Advances in Dynamical Systems and Applications.
ISSN 0973-5321, Volume 16, Number 2, (2021) pp. 1283-1301

https://www.ripublication.com/adsa.htm

# IoT Aware Czekanowski's Dice Smart Contractive Blockchain Based Access Control for E-Learning in Cloud

**N. R. Chilambarasan [1] , Dr. A. Kangaiammal [2]**

*[1] Ph.D Research Scholar (Part Time), PG & Research Department of Computer Science, Govt. Arts College (Autonomous), Salem-636 007, India.*
*ORCID: 0000-0002-6402-7662*

*[2] Assistant Professor, Department of Computer Applications, Govt. Arts College (Autonomous), Salem-636 007, India.*

**Abstract**

Security is a major issue in the E-learning platforms due to increasing popularity and many people are taking online courses. E-learning is a process of distance learning since the learners and the teacher exist in different locations. Various significant elements must be considered into account namely authentication, access control, and Information security obtained using schemes such as cryptography and network protocols. A novel technique called Czekanowski's Dice Indexed Smart Contract Blockchain andJackknife Regressed Deep Reinforcement Learning (CDISCB-JRDRL) is introduced to address key security issues such as access control are taken into consideration in developing and using an e-learning platform. The proposed CDISCB-JRDRL technique consists of two major processes namely secured access control and data analysis. The Internet of Things (IoT) devices are implemented to sense and monitor student behaviors during the E-learning process. These sensed data are securitized by avoiding unauthorized access. In order to improve security, an access control system based on blockchain technology and uses smart contracts for access control judgment without believing external third parties. In the second process, a Jackknife regressed deep reinforcement learning is employed to analyze the student data collected from the IoT devices to make optimal action. The students data are analyzed using the Jackknife regression function by learning the feature and predict the student performance with higher accuracy. An experiment is conducted on theE-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 student data. The results discussed show that CDISCB-JRDRL technique provides the improved performance in terms of achieving higher security and data analysis than the existing methods.

**Keywords:** Cloud; E-Learning; Secure Access Control; Smart Contracts; Blockchain; Jackknife Regression; Deep Reinforcement Learning.

## 1. INTRODUCTION

The use of e-learning systems is an interesting one due to their large applicability in distance education and in institutionalized education also. In recent days, several universities and organizations enhance and develop their educational strategies through the e-learning system to attract more learners. Due to the rapid growth of the Internet of Things (IoT), a large amount of data is shared between the students, teachers, and examiners in e-learning. In this case, secure accessibility and data distribution by smart devices is a challenging one. The cloud-based e-learning system provides fine-grained access control and security conservation of data shared in distance education.

A novel fog computing e-learning scheme was introduced [1] to improve the efficiency of learning and also grants access control using different cryptographic techniques. The designed scheme achieves a high data confidentiality rate but the integrity verification was not performed. A Secure E-learning System (SES) was introduced in [2] to exchange theacademic activities related materials through the trusted cloud server. Though the system performs the authentication to ensure security, the performance of data confidentiality was not improved.

An enhanced attribute-based access control method was introduced in [3] to improve the security. However, the scheme failed to introduce a novel access control structure for achieving higher confidentiality. A time and attribute-based dual access control method were developed in [4] to improve the data integrity. However, the higher data confidentiality rate was not attained. A novel secure cloud storage framework was introduced in [5] for access control using the Ethereumblockchain technology. The designed framework failed to improve the data integrity. A novel secure and effective multi-authority access control method was designed in [6] of the cloud storage system for IoT to improve the security with minimum computational overhead. The designed method failed to perform data integrity verification.

A secure fine-grain access control system was introduced in [7] for increasing the security and confidentiality of data. However, the efficient hash generation was not performed to increase the data integrity. A secure, efficient, and fine-grained data access control approach was developed in [8] for IoT to update access policies. However, the approach failed to perform authentication based access control.

A cloud-based e-learning based access control method was developed in [9] to prevent the cloud resources from illegal user access. However, the method failed to

apply the performance level prediction based on the e-learning process. A novel encoding scheme was introduced in [10] before storing the message on the e-learning storage system to improve security. But, it failed to improve the effective e-learning in a cloud-based system.

The major contributions of the proposed CDISCB-JRDRL technique are summarized:

- To improve the security of data access in the cloud, a CDISCB-JRDRL technique is introduced.
- A Czekanowski's dice indexed smart contract blockchain technology is applied in the CDISCB-JRDRL technique for secure access control in the cloud. During the transaction, the permission decision contract is applied to the blockchain to avoid unauthorized access based on the authentication. This helps to improve the data confidentiality rate.
- To increase the data integrity rate, the Davis Meyer compression function is applied to the blockchain to generate the hash value for each data during the transaction. This helps to increase data integrity.
- To increase the prediction accuracy and minimize the time, the CDISCB-JRDRL technique uses Jackknife Regressed Deep Reinforced Learning to analyze the student data and predict the performance level.
- Finally, extensive simulations are conducted to estimate the performance of the CDISCB-JRDRL technique and other related works. The observed result demonstrates that CDISCB-JRDRL technique outperforms well than the other methods.

The rest of this paper is arranged into five various sections. Section 2 describes the proposed CDISCB-JRDRL technique with different sub-processes. In Section 3, experiments are conducted with the dataset to illustrate the performance of the CDISCB-JRDRL technique. Section 4 provides comparative results discussions of the different parameters with the help of a table or graphical representation. Section 5 introduces the related works. Finally, the last section ends the work with the conclusion.

## 2. Methodology

Access control is the most important security concern in resource and information protection in cloud computing. Cloud computing provides instantaneous storage services for the huge data generated from the IoT devices. IoT devices are computing devices to monitor and collect student information during the E-learning process. This information is stored on the cloud server. However, the security factor in sharing the educational content is significant and creates several security challenges. Based on this motivation, a novel CDISCB-JRDRL technique is introduced to prevent authorized access and also provide security of the data in a cloud server.

