Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.036217
Article

Blockchain-Based Decentralized Authentication Model for IoT-Based E-Learning and Educational Environments

Osama A. Khashan[1,*], Sultan Alamri[2], Waleed Alomoush[3], Mutasem K. Alsmadi[4], Samer Atawneh[2] and Usama Mir[5]

[1]Research and Innovation Centers, Rabdan Academy, P.O. Box 114646, Abu Dhabi, United Arab Emirates
[2]College of Computing and Informatics, Saudi Electronic University, Riyadh, 13316, Saudi Arabia
[3]School of Information Technology, Skyline University College, P.O. Box 1797, Sharjah, United Arab Emirates
[4]Department of MIS, College of Applied Studies and Community Services, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam, Saudi Arabia
[5]Department of Computer Science, University of Windsor, Windsor, N9J3Y1, Canada
*Corresponding Author: Osama A. Khashan. Email: okhashan@ra.ac.ae
Received: 21 September 2022; Accepted: 23 December 2022

Abstract: In recent times, technology has advanced significantly and is currently being integrated into educational environments to facilitate distance learning and interaction between learners. Integrating the Internet of Things (IoT) into education can facilitate the teaching and learning process and expand the context in which students learn. Nevertheless, learning data is very sensitive and must be protected when transmitted over the network or stored in data centers. Moreover, the identity and the authenticity of interacting students, instructors, and staff need to be verified to mitigate the impact of attacks. However, most of the current security and authentication schemes are centralized, relying on trusted third-party cloud servers, to facilitate continuous secure communication. In addition, most of these schemes are resource-intensive; thus, security and efficiency issues arise when heterogeneous and resource-limited IoT devices are being used. In this paper, we propose a blockchain-based architecture that accurately identifies and authenticates learners and their IoT devices in a decentralized manner and prevents the unauthorized modification of stored learning records in a distributed university network. It allows students and instructors to easily migrate to and join multiple universities within the network using their identity without the need for user re-authentication. The proposed architecture was tested using a simulation tool, and measured to evaluate its performance. The simulation results demonstrate the ability of the proposed architecture to significantly increase the throughput of learning transactions (40%), reduce the communication overhead and response time (26%), improve authentication efficiency (27%), and reduce the IoT power consumption (35%) compared to the centralized authentication mechanisms. In addition, the security analysis proves the effectiveness of the proposed architecture in resisting various attacks and ensuring the security requirements of learning data in the university network.

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Keywords: Blockchain; decentralized authentication; Internet of Things (IoT); E-learning; IoT security

1 Introduction

Electronic learning (e-learning) is a cutting-edge technology that provides a powerful and scalable learning platform. It allows students and instructors to work together from any geographic location in real time. Nowadays, e-learning applications are largely implemented in educational institutions by allowing learners to access numerous educational resources at any time, do homework, and exchange learning data and records electronically between the educational entities [1]. Accordingly, modern technologies such as the Internet of Things (IoT), mobile networking, and cloud computing, have been successfully used with e-learning. This integration technology offers great potential to improve the teaching and learning process, and enhance communication practices among learners. It also increases the learning efficiency and performance [2].

Many educational institutions still use an inappropriate and outdated method of managing student records and credentials. When a student transfers from one institution to another, their information and prior educational record must be made available to the new institution. This means that the student or the institute must communicate with multiple institutions, in order for the student's learning record to be delivered directly to the relevant parties upon request [3]. This is a time-consuming process, as institutions have to verify records and respond accordingly. In addition, non-uniform assessment systems and the diversity of learning data make it difficult to verify learning records or grades. E-learning data is confidential and only accessible by authorized users. Nevertheless, there are several security-related deficiencies in most e-learning systems that have raised concerns about the privacy and the security of electronic learning data [4].

IoT technology provides a more effective electronic teaching-learning platform with a variety of distance learning objects. The integration of IoT into the field of education allows us to connect with different heterogeneous learning systems, exchange learning data in a standard way, and collaborate with educational objects seamlessly. It allows learners to communicate and access various data sources in real time and with a high degree of interaction. Furthermore, it can improve operational efficiency, increase resource sharing, reduce costs, and provide communication efficiency [5]. However, the inclusion of IoT in the learning process raises several issues that need to be addressed in detail. The growing number of interconnected IoT and other Internet Protocol (IP-based) things have the potential to generate massive amounts of learning data that are offloaded to cloud servers for centralized data processing and storage [6]. This large volume of data may cause performance deficiencies, as well as latency and throughput issues, and make data management even more complicated. On the other hand, sensitive learning data transmitted in the network are vulnerable to various security risks, including data privacy and integrity violations. These security challenges are augmented by the resource-constrained nature of IoT devices such as limited energy, restricted memory, and low processing capabilities, making it difficult to apply the traditional security mechanisms in an IoT environment. The implementation of complex security methods can exhaust the energy of the objects and degrade the efficiency of e-learning applications that require real-time communication and instant data sharing [7]. Several studies have proposed various authentication schemes to overcome the security issues in IoT using a centralized authentication mechanism. However, these approaches suffer from critical drawbacks including a single point of failure, low scalability, and high computation and communication overheads, preventing them from being successful solutions for distributed e-learning systems [8].

