Miyaguchi–Preneel Snefru Cryptographic Blockchain and Maximum Likelihood Consensus Deep Convolutional Q-Learning for Secure Data Access in E-Learning

N R Chilambarasan [1], A Kangaiammal [2]

[1] PhD Research Scholar (Part Time), PG & Research Department of Computer Science,
[2] Assistant Professor, Department of Computer Applications

Government Arts College (Autonomous), Salem-7, Tamil Nadu, India

Abstract

E-learning is a novel perception that includes all educational activities of an individual or group working online, synchronously or asynchronously, connecting via various devices through the internet. The e-learning system has faced some concerns related to security, availability and reliability. To overcome these challenges, an important security approach is required to preserve the data of the e-learning system. A novel Miyaguchi–Preneel Snefru Cryptographic Blockchain and Maximum Likelihood Consensus Deep Convolutional Q-Learning Network (MPSCB-MLCDCQN) is introduced with three different processes namely data collection, access control and data analysis. In the proposed MPSCB-MLCDCQN, Internet of Things (IoT) devices are employed to sense and collect student activities during the e-learning process. Secondly, secure data access is performed through the Miyaguchi–Preneel Snefru hashes decentralized blockchain technology for avoiding unauthorized access. Finally, the Maximum Likelihood Consensus Deep Convolutional Q-Learning Network (MLCDCQN) is applied to analyze the student data collected from the IoT devices to make optimal action. The student data are analyzed using the Maximum Likelihood Consensus regression function by learning the features of input data and predicting the student performance behavior with higher accuracy. A comprehensive experiment of the proposed MPSCB-MLCDCQN is conducted using e-learning activities' dataset in a CloudSim simulator with certain performance metrics such as confidentiality rate, data integrity rate, processing time and prediction accuracy with respect to a number of student data. The results discussed show that the MPSCB-MLCDCQN technique provides improved performance in terms of achieving higher security and data analysis than the existing methods.

Keywords: Cloud, E-learning, Secure Access Control, Miyaguchi–Preneel Hash Decentralized Blockchain, Maximum Likelihood Consensus Regression, Deep Convolutional Q-Learning Network

1. Introduction

Currently, several universities and organizations make a profit from the information technologies to extend their educational policy and attract more learners. Therefore, distance e-learning technologies are implemented by universities to provide a more flexible education system. In the e-learning process, a number of learners sign up for online courses. This development is mainly provided by Cloud Computing. In the cloud-based educational context, the security factor in distribution of the educational content is significant and creates several security challenges, such as access control and security preservation of content learning.

A fog computing e-learning scheme was introduced in [1] to enhance the efficiency of learning data analysis and minimizes the encryption problem in terms of computation cost on user's devices. However, the higher performance of integrity level was not achieved. An IoT-applicable access control model was developed in [2] under double-layer blockchain architecture for secret sharing. But the designed model failed to provide an architecture decentralized for efficient IoT access control.

A blockchain-based group key management approach was introduced in [3] for securing keys and establishing secure data transmission in fog-based IoT systems. A Model of Digital Identity (MDI) was developed in [4] for e-learning systems to increase the performance of information security. However, it failed to highlight the development of a new security tool in e-learning environments for enhancing information security.

Integration of Blockchain and Federated Learning (BCFL) framework was introduced in [5] for secure data distribution. But the performance failed in analyzing the data confidently and with integrity during the data distribution. A Novel Online Teaching and Assessment (NOTA) method was designed in [6] using Blockchain to provide distant access. But the efficient hash function was not introduced to Blockchain technology to enhance the integrity of data access.

Machine learning models were developed in [7] to predict the student's performance as low or high. But it failed to compare the designed model with considered more sophisticated machine learning algorithms for accurate classification. A Behaviour Classification based E-learning Performance (BCEP) prediction approach was introduced in [8] for online student performance behavior classification. But it was not accurate to ensure the quality of online learners' learning.

A Blockchain-based framework was developed in [9] for secure storing, and exchanging the networking sensitive data. But it failed to explain blockchain technology with a reasonable cost in more detail. In [10], a fundamental investigation of security and confidentiality risks for online education environments was presented.

1.1 Contributions of MPSCB-MLCDCQN

The followings are the major contributions of MPSCB-MLCDCQN:

- Proposed MPSCB-MLCDCQN to enhance the data integrity and confidentiality in e-learning systems using Miyaguchi–Preneel Snefru hashes Decentralized blockchain technology. Contrary to the conventional blockchain, the proposed technique uses the Snefru cryptographic function to

generate the hash value with help of the Miyaguchi–Preneel compression function. The hashed data are accessed by the authorized user to preserve the integrity of data during data sharing.

- To improve student performance prediction accuracy and minimize time consumption, MPSCB-MLCDCQN develops the Maximum Likelihood Consensus Deep Convolutional Q-Learning Network. The proposed Maximum Likelihood Consensus regression is applied to a state-space of a Deep Convolutional Q-Learning Network for analyzing the student data and the mean of the particular class. The target classification results are observed at the action state of the Deep Convolutional Q-Learning Network.
- Finally, a series of experimental evaluations are carried out with the different metrics to find that the performance of MPSCB-MLCDCQN outperforms than the other related approaches.

1.2 Outlines

The remainder of this paper is organized as follows. Section 2 presents the related work. Section 3 describes our proposed MPSCB-MLCDCQN with IoT automated secured data accessing in detail. Section 4 presents the implementation detail and dataset description. Section 5 discusses the performance analysis in detail with the aid of tables and graphs. Finally, Section 6 concludes the paper.

2. Related Works

A blockchain-based access control method was designed in [11] for the data generated by IoT devices. However, the performance of data confidentiality and integrity was not considered by using the access control method. A lightweight and decentralized secure access control model was developed in [12] for IoT based on a multi-agent system and a blockchain to improve the secure communication between the devices. But it was not efficient to achieve a high level of security.

A fabric-IoT called Hyperledger Fabric blockchain framework was developed in [13] for the access control system. But it failed to enhance the scalability of the framework and support more IoT application integration. A new model was introduced in [14] based on zero-knowledge proof and smart contract technology using blockchain for enhancing the security of the IoT. However, the performance of integrity of secured data access was not achieved. A Dynamic-IoTrust decentralized access control method was introduced in [15]. But it failed to reduce the complexity and cost as well as processing time of the system.