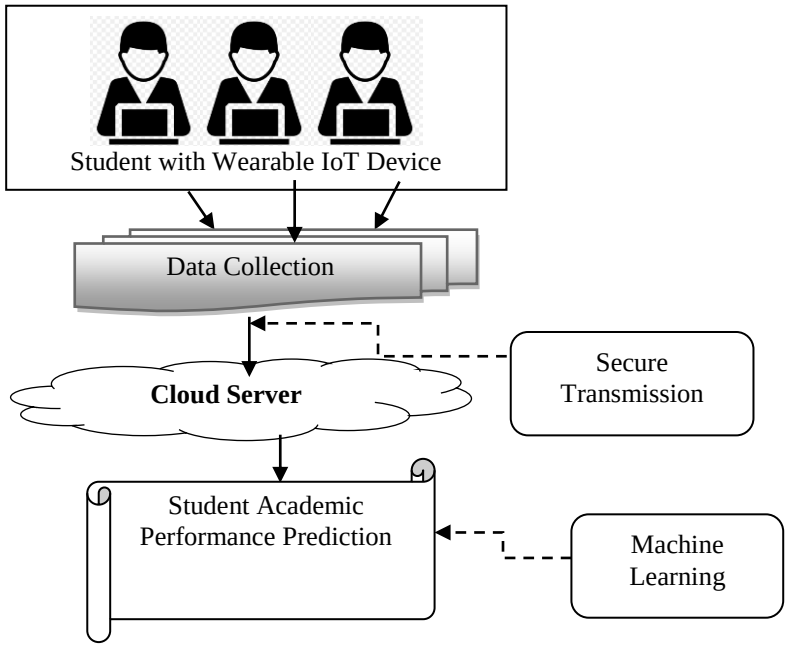


**Fig. 1.** Architecture of proposed CDISCB-JRDRL Technique

Figure 1 shows the architecture diagram of the proposed CDISCB-JRDRL technique to provide secure access control with higher confidentiality and integrity in the cloud. The architecture comprises the number of students who participated during the E-learning process and the data generated from the IoT is $D_s = D_1, D_2, D_3 \ldots . D_n$ to be sent to the cloud server in a secured manner. The security of the data transmission is achieved through blockchain-based technology. With the received data, the student academic level prediction is said to be achieved using jackknife regressed deep reinforced learning with higher accuracy. These processes of CDISCB-JRDRL are briefly described in the following subsections.

### 2.1. *Czekanowski's Dice Indexed Smart Contract Blockchain Technology*

In the cloud, secure access control is the major concern for resource and information protection of IoT devices. This CDISCB-JRDRL technique proposes a novel blockchain technology and uses smart contracts for access control in the open IoT environment. A smart contract is a self-executing contract that exists between two parties along with the terms of the agreement or certain rules that are encoded as a set of lines of code stored in the blockchain. The smart-contracts interact with one user to another, through the communications called transactions. These contracts stored in a blockchain automatically perform legally relevant events along with the terms of certain rules without believing external third parties.

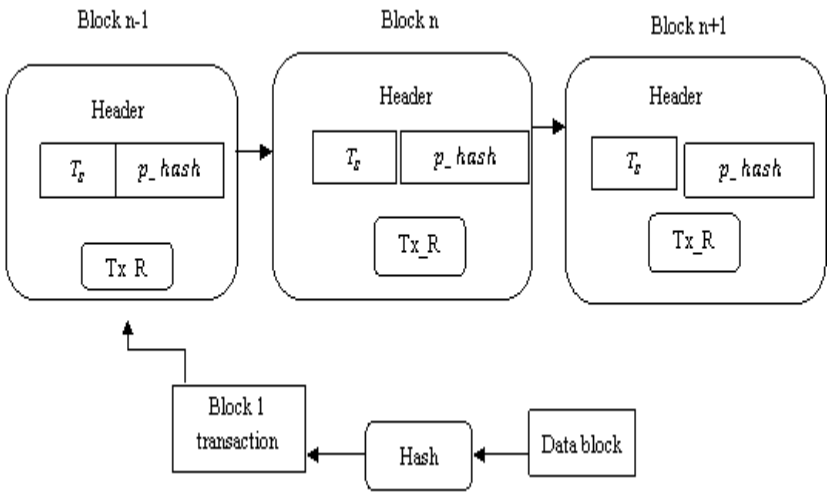


**Fig. 2.** Hash-based Blockchain Technology

Figure 2 shows the construction of a blockchain that consists of a number of blocks and each block has a block header, timestamp ($T_s$), root hash (Tx_R), and a hash of the previous block ($p\_hash$). Each block has a transaction for transmitting the student data collected from the IoT devices. The root hash is generated using Davies–Meyer compression function to improve the security of data. As shown in the blockchain construction, the data block has a student's information during the E-learning. In order to construct the blockchain, the registration process is carried out to register the information for each device. When the device (IoT) wants to join the chain for the transaction, they first need to register the information to a cloud server.

After entering the information, the server sent successfully registered messages and it also generates the ID and password for each registered device. The generated ID and password are also stored in the cloud server. During the transaction, different contracts are used such as permission decision contracts and access control policy contracts. By implementing the permission decision contract to the blockchain, the device first verifies its authenticity. The registered device first login to the server and the server verify the ID and password generated at the time of the registration. The authentication process is done with the help of Czekanowski's dice similarity index. By applying Czekanowski's dice index, the similarity between the entered ID, password, and registered ID, the password is measured as given in Equation 1.

$$\omega = 1 - 2 * \left|\frac{E \cap S}{E \cup S}\right| \quad (1)$$

Where '$\omega$' denotes a Czekanowski's dice similarity coefficient, $E$ indicates entered ID, password, $S$ denotes a registered ID, password. From (2), the intersection symbol '$\cap$' designates a mutual dependence, the union symbol '$\cup$' denotes an available ID and passwords in a server. The similarity coefficient $(\omega)$ provides the integer value in the range from 0 to 1. The coefficient returns high similarity and then the ID and passwords are matched. Otherwise, these two IDs and passwords are not matched. If these two IDs and passwords get matched, then the user is said to be authorized. By

applying the permission decision contract, the rule is formulated using the algorithmic formalism are $IF$ (condition) and $then$ (conclusion) for deciding to provide the access or not. The condition part verifies the similarity value and the conclusion part provides the desired results. If the coefficient provides the high similarity value, then the entity is authorized and the server allows to access using access control policy. Otherwise, the server decline the access.