In this paper, we address security and efficiency issues in current traditional centralized authentication systems. To this end, we propose an energy-efficient secure architecture that provides lightweight authentication, identity verification, and end-to-end protection of students' learning records in educational environments. This approach would help students to transfer their learning records from one institution to another in a secure and authenticated manner. The security model is based on blockchain technology and can be integrated into IoT-based learning systems with limited computations, lower energy, and minimum memory requirements to provide real-time protection of the collected data.

1.1 Motivation

Different technologies and methods have been proposed to improve the security and efficiency of e-learning systems. The rapid increase in the use of IoT devices in the field of education could offer greater flexibility and convenience for learners than conventional devices. However, such e-learning data often includes important and sensitive information that should not be accessed by unauthorized parties. Furthermore, the volume of data and the diversity of connected resource-constrained IoT devices in the e-learning field have resulted in increased security and data latency issues. However, methods of verifying the authentication of e-learning data and users belonging to different educational institutions and enabling the ease of movement among them are less well researched. Most existing approaches consider centralized authentication of connected network devices. The challenges for secure IoT-based learning systems arise from the centralized IoT architecture that requires IoT devices to be authenticated through a single server or some trusted third parties. It is very difficult to rely on centralized authentication systems, as educational parties have no control over the data collected and shared during centralized authentication, and they have no guarantee that the centralized service provider follows certain security measures [9]. Therefore, distributed security approaches for identity management and secure authentication between e-learning parties are essential.

Some schemes have developed authentication solutions based on the blockchain technology. However, these schemes are not designed to handle real-time authentication requests of different e-learning systems. Existing decentralized authentication schemes suffer from challenges related to efficiency, higher energy consumption, and limited connectivity, as IoT nodes are unable to communicate with systems belonging to different education institutions. These issues have led to the conclusion that existing blockchain frameworks need to be modified before they can be used in new computing environments [10]. Therefore, there is a need for a mechanism that efficiently applies blockchain technology in the e-learning domain. In addition, the need for delay-sensitive and energy-efficient authentication and authorization mechanisms is becoming more imperative for systems that use resource-constrained and heterogeneous devices such as the IoT [11]. Thus, in this work, an innovative decentralized blockchain-based authentication model is implemented for e-learning and educational environments. The model effectively solves the existing problems and provides a reliable and energy-efficient mechanism to protect the IoT-based e-learning users.

1.2 Major Contributions

The main contributions of this paper are as follows:

- We propose a decentralized authentication architecture using blockchain technology to create a secure learning network by allowing learners and educational institutions to ensure an authenticated and authorized access to the protected learning records.

- The proposed architecture improves the authentication efficiency by applying a lightweight authentication method that enables verified student IoT devices and intercommunication in the university network to securely transmit and share the learning data.
- We test the proposed architecture and analyze it in terms of performance and security. The results and comparisons show that the architecture can significantly increase throughput, improve efficiency, and response time. It can also reduce devices and network overheads and minimize power consumption. The results also demonstrate the robustness of the architecture against well-known attacks and its ability to meet security requirements of learning records in the university network.

1.3 Paper Structure

The rest of this paper is organized as follows. Section 2 presents a case study and provides an overview of the background. Related work is presented in Section 3. We explain the proposed architecture in Section 4. Section 5 discusses the evaluation and simulation results. Section 6 concludes the paper with some future perspectives.

2 Overview

In this section, we provide a use case that describes the decentralized blockchain architecture of a university network used in the proposed work, followed by an overview of the blockchain technology.

2.1 Use Case Study

We consider the university scenario as a case study due to its importance in IoT-based smart education systems. In the given scenario, a group of users (students, instructors, administration and other staff members) in the university communicate with each other, such that each user is managed by a university management station (*MS*), respectively.

Most of the common authentication systems are centralized; therefore, it is difficult to authenticate the new users who are not part of the university network. The proposed approach exploits the decentralized blockchain designed to run IoT devices with limited processing power, storage space, and battery life. This makes it possible for an institution to verify and authenticate the learning records and credentials when a student attends or undertakes courses in various affiliated universities and colleges, or when an instructor teaches courses at multiple institutions.