Privacy Protected Blockchain-based Architecture was introduced in [16] for secure distribution of the Students' records. But it failed to deploy the architecture over a permission blockchain platform. An integration of Hyperledger Fabric blockchain and IoT devices were developed in [17] to increase the access control and trust for IoT devices. The system failed to evaluate different security performance matrices.

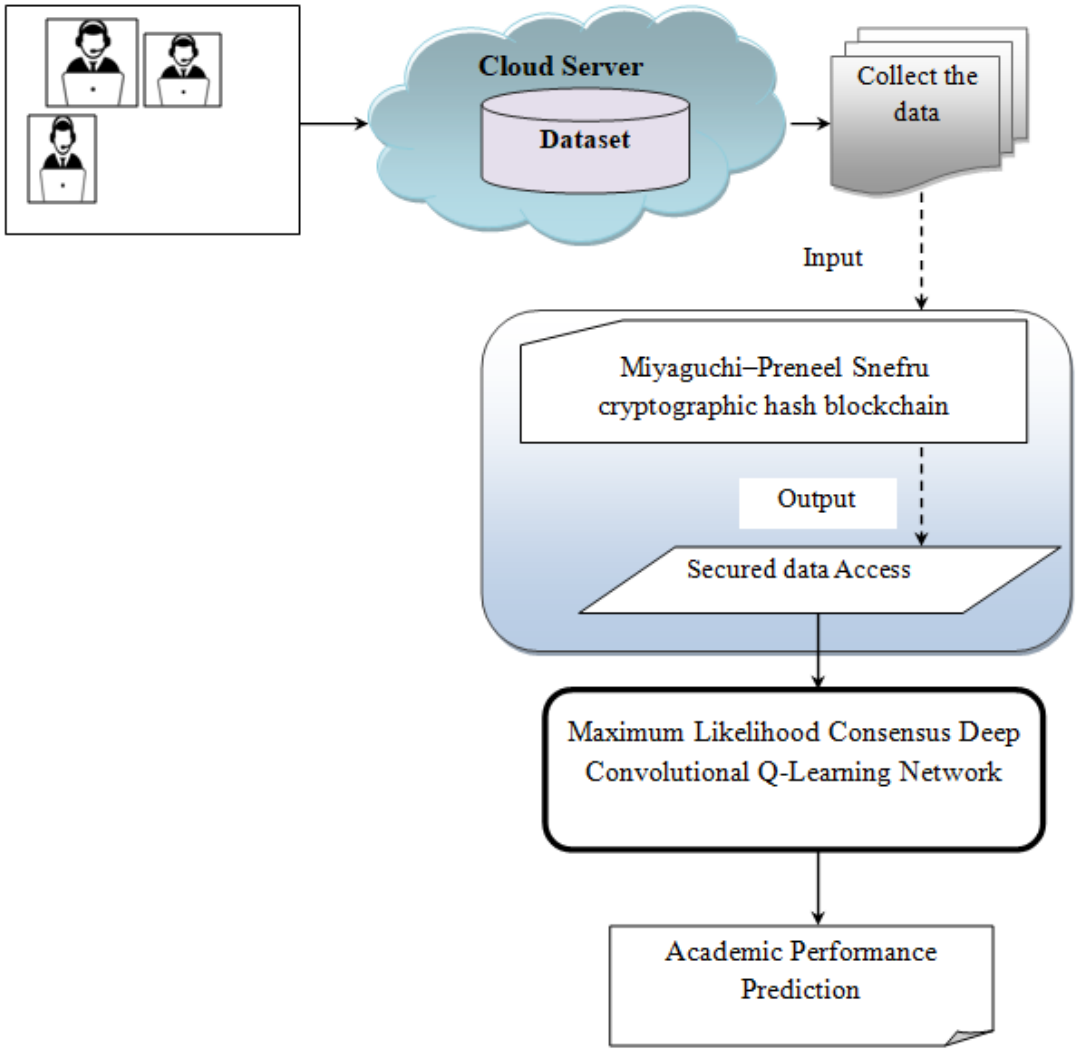
Blockchain-based federated learning methodologies were developed in [18] for high potential privacy and security. An access control method was developed in [19] based on blockchain for IoT endpoints. A novel blockchain-based access control protocol was designed in [20] for secure communication.

3. Methodology

A novel MPSCB-MLCDCQN is developed in this section with three different processes namely data collection, access control and data analysis. Security analysis of MPSCB-MLCDCQN demonstrates reliability towards achieving data confidentiality, access control and deploying the access control procedures on the blockchain. However, the various transaction data on the public blockchain face an additional Security issue for IoT devices. In the proposed MPSCB-MLCDCQN, Internet of Things (IoT) devices are employed to sense and collect the data and perform secure data access by avoiding unauthorized access. The collected data are analyzed for prediction.

Figure 1 depicts the overall architecture of the proposed MPSCB-MLCDCQN technique that includes three stages. First, IoT devices are used for collecting the data in terms of student activities after the data collection. The data access control is performed using the Miyaguchi–Preneel Snefru cryptographic hash blockchain. After accessing the data, the performance of student activities is predicted by using the Maximum Likelihood Consensus Deep Convolutional Q-Learning Network. An elaborate description of the proposed MPSCB-MLCDCQN technique is presented in the forthcoming sections.

Figure 1: Architecture of the Proposed MPSCB-MLCDCQN Technique



3.1 Miyaguchi–Preneel Snefru Cryptographic Hash Blockchain for Secure Data Access

The development of information technology and the Internet of Things (IoT) enables the educational institutions which generate more and more of big data which needs to be stored, processed efficiently, and securely shared among the authorized entities. Many different schemes were introduced for sharing sensitive data but it still faces some challenges to achieve data privacy. Furthermore, most data-sharing schemes have no integrity verification. To solve the above mentioned conditions, a novel, efficient and a secure data sharing scheme is required. One of such kind is Miyaguchi–Preneel Snefru cryptographic hash block chain, which provides improved data confidentiality and integrity. The scheme guarantees security and authorized access to shared sensitive student data.

The proposed MPSCB-MLCDCQN technique uses the decentralized blockchain which involves with multiple users, i.e. group of users. The decentralized technology did not have a central authority.

Data sharing on the decentralized blockchain are conducted directly between the entities without any intermediary organization, among the members, eliminating the need for a middleman.

