Advances in Dynamical Systems and Applications.
ISSN 0973-5321, Volume 16, Number 2, (2021) pp. 1349-1370

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

Reinforced Streebog Cryptographic Hash Blockchain Based Access Control for E-Learning in Cloud

N.R. Chilambarasan*, A. Kangaiammal

**Ph.D Research Scholar (Part Time), PG & Research Department of Computer Science, Government Arts College (Autonomous), Salem-7., India.*

**Assistant Professor, Department of Computer Science, Salem Kongunaadu College of Arts and Science, Salem – 302, India.*

Assistant Professor, Department of Computer Applications, Government Arts College (Autonomous), Salem-7., India.

**Corresponding author.*

Abstract

Contemporary E-learning platforms become both community and collaborative where valuable resources of E-learning are managed and shared within the community. Such type of collaborative dynamic E-learning platform is in the increasing demand. In the context of E-learning platforms, the extent of research focusing on access control is increasing. However, conventional centralized server architectures have to be replaced due to low scalability, lack of community-based access control, low robustness, and so on. Hence, decentralized access control systems built on E-learning platforms with the aid of Blockchain and Machine Learning (ML) algorithm called, Streebog Cryptographic Hash Blockchain-enabled Secure Decentralized Access Control and Double Q-Learning (SCHBSDAC-DQL) technique is proposed. The proposed SCHBSDAC-DQL technique, on one hand, is based on the blockchain model to provide the distributed characteristic dynamically endorsed in the IoT and on other hand on machine learning algorithms. The IoT devices are deployed to sense and monitoring student activities during the E-learning process. At first, the sensing data are collected for secure transmission. After that, Streebog Cryptographic Hash Blockchain-enabled secure decentralized access control framework is developed for students in the

E-Learning platform. Streebog Cryptographic technique is applied to generate the hash for each input data with the help of the one-way compression function. SmartContract theory-based model is applied to the Blockchain to ensure a distributed framework and access control without believing external third parties resulting it increases in the data confidentiality rate. Next, a Double Q-Learning algorithm is designed for analyzing student activities to make optimal action. The Double Q-Learning algorithm is used to find the maximum reward attainable from future states to reward for achieving its current state. Based on the learning process, the performance levels of students are identified through the E-learning process. Experimental evaluation is carried out on certain factors such as confidentiality rate, data integrity rate, and processing time, with respect to a number of student data. The empirical results demonstrate that our proposed SCHBSDAC-DQL provides an efficient solution for secure decentralized access control while preserving sensitive information.

Keywords: E-learning, Cloud, Access control, Streebog Cryptographic Hash Blockchain, Smart Contract, Access control, Double Q-Learning.

INTRODUCTION

The computing domain for E-learning is dynamic in nature due to the exposure of new smart learning and teaching process. Besides, the learning models are also said to be uncertain. Hence, e-learning systems need to develop more materials and methods to converge the growing requirements of millions of learners across the globe. E-learning is popularity and the number of learners enrolled in online courses. This trend is explained by the occasion provided by Cloud Computing. In the cloud-based E-learning system, the security aspect in sharing the educational content is significant and creates abundant security challenges, such as access control and security preservation of content learning. In addition, educational institutions include a huge amount of academic database comprises of the student details. These student databases along with other attributes are taken into consideration like student ID, learning activities. It also assists in identifying student performance levels through machine learning techniques.

A novel fog computing e-learning scheme was introduced [1] into the e-learning system to increase the efficiency of learning data analysis and also grants the access control to learning content by encrypting the content using different cryptographic techniques. Though the scheme increases the data confidentiality rate, the integrity verification was not performed to further improve the security. A Distributed Course Recommender system was presented in [2] for the E-learning platform to identify the relationships between student activities. However, with the centralized nature and

more dependency of the server, the performance of the access control system is said to be compromised.

Online behavior analysis was developed in [3] depends on the student profile for intelligent e-learning. However, the deep analysis and security considerations remained unsolved. A Secure E-learning System (SES) was developed in [4] for the distribution of examinations related materials by preventing a variety of security attacks. However, the performance of data confidentiality was not improved. An artificial neural network was developed in [5] for effectively predicting student performance. However, the designed network failed to consider the security aspects of the E-learning system. A new multilevel classification approach was introduced in [6] to protect from the different security attacks across various cloud services. The model failed to improve E-learning security performance. A Blockchain IoT applications were presented in [7] for providing the security and confidence in this large incoming information source.

An E-learning User Interface (ELUI) model was developed in [8] to predict the student attitude toward future use. A learning path planning algorithm was developed in [9] depends on the collaborative analysis of learning behavior. A logit leaf model (LLM) was designed in [10] to predict the student dropout-based on online learning environments. However, the access control mechanism remained unsolved.

CONTRIBUTION OF THE WORK

The major contribution of the proposed SCHBSDAC-DQL technique is summarized as given below,

To improve secure access control in the cloud-based E-learning system, the SCHBSDAC-DQL technique is introduced. To increase confidentiality and integrity, the Streebog Cryptographic Hash Blockchain-enabled Secure Decentralized Access Control is employed in the SCHBSDAC-DQL technique for improving the security. The Streebog Cryptographic technique generates the hash value for the student data collected from the E-learning process compression function. The SmartContract theory-based model is also implemented in the Blockchain technology to execute the legally relevant events without believing external third parties. Applying the Double Q learning algorithm in the SCHBSDAC-DQL technique to determine the student academic performance level with minimum processing time. Finally, security analysis and extensive experimental assessment are performed in various performance metrics to highlight the advantage of the proposed SCHBSDAC-DQL technique over conventional techniques.

ORGANIZATION OF THE PAPER

The rest of paper is arranged into different sections as follows. Section 2 introduces the related works. Next, a detailed construction of our proposed SCHBSDAC-DQL technique is described in section 3. Section 4 provides the experimental settings and implementation scenarios. In sections 5, the performance of different proposed and existing methods is discussed. Finally, end the paper with a conclusion.

RELATED WORKS

The student performance analysis was performed in [11] with fewer available attributes. But, the machine learning algorithms were not implemented to improve prediction performance. In [12], data mining techniques were introduced to build a browsing behavioral method for supporting E-learning resources. Different data mining methods were developed in [13] to find the performance of undergraduate students. The security aspects were not considered. The activities of the student during the learning process were analyzed in [14] using correlations, multiple regressions, and process mining.