In addition, the student data are hashed during the transaction in order to further improve the security and also increase the data integrity. In cryptography, Davies–Meyer compression function is applied to generate the hash. Let us consider, the number of student data $D_s = D_1, D_2, D_3 \ldots . D_n$ . The input data is divided into a number of message blocks with a fixed size as in Equation 2.

$$D = m_1, m_2, m_3, \ldots m_n \tag{2}$$

Where, $m_1, m_2, m_3, \ldots m_n$ indicates the number of message blocks. Then the input message block is given to the Davis Mayer compression function. The compression function receives the input message block ($m_i$) and previous hash.

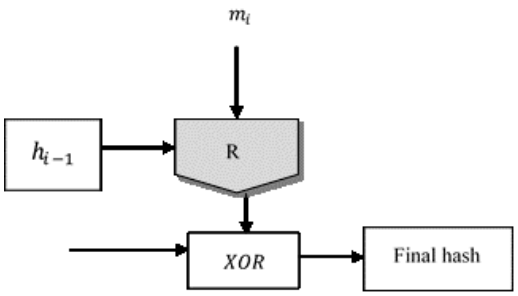


**Fig. 3.** Davis Mayer Compression Function

Figure 3 depicts the Davis Mayer compression that takes the input message block '$m_i$' and the previous hash value ($h_{i-1}$) is initially preset. From the figure, 'R' denotes a block cipher. The message block ($m_i$) as the key to a block cipher XORed with the previous hash value and the message block ($m_i$). In the first round, the previous hash value is set. The output of the compression function is expressed as in Equation 3.

$$H = [R_{m_i}(h_{i-1}) \oplus h_{i-1}] \tag{3}$$

From (3),$Hd$enotes a final hash value generated from the Davis Mayer compression function. The hash of one message block is not similar to another input block. The output hash is taken from the final compression function. Then the student data are securely transmitted and avoid unauthorized access.

Algorithm 1 describes the step by step process of secure access control. By applying the permission decision contract to the blockchain technology, the IoT devices register their details to the cloud server. Consequently, the server generates the ID and password for each registered device. During the transaction, the cloud server first verifies the authenticity of devices using Czekanowski's dice similarity. If the

password and ID are exactly matched, the similarity coefficient returns '1', the cloud server grants the permission to access, and hence it improves the security. Otherwise, the server denied access. Finally, the Davis Meyer compression function is applied to the blockchain technology to generate the hash value for each student data during the transaction. This helps to improve data integrity and confidentiality.

| **// Algorithm 1: Czekanowski's Dice Indexed Smart Contract Blockchain Technology** |
|---|
| **Input**: E-learning dataset, Number of devices $d_1, d_2, \ldots d_m$ , Number of students data $D_1, D_2, \ldots D_n$<br>**Output:** Improve the secure data access |
| **Begin**<br>**Step 1**: Collect **the data $D_1, D_2, \ldots D_n$ from dataset**<br>**Step 2: For each transaction 't'**<br>**Step 3:** Construct blockchain using permission decision contract<br>**Step 4**: **For each device '$d$'**<br>**Step 5:** Register details to the server<br>**Step 6:** Server generates ID and password<br>**Step 7:** **End for**<br>**Step 8: Device login into the system with 'ID' and password**<br>**Step 9: Server verifies** the ID and password<br>**Step 10:if** $(\omega = 1)$ **then**<br>**Step 11:**Grants permission to access<br>**Step 12: else**<br>**Step 13:** Denied the access<br>**Step 14: For each transaction 't'**<br>**Step 15:** Divide into data '$D$ ' into message blocks $m_1, m_2, m_3, \ldots m_n$<br>**Step 16: for eachblock$m$**<br>**Step 17:** Generate hash value '$H$'<br>**Step 18: End for**<br>**Step 20:** Obtain the final hash<br>**Step 21: End for**<br>**End** |

### 2.2. *Jackknife Regressed Deep Reinforcement Learning-based Performance Level Prediction*

After receiving the student information from the IoT devices, a performance prediction are carried out using jackknife regressed deep reinforcement learning. Deep reinforcement learning is a type of machine learning that integrates the concept

of reinforcement learning (RL) as well as deep learning. Deep learning is a family of machine learning based on artificial neural networks.

Reinforcement learning considers the state-action pair at each time step to predict the performance level. In-state space, the student behaviors (or activities) during the E-learning process are analyzed using a jackknife regression-based deep neural network. Then the analyzed results are obtained at the action space.