In the proposed architecture, each university is part of the education network that includes information about students, instructors, staff, and students' learning records. Also, each university has an *MS* unit to manage its users and can securely communicate with all other affiliated universities over the distributed network. Fig. 1 shows the general architecture of the blockchain-based decentralized communication between the *MS* units in the affiliated university network. With this architecture, learners can join multiple universities represented in the communication links, for example, the transmission of learners between U-1 and U-2 universities, the process is managed by the *MS* units in both universities. Thus, the authenticated learners can easily move through their distributed identity without having to undergo repetitive authentication on their devices at other universities. Specifically, if a device is currently registered and approved by the *MS* unit in one of the universities, the node will also be trusted in other universities in the network and can easily communicate with all other nodes. In addition, students' learning data, record of examination results, and information about work done in labs and learning projects can be transparently transmitted from user devices to be propagated within the blockchain network.

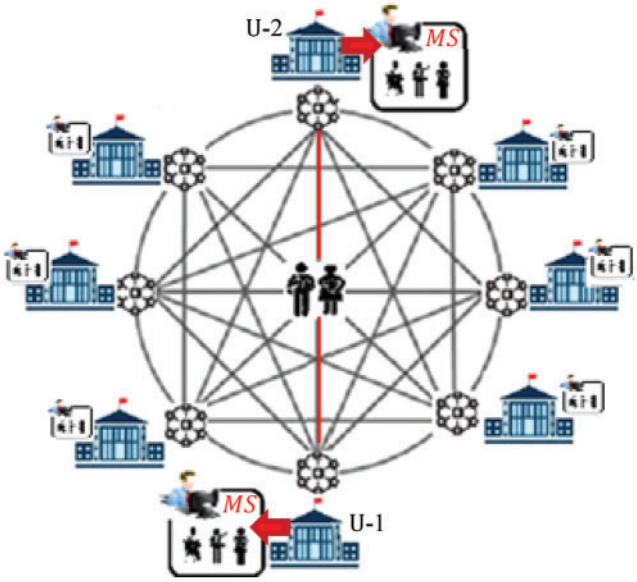

Figure 1: Architecture of blockchain-based university network

The proposed approach can help to break down the structural barriers of institutions, and allow the records and the learning history of students to be maintained across different institutions. This makes it possible to trace the academic records securely, and fraudulent, fake or illegal transactions can be detected more quickly. It can also significantly reduce the time required to authenticate users and devices, speeding up the process of verifying academic records and certificates without contacting or waiting for the responses from the other institutions.

2.2 Blockchain Technology

Blockchain technology provides new ways of designing a decentralized system architecture. Blockchain is intended to improve security and trust between users where the transaction data can be shared across an unsecured network of participants without the mediation of centralized third parties [12]. Blockchain was originally developed by Satoshi Nakamoto in 2008 [13] as a peer-to-peer money exchange technique via a digital cryptocurrency known as Bitcoin. Since then, a great deal of research has been devoted to developing blockchain, as it offers reliability, fault tolerance, privacy, and scalability, and can also be implemented in various fields [14]. Blockchain is a distributed technology comprising a series of blocks that contain transaction records of assets in a peer-to-peer network. Every node of a blockchain network contains a complete copy of all transactions executed within the network [15]. Fig. 2 shows the basic structure of a blockchain. Every block is connected to the next block in the blockchain using its hash to a hash-supported chain (i.e., block N is fed by the N-1 block hash). The first block is called the genesis block as it does not have a parent block. Generally, a block consists of two parts. The first part is called the block header and encapsulates header information such as the block version, the hash values of the current and previous blocks, transaction timestamp, Merkle tree root (which identifies the hash value of all transactions in the block), and a 4-byte nonce value [16]. The second part is called the block body. It consists of a transaction counter and a list of executed and validated transactions (depending on the block size and the volume of each transaction)

[17]. Transactions are grouped together and sent to the blockchain in a block format where all blocks are linked in a sequential order to form an organized chain structure [8].