A novel prediction algorithm was designed in [15] for estimating the student's performance based on classification and clustering approaches. But the algorithm failed to support huge varieties of features of the student academic dataset. An ensemble meta-based tree scheme (EMT) classifier was introduced in [16] to determine student performance. However, the model failed to consider the more features for predicting the performance of the students.

A unified structure was introduced in [17] to construct a new supervised cluster-based (CB) classifier for increasing the student performance. However, it failed to increase the number of records in the dataset with a distinction of students in different fields.

A new conceptual approach was developed in [18] for security and privacy factors related to e-learning. An incorporated cloud model was developed in [19] for intelligent eLearning system to guarantee safety and accessibility. Fog based Recommendation System (FBRS) was developed in [20] for enhancing the performance of the E-Learning environment.

METHODOLOGY

As an efficient mode for education, the E-Learning supported more understanding and skills than conventional education and also is beyond the limitation of time and space-based on new information and communication technologies. E-Learning is the process of learning the audio, video, text, images, and animations, etc through electronic media with the help of the internet.

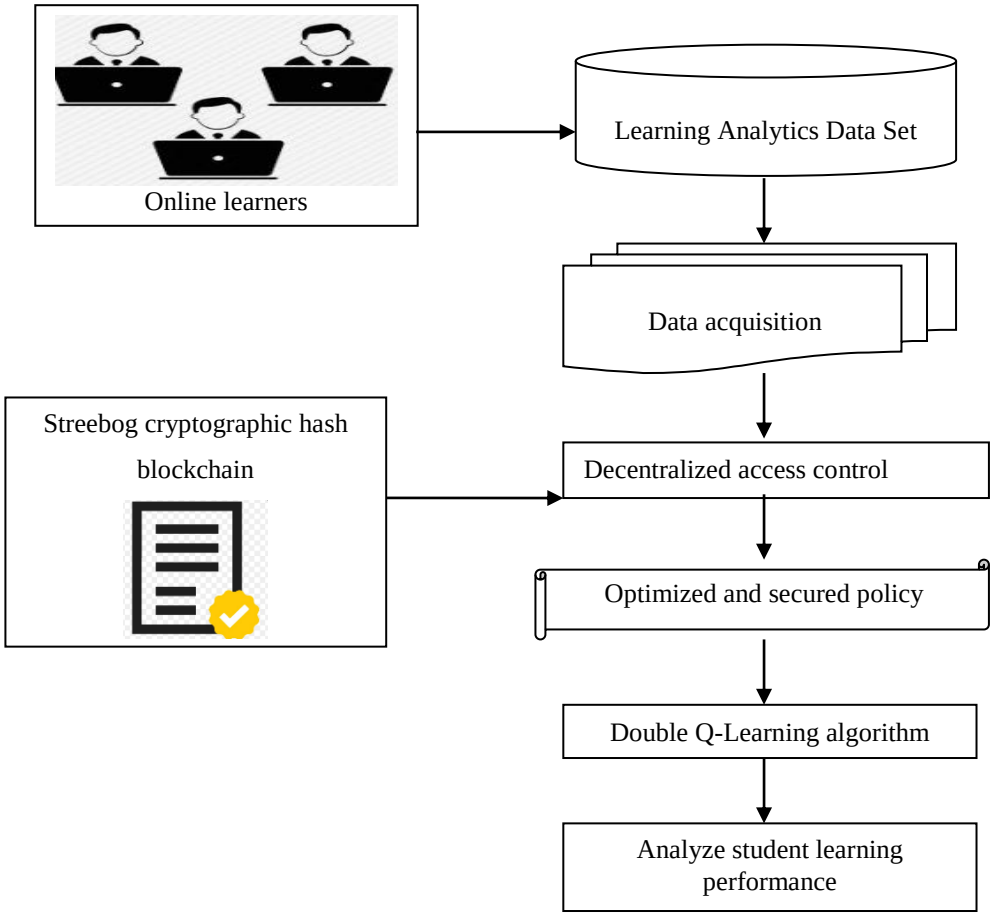


Figure 1 architecture of proposed SCHBSDAC-DQL technique

In recent days, educational institutions discover that the E-Learning system makes an impact on the teaching and learning process to develop traditional classroom teaching and it also offers courses to a larger population of learners with any geographical area. Security is a significant concern in the actual educational context where E-learning enhances in popularity and more and more students are taking online classes. Numerous important elements that must be taken into security aspects are authentication, access control, data integrity, content protection, and so on. While developing the security policies for cloud-based E-learning, an efficient mechanism is needed for preventing unauthorized operations to access another student's account and view sensitive information. Since cloud computing is to control and access data for institutions on the cloud servers. Meeting the security necessity in an E-learning system is an especially complex issue since it is necessary to protect the content, services, and personal data from unauthorized access except for the system administrators. In order to provide the security access of student activities data, an efficient cryptographic technique is developed to ensure that information and data are not disclosed to any unauthorized access. In this paper, a novel SCHBSDAC-DQL

technique highlights some key security issues taken into consideration in developing and using an E-learning platform.

Figure 1 illustrates the architecture diagram of the proposed SCHBSDAC-DQL technique to provide security by access control in the E-learning platform. The architecture includes the number of students (i.e. learners) and their activities and learning information is stored in the dataset. The learning information is collected from the dataset. The student E-learning dataset includes heterogeneous instances since the variety of features generated. This information is needed for preventing unauthorized operations to access the student's sensitive information. In order to improve security, cryptographic hash-based blockchain technology is applied. In addition, student academic performance analysis is done with the novel machine learning called Doube Q-Learning algorithm. These processes are explained in following subsections.

Streebog Cryptographic Hash Blockchain-enabled Secure Decentralized Access Control

A streebog cryptographic hash blockchain-enabled secure decentralized access control technique is introduced in the SCHBSDAC-DQL technique for improving the security. To participate more students in the E-Learning platform, a SmartContract model is applied in Blockchain technology. A smart contract is a transaction protocol that is aimed to automatically execute legally relevant events along with the terms of a contract or an agreement without believing external third parties.