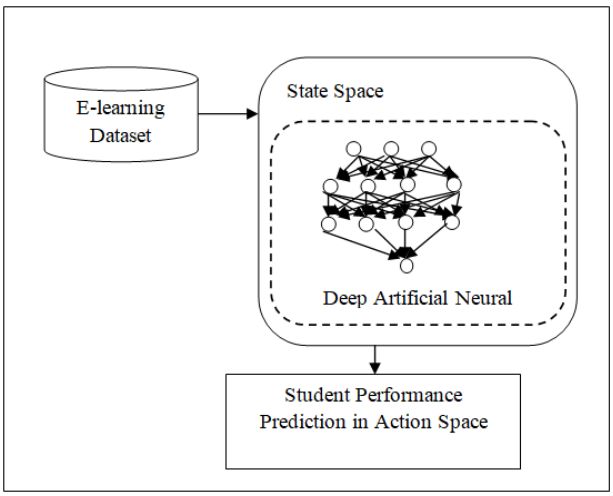


**Fig. 4.** Davis Mayer Compression Function

Figure 4 illustrates the structure of the deep artificial network which comprises many layers for learning the given input data. The deep learning architecture includes a number of neurons like the nodes which are connected from one layer to successive layers in a forward manner and creates the whole neural network. The deep architecture uses the input layer, two hidden layers, and one output layer. The input student data $D_1, D_2, D_3 \ldots . D_n$ are given to the input layer. The neurons' activity at the input layer at a time '$i\ (t)$' is given in Equation 4.

$$i\ (t) = \sum_{i=1}^{n} D_i * q_1 + c \tag{4}$$

Where input layers collect the student data '$D_i$' with regulating weight ' $q_1$' between the input and hidden layer 1, '$c$' represents the bias. Then the input is fed into the first input layer where the data are analyzed using the jackknife regression function. Let us consider the number of classes $\beta_1, \beta_2, \ldots . \beta_s$ i.e Grade level (i.e. poor, average, and high) and the mean of the particular class is estimated as given in Equation 5.

$$\mu = \frac{1}{n} \sum_{i=1}^{n} D_i \tag{5}$$

Where, $\mu$ indicates a mean of the particular class, '$n$' indicates a number of input data $D_i$. Then it transforms into a second hidden layer to estimate the variance of data from the mean of a particular class as in Equation 6.

$$\sigma_v = |D_i - \mu| \tag{6}$$

Where, $\sigma_v$ jackknife variance,$\mu$ denotes a mean of class, $D_i$ represents the student data. From the analysis, the data close to the mean value of the class is categorized. Based on this behavior analysis, the teachers evaluate the student's performance in terms of grade level in the future state. Grades are assigned as letters or percentage out of a possible total. The output of the hidden layer is given in Equation 7.

$$K(t) = \sum_{i=1}^{n} D_i * q_1 + q_2 * K\ (t-1) \tag{7}$$

Where, $K(t)$ denotes an output of the hidden layer, $D_i$ indicates the strident data, $q_1$ denotes a weight between input and hidden layer, $q_2$ indicates a weight of hidden layers, $K\ (t-1)$ denotes an output of the first hidden layer. Then the hidden layer output is transferred into the output layer.

$$Z(t) = q_3 * K(t) \tag{8}$$

From Equation 8, $Z(t)$ indicates results from the output layer, $q_3$ denotes a regulating weight between the hidden and output layer, and $K(t)$ denotes an output of the hidden layer.

Algorithm 2 describes the step by step process of student performance level prediction with higher accuracy. Initially, the input student data are collected from the dataset at the input layer. The input is transferred into the first hidden layer where the analysis is carried out by initializing the classes and their mean values using the jackknife regression function. The jackknife regression function measures the deviation and categorizes the data. Based on the result, the student performance is correctly predicted with minimum time.

| **// Algorithm 2: Jackknife Regressed Deep Reinforcement Learning-Based Performance Level Prediction** |
|---|
| **Input**: Student data $\boldsymbol{D_1, D_2, \ldots D_n}$<br>**Output:** increase accuracy of student performance level prediction |
| **Begin**<br>**Step 1**: Collect the data $D_1, D_2, D_3 \ldots . D_n$ as input<br>**Step 2**: Initialize the classes $\beta_1, \beta_2, \ldots . \beta_s$// **hidden layer 1**<br>**Step 3:For each class '**$\beta_i$'<br>**Step 4**: Compute mean '$\mu$'<br>**Step 5:** Calculate the variance $\sigma_v$ // **hidden layer 1**<br>**Step 6:** Categories the data<br>**Step 7**: **End for**<br>Step 8: Find student learning performance<br>**End** |

## 3. EXPERIMENTAL SETUP

In this section, experimental evaluation of the proposed CDISCB-JRDRL technique and two existing methods namely fog computing e-learning scheme [1], SES [2] are implemented using Java language and CloudSim simulator. An Educational Process Mining (EPM): A Learning Analytics Data Set is implemented for estimating the performance of the proposed technique and the existing methods. This dataset is taken from the UCI machine learning repository [21] and it is constructed from the recordings of 115 student's activities through a logging application from the server for learning with an educational simulator for e-learning in digital electronics. The data set consists of the 115 student's students' series of activities generated from the IoT devices during six different sessions. There are 6 folders consists of student's activities generated per session. In addition, the dataset includes 230318 instances and 13 attributes in terms of integers. The attributes are Session, Exercise, Activity, Start-time, End-time, Idle-time, Mouse-wheel, Mouse-wheel-click, Mouse-click-left, Mouse-click-right, Mouse-movement and Keystroke. The associated task performed by the dataset is classification, regression, and clustering. These received student data are securely sent to the server by applying the hash-based blockchain technology and then activities are analyzed to predict the performance level.

## 4. PERFORMANCE RESULTS ANALYSIS

In this section, the performance analyses of the proposed CDISCB-JRDRL and existing fog computing e-learning scheme [1], SES [2] are discussed based on four different metrics as data confidentiality rate, integrity rate, processing time, and accuracy. The performance of proposed and existing methods are analyzed using a table and graphical representation.

### 4.1. Impact of Confidentiality Rate

Confidentiality Rate refers to the ratio of the number of student data only accessed by authorized entities. The confidentiality rate is formulated as given in Equation 9.

$$Rate_{con} = \left(\frac{n_{aae}}{n}\right) * 100 \tag{9}$$

From Equation 9, $Rate_{con}$ indicates the confidentiality rate, '$n$' denotes the number of student data generated from IoT device, '$n_{aae}$' represents the number of data accessed by the authorized entity.The confidentiality rate is measured in terms of percentage (%).