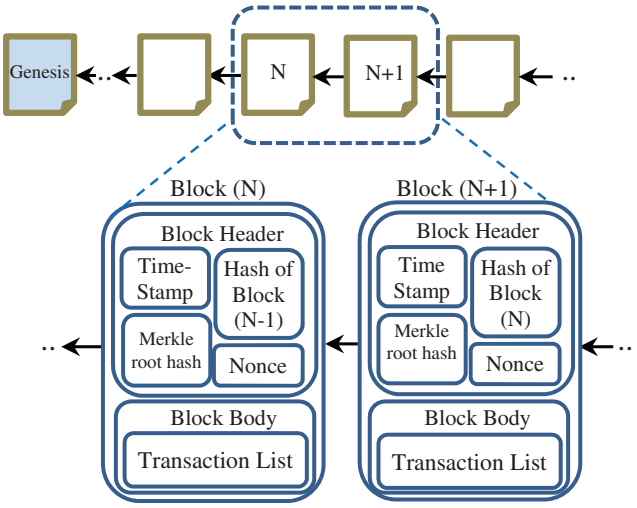

Figure 2: Basic structure of blockchain

Blockchain uses cryptographic algorithms to verify the authentication and the validity of transactions and blocks. When a new block is generated, it is distributed to all other nodes in the network. Then, each node checks the validity of the block. If it is legitimate, it adds the block information to its own blockchain [18]. Once a block is added to the blockchain network, it becomes immutable and cannot thus be tampered with. If a malicious user attempts to make any changes to the transactions in a block, the corresponding changes must be made to all subsequent blocks that are linked through hashes [19]. A blockchain relies on a consensus method that is maintained by all network nodes to determine the shared state between the nodes. If one of the nodes fails, the remaining nodes in the network can continue to function normally. As blockchain is a kind of trustless system that does not depend on any regulations or rules, this makes it the ideal solution to overcome the shortcomings in the traditional centralized third-party authentication, which are often vulnerable to malicious attacks and hence, are untrustworthy [20]. Blockchain-based development has evolved over three stages. Blockchain 1.0 is the first stage and was developed for cryptocurrencies. The second stage is Blockchain 2.0 which was designed for smart contracts that meet specific conditions before being registered on the blockchain. Blockchain 3.0 is the current stage and is designed for applications in different fields [21].

3 Related Work

Due to the distributed and decentralized characteristics of blockchain and its ability to fit with the IoT, it has been applied in a range of non-financial sectors such as health [22], industry [23], and agriculture [24]. Blockchain-based authentication is a hot topic in current research, with many research studies establishing the connection between IoT and blockchain to achieve authentication and management of devices as can be seen in [14,19,25], respectively.

In the education sector, many applications have been developed to harness the potential benefits of blockchain, as per the work done in [26,27]. However, studies have also shown that blockchain implementation in education is still immature and is mostly used to share academic certificates or validate learners' grades [28]. The University of Nicosia was the first educational institution to use

blockchain-based architecture to manage educational records received from the Massive Open Online Courses (MOOC) education platform [29]. The Massachusetts Institute of Technology [30] developed an online learning platform based on blockchain technology. Sony Global Education also developed a blockchain-based system for the open sharing of records and the academic proficiency [31]. In [32], the authors introduced a blockchain framework to maintain and control access to lifelong learning records of students, using smart contracts. In another study [33], the authors presented a blockchain-based learning analytics scheme to maintain learning records using the Ethereum blockchain platform. In a study conducted in [34], an automated system was proposed using the Hyperledger blockchain to share students' academic records when requested by other institutions, and to provide security against academic frauds. The authors in [35] presented a blockchain-based framework that easily verifies the academic records of the education stakeholders without having to go through the entire tedious process of document verification each time. Other work done in [36] introduces a student status management system using blockchain. In this system, the model is designed to organize the processes of administration and learning sessions and affiliation, where the data is loaded to a blockchain running on nodes to preserve its privacy and security. A study conducted in [37] investigated the benefits of integrating IoT and blockchain into education systems to enable efficient interaction between students, teachers, employers, and recruiters. The effectiveness of combining intelligent techniques such as machine learning with blockchain in education has been studied in [38], where predictions of errors can be obtained beforehand to securely store actual results. Table 1 summarizes the blockchain-based authentication schemes in e-learning in education field.

Nevertheless, in the education sector, current blockchain-based systems still face several challenges. For instance, verifying the authenticity of certification issuers and who they claim to be, and confirming that the certificates and the educational records belong to the students who are seeking them, are key issues [18]. Furthermore, preserving the privacy of blockchain transactions due to the public key data being publicly visible is another major issue, where the user's transactions can be linked to reveal their information [39]. The slow speed of blockchain transaction processing is also a major challenge that education systems face. This is because the size of the blocks increases as the transactions continue and the size of records grows, especially when IoT devices are integrated to reduce the capacity constraints [27].

Table 1: Summery of blockchain-based authentication schemes in e-learning and education field

Scheme	Main usage	Authentication mechanism	Advantages	Disadvantages
Khalid et al. [14]	Multiple fields	Public blockchan, smart contracts, and public key encryption.	Improve authentication time, and scalability. Plus, reduction in power consumption.	Security issues as devices are managed by centralized edge servers connected to the blockchain with high transmission latency.