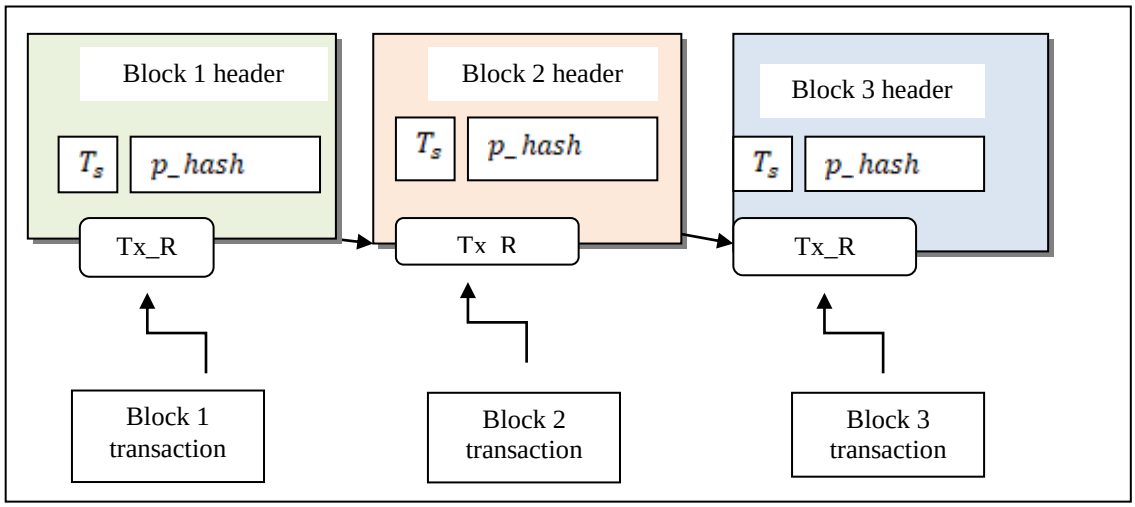


Figure 2 : Construction of Blockchain

Figure 2 demonstrates the construction of blockchain that includes the different blocks to form a chain. In the chain, each block consists of a cryptographic hash of the

previous block ($p\_\ hash$), a timestamp (T_s), and root hash (Tx_R). The blockchain has different transaction data (generally represented as a hash). Each transaction comprises the student learning information. Moreover, each block has a block header. As shown in the blockchain, the hash of the previous block ($p\_\ hash$) is used for block verification. Time steps (T_s) refers to the time when the block was created. Each block transaction comprises the student information collection from the dataset. The root hash value is generated using Streebog cryptographic hash function to improve the security by avoiding unauthorized access.

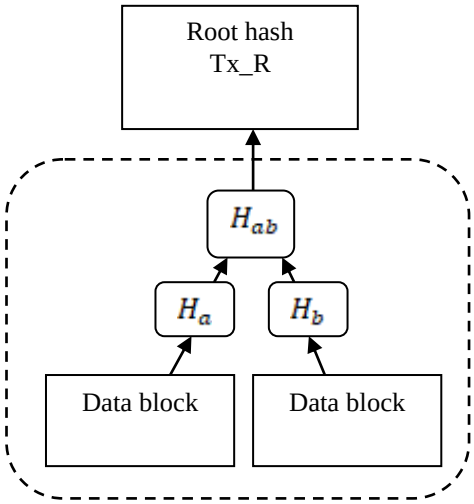


Figure 3 Streebog cryptographic hash generation

Figure 3 illustrates the Streebog cryptographic hash generation. As shown in the figure, the data (i.e. student's information) is given to the data block. Then the Streebog cryptography function generates a hash of each data (H_a), (H_b) and the concatenation of the two hash value (H_{ab}) is given root hash of the block in the chain. A Streebog cryptographic function operates on 512-bit blocks of input and it transfers fixed-length hash value. The Streebog cryptographic function is used for managing the inputs of arbitrary size and fixed size of bit string (i.e. hash). If any modifications in the input data and cause a severe change in the hash value. Therefore, the Streebog cryptographic function is applied to guarantee security. The Streebog cryptographic function uses the compression function to generate the fixed size of the hash value. The operation of the compression function is illustrated in figure 4.

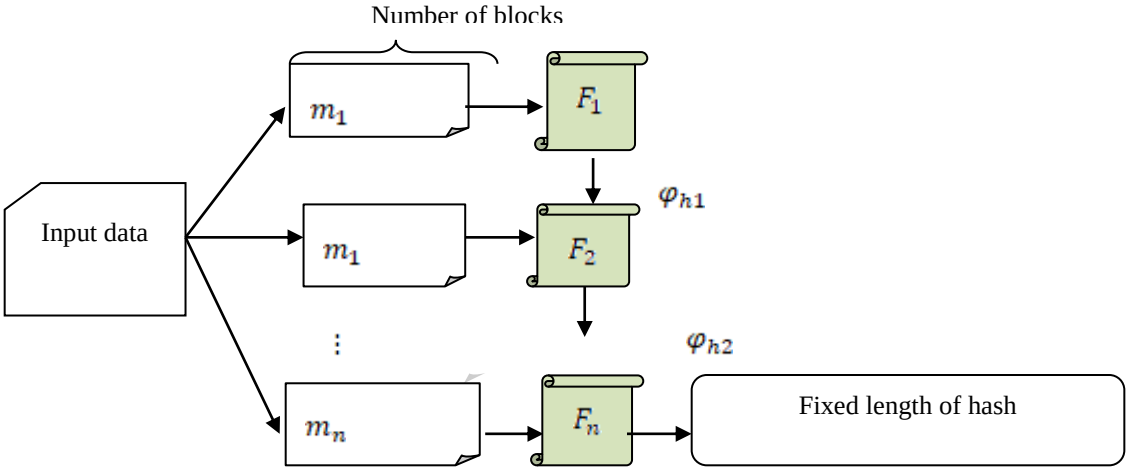


Figure 4 block diagram of hash generation using one-way compression

Figure 4 illustrates the block diagram of the hash generation with a one-way compression function. Let us consider the number of student data $D_s = D_1, D_2, D_3 \ldots . D_n$. By applying Streebog cryptographic function, the input data is divided into a number of blocks with a fixed size.