Table 1 reports the experimental results of confidentiality rate versus a number of student data 100 to 1000 taken from IoT device during the E-learning process. The observed results indicate that the CDISCB-JRDRL technique achieves higher confidentiality than the other two existing methods namely fog computing e-learning scheme [1], SES [2]. Let us consider 100 data for experimentation in the first run, 92 data are correctly accessed by the authorized entity and the confidentiality rate is 92% using the CDISCB-JRDRL technique. Subsequently, the 86 and 83 data are correctly accessed by the authorized entity using [1], [2], and observed data confidentiality

rates are 86% and 83% respectively. Similarly, various runs are observed for each method and the overall results are compared to existing results. The average of ten comparison results of the CDISCB-JRDRL technique indicates that the confidentiality rate is found to be increased by 7% when compared to [1] and 11% when compared to [2] respectively.

**Table 1:** Comparison of Confidentiality Rate

| Number of Data | Confidentiality Rate (%) | | |
|---|---|---|---|
| | Fog Computing E-Learning Scheme | SES | CDISCB-JRDRL |
| **100** | 86 | 83 | 92 |
| **200** | 87 | 84 | 93 |
| **300** | 86 | 82 | 92 |
| **400** | 88 | 85 | 93 |
| **500** | 87 | 84 | 94 |
| **600** | 86 | 83 | 92 |
| **700** | 88 | 86 | 94 |
| **800** | 86 | 83 | 93 |
| **900** | 87 | 84 | 92 |
| **1000** | 86 | 83 | 93 |

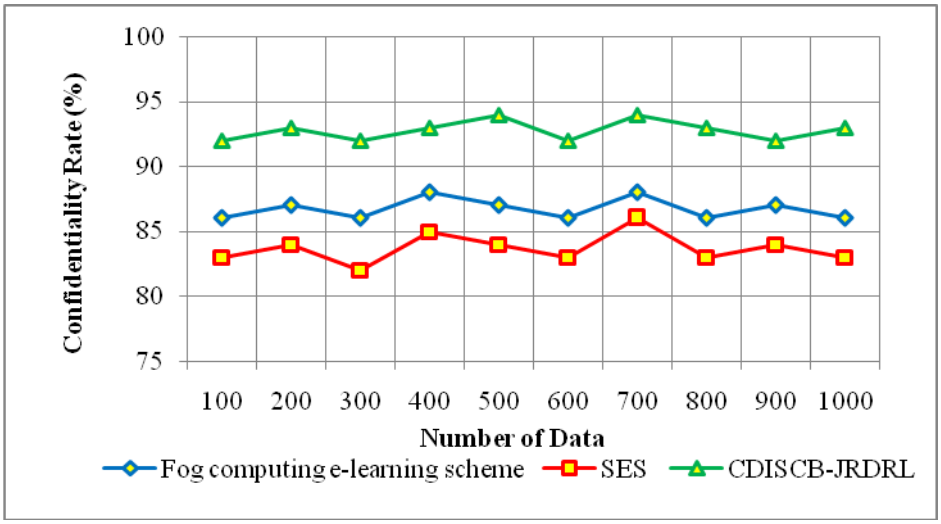


**Fig. 5.** Performance Results of Confidentiality Rate

Figure 5 demonstrates the level of confidentiality rate when the number of student data is varied from 100 to 1000. As shown in the graphical plot, it is noticed that the

CDISCB-JRDRL technique achieves higher data confidentiality than the conventional methods. This significant improvement is achieved due to the application of Czekanowski's dice indexed smart contract blockchain technology. During the transaction, the smart contract is applied to allow the data access based on the authentication. Each IoT device registers their details and it verifies their authenticity during the transaction. Czekanowski's dice index is applied to verify the authenticity. Based on the verification, the permission decision contract uses a certain rule to provide the access control policy for the authorized entity. Otherwise, the server declines the access. Therefore, the authorized entity allows accessing and avoiding unauthorized access. This process increases the data confidentiality rate.

### 4.2.Impact of Data Integrity Rate

Data integrity rate is defined as the number of data that are not modified or altered by any third party to the number of data taken for transmission. The data integrity rate is mathematically formulated as given in Equation 10.

$$Rate_{Int} = \left(\frac{n_{aa}}{n}\right) * 100 \tag{10}$$

From (10),$Rate_{Int}$ represents a data integrity rate, '$n_{aa}$' indicates the number of data not altered or modified, '$n$' indicates a total number of data. The data integrity rate is measured in terms of percentage (%).

**Table 2:** Comparison of Data Integrity Rate

| Number of Data | Data Integrity Rate (%) | | |
|---|---|---|---|
| | Fog computing E-Learning Scheme | SES | CDISCB-JRDRL |
| **100** | 85 | 82 | 91 |
| **200** | 86 | 83 | 92 |
| **300** | 85 | 80 | 91 |
| **400** | 87 | 83 | 92 |
| **500** | 86 | 82 | 93 |
| **600** | 85 | 81 | 91 |
| **700** | 87 | 84 | 93 |
| **800** | 85 | 82 | 92 |
| **900** | 86 | 83 | 91 |
| **1000** | 85 | 81 | 92 |

Table 2 provides the experimental results of the data integrity rate with respect to the number of student data. The tabulated results show that a CDISCB-JRDRL provides better performance in terms of achieving a higher integrity rate than the existing

methods. From the observed results, a total ten integrity rates are observed for each method. In the first run, the experiment is conducted with 100 student data, the integrity rate of CDISCB-JRDRL is 91%. Besides, the integrity rates are 85% and 82% using fog computing e-learning scheme [1], SES [2] respectively. Similarly, the other runs are performed and results are obtained. The overall integrity rate of the CDISCB-JRDRL is compared to the results of existing methods. The average of ten results confirmed that the data integrity rate of CDISCB-JRDRL is increased by 7% and 11% when compared to the existing fog computing e-learning scheme [1], SES [2] respectively.