(Continued)

Table 1: Continued

Scheme	Main usage	Authentication mechanism	Advantages	Disadvantages
Chen et al. [28]	Education field	Private blockchain and smart contracts.	Secure sharing and storage of educational records and intellectual work.	High computation complexity and blockchain consensus overhead.
Ocheja et al. [32]	Educational institutions	Blockchain, smart contracts, hash and public key encryption.	Improve privacy and security of learning records.	Low performance and long authentication delay.
Ocheja et al. [33]	Educational institutions	Blockchain based using Ethereum and smart contracts.	Improve the security and privacy of learning data, and strong control over access of private learning data by the user.	Not suitable for real-time access based systems due to high computational complexity.
Badr et al. [34]	Academic institutions	Hyperledger private blockchain.	Enhance the automation, integrity, and validation of academic records.	High overhead and high rejection of system requests.
Shah et al. [38]	Education field	Blockchain and machine learning	Enhance data persistence and learning records security.	Suffer from high computational power, poor performance, and limited data sharing.
Guo et al. [40]	Online education	Blockchain and smart contracts.	Enhance the management and sharing of multimedia educational resources and improve the protection of multimedia digital rights.	High computation requirements and power consumption make the scheme inefficient for devices with limited resources.

(Continued)

Table 1: Continued

Scheme	Main usage	Authentication mechanism	Advantages	Disadvantages
Shaikh et al. [41]	Academic institutions	Blockchain and hash function.	Improve security, integrity, and verification of academic credentials and certificates.	Complex authentication, and transparency limitations.

4 Proposed Architecture

In this section, we explain the architecture of the proposed decentralized blockchain-based authentication system for an affiliated university network. We also discuss the workflow architecture, encryption of learning transactions, and the user authentication process. Table 2 lists the symbols and their definitions used in the paper.

Table 2: Symbols and their definitions used in this work

Symbol	Definition
$Bchn$	Blockchain university network
U_k	Affiliated university k
MS_k	Management station in university k
S	Student
I	Instructor
St	Staff member
B	Learning block
$Trns_n$	Transaction n
Pk	Public key
Ptk	Private key
Sk	Symmetric key
ID_i	Identifier of user i
C	Ciphertext
Bv	Block version
mB	Mined block
$PreBH$	Previous block hash
Ts	Time stamp
MkH	Merkle tree root hash value
HB	Hashed block header
Df	Mining difficulty
Pl	Block payload (array of block transactions)

4.1 Blockchain-Based Affiliated University Network

In the proposed architecture, each university belongs to a network of affiliated universities and colleges comprising students, instructors, and administrative staff. Each university can communicate with others in the network in a secure and authenticated manner using the blockchains, thus providing an integrated education system.

An *MS* unit is defined in each university, where the university staff manages the learning transactions and monitors the network behavior at runtime. Fig. 3 shows an overview of user interactions at each university in the blockchain network. In this proposed architecture, we assume that all user devices are resource constrained in terms of power, memory, and computational capabilities required to communicate with the blockchain. User devices that are not registered or verified by the blockchain cannot be authenticated and therefore are not allowed to communicate with legitimate devices either in the same university or outside. This procedure reduces the possibility of a malicious device interacting with legitimate devices. The authorized university personnel can verify the learning records of students from any affiliated university in the blockchain and get public access to all records across the network. For example, the students can undertake courses, and the instructors can apply to teach courses at other affiliated universities within the network via the blockchain because their academic information is available to all relevant university personnel regardless of their location. Also, the system enables institutions to issue certificates to graduating students on the blockchain and allows other academic institutions or employment organizations to verify the authenticity and the integrity of these certificates. To validate the transactions and verify the execution of the operations, records are created for these transactions. The learning transaction records are then shared across the blockchain network to provide authentication and authorization to users and their registered devices in a distributed manner.

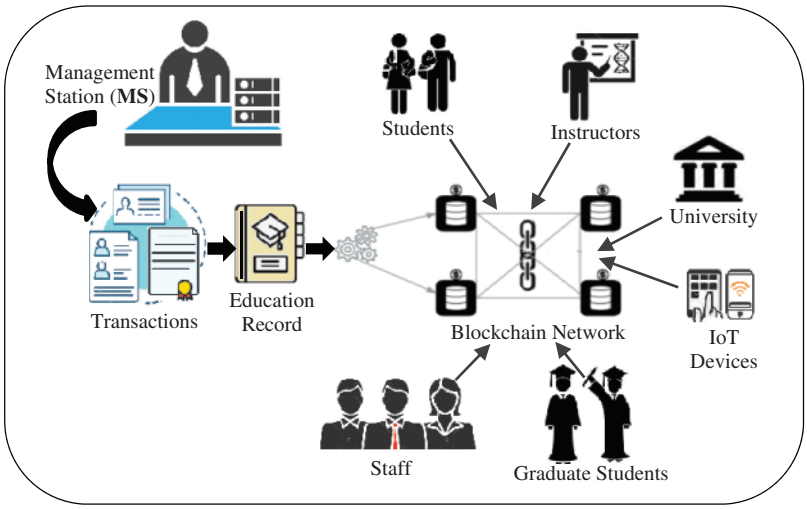

Figure 3: Overview of user interactions at each university within the blockchain network