$$D_s \rightarrow m_1, m_1, m_2, \ldots m_n \tag{1}$$

Where,D_s denotes an input size of student data, $m_1, m_1, m_2, \ldots m_n$ designates a message block with a fixed size. Then the message block is given to the compression function (F) which takes an input message block (m_1) and providing the hash value (φ_{h1}). The generated hash is $\varphi_{h0} \in \{0,1\}$ built by iterating the compression function '$F_1, F_2, \ldots F_n$' in order to provide a final hash with fixed length (φ_{hn}). Given an input $m1$ whose output is φ_{h1}, then the output is obtained as follows,

$$\varphi_{h1} \overset{F_1}{\rightarrow} (\varphi_{h0}, m_1) \tag{2}$$

Where, φ_{h1} denotes a hash of the block m_1, φ_{h0}denotes a constant pre-specified initial hash value, F_1 denotes a compression function. The hash of one input block is not the same as another input block

$$\varphi_{h1} \neq \varphi_{h2} \tag{3}$$

Similarly, the final hash is generated as given below,

$$\varphi_{hn} \overset{F_n}{\rightarrow} \left(\varphi_{h_{i-1}}, m_i\right) \quad \text{Where } i = 1,2,3 \ldots . n \tag{4}$$

Where, φ_{hn} indicates the final output hash, $\varphi_{h_{i-1}}$ denotes a hash of the previous block, m_i indicates an input block. Followed by, the generated hash is given to the root hash of the blockchain. This shows the authorized users only view and access resulting it increases data confidentiality and integrity. The algorithmic process of the

access control is briefly described as given below.

// Algorithm 1 Streebog cryptographic hash blockchain-enabled Secure Decentralized Access Control

Input: E-learning dataset, Number of students data $D_1, D_2, \ldots D_n$

Output: Improve the security of access

Begin

1. Collect **the data $D_1, D_2, \ldots D_n$ from dataset**
2. **For each transaction 't'**
3. Construct blockchain
4. **For each D_1**
5. Divide into message blocks $m_1, m_2, m_3, \ldots m_n$
6. **for each block m**
7. **Generate hash value**
8. **End for**
9. Obtain the final hash 'φ_{hn}'
10. **End for**
11. **Improve the security of access**
12. **End for**

End

The step by step process of the proposed Streebog cryptographic hash blockchain-enabled Secure Decentralized Access Control is described in algorithm 1. The E-learning dataset comprises the student information is collected and is transmitted into the server through the internet. Before the data transmission, the collected data are securitized by applying the Streebog cryptographic hash-based blockchain technology. The input sizes of data are divided into several message blocks with a fixed size. Subsequently, the compression function is applied to generate a hash for each block. For each transaction, the hashed results are used resulting in it avoid unauthorized users and it is only accessed by the authorized entity. This helps to improve the data confidentiality rate. Without the dependency on the third party for ensuring access control, the average higher confidentiality rate incurred in the cloud environment is said to be improved.

Double Q-Learning algorithm

After providing the security to the collected student data at the time of the E-learning process, the future states of the optimal action is determined by applying a Double Q-Learning algorithm. A novel machine learning technique called Double Q-Learning is a model-free reinforcement learning algorithm that discovers an optimal policy in the sense of maximizing the expected value of the total reward over any and the entire consecutive steps, starting from the current state.

By applying the Double Q-Learning algorithm, the state-action pair (δ, α) is considered at each time step to predict the future state. In this technique, an action space includes the necessary information regarding the student behaviors (or activities) during the E-learning process, the state space used to provide the optimal future value at the given time.

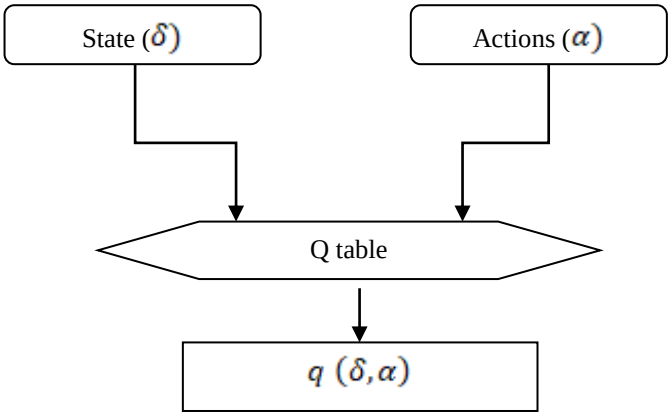


Figure 5 construction of state-action pair generation

Figure 5 illustrates the construction of a state-action pair generation. In the current state, the student behaviors such as the data are presented per session, per student, per exercise and the numbers of activities are learned. 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.

Let us consider the two (i.e. double) separate value functions u, v are trained in a mutually symmetric, and the update is expressed as given below.

$$\alpha^* = \arg\max q_t^v\ (\delta_{t+1}, \alpha_t) \tag{5}$$

$$q_{t+1}^u\ (\delta_t, \alpha_t) = q_t^u\ (\delta_t, \alpha_t) + \beta_t(\delta_t, \alpha_t)(R_t + \omega q_t^v(\delta_{t+1}, \alpha^*) - q_t^u\ (\delta_t, \alpha_t)) \tag{6}$$

$$\mathrm{b}^* = \arg\max q_t^b\ (\delta_{t+1}, \alpha_t) \tag{7}$$

$$q_{t+1}^v\ (\delta_t, \alpha_t) = q_t^v\ (\delta_t, \alpha_t) + \beta_t(\delta_t, \alpha_t)(R_t + \omega q_t^u(\delta_{t+1}, \mathrm{b}^*) - q_t^v\ (\delta_t, \alpha_t)) \tag{8}$$

Where, $q_{t+1}^u\ (\delta_t, \alpha_t)$, $q_{t+1}^v\ (\delta_t, \alpha_t)$ denotes an updated value of the two separate

value functions u, v , $q_t^u(\delta_t, \alpha_t), q_t^v(\delta_t, \alpha_t)$ indicates the old value, β_t denotes a learning rate $(0 < \beta_t < 1)$, R_t denotes rewards received when moving from the state δ_t to δ_{t+1} . ω denotes a discount factor which is a number between 0 and 1. $\arg\max q_t^u(\delta_{t+1}, \alpha_t)$, $\arg\max q_t^v(\delta_{t+1}, \alpha_t)$ represents the maximum predicted reward from all possible actions. This is also known as an estimated optimal future value at the future stateδ_{t+1}. Finally, the average of these two updated values for each action is taken as optimal in the future state. Based on the updated results values, the Double Q-Learning algorithm is used to analyze the student learning performance. The algorithmic process of the Double Q-Learning is described as given below,

Algorithm 2: Double Q-Learning

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

Output: Identify student performance level

Begin

1. Initialize q_t^a, q_t^b
2. Analyze the student behavior
3. Define $\alpha^* = \arg\max q_t^a(\delta_{t+1}, \alpha_t)$
4. Update $q_{t+1}^a(\delta_t, \alpha_t)$
5. Define $b^* = \arg\max q_t^b(\delta_{t+1}, \alpha_t)$
6. Update $q_{t+1}^b(\delta_t, \alpha_t)$
7. Take average $q_{t+1}^a(\delta_t, \alpha_t)$ and $q_{t+1}^b(\delta_t, \alpha_t)$
8. Obtain the final optimal value
9. Find student learning performance

End

Algorithm 2 illustrates the step by step process of Double Q-Learning for finding the student learning performance. The student learning performance is analyzed and found the optimal solution at a future state. Based on the predefined current value of the two functions, the maximum rewards are predicted through the updating process in an accurate manner. As a result, student learning performances are determined.