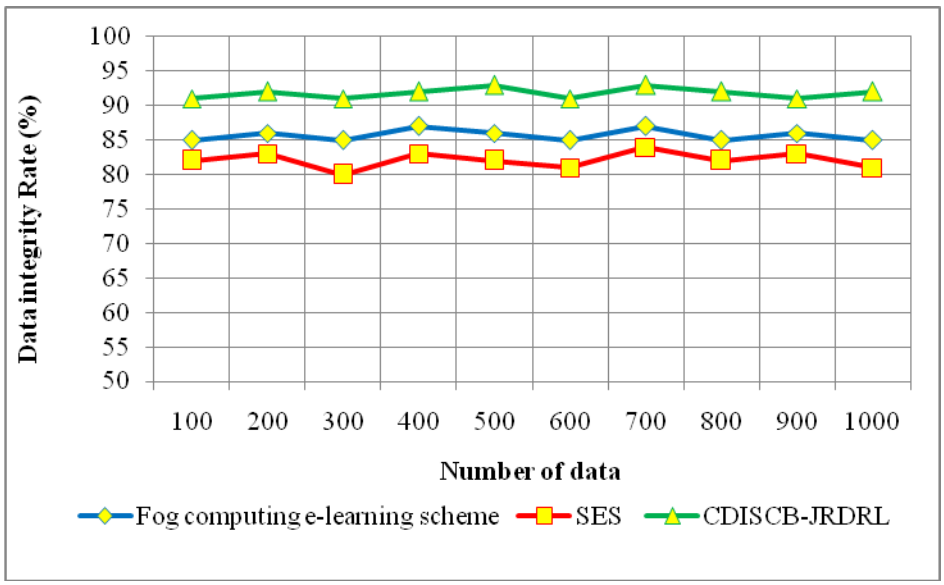


**Fig. 6.** Performance Results of Integrity Rate

Figure 6 shows the performance analysis of data integrity rate versus a number of student data taken from the dataset. As shown in the chart, the data integrity rate is comparatively higher using the CDISCB-JRDRL technique than the other methods. This is due to the application of the Davis Meyer compression function for generating the hash value in the data transaction. The compression function generates the fixed size of the hash for each input student data. Any alteration in the student data and it causes drastic changes in the generated hash value. Therefore, the data modification by the unauthorized entity is reduced hence it improves the data integrity rate.

### 4.3.*Impact of Processing Time*

The processing time is defined as the amount of time taken by the algorithm to discover the student performance level during the E-learning process. Therefore, the processing time is measured as given in Equation 11.

$$PT = n * [Time(ISD)] \tag{11}$$

From (11), $PT$ indicates a processing time, '$n$' indicates the number of student data, $Time(ISD)$ refers to the time taken to analyze the single- student data. The overall processing time is measured in terms of milliseconds (ms).

**Table 3:** Comparison of Processing Time

| Number of Data | Processing Time (ms) | | |
|---|---|---|---|
| | Fog computing E-Learning Scheme | SES | CDISCB-JRDRL |
| **100** | 33 | 36 | 31 |
| **200** | 36 | 40 | 34 |
| **300** | 43 | 45 | 39 |
| **400** | 48 | 52 | 44 |
| **500** | 53 | 55 | 51 |
| **600** | 57 | 59 | 55 |
| **700** | 59 | 62 | 57 |
| **800** | 62 | 66 | 60 |
| **900** | 65 | 68 | 63 |
| **1000** | 68 | 70 | 65 |

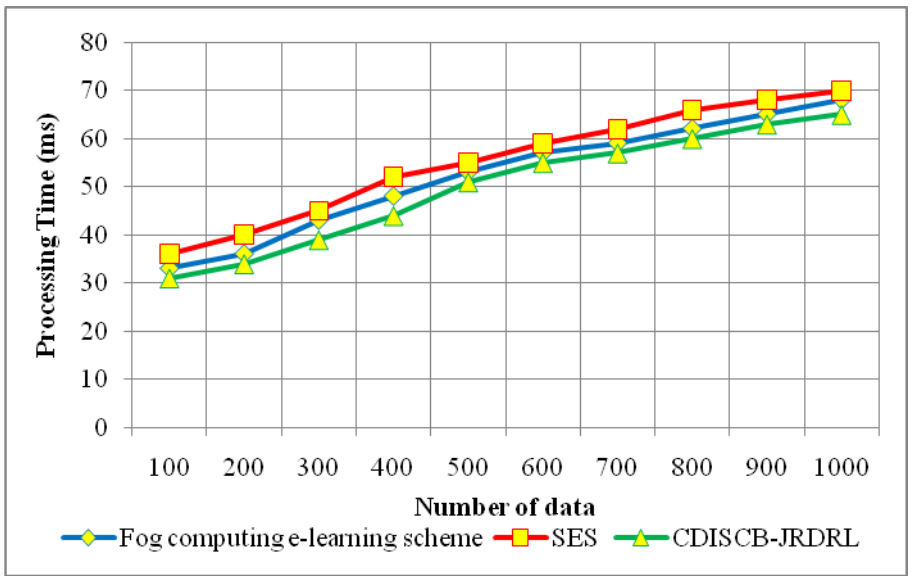


**Fig. 7.** Performance Results of Processing Time

Table 3 and Figure 7 illustrate the performance of processing time using three different methods namely CDISCB-JRDRL and existing fog computing e-learning scheme [1], SES [2]. Among the three methods, CDISCB-JRDRL consumed minimum time for predicting student performance. Initially, the experiment is conducted with 100 data, CDISCB-JRDRL technique consumes $31ms$ and the processing time of [1] [2] is $33ms$ and $36ms$ respectively. Likewise, the other results are observed with a variety of input data. The average results indicate that the CDISCB-JRDRL technique is considerably reduced by 5% and 10% when compared to existing [1] and [2] respectively. This improvement is achieved through the application of the Jackknife regressed deep reinforcement learning concept in the CDISCB-JRDRL technique. Deep learning analyzes the student data using Jackknife regression to predict the student performance grade in terms of poor, average, and higher. This in turn minimizes the time of performance prediction.