Figure 2: Decentralized Blockchain

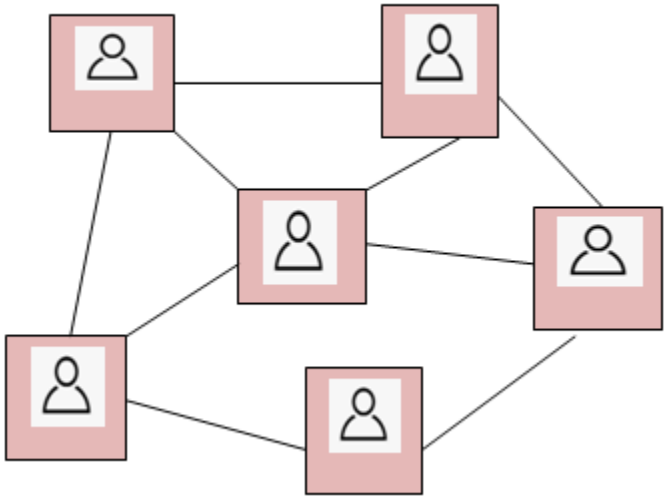


Figure 2 given above illustrates the process of decentralized data sharing among the group users in the educational institution. During the data sharing, security and data confidentiality are achieved through the Miyaguchi–Preneel Snefru cryptographic blockchain.

Figure 3: Block Diagram of Miyaguchi–Preneel Snefru Cryptographic Hash Decentralized Blockchain Model

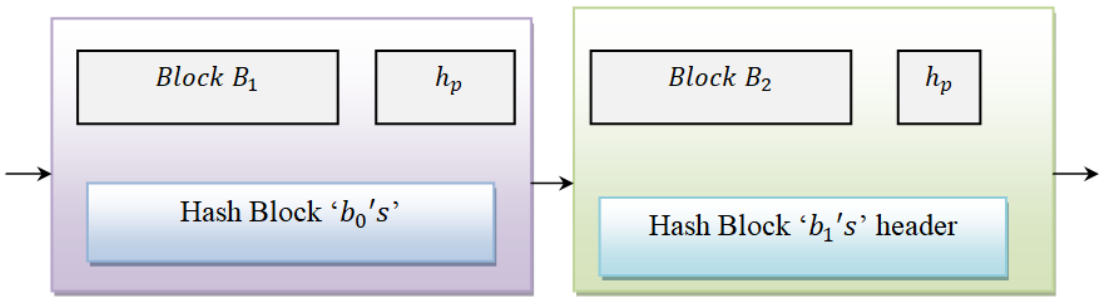


Figure 3 illustrates the block diagram of the Snefru cryptographic hash decentralized Blockchain model. The network model includes a block header, timestamp (T_s), Hash Block (b_i), and a previous hash block (h_p). Each block has a unique transaction for transmitting the student data collected from the IoT devices. The hash block is used to generate the cryptographic hashes data of arbitrary length. The proposed blockchain uses the Snefru cryptographic hash to generate the hash for each student's data during the transaction.

The Snefru cryptographic hash generates the hashes for each input of arbitrary length into 128-bit values. Snefru cryptographic hash uses a padding method that includes an additional padding block together with the length of the input message (i.e. data). By applying a Snefru cryptographic hash, the input message is divided into a number of blocks as shown in Figure 3.

Figure 4: Miyaguchi–Preneel Snefru Cryptographic Hash

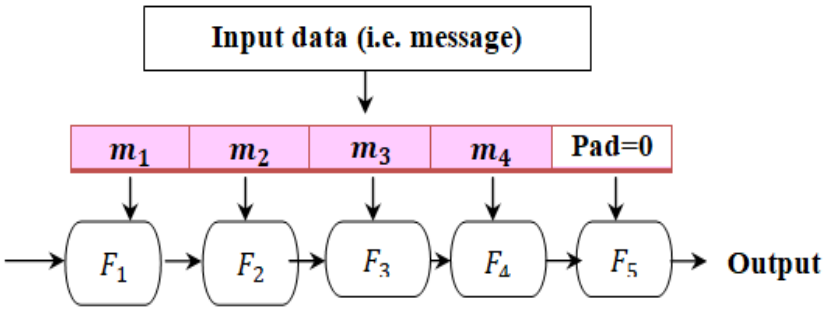


Figure 4 illustrates the Miyaguchi–Preneel Snefru cryptographic hash function to generate the output hash. As shown in Figure 3, m_1, m_2, m_3, m_4 indicates that the message block, F_1, F_2, F_3, F_4 denotes a Miyaguchi–Preneel compression function, the last block is padded by '0's (i.e. Pad = 0). The proposed Snefru cryptographic hash uses the Miyaguchi–Preneel compression function to generate the hash for each message block.

By applying Miyaguchi–Preneel compression function, the output of ciphertext is then XORed with the message block and then also XORed with the previous hash value to produce the next hash value. The previous hash value is fed as the key to the block cipher. In the first round, when there is no previous hash value it, uses a pre-specified initial value ($h_0 = 0$).

The output of the Miyaguchi–Preneel function '$h\ (F)$' is generated as given below,

$$h\ (F)\ = [K_{(D_{h_{i-1}})}(m_i) \oplus h_{i-1} \oplus m_i] \quad (1)$$

Where message block 'm_i' and the previous hash value (h_{i-1}) is initially preset to '0'. 'K' denotes a block cipher, D indicates a key to a block cipher XORed with the previous hash value ' h_{i-1}' and the message block (m_i). The output hash is taken from the final compression function and added with the padding Pad value as given below:

$$h = (h\ (F) \parallel Pad\ ) \quad (2)$$

Where h indicates a final hash of the message, $h\ (F)$ indicates an output of compression function, Pad denotes padding, '||' denotes a concatenation operator. The proposed technique allows the authorized user to access the data and avoids unauthorized access. This process improves the data integrity and confidentiality during the transaction.

Algorithm 1: Miyaguchi–Preneel Snefru Cryptographic Hash Blockchain for Secure Data Access

Input: E-learning dataset, Number of IoT devices $d_1, d_2, \ldots d_m$, Students' Data $D_1, D_2, \ldots D_n$

Output: Improve the secure data access

Begin
  Collect the student's data $D_1, D_2, \ldots D_n$ from dataset
  For each transaction 't'
    Construct blockchain
    For each data D_i
      Divides into message blocks $m_1, m_2, m_3, \ldots m_n$
      For each block 'm'
        Apply compression function on the generate the hash $h\ (F)$
        Add padding with $h\ (F)$
        Obtain final hash 'h'
      End for
    End for
  End for
End

Algorithm 1 given above illustrates the step-by-step process of secure data access of student e-learning activities. The IoT generated a large volume of data to ensure accurate and timely data analytics. First, the blockchain is constructed based on two concepts such as Miyaguchi–Preneel compression function applied to a Snefru cryptographic hash. The input message is divided into the number of blocks. Then the Miyaguchi–Preneel compression function generates the hash value of the original data. Finally, the output of the compression function is combined with the padding value to get the final hash value. This hash value is distributed to the authorized users for achieving higher data confidentiality and integrity.