EXPERIMENTAL SETTINGS

Experimental assessment of the proposed SCHBSDAC-DQL technique and existing fog computing e-learning scheme [1], Distributed courses recommender system [2] are implemented using Java language with CloudSim. To perform secure access in the cloud, the Educational Process Mining (EPM): A Learning Analytics Data Set is used for evaluating the performance of the proposed technique.

Dataset description

The Educational Process Mining (EPM): A Learning Analytics Data Set is taken from the UCI machine learning repository.

[https://archive.ics.uci.edu/ml/datasets/Educational+Process+Mining+%28EPM%29%3A+A+Learning+Analytics+Data+Set]. Educational Process Mining data set is constructed from the recordings of 115 student's activities through a logging application while learning with an educational simulator which is used for e-learning in digital electronics. The data set includes different students' time series of activities during six different sessions. There are 6 folders containing student's data per session. The dataset also comprises the 230318 instances and 13 attributes and their characteristics are integers. The associated task performed by the dataset is classification, regression, and clustering. The student data are securitized by applying the hash-based blockchain technology during the transaction. Then the student learning performance is identified through their activities. The features are listed in table 1.

Table I attribute description

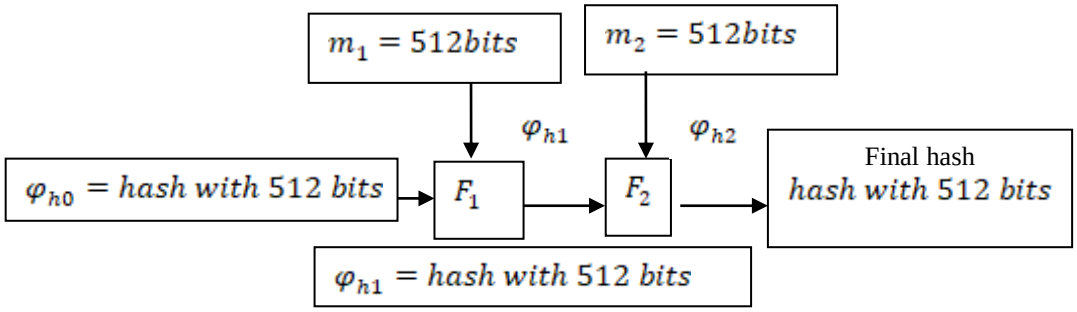
S.no	Features	Description
1	Session	Number of lab sessions from 1 to 6.
2	Student-ID	115 students' ID number (1,2,3….115)
3	Exercise	It shows the working Ex. The ID of the student. (Es_2_1 represents Session 2, Exercise 1).
4	Activity	The activities are grouped into 15 categories related to Exercise, Using Deeds Simulator, Using Text Editor, Working on Diagram, Working on Properties Window, Viewing Study Materials, Using Finite State Machine Simulator, Using Aulaweb, Blank, and other irrelevant Activities
5	Start-time	Starting date and time of a specific activity.

6	End-time	Ending date and time of a specific activity.
7	Idle-time	The duration of idle time between the start and end time.
8	Mouse-wheel	Volume of mouse wheel operations during an activity.
9	Mouse-wheel-click	Number of mouse wheel clicks during an activity.
10	Mouse-click-left	Number of left mouse clicks during an activity.
11	Mouse-click-right	Number of right mouse clicks during an activity.
12	Mouse-movement	Distance moved by the mouse movements during an activity.
13	Keystroke	Number of key presses during an activity.

Implementation scenario

In this section, the implementation of the proposed SCHBSDAC-DQL technique is discussed with the Educational Process Mining (EPM): A Learning Analytics Data Set. The Educational Process Mining (EPM): A Learning Analytics Data Set is applied for the proposed SCHBSDAC-DQL technique, different processes are carried out such as secure access control and performance level prediction.

Let us consider the number of students data is taken as input in the ranges from 50 to 500. Let us consider the size of single-user data is 1024bits. By applying the Streebog cryptographic hash blockchain, the input 1024bits are divided into a number of blocks with a fixed size $m_1 = 512bits, m_2 = 512bits$. Let us consider the initial hash (φ_{h0}) with 512bits. The input is given to the compression function 'F_1'



The compression function mixes two inputs and generates fixed size of hash. Then these generated hashes are distributed in the blockchain technology to avoid unauthorized access. This hashed student behavior information's are accessed by the authorized entity.

Let us consider the two (i.e. double) separate value functions a, b are trained in a mutually symmetric, and the update is expressed as given below. Let us consider $q_t^a\ (\delta_t, \alpha_t) = 0.5,\ q_t^b\ (\delta_t, \alpha_t) = 0.6, \beta_t(\delta_t, \alpha_t) = 0.4$, Let us consider the positive reward $R_t = 1$, $\omega = 0.9$

$$\alpha^* = \arg\max q_t^b\ (\delta_{t+1}, \alpha_t) = 0.9$$

$$q_{t+1}^a\ (\delta_t, \alpha_t) = q_t^a\ (\delta_t, \alpha_t) + \beta_t(\delta_t, \alpha_t)\big(R_t + \omega q_t^b(\delta_{t+1}, \alpha^*) - q_t^a\ (\delta_t, \alpha_t)\big)$$

$$q_{t+1}^a\ (\delta_t, \alpha_t) = 0.5 + 0.3(1 + 0.9 - 0.5) = 0.92$$

$$\mathrm{b}^* = \arg\max q_t^b\ (\delta_{t+1}, \alpha_t) = 0.8$$

$$q_{t+1}^b\ (\delta_t, \alpha_t) = q_t^b\ (\delta_t, \alpha_t) + \beta_t(\delta_t, \alpha_t)\big(R_t + \omega q_t^a(\delta_{t+1}, \mathrm{b}^*) - q_t^b\ (\delta_t, \alpha_t)\big)$$

$$q_{t+1}^b\ (\delta_t, \alpha_t) = 0.6 + 0.4(1 + 0.8 * 0.6 - 0.6)$$

$$q_{t+1}^b\ (\delta_t, \alpha_t) = 0.6 + 0.4(1 + 0.54 - 0.6) = 0.952$$

Finally, the average of these two updated values for each action is taken as optimal at future state,

$$Average = \frac{0.92+0.952}{2} = 0.936$$

The obtained value indicates that the performance of the student through the E-learning is higher. This helps to predict the performance of the end semester results of the students based on the student activities during the E-learning.