4.2 Workflow Structure

The proposed solution consists of two main phases: the user registration phase, and the authentication and execution phase. In the registration phase, the education institutions, and their users' devices are registered. This allows the systems of affiliated universities to register in the network

and ensures that all its users and their smart devices can be uniquely identified. Next, the phase consists of authenticating users and devices and executing operations, so that the users' devices are authenticated through the decentralized blockchain network. When authentication conditions are met, the authorized users and devices belonging to different university systems can communicate with each other and share important learning information.

4.2.1 Registration Phase

In this phase, the users and devices of each university are registered within the blockchain network (*Bchn*) by the management station (*MS*) which acts as the university's validator. To register a user i who can be a student S_i, an instructor I_i, or a staff member St_i in the university U_k, the following steps are performed.

1. The user's device sends a registration request to MS_k to join the university $U_k \cdot MS_k$ responds by generating a key pair (public key (*Pk*) and private key (*Ptk*)) for the user who sent the request.
2. MS_k then generates a unique identifier *ID* to be used for identifying the user's device on the blockchain network. The user's ID_i is uniquely generated by MS_k for that user and is stored on his/her device.
3. Next, a symmetric key *Sk* is computed for each user registered in the system based on the unique information of a user using the hash of user's *ID*, and the media access control (MAC) address of the user's device. This *Sk* encrypts all user learning data using a lightweight symmetric encryption algorithm.
4. Each user is then given a key pair, a symmetric key, and a unique identifier, which are securely distributed to the corresponding device for use only by that user.

Thus, *MS* begins to register users on the blockchain-based university network. In this approach, a public or private blockchain can be used to connect the university network. This allows each affiliated university to securely transmit and store learning information in records using the users' keys. Moreover, this reduces the computational load and authentication time by allowing affiliated university users to directly read or record academic information. The process of registering a student, an instructor, or a staff at an affiliated university is set out in Algorithm 1.

Algorithm 1: User registration in the affiliated university

1. **Input** U, S, I, St
2. **Output** Pk_i, Ptk_i, ID_i, Sk_i
3. **Begin**
4. **for** $\forall\ U \in Bchn$ **do**
5. **for** *each* $S,\ I,\ St \in U_k$ **do**
6. *Generate* Pk_i, Ptk_i, ID_i
7. *Compute* $Sk_i = SHA\ (ID_i + MAC$ for device of user $i)$
8. *Add user* $ID_i = (S, I, St) \rightarrow Bchn$
9. *Send* $Pk_i, Ptk_i, ID_i, Sk_i \rightarrow$ User $i \in U_k$
10. **end for**
11. **end for**
12. **End**

4.2.2 Authentication and Execution Phase

After the registration phase, the authentication phase is performed for the users' devices before any operation is carried out such as transfer of learning transactions, sharing of educational records, or when a student or instructor joins (solely or in part) to another affiliated university to undertake or teach courses. When a request is received from a student or an instructor to join a university U_k that is managed by the MS_k, the registration procedure is called, and the user securely receives the public and private key pair. Upon successful registration, when the user wants to send the learning transactions to the blockchain, the legitimacy of the device and the received transaction packets are verified using the following authentication steps:

1. MS_k checks the legitimacy of user i and verifies the identification of ID_i in the blockchain. If the user's device is authenticated and the ID_i is identified, the user i is allowed to send the learning transactions (*Trns*).
2. If the user device with ID_i is not verified by the blockchain, the transaction will not be approved, and the process will automatically be terminated with an error.
3. After the correct authentication of the user device, the device encrypts the learning transaction using the symmetric encryption key Sk_i.
4. The received user's public key Pk_i from MS_k, it is then used to encrypt the symmetric key Sk_i and attach it encrypted with the transmitted learning transaction.
5. When MS_k receives the academic transaction, it verifies the authenticity of the transaction by checking if the public key Pk_i used for encrypting the symmetric key Sk_i is registered with the blockchain. It must be the same public key that was previously distributed by MS_k to users. Here, the MS_k applies the user's Ptk_i to decrypt Sk_i which is stored in an encrypted format with the transmitted transaction. If MS_k succeeds in retrieving the Sk_i, it compares the key with the one stored at MS_k, and verifies its ability to decrypt the ciphered transaction. If the keys are the same and the transaction is successfully decrypted, it can be confirmed that the transaction is associated with a legitimate user and has not been altered during transmission. Otherwise, the transaction is not legitimate and hence, will not be processed.
6. After the authentications are confirmed, the MS_k allows the learning transaction to be recorded in a block. This block is then distributed and the educational ledger is updated in the blockchain network.