3.2 Maximum Likelihood Consensus Deep Convolutional Q-Learning Network for Performance Prediction

After transmitting the student data to the authorized user, the proposed MPSCB-MLCDCQN technique executes the performance prediction in the educational entities and institutes. Due to the large volume of data in educational databases, predicting the performance of students has become more complex. Therefore, the proposed MPSCB-MLCDCQN technique uses the Maximum Likelihood Consensus Deep Convolutional Q-Learning Network (MLCDCQN) for accurate prediction with minimum time consumption.

Figure 5: Block Diagram of Academic Performance Prediction

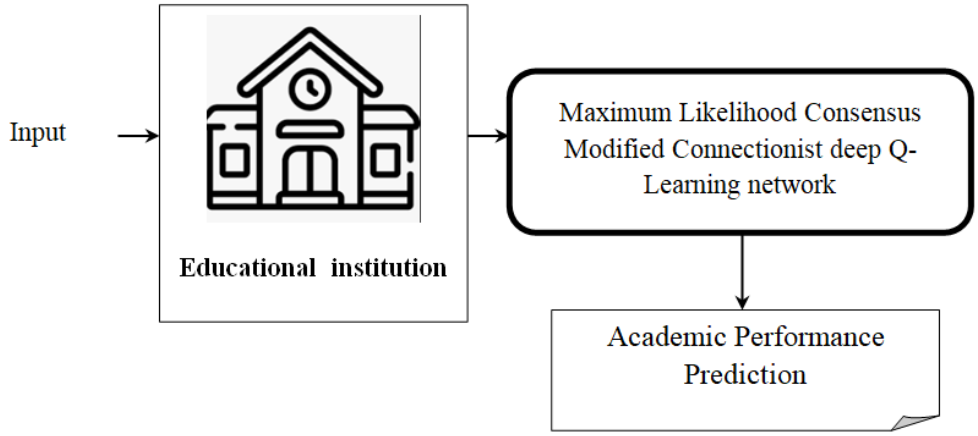


Figure 5 given above illustrates the block diagram of Academic Performance Prediction using Maximum Likelihood Consensus Deep Convolutional Q-Learning Network. In a deep Convolutional Q-Learning network, a convolutional neural network is to approximate the Q-value function. The deep Convolutional Q-Learning network consists of two major states such as state and action. The state space is given as the input and the Q-value of all possible actions is generated as the output in the active state. The integration of Q-learning and Convolutional Neural Networks is illustrated below:

Figure 6: Schematic Construction of Deep Convolutional Q-Learning Network

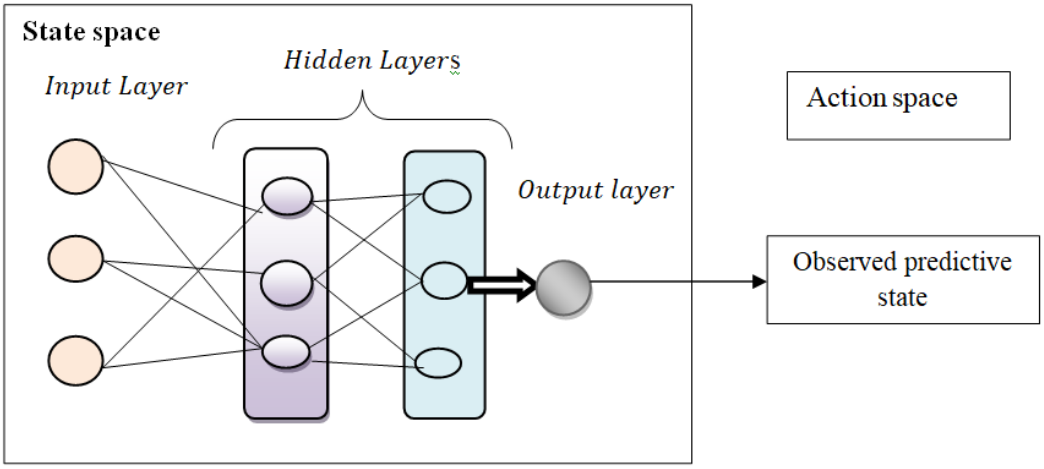


Figure 6 represents the schematic construction of a deep Convolutional Q-Learning network for accurate prediction. A deep Convolutional Q-Learning network uses the input layer to receive the input data. The input is transformed into the first hidden layer where the data analysis is performed using Maximum Likelihood Consensus regression.

Maximum Likelihood Consensus regression is a machine learning technique to estimate the relationships between dependent variables, i.e. prediction outcomes and one or more independent

variables. The proposed regression function analyzes the data using Maximum Likelihood estimation and provides the outcomes in terms of grade-level poor, average, and high.

$$R = \frac{1}{\sqrt{2\pi}v} \exp\left[-\frac{1}{2}\left(\frac{D_i-\mu}{v}\right)^2\right] \quad (3)$$

$$Y = \arg\max R \quad (4)$$

Where R denotes a likelihood function output, 'v' denotes a deviation, D_i indicates features, 'μ' denotes a mean, Y indicates a regression output, $arg\,max$ denotes an argument of maximum function. The data closer to the mean value is categorized into a particular class. Based on the regression analysis, the student performance grade level is obtained at action state. The state is calculating Q-Value in the state.

$$Q_n\ (\alpha_s, \beta_s) = Q\ (\alpha_s, \beta_s) + \rho.[\ Z_t + \delta\ \arg\max R - Q\ (\alpha_s, \beta_s)] \quad (5)$$

Where, $Q_n(\alpha_s, \beta_s)$ denotes a updated Q-Value, $arg\,max$ denotes an argument of maximum function, R indicates a regression output, $Q\ (\alpha_s, \beta_s)$ denotes a current Q-value, ρ denotes a learning rate $0 < \rho < 1$, Z_t denotes a reward, δ indicates a discount factor only slightly lesser than 1, α_s, β_s denotes a action and state space respectively. Based on the above estimated results, performance grade level is accurately predicted. The algorithmic process of proposed technique Maximum Likelihood Consensus Deep Convolutional Q-Learning Network (MLCDCQN) is described as given below:

Algorithm 2: Maximum Likelihood Consensus Deep Convolutional Q-Learning Network based Performance Prediction

Input: Student data $\boldsymbol{D_1, D_2, \ldots D_n}$

Output: Increase performance level prediction accuracy

Begin

Collect the data $D_1, D_2, D_3 \ldots . D_n$ in input layer

Initialize the classes and mean μ_1, μ_2, μ_3 / hidden layer 1

For each mean 'μ_i'

For each data 'D_i'

Measure the likelihood 'R'

End for

End for

Given the regression output into a action state

Obtain the Q-value '$Q_n(\alpha_s, \beta_s)$'

Find student performance level prediction

End

Algorithm 2 given above illustrates the step by step process of student performance level prediction using Maximum Likelihood Consensus Deep Convolutional Q-Learning Network. Initially, the input student data are collected from the dataset at the input layer. The input is sent to the hidden layer where the Maximum Likelihood Consensus regression is applied for analyzing the data and mean values. Then the estimated output is given to the action state to obtain the Q-value. As a result, student performance grade level is correctly predicted with minimum time.

4. Experimental Setup

Experimental evaluation of the proposed MPSCB-MLCDCQN technique and two existing methods namely fog computing e-learning scheme [1], IoT-applicable access control model [2] are implemented using Java language and CloudSim simulator. An Educational Process Mining (EPM): A Learning Analytics Data Set is taken from UCI Machine Learning Repository [21]. The dataset consists of 2,30,318 instances and 13 attributes. The dataset is constructed from the recordings of 115 student's activities through e-learning using IoT devices during six different sessions. There are 6 folders consists of student's activities generated per session. The associated task performed by the dataset is classification, regression, and clustering. The attribute description is in the Table 1.

Table 1: Attribute Description

Sr. No.	Attributes	Description
1	session	The number of laboratory session from 1 to 6.
2	student_id	It shows the id of student from 1 to 115
3	exercise	It shows the id of the exercise the student is working on.
4	activity	The activities are labeled based on the title of web pages that are on focus / in the view of the student. To read about the details of activity labels, see 'activities_info.txt'.
5	start_time	It shows the start date and time of a specific activity with the format: dd.mm.yyyy hh:mm:ss
6	end_time	It shows the end date and time of a specific activity with the format: dd.mm.yyyy hh:mm:ss
7	idle_time	It shows the duration of idle time between the start and end time of an activity in milliseconds.
8	mouse_wheel	It shows the amount of mouse wheel during an activity.
9	mouse_wheel_click	It shows the number of mouse wheel clicks during an activity.
10	mouse_click_left	It shows the number of mouse left clicks during an activity.
11	mouse_click_right	It shows the number of mouse right clicks during an activity.
12	mouse_movement	It shows the distance covered by the mouse movements during an activity.

13	keystroke	It shows the number of keystrokes during an activity.

5. Performance Results and Discussion

In this section, performance results and discussion of the MPSCB-MLCDCQN technique and fog computing e-learning scheme [1], IoT-applicable access control model [2] are described. The performance results are compared with the various metrics such as confidentiality rate, integrity rate, prediction accuracy and prediction time. The tabulation and graphical results indicates the performance of proposed and existing methods.

- **Confidentiality Rate:** It is measured as the ratio of the number of data only accessed by authorized users. The formula for calculating the data confidentiality rate is given below:

$$Rate_{con} = \left[\frac{n_{aae}}{n}\right] * 100 \quad (6)$$

Where, $Rate_{con}$ indicates the confidentiality rate, 'n' indicates the number of student data generated from IoT device, 'n_{aae}' symbolizes the number of data accessed by the authorized users. The confidentiality rate is measured in terms of percentage (%).

- **Data Integrity Rate:** It is the ratio between the number of data that are not altered by any third party to the number of data used for transmission. The data integrity rate is measured as given below:

$$Rate_{Int} = \left[\frac{n_{aa}}{n}\right] * 100 \quad (7)$$

Where, $Rate_{Int}$ symbolizes a data integrity rate, 'n_{aa}' designates the number of data not altered, 'n' indicates a total number of data. The data integrity rate is computed in terms of percentage (%).

- **Prediction Accuracy:** It is measured as a ratio of the number of student data that is correctly accessed and the activities are predicted to the total number of student data generated from the IoT devices. The formula for calculating the prediction accuracy is given below:

$$PA = \left[\frac{Number\ of\ student\ data\ correctly\ predicted}{n}\right] * 100 \quad (8)$$

Where, PA symbolizes a prediction accuracy, 'n' indicates the number of student data. The prediction accuracy is measured in terms of percentage (%).

- **Processing time:** It is defined as the amount of time consumed by the algorithm to predict the performance grade level. The formula for calculating the prediction time is given below:

$$PT = n * Time\ (ASD) \quad (9)$$

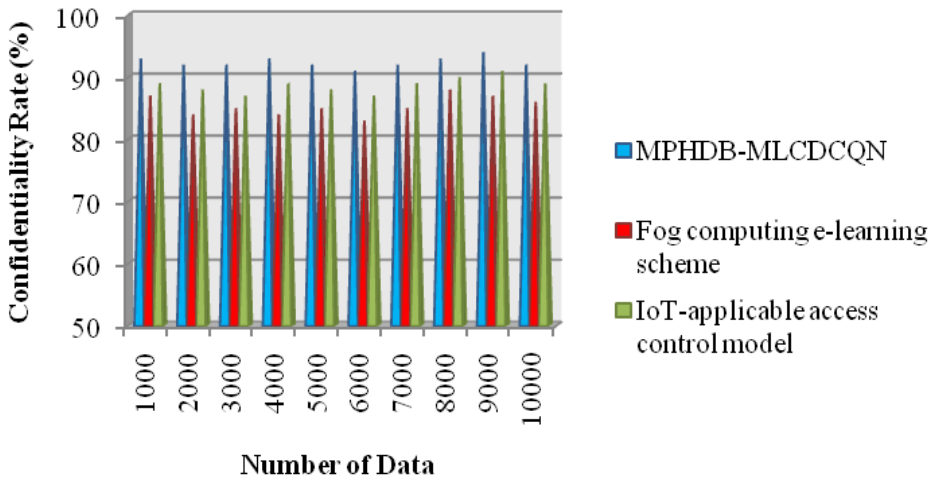
Where, 'PT' represents a prediction time, 'n' indicates the number of student data, $Time\ (ASD)$ indicates a time for predicting the performance level of single student data. The prediction time is measured in terms of milliseconds (ms).