RESULTS AND DISCUSSION

The experimental results of the different methods are discussed with respect to various performance metrics such as data confidentiality rate, integrity rate, and processing time. These metrics are described as given below.

Confidentiality rate: Confidentiality rate is the most significant security parameter in the cloud. The data confidentiality rate is measured as the ratio of the number of student data only accessed by authorized entities. Therefore, the confidentiality rate is mathematically calculated as given below,

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

Where, $Rate_{con}$ specifies a confidentiality rate, 'n' represents the number of student data, 'n_{aae}' refers to the number of data accessed by the authorized entity. The confidentiality rate is measured in terms of percentage (%).

Data integrity rate: It is another security parameter in access control that referred to the number of data that are not altered by any third party to the number of data. The

formula for calculating the integrity rate is given below

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

Where $Rate_{Int}$ symbolizes a data integrity rate, ' n_{aa}' denotes the number of data not altered by others, 'n' denotes a total number of data. The data integrity rate is measured in percentage (%).

Processing time: It is defined as an amount of time consumed by the algorithm to find the student performance level during the E-learning process. The processing time is expressed as given below,

$$PT = n * [Time\ (ISD)] \quad (11)$$

Where PT denotes a processing time, 'n' denotes the number of student data, $Time\ (ISD)$ indicates time taken to analyze the single- student data. The overall processing time of the algorithm is measured in milliseconds (ms).

Table II Confidentiality rate

Number of data	Confidentiality rate (%)		
	SCHBSDAC-DQL	**Fog computing e-learning scheme**	**Distributed courses recommender system**
50	94	88	82
100	92	86	83
150	95	90	87
200	94	88	86
250	92	87	85
300	93	86	83
350	95	89	86
400	93	86	84
450	94	89	86
500	93	88	84

Table II describes the performance analysis of the confidentiality rate versus the number of student data taken in the counts from 50 to 500. The reported results of the confidentiality rate using three methods are shown in the table II. From the observed

results, it indicates that the SCHBSDAC-DQL achieves a higher data confidentiality rate**.** For example, 50 student's data are considered for experimentation. By applying the SCHBSDAC-DQL technique, 47 data are correctly accessed by the authorized entity and the confidentiality rate of the proposed SCHBSDAC-DQL technique is 94% whereas the confidentiality rate of existing fog computing e-learning scheme [1],

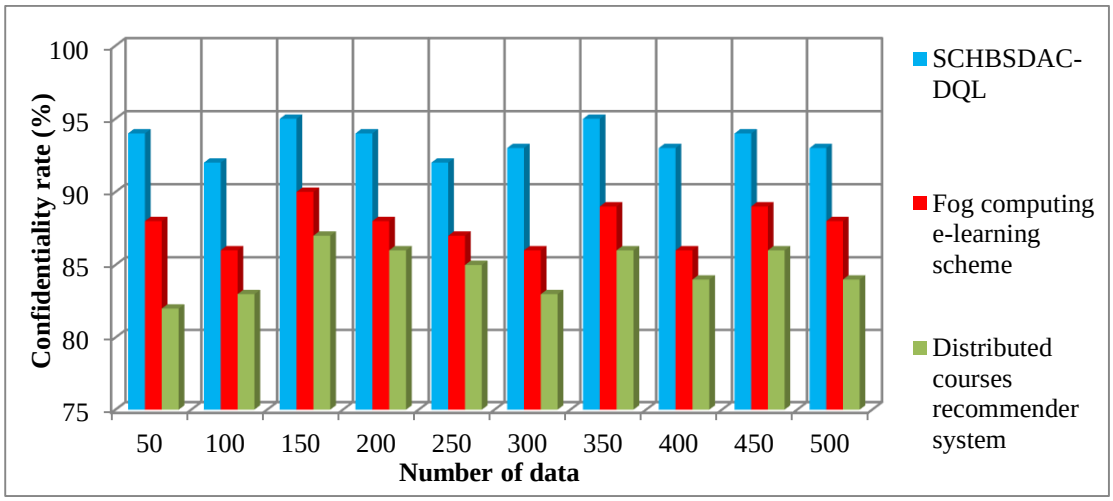


Figure 6 graphical illustration of confidentiality rate

Distributed courses recommender system [2] is observed as 88% and 82%. For each method, ten runs are performed and results are compared. The results of the proposed SCHBSDAC-DQL technique are compared to the existing methods. The comparison of ten runs proves that the proposed technique achieves the improved performance of data confidentiality rate by 7% when compared to [1] and [2] respectively.

Figure 6 exhibits the confidentiality rate of three methods namely the SCHBSDAC-DQL technique and existing fog computing e-learning scheme [1], Distributed courses recommender system [2]. The numbers of data are taken in the horizontal direction and the results of the confidentiality rate are obtained in a vertical direction. As shown in the graph, the blue color column indicates the confidentiality rate using SCHBSDAC-DQL whereas the red and green color column shows the confidentiality of existing [1] [2] respectively. The graphical plot shows that the proposed technique achieved a higher data confidentiality rate. The reason for this significant improvement is to applying the Streebog cryptographic hash function in the blockchain technology. The cryptographic technique generates the hash value for each student data collected during the E-learning process. The one-way compression function is implemented in the Streebog cryptographic function to generate the fixed size of the hash value. The hashed data are distributed in the blockchain. This helps

to protect the student data from unauthorized access and improve the confidentiality rate. Moreover, the smartcontract is implemented into the blockchain technology to automatically perform legally relevant data transactions without believing external third parties.