Algorithm 2 shows the sequence of operations used to authenticate a student's device or a transaction in the blockchain. When a student wishes to transfer to study at another affiliated university, or when an instructor would like to teach courses at another university, there are two types of transfer. The first is the complete migration of the student or the instructor to the new university. The second is a partial enrolment if the student wants to undertake a course at another university, or if the instructor chooses to teach courses at other affiliated universities in addition to instrucor's work at the current university.

Algorithm 2: Device and transaction authentication by *MS* unit

1. **Input** ID_i, *Trns*
2. **Output** C_{Trns}, C_{Sk_i}, *Bchn_ledger(B)*
3. **Begin**
4. **if** ($S||I||St$ *Call Join_Uni* (U_k)) **then**

(Continued)

Algorithm 2: Continued

```
5.      Request (ID)
6.      if (S||I||St ∈ U_k_UserList) then
7.           user_auth = 1
8.      else
9.          user_auth = 0
10.     end if
11.   end if
12.   while (S||I||St Call_SendTrans (Trns)) do
13.     if (auth = 1) do
14.       C_Trns ← Encrypt (Trns, Sk_i) //encrypting Trns using user's Sk
15.       C_Ski ← Encrypt (Sk_i, Pk_i) //encrypting Sk using user's Pk
16.     else
17.        Terminate_trans (Trns)
18.     end if
19.     Send (C_Trns, C_Ski)
20.   end while
21.   //Verifying transactions authenticity by MS
22.   for ∀ Trns_i ∈ MS_k_Trans do
23.     Sk_i ← Decrypt (C_Ski, Ptk_i) //decrypting C_Ski using user's Ptk
24.     if (Decrypt (C_Trns, Sk_i) == true) then
25.       trans_auth = 1
26.       B ← Add (Trns_i) // adding Trns to block
27.       Update (Bchn_ledger) // updating blockchain educational ledger
28.     else
29.       trans_auth = 0
30.     end if
31.   end for
32. End
```

Algorithm 3: Transfer of students and instructor between the universities

```
1. Input ID_i, transfer_type
2. OutputConfirmTransfer
3. Begin
4.   S_i/I_i Call Join_Uni (U_Target)
5.   S_i/I_i Send (ID_i, transfer_type)
6.   if (user_auth == 1) then
7.     if (transfer_type == 1) then //complete transfer
8.       U_Current(Send (Pk_i, Ptk_i)) → U_Target
9.       U_Target (Decrypt (C_Ski, Ptk_i) → Sk_i)
10.      U_Target → Generate (Pk_i_New, Ptk_i_New)
11.      U_Target (Send (Pk_i_New, Ptk_i_New) → S_i||I_i)
12.      U_Target Encrypt (Sk_i, Pk_i_New)
```

(Continued)

Algorithm 3: Continued

```
13.       else // partial transfer
14.          U_Current (Send (Pk_i, Ptk_i)) → U_Target
15.       end if
16.    end if
17. End
```

In the complete migration scenario, if student S_1 or instructor I_1 wants to move from university U_A to the affiliated university U_B managed by MS_B, S_1 sends a join request to MS_B. In this case, MS_B communicates with MS_A to take the key pair (Pk_1, Ptk_1) of S_1 without the need to re-authenticate S_1 in the blockchain. Next, MS_B decrypts the ciphered Sk_1 which was used to encrypt the learning transactions of S_1. MS_B then generates a new key pair (Pk_{1b}, Ptk_{1b}) for S_1 in order to re-encrypt the Sk_1. Student's new key pair is shared only with the target MS, and since there is a possibility that the key pair may be compromised during transmission, it needs to be protected by the encryption. After the MS_B conducts the cryptographic operations, it updates the learning block of S_1 on the blockchain. The same scenario is implemented when the I_1 migrates to another university. If S_1 wants to study course(s) at another affiliated university say U_C in addition to his/her current study at U_A, then MS_C communicates with MS_A to take the student's key pair without re-authentication of S_1 in the blockchain. The same key pair is used by both U_A and U_C without the need to generate new keys by U_C. Since both universities have the same key pair, they have the ability to decrypt Sk_1 in order to access the encrypted student's academic record and thus, both will be able to read and write the information. The same scenario applies when an instructor joins multiple universities in order to teach courses. The complete or partial transfer of students or instructors between universities is described in Algorithm 3. Fig. 4 shows the entire workflow of the proposed architecture.