Table 2: Comparison of the Confidentiality Rate

Number of Data	Confidentiality Rate (%)		
	MPHDB-MLCDCQN	Fog Computing E-Learning Scheme	IoT-Applicable Access Control Model
1000	93	87	89
2000	92	84	88
3000	92	85	87
4000	93	84	89
5000	92	85	88
6000	91	83	87
7000	92	85	89
8000	93	88	90
9000	94	87	91
10000	92	86	89

The performance results of the data confidentiality rate using the three techniques - MPSCB-MLCDCQN technique, fog computing e-learning scheme [1], and IoT-applicable access control model [2] - are depicted in the Table 2 and Figure 6. The number of student data are taken as input is in the range from 1,000 to 10,000. For each method, ten results are observed with respect to various counts of input. The observed results indicates that the MPSCB-MLCDCQN technique outperforms well in terms of achieving a higher data confidentiality rate than the other two existing methods. The overall performance of MPSCB-MLCDCQN technique indicates that the performance of data confidentiality rate is improved by 8% and 4% when compared to existing methods.

Figure 7: Performance Results of Data Confidentiality Rate



To discover the best performance, the MPSCB-MLCDCQN technique uses Miyaguchi–Preneel hash decentralized blockchain technology for avoiding the unauthorized access during the data transaction. The proposed decentralized blockchain technology uses the Miyaguchi–Preneel Snefru cryptographic function to generate the hash value and securely communicating the data among the authorized users. This helps to minimize the unauthorized access hence it improve the confidentiality rate.

Table 3: Comparison of the Data Integrity Rate

Number of Data	Data Integrity Rate (%)		
	MPSCB-MLCDCQN	Fog Computing E-Learning Scheme	IoT-Applicable Access Control Model
1000	92	85	87
2000	91	83	86
3000	91	83	86
4000	92	85	88
5000	91	85	86
6000	90	83	86
7000	91	85	88
8000	92	87	89
9000	93	86	88
10000	91	85	87

Figure 8: Performance Results of the Data Integrity Rate

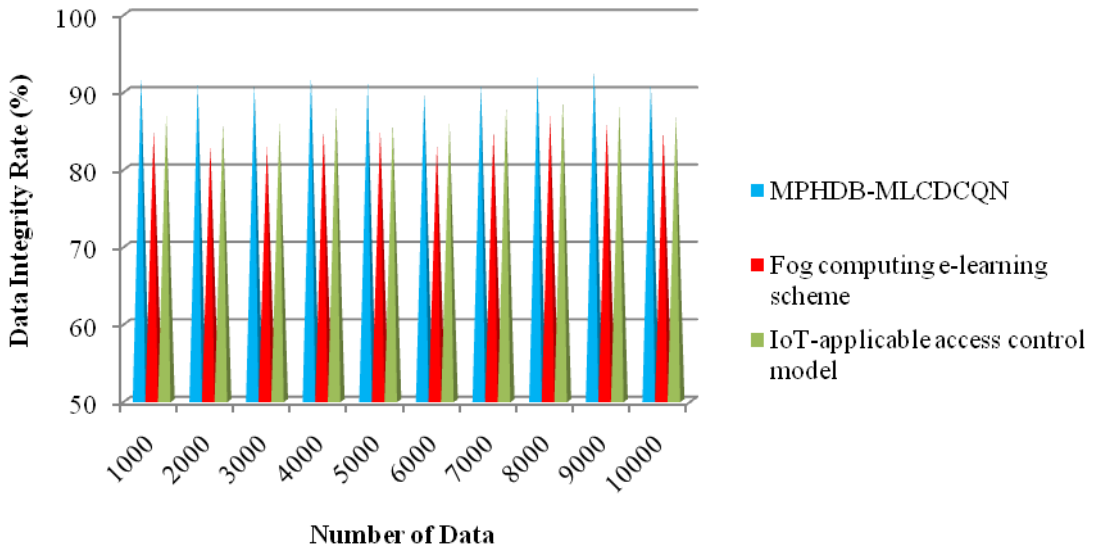


Table 3 and Figure 8 depicts the performance results of integrity rate using three different techniques - MPSCB-MLCDCQN technique, fog computing e-learning scheme [1], and IoT-applicable access control model [2] - along with the number of student data collected from the dataset. For the experimental consideration, the number of student data taken are in the range from 1,000 to 10,000. Compared to existing methods, the MPSCB-MLCDCQN technique provides the superior performance in the integrity rate. The different results are observed for each method. The overall observed results indicate that the MPSCB-MLCDCQN technique increases the integrity rate by 8% compared to [1] and 5% compared to [2]. This is due to the application of Miyaguchi–Preneel Snefru cryptographic hash function is applied to a blockchain technology. The input message is divided into the number of blocks. Then the Miyaguchi–Preneel compression function generates the hash value of the original data. Finally, the output of compression function is combined with the padding and to get the final hash value. This process of proposed MPSCB-MLCDCQN technique increases the integrity rate.

Table 4: Comparison of Prediction Accuracy

Number of Data	Prediction Accuracy (%)		
	MPSCB-MLCDCQN	Fog Computing E-learning Scheme	IoT-Applicable Access Control Model
1000	91	85	87
2000	90	81	85
3000	90	82	85
4000	91	83	87
5000	90	84	85
6000	89	82	85
7000	90	84	87