### 4.4.*Impact of Prediction Accuracy*

Prediction accuracy is defined 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. The accuracy is formulated as given in Equation 12.

$$PA = \left[\frac{Number\,of\,student\,data\,correctly\,predicted}{n}\right] \quad (12)$$

From (12), $PA$ represents a prediction accuracy, '$n$' indicates the number of student data. The prediction accuracy is measured in terms of percentage (%).

**Table 4:** Comparison of Prediction Accuracy

| Number Of Data | Prediction Accuracy(%) | | |
|---|---|---|---|
| | Fog computing e-learning Scheme | SES | CDISCB-JRDRL |
| **100** | 88 | 85 | 95 |
| **200** | 87 | 83 | 93 |
| **300** | 90 | 85 | 94 |
| **400** | 88 | 86 | 93 |
| **500** | 87 | 83 | 92 |
| **600** | 88 | 85 | 93 |
| **700** | 87 | 83 | 94 |
| **800** | 88 | 85 | 93 |
| **900** | 90 | 87 | 94 |
| **1000** | 88 | 86 | 93 |

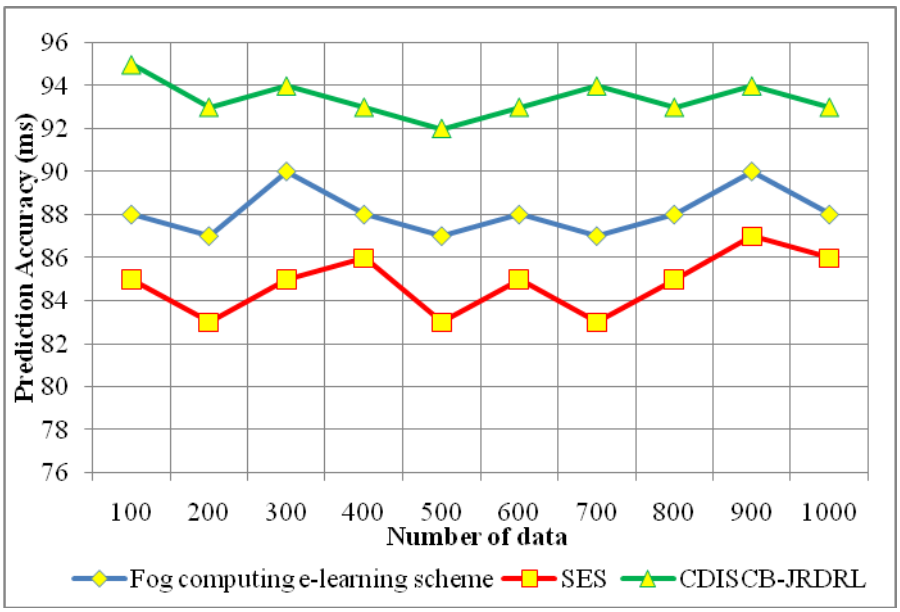


**Fig. 8.** Performance Results of Prediction Accuracy

Table 4 and figure 8 shows the performance of the prediction accuracy with respect to the number of data. The observed results indicate that a variety of results are obtained for the different numbers of data. From the comparison results, it indicates that the CDISCB-JRDRL technique achieves higher prediction accuracy. As shown in the tabulated results, the experiment is conducted with 100 data, the accuracy is 95%. Besides, the prediction accuracy is 88% and 85% using fog computing e-learning scheme [1], SES [2] respectively. The average of ten results noticeably proved that the prediction accuracy is considerably increased using the CDISCB-JRDRL technique by 6% and 10% when compared to existing [1], [2] respectively. The higher accuracy is obtained using deep reinforcement learning in the CDISCB-JRDRL technique. Deep learning deeply analyzes the student data using the jackknife regression function. Based on the analysis, the student's future performance level is correctly predicted with higher accuracy.

## 5. RELATED WORKS

An integrated cloud model was developed in [11] for an intelligent e-Learning system to guarantee security and accessibility. But the model failed to use the advanced technology to achieve higher security. A sustainable quality assessment model was introduced in [12] for the e-learning systems. However, the security requirements were not achieved in the e-learning systems. A new security scheme was introduced in [13] for online evaluation including e-learning. However, it failed to provide a significant model to assure and achieve student authentication. A novel secure data search and sharing method was developed in [14] to significantly reduce the

computing and communication overhead. However, the method failed to perform the authentications for avoiding unauthorized access. Integration of the K-Means Clustering and Multiple Linear Regression approach was developed in [15] for student performance analysis on e-learning. But the security factors remain a challenging issue.

A short signature algorithm was designed in [16] to guarantee the data integrity and availability of a cloud-based storage system. However, the performance of the data confidentiality rate was not improved. A cloud-enabled IoT multifactor authentication and lightweight cryptography encryption schemes were developed in [17] to prevent the big data system. However, the scheme failed to perform the mutual authentication between gateway devices and IoT devices.

An Identity based access control method was introduced in [18] to guarantee the secure access of the services and data only by the authenticated users. However, the approach failed to ensure data integrity. A new remote user authentication method was developed in [19] for cloud-IoT applications to minimize the computational overhead. But the higher security was not achieved. Accountable privacy-preserving attribute-based approach was developed in [20] for securely distributing the outsourced data through the public cloud servers.

