing methods. The comparison results prove that the processing time of the JRSSC-DASL technique is considerably reduced by 9% compared to ref. [1] and 15% compared to ref. [2].

4.1.4 Memory usage

The final performance metric is memory usage which is defined as an amount of memory consumed by the algorithm for performing secure communication. The overall memory usage is calculated as given below:

\[ MU = N \times Mem [d] \quad (13) \]

From Equation (13), \( MU \) specifies the memory usage, \( N \) specifies the number of data \( (d) \) and \( Mem \) specifies memory consumption for processing the data. The memory usage is measured in terms of megabytes (MB).

Table 4 describes the experimental results of memory usage versus a number of data using three methods. In order to calculate the memory consumption to perform the secure data transmission, the number of data is taken in the range of 1000 to 10,000. The plots with various results are illustrated in Figure 9. The performance results of the memory consumption of three different methods are illustrated in Figure 9. The chart proves that the proposed JRSSC-DASL technique consumes less amount of memory space for processing the secure data communication. The reason for less memory consumption is the proposed JRSSC-DASL technique that performs the encryption process before the data transmission. Due to data encryption, the size of the input data is reduced and hence the memory consumption also minimised. The performance of the proposed JRSSC-DASL technique is compared to the existing results. The overall comparison results prove that the memory consumption of the proposed JRSSC-DASL technique is said to be minimised by 12% compared to ref. [1] and 19% compared to ref. [2].
5 | CONCLUSION

This paper examines a deep artificial structure learning-based IoT-enabled CPS security system is introduced. The proposed DL models learn the normal performances of the IoT system and also provide detailed analytics of the input data. The aim of the JRSSC-DASL technique is to provide a higher security level and to achieve high confidentiality rate and less time consumption. First, in this work, data analysis is performed based on the JR function. Next, with the classified data, SS cryptographic is applied for encryption and decryption to improve the security. Finally, the cloud server decrypts the data for improving the security of data communication. Experimental evaluations are conducted to estimate the performance of the proposed JRSSC-DASL technique with two existing methods in terms of different factors. The results confirm that the efficiency of the JRSSC-DASL technique is achieved in terms of high data confidentiality and less processing time and memory usage than conventional methods.

ORCID

Rizwan Patan https://orcid.org/0000-0003-4878-1988

REFERENCES

1. Farivar, F., et al.: Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. IEEE Trans. Ind. Infr. 16(4), 2716–2725 (2020)
2. Li, F., et al.: Enhanced cyber-physical security in internet of things through energy auditing. IEEE IoT J. 6(3), 5224–5231 (2019)
3. Li, F., et al.: Privacy-aware secure anonymous communication protocol in CPSS cloud computing. IEEE Access 8, 62660–62669 (2020)
4. Muniasamy, K., et al.: Formal methods based security for cloud-based manufacturing cyber physical system. IFAC 52(13), 1198–1205 (2019)
5. Gushev, M., Dew computing architecture for cyber-physical systems and IoT. Internet of Things, 11, 1–22 (2020)
6. Xu, J., et al.: Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber-physical system. Future Gener. Comput. Syst. Elsevier, 108, 1287–1296 (2020)
7. Anharan, V., et al.: Machine learning quorum decider (MLQD) for large scale IoT deployments. Procedia Comput. Sci. Elsevier, 151, 959–964 (2019)
8. Renuka, K.M., et al.: Design of a secure password-based authentication scheme for M2M networks in IoT enabled cyber-physical systems. IEEE Access 7, 51014–51027 (2019)
9. Lu, C.-H., IoT-enabled adaptive context-aware and playful cyber-physical system for everyday energy savings. IEEE Trans. Hum.-Mach. Syst. 48(4), 380–391 (2018)
10. Darabseh, A., Freris, N.M., A software-defined architecture for control of IoT cyberphysical systems. Cluster Comput. Springer, 22, 1107–1122 (2019)
11. Sharma, V., et al.: BRiOT: behavior rule specification-based misbehavior detection for IoT-embedded cyber-physical systems. IEEE Access 7, 118556–118580 (2019)
12. Gupta, M., et al.: Security and privacy in smart farming: challenges and opportunities. IEEE Access 8, 34564–34584 (2020)
13. Alguliyev, R., Imamverdiyev, Y., Sukhostat, L., Cyber-physical systems and their security issues. Comput. Ind. 100, 212–223 (2018)
14. Heartfeld, R., et al.: Avgoustinos Filippoupolitis, Etienne Roelsch, “A taxonomy of cyber-physical threats and impact in the smart home. Comput. Secur. Elsevier, 78, 398–428 (2018)
15. Hahn, C., Kwon, H., Hur, J., Trustworthy delegation toward securing mobile healthcare cyber-physical systems. IEEE IoT J. 6(4), 6301–6309 (2019)
16. 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)
17. Kumaria, D., Singha, K., Manjul, M., Performance evaluation of Sybil attack in cyber physical system. Procedia Comput. Sci. Elsevier, 167, 1013–1027 (2020)
18. 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)
19. Mora, H., et al.: An IoT-based computational framework for healthcare monitoring in mobile environments. Sensors 17, 1–25 (2017)
20. Loubet, G., Takaes, A., Dragomirescu, D., Implementation of a battery-free wireless sensor for cyber-physical systems dedicated to structural health monitoring applications. IEEE Access 7, 24679–24690 (2017)

How to cite this article: Kannan C, Dakshinamoorothy M, Ramachandran M, Patan R, Kalyanaraman H, Kumar A. Cryptography-based deep artificial structure for secure communication using IoT-enabled cyber-physical system. IET Commun. 2021;15:771–779. https://doi.org/10.1049/cmu2.12119