8000	91	86	87
9000	92	85	86
10000	90	84	85

Figure 9: Performance Results of the Prediction Accuracy

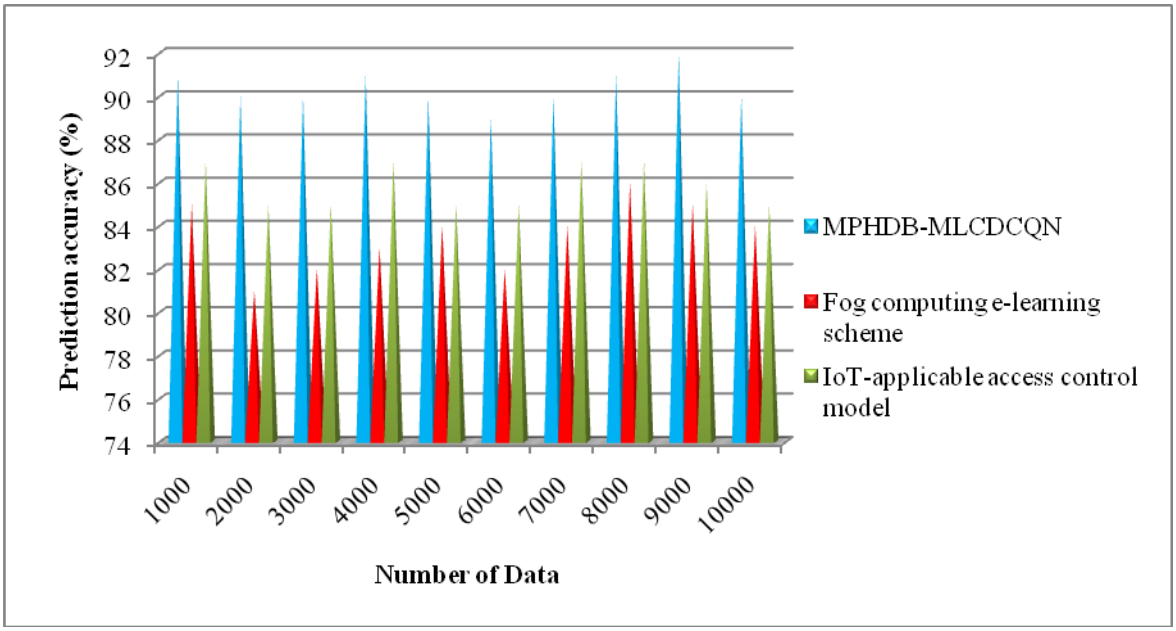


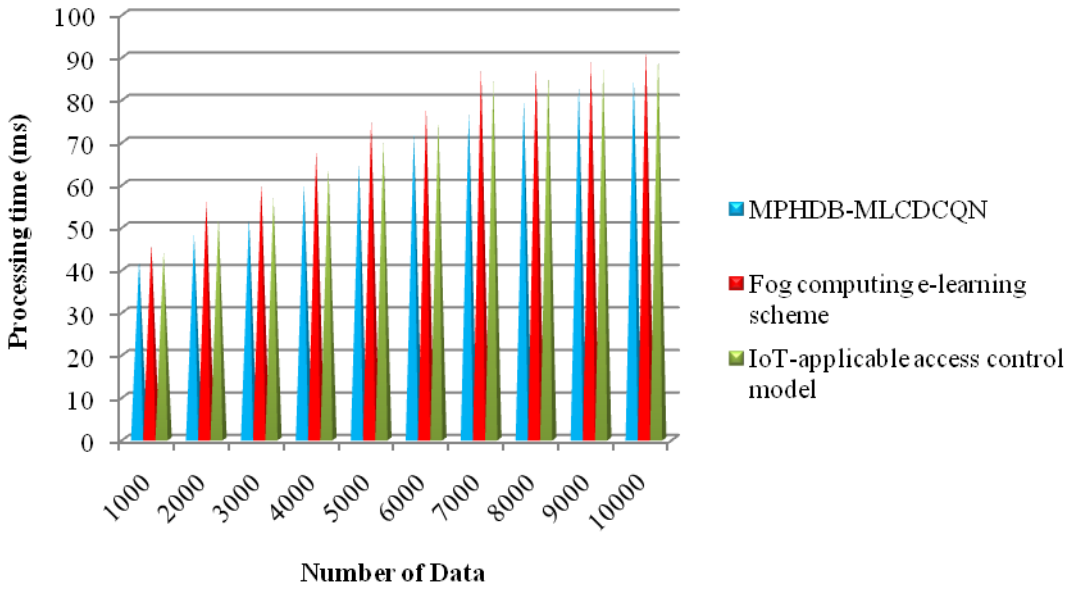
Table 4 and Figure 9 show the prediction accuracy of three methods using number of student data in the range from 1,000 to 10,000. Among three different methods, the performance of prediction accuracy using MPSCB-MLCDCQN is higher compared to the existing methods, because of applying a Maximum Likelihood Consensus Deep Convolutional Q-Learning Network. Initially, the input student data is analyzed in deep convolutional network using Maximum Likelihood Consensus regression for analyzing the data and mean values of the particular class. Then the estimated output is given to the action state to obtain final prediction results. As a result, student performance grade level is correctly predicted with minimum time. The overall accuracy of MPSCB-MLCDCQN technique is improved by 8% and 5% compared to the existing methods [1] [2].

Table 5: Comparison of the Processing Time

Number of Data	Processing Time (ms)		
	MPSCB-MLCDCQN	Fog Computing E-learning Scheme	IoT-Applicable Access Control Model
1000	42	46	44
2000	48	56	52
3000	52	60	57
4000	60	68	64
5000	65	75	70

6000	72	78	75
7000	77	87	84
8000	80	88	86
9000	83	89	87
10000	85	92	90

Figure 10: Performance Results of the Processing Time



Finally, the processing time for student performance processing is measured with respect to number of data taken as input from 1,000 to 10,000. The processing time for MPSCB-MLCDCQN is lesser compared to the existing methods [1] and [2] on varying number of data acquired from distinct devices. The overall performance of MPSCB-MLCDCQN is compared to the Fog computing e-learning scheme and IoT-Applicable Access Control Model. The performance outcomes indicate that the processing time is found to be minimized by 10% and 6% compared to the existing [1] and [2] because of the application of Maximum Likelihood Consensus Deep Convolutional Q-Learning Network. The Deep Convolutional Q-Learning technique uses the Maximum Likelihood Consensus regression in the hidden layer to analyze the data and find the target prediction results.

6. Conclusion

In this work, an effective MPSCB-MLCDCQN is developed to enhance the performance of secure data access and student performance level prediction. The MPSCB-MLCDCQN increases the security of devices' data being sent in via a secured channel with higher data integrity and confidentiality rate. First, the student learning data are collected using IoT. Then the Miyaguchi–Preneel Snefru hash decentralized blockchain technology applied for avoiding unauthorized access. Therefore, secured data access is said to take place with high confidentiality and integrity. After accessing the data, the authorized entity predicts the performance level using Maximum Likelihood Consensus regression

applied to Deep Convolutional Q-Learning Network. The performance of MPSCB-MLCDCQN is evaluated based on data confidentiality, data integrity, prediction accuracy and processing time. Comparison is also made with existing methods, and the results indicate that the data confidentiality, data integrity and prediction accuracy are found to be higher compared to the contemporary works. The simulation results demonstrate that the MPSCB-MLCDCQN provides better performance by reducing the processing time.