Table III Data integrity rate

Number of data	Data integrity rate (%)		
	SCHBSDAC-DQL	**Fog computing e-learning scheme**	**Distributed courses recommender system**
50	92	86	80
100	91	85	82
150	94	88	85
200	93	87	85
250	91	86	84
300	92	85	82
350	94	88	85
400	91	85	83
450	93	88	84
500	92	87	83

Table III exhibits the integrity rate of the SCHBSDAC-DQL technique over the existing methods fog computing e-learning scheme [1], Distributed courses recommender system [2] are reported in Table III. In order to statistically estimate the integrity rate, the student data are taken in the counts from 50 to 500. For each run, different counts of data are taken as an input. From the observed result, the integrity rate of the proposed technique is 92% and the integrity rates of the existing [1] [2] are 86% and 80% respectively. For each method, a totally ten different results are observed. The obtained results indicate that the proposed technique outperforms well

in terms of achieving a higher integrity rate. The average of ten results indicates that the integrity rate of SCHBSDAC-DQL considerably increased by 7% and 11% when compared to the existing fog computing e-learning scheme [1] Distributed courses recommender system [2] respectively.

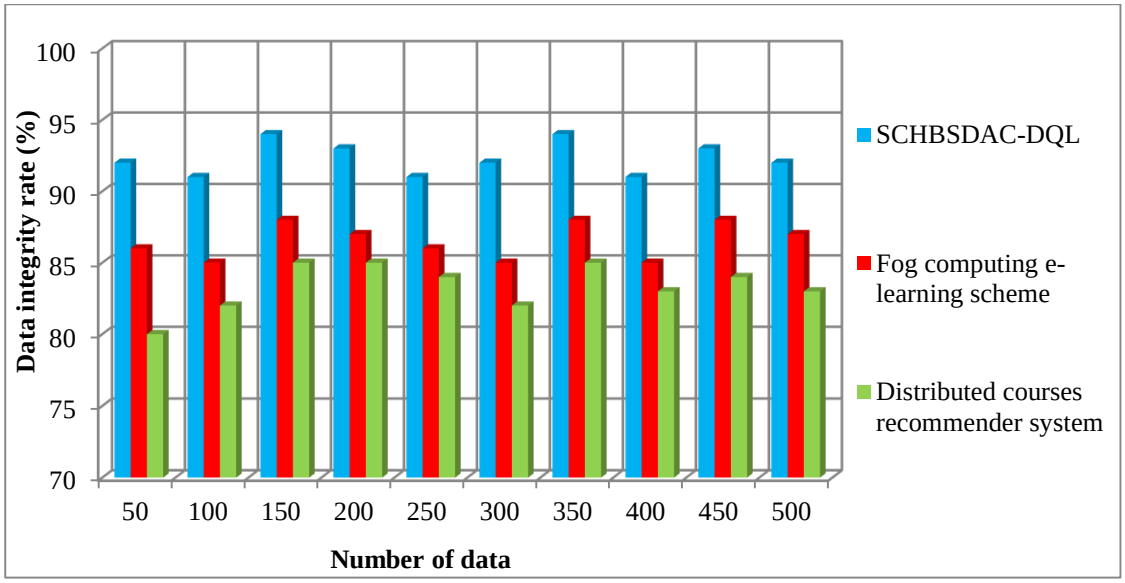


Figure 7 graphical illustration of integrity rate

The graphical illustration of the data integrity rate of three methods is illustrated in figure 7. The results of the experimentation are shown in figure 7, where the horizontal axis illustrates the number of student data and the horizontal axis demonstrates the data integrity rate (in percentage). The above graphic representation illustrates the data integrity rate of the SCHBSDAC-DQL is higher when compared to the existing fog computing e-learning scheme [1] Distributed courses recommender system [2] respectively. This significant improvement is achieved with the help of one way compression function in a Streebog cryptographic hash function. The compression function generates the fixed size of the hash while giving the input. If any modification in the input data it causes a severe modification in the hash value. This helps to easily identify any alteration in the input student sensitive information. As a result, the SCHBSDAC-DQL increases the performance results.

Table IV processing time

Number of data	Processing time (ms)		
	SCHBSDAC-DQL	**Fog computing e-learning scheme**	**Distributed courses recommender system**
50	28	30	35
100	33	35	40
150	38	42	45
200	42	46	50
250	50	55	60
300	54	57	63
350	56	60	65
400	60	64	68
450	65	70	72
500	70	75	78

Table IV shows the processing time of student learning performance analysis with respect to the number of student data. The processing time is measured as an amount of time consumed to perform student learning performance. The tabularized processing time is obtained for the different counts of input. The processing time of all the methods gets increased while increasing the number of student data. The experiment is accomplished with 50 data, SCHBSDAC-DQL technique consumes the time of $28ms$ and the processing time of fog computing e-learning scheme [1] Distributed courses recommender system [2] are observed as $30ms$ and $35ms$ respectively. Similarly, the other runs are performed with different counts of input. The overall processing time of the SCHBSDAC-DQL technique is evaluated with the other two conventional methods. The average of ten results noticeably proved that the processing time taken is significantly reduced by 7% and 15% when compared to other related methods [1] [2].