## 6. CONCLUSION

In this paper, a novel secure access control technique in an e-learning system called CDISCB-JRDRL is introduced to ensure reliable academic activities via trusted servers in the cloud. With the rapid growth of communication technology, secure communication plays a vital role in the field of education technology. This contribution is achieved through Czekanowski's dice indexed smart contract blockchain technology. During the data communication, the permission decision contract is used to the blockchain for avoiding unauthorized access from the server. The server verifies the authenticity of the user based on Czekanowski's dice index. This helps to increase data confidentiality. Then the Davis Mayer compression function generates the hash value for increasing the data integrity. Next, the Jackknife regressed deep reinforcement learning is applied in CDISCB-JRDRL to analyze the student data to predict the performance level prediction with higher accuracy and minimum time. The comprehensive experiment is conducted to estimate the performance of the proposed CDISCB-JRDRL with two existing methods in terms of different metrics such as confidentiality rate, data integrity rate, processing time, and prediction accuracy. The results and discussion confirm that the CDISCB-JRDRL outperforms well in terms of achieving higher data confidentiality, integrity, and prediction accuracy, and lesser processing time than the conventional methods

**REFERENCES**

[1] Arij Ben Amor, Mohamed Abid, ArefMeddeb, "Secure Fog-Based E-Learning Scheme", IEEE Access, Volume 8, 2020, Pages 31920 – 31933.

[2] SaminaKausar, Xu Huahu, Ata Ullah, Zhu Wenhao& Muhammad YasirShabir, "Fog-Assisted Secure Data Exchange for Examination and Testing in E-learning System", Mobile Networks, and Applications, Springer, 2020, Pages 1-17.

[3] Praveen Kumar Premkamal, Syam Kumar Pasupuleti, Abhishek Kumar Singh & P. J. A. Alphonse, "Enhanced attribute based access control with secure deduplication for big data storage in cloud", Peer-to-Peer Networking and Applications, Springer, 2020, Pages 1-19.

[4] Qian Zhang, Shangping Wang, Duo Zhang, Jifang Wang, Yaling Zhang, "Time and Attribute Based Dual Access Control and Data Integrity Verifiable Scheme in Cloud Computing Applications", IEEE Access, Volume 7, 2019, Pages 137594 – 137607.

[5] Shangping Wang, Xu Wang, Yaling Zhang, "A Secure Cloud Storage Framework With Access Control Based on Blockchain", IEEE Access, Volume 7, 2019, Pages 112713 – 112725.

[6] ShumingXiong, Qiang Ni, Liangmin Wang, Qian Wang, "SEM-ACSIT: Secure and Efficient Multiauthority Access Control for IoT Cloud Storage", IEEE Internet of Things Journal, Volume 7, Issue 4, 2020, Pages 2914 – 2927.

[7] Qi Xia, Emmanuel BoatengSifah, Kwame Opuni-BoachieObourAgyekum, Hu Xia, Kingsley NketiaAchea, "Secured Fine-Grained Selective Access to Outsourced Cloud Data in IoT Environments", IEEE Internet of Things Journal, Volume 6, Issue 6, 2019, Pages 10749 – 10762.

[8] Qinlong Huang, Licheng Wang &Yixian Yang, "DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices", World Wide Web, Springer, Volume 21, 2018, Pages 151-167.

[9] S. Kanimozhi, A. Kannan, K. Suganya Devi, K Selvamani, "Secure cloud-based e-learning system with access control and group key mechanism", Concurrency and Computation Practice and Experience, Wiley, 31, Issue 12, 2019, Pages 1-10.

[10] G. Sahaya Stalin Jose & C. Seldev Christopher, "Secure cloud data storage approach in e-learning systems", Cluster Computing, Springer, Volume 22, 2019, Pages 12857-12862

[11] Fahad A. Alghamdi, "An Integrated Cloud model for intelligent E-Learning system", International Journal of Applied Engineering Research, Volume 13, Issue 14, 2018, Pages 11484-11490.

[12] ShahidFarid, Rodina Ahmad, MujahidAlam, Atif Akbar, Victor Chang, "A sustainable quality assessment model for the information delivery in E-learning systems", Information Discovery and Delivery, Volume 46, Issue 1, 2018, Pages 1-25.

[13] YassineKhlifi, Hassan A. El-Sabagh, "A Novel Authentication Scheme for E-assessments Based on Student Behavior over E-learning Platform", Volume 12, Issue 04, 2017, Pages 62-89.

[14] Ye Tao, Peng Xu, Hai Jin, "Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage", IEEE Access, Volume 8, 2019, Pages 15963 – 15972.

[15] SlavkoRakic, NemanjaTasic, UgljesaMarjanovic, SelverSoftic, EgonLüftenegger, IoanTurcin, "Student Performance on an E-Learning Platform: Mixed Method Approach", International Journal of Emerging Technologies in Learning, Volume 15, Issue 02, 2020, Pages 187-203.

[16] Hongliang Zhu, Ying Yuan,Yuling Chen, YaxingZha, Wanying Xi, Bin Jia, Yang Xin, "A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature", IEEE Access, Volume 7, 2019, Pages 90036 – 90044.

[17] Saleh Atiewi; Amer Al-Rahayfeh; MuderAlmiani; Salman Yussof; Omar Alfandi; AhedAbugabah; YaserJararweh, "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography", IEEE Access, Volume 8, 2019, Pages 113498 – 113511.

[18] B. B. Gupta and MeghaQuamara, "An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards", Procedia Computer Science, Elsevier, Volume 132, 2018, Pages 189-197.

[19] Geeta Sharma and SheetalKalra, "A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications", Journal of Information Security and Applications, Elsevier, Volume 42, 2018, Pages 95-106.

[20] Sana Belguith, NesrineKaaniche, Maryline Laurent, AbderrazakJemai, RabahAttia, "Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds", Journal of Parallel and Distributed Computing, Elsevier, Volume 135, 2020, Pages 1–20.

[21] Educational Process Mining (EPM): A Learning Analytics Data Set

[https://archive.ics.uci.edu/ml/datasets/Educational+Process+Mining+%28EPM%29%3A+A+Learning+Analytics+Data+Set].