References

1. Arij Ben Amor, Mohamed Abid, Aref Meddeb, "Secure Fog-Based E-Learning Scheme", IEEE Access, Volume 8, 2020, Pages 31920–31933. https://doi.org/10.1109/ACCESS.2020.2973325
2. Ziyuan Li, Jialu Hao, Jian Liu, Huimei Wang, and Ming Xi, "An IoT-Applicable Access Control Model Under Double-Layer Blockchain", IEEE Transactions on Circuits and Systems, Volume 68, Issue 6, 2021, Pages 2102–2106, https://doi.org/10.1109/TCSII.2020.3045031
3. Tong Chen, Lei Zhang, Kim-Kwang Raymond Choo, Rui Zhang, Xinyu Meng, "Blockchain-Based Key Management Scheme in Fog-Enabled IoT Systems", IEEE Internet of Things Journal, Volume 8, Issue 13, 2021, Pages 10766–10778. https://doi.org/10.1109/JIOT.2021.3050562
4. Dragan Korać, Boris Damjanović, Dejan Simić, "A model of digital identity for better information security in e-learning systems", The Journal of Supercomputing, Springer, Volume 78, 2022, Pages 3325–3354. https://doi.org/10.1007/s11227-021-03981-4
5. Dun Li, Dezhi Han, Tien-Hsiung Weng, Zibin Zheng, Hongzhi Li, Han Liu, Arcangelo Castiglione, Kuan-Ching Li, "Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey", Soft Computing, 2022, Volume 26, Pages 4423–4440. https://doi.org/10.1007/s00500-021-06496-5
6. Anissa Cheriguene, Taieb Kabache, Chaker Abdelaziz Kerrache, Carlos T. Calafate, Juan Carlos Cano, "NOTA: A Novel Online Teaching and Assessment Scheme using Blockchain for Emergency Cases", Education and Information Technologies, Springer, Volume 27, 2022, Pages 115–132. https://doi.org/10.1007/s10639-021-10629-6
7. Ghassen Ben Brahim, "Predicting Student Performance from Online Engagement Activities Using Novel Statistical Features", Arabian Journal for Science and Engineering, Springer, 2022. https://doi.org/10.1007/s13369-021-06548-w
8. Feiyue Qiu, Guodao Zhang, Xin Sheng, Lei Jiang, Lijia Zhu, Qifeng Xiang, Bo Jiang, Ping-kuo Che, "Predicting students' performance in e-learning using learning process and behaviour data", Scientific Reports, Volume 12, 2022. https://doi.org/10.1038/s41598-021-03867-8
9. Shadab Alam, Huda Abdullah Yousef Ayoub, Rafan Abdulhaq Ahmed Alshaikh, Asmaa Hayawi Hussen AL-Hayawi, "A Blockchain-based framework for secure Educational Credentials", Turkish Journal of Computer and Mathematics Education, Volume 12, Issue 10, 2021, Pages 5157-5167
10. Anton Kamenskih, "The analysis of security and privacy risks in smart education environments", Journal of Smart Cities and Society, Volume 1, 2022, Pages 17–29. https://doi.org/10.3233/SCS-210114
11. Xiaoshuang He, Hechuan Guo, Xueyu Cheng, "Blockchain-Based Privacy Protection Scheme for IoT-Assisted Educational Big Data Management", Wireless Communications and Mobile

Computing, Hindawi, Volume 2021, August 2021, Pages 1-11. https://doi.org/10.1155/2021/3558972

12. Sultan Algarni, Fathy Eassa, Khalid Almarhabi, Abduallah Almalaise, Emad Albassam, Khalid Alsubhi, Mohammad Yamin, "Blockchain-Based Secured Access Control in an IoT System", Applied Science, Volume 11, Issue 4, 2021, Pages 1-16. https://doi.org/10.3390/app11041772
13. Han Liu, Dezhi Han, Dun Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT", IEEE Access, Volume 8, 2020, Pages 18207–18218. https://doi.org/10.1109/ACCESS.2020.2968492
14. Lihua Song, Xinran Ju, Zongke Zhu, Mengchen Li, "An access control model for the Internet of Things based on zero-knowledge token and blockchain", EURASIP Journal on Wireless Communications and Networking, Springer, 2021, Pages 1-20. https://doi.org/10.1186/s13638-021-01986-4
15. Eman J. Samkri, Norah S. Farooqi, "Dynamic-IoTrust: A Dynamic Access Control for IoT Based on Smart Contracts", International Journal of Engineering & Technology, Volume 10, Issue 2, 2021, Pages 139-147. https://doi.org/10.14419/ijet.v10i2.31553
16. Raaj Anand Mishra, Anshuman Kalla, An Braeken, Madhusanka Liyanage, "Privacy Protected Blockchain-Based Architecture and Implementation for Sharing of Students' Credentials", Information Processing and Management, Elsevier, Volume 58, Issue 3, 2021, Pages 1-25. https://doi.org/10.1016/j.ipm.2021.102512
17. Adnan Iftekhar, Xiaohui Cui, Qi Tao, Chengliang Zheng, "Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain-Based Applications", Entropy, Volume 23, Issue 8, 2021, Pages 1-19. https://doi.org/10.3390/e23081054
18. Dong Li, Zai Luo, Bo Cao, "Blockchain-based federated learning methodologies in smart environments", Cluster Computing, Springer, 2021. https://doi.org/10.1007/s10586-021-03424-y
19. Yustus Eko Oktian, Sang-Gon Lee, "BorderChain: Blockchain-Based Access Control Framework for the Internet of Things Endpoint", IEEE Access, Volume 9, 2020, Pages 3592–3615. https://doi.org/10.1109/ACCESS.2020.3047413
20. Basudeb Bera, Sourav Saha, Ashok Kumar Das, Athanasios V. Vasilakos, "Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System", IEEE Internet of Things Journal, Volume 8, Issue 7, 2021, Pages 5744–5761. https://doi.org/10.1109/JIOT.2020.3030308
21. Educational Process Mining (EPM): A Learning Analytics Data Set, UCI Machine Learning Repository, Center for Machine Learning and Intelligent Systems. https://archive.ics.uci.edu/ml/datasets/Educational+Process+Mining+%28EPM%29%3A+A+Learning+Analytics+Data+Set