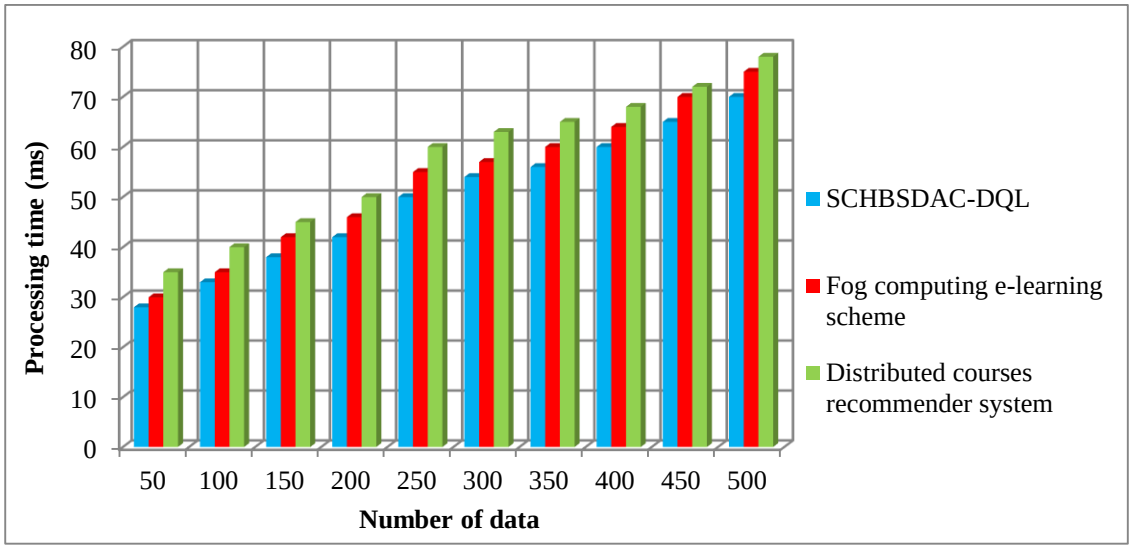


Figure 8 graphical illustration of processing time

Figure 8 perceives the performance results of time consumption for student learning performance. The graphical plot indicates that the processing time gets increased while increasing the number of input counts. Among the different methods, the proposed SCHBSDAC-DQL technique outperforms well in terms of achieving lesser processing time. The appropriate reason for the reduction of the processing time is to apply the Double Q learning. The proposed machine learning technique analyzes student data. Based on the analysis, the student learning performance is identified with lesser time consumption.

CONCLUSION

To guarantee data confidentiality and access control, the SCHBSDAC-DQL technique is proposed for secure data sharing for a cloud-assisted E-learning system. Security analysis demonstrates that our SCHBSDAC-DQL technique achieves higher access control. The proposed SCHBSDAC-DQL technique learns the input student data collected from the dataset. Initially, in this SCHBSDAC-DQL technique, a Streebog cryptographic hash blocks chain technology for providing the security by converting the input data into a fixed-length of hash with the help of a compression function. This helps to avoid unauthorized access and improve the confidentiality rate. Next, the double Q learning algorithm is applied to analyze the student learning performance based on the activities. Experimental evaluation is performed to estimate the performance of the SCHBSDAC-DQL technique over the two conventional methods and different performance metrics such as confidentiality rate, data integrity

rate, and processing time. The quantitatively validate results shows that the SCHBSDAC-DQL technique achieves improved performance in data confidentiality, integrity with lesser processing time than the conventional techniques.

REFERENCES

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

[2] Karim Dahdouh, Ahmed Dakkak, Lahcen Oughdir, Abdelali Ibriz, "Large scale e-learning recommender system based on Spark and Hadoop", Journal of Big Data, Springer, 2019, Pages 1-23

[3] Kun Liang, Yiying Zhang, Yeshen He, Yilin Zhou, Wei Tan, Xiaoxia Li, "Online Behavior Analysis-Based Student Profile for Intelligent E-Learning", Journal of Electrical and Computer Engineering, Hindawi, Volume 2017, Mar 2017, Pages 1-7

[4] Samina Kausar, Xu Huahu, Ata Ullah, Zhu Wenhao & Muhammad Yasir Shabir, "Fog-Assisted Secure Data Exchange for Examination and Testing in E-learning System", Mobile Networks and Applications, 2020, Pages 1-17

[5] Şeyhmus Aydoğd, "Predicting student final performance using artificial neural networks in online learning environments", Education and Information Technologies, Volume 25, 2020, Pages 1913-1927

[6] Syed Asad Hussain, Mehwish Fatima, Atif Saeed, Imran Raza, Raja Khurram Shahza, "Multilevel classification of security concerns in cloud computing", Applied Computing and Informatics, Elsevier, Volume 13, Issue 1, 2017, Pages 57-65

[7] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", Future Generation Computer Systems, Elsevier, Volume 88, 2018, Pages 173-190

[8] Wejdan Farhan, Jamil Razmak, Serge Demers, Simon Laflamme, "E-learning systems versus instructional communication tools: Developing and testing a new e-learning user interface from the perspectives of teachers and students", Technology in Society, Elsevier, Volume 59, 2019, Pages 1-12

[9] Zhaoyu Shou, Xianying Lu, Zhengzheng Wu, Hua Yuan, Huibing Zhang, Junli Lai, "On Learning Path Planning Algorithm Based on Collaborative Analysis of Learning Behavior", IEEE Access, Volume 8, 2020, Pages 119863 – 119879

[10] Kristof Coussement, Minh Phan, ArnoDe Caigny, Dries F.Benoitc, Annelies Raesd, "Predicting student dropout in subscription-based online learning

environments: The beneficial impact of the logit leaf model", Decision Support Systems, Elsevier, Volume 135, August 2020, Pages 1-11

[11] Edward Wakelam, Amanda Jefferies, Neil Davey, Yi Sun, "The potential for student performance prediction in small cohorts with minimal available attributes", British journal of educational technology, Wiley, Volume 51, Issue 2, 2020, Pages 347-370

[12] Sunil1, Prof. M. N. Doja, "Data Mining Techniques to Discover Students Visiting Patterns in E-learning Resources", International Journal of Computer Science and Mobile Computing, Volume 6, Issue 6, 2017, Pages 363 – 368

[13] Raheela Asif, Agath Merceron, Syed Abbas Ali, Najmi Ghani Haider, "Analyzing undergraduate students' performance using educational data mining", Computers & Education, Elsevier, Volume 113, 2017, Pages 177-194,

[14] R. Conijn, A. Van den Beemt, P. Cuijpers, "Predicting student performance in a blended MOOC", Journal of Computer Assisted Learning, Wiley, Volume 34, Issue 5, Pages 615–628.

[15] Bindhia K. Francis & Suvanam Sasidhar Babu, " Predicting academic performance of students using a hybrid data mining approach", Journal of Medical Systems, Springer, volume 43, 2019, Pages 1-15

[16] Erbug Celebi, and Rami S. Alkhawaldeh, "EMT: ensemble meta-based tree model for predicting student performance, Scientific Programming, Hindawi, Volume 2019, February 2019, Pages 1-13

[17] Ammar Almasri, Rami S. Alkhawaldeh & Erbuğ Çelebi, "Clustering-Based EMT Model for Predicting Student Performance", Arabian Journal for Science and Engineering, Springer, 2020, Pages 1-12

[18] Radwan Ali, Humayun Zafar, "A Security and Privacy Framework for e-Learning", International Journal for e-Learning Security (IJeLS), Volume 7, Issue 2, 2017, Pages 556-566

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

[20] Taghreed S. Ibrahim, Ahmed I. Saleh, Nehad Elgaml, Mohamed M. Abdelsalam, "A fog based recommendation system for promoting the performance of E-Learning environments", Computers and Electrical, Elsevier, Volume 87, 2020, Pages 1-29