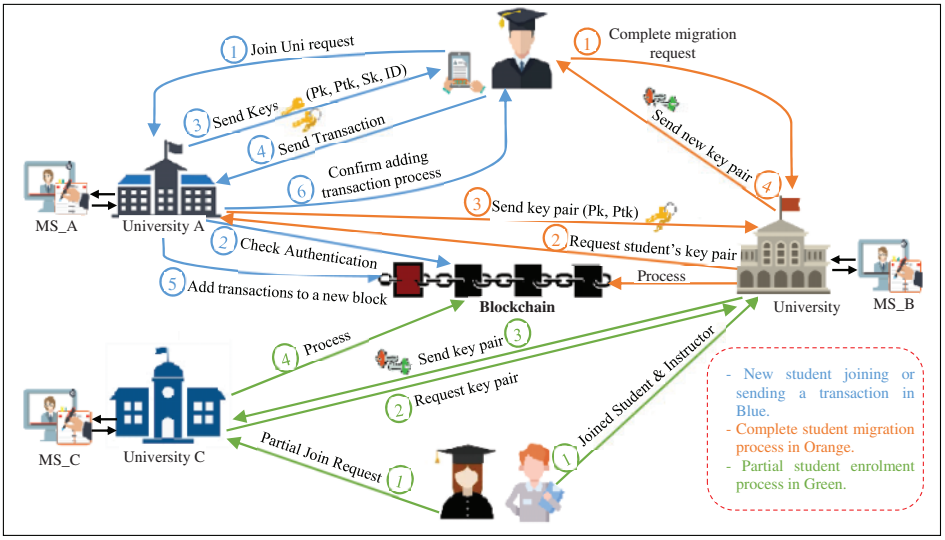

Figure 4: Structure of the proposed mechanism

Thus, through the proposed blockchain architecture, students' learning information can be securley communicated and shared among the affiliated universities in the network with minimum authentication delay and communication overhead. Moreover, students and instructors can easily

migrate and move from one affiliated university to other geographically distant universities that belong to the same network.

4.3 Blockchain and Cryptographic Operations

The proposed solution implements a hybrid mechanism using lightweight symmetric and asymmetric cryptographic algorithms. In the symmetric encryption, the corrected block tiny encryption algorithm (XXTEA) [42] is used to encrypt the learning transactions. In contrast, elliptic curve cryptography (ECC) [43] is used as an asymmetric cipher to encrypt the symmetric key Sk. These encryption algorithms were selected based on comparing several ciphers presented in [44]. The processing speed of these algorithms is faster than the most popular ciphers such as the Advance Encryption Standard (AES) and the Rivest–Shamir–Adleman (RSA) encryption algorithms [45]. They require less power while being able to provide a reasonable level of security, making them suitable for implementation in resource-constrained IoT devices [5]. The XXTEA is a lightweight encryption algorithm that operates on blocks of multiple 32-bit words, using a 128-bit key length. Its internal structure consists of shift, XOR, and addition operations. In XXTEA, a single full cycle consists of the loop of block words, the number of full cycles, the round function (which includes both the direct neighbors of each word in the block), and the key. Each full cycle contains n rounds, where n equals the number of block words. In each block, the number of full cycles can be calculated as $6 + 52/n$ [46]. After the encryption is completed, the generated ciphertext can be the same size as the original text. Moreover, changing a single bit in XXTEA will result in a change in half of the block bits. When a new learning transaction is issued by a user device, the MS unit validates the transaction data so that valid transactions are collected in a pool of transactions. Then, it calculates the hash value and nonce value, and performs the mining process named Proof of Work (PoW) to consider adding transactions to the latest block in the blockchain network. After the block is distributed through the affiliated university network, the PoW process is performed by MS units to ensure that there was no additional data when all block headers were stored and verified during the chain validity process. Algorithm 4 sets out the steps of the mining process done by the MS unit, while Algorithm 5 describes the proofing steps for mined blocks by MS units in the affiliated university network.

Algorithm 4: Mining process by the MS unit

1. **Input** Bv, $PrBH$, Ts, Df, $Trns\_pool$ [$Trns_1, \ldots,$ $Trns_n$]
2. **Output** $Nonce$
3. **Begin**
4. $val \leftarrow GenerateRandom\ (\ ) \in [1,\ n]$
5. $MkH \leftarrow Calculate\ (\ )$
6. $HB \leftarrow Creat\_HashBlockHeader\ (B)$
7. **if** ($B\_info = Bv$ and $PrBH ==$ TRUE) **then**
8. $Nonce = 0$
9. $Compute\ (Hash\ (mining\_result)) \rightarrow out$
10. **while** (NOT PoW) do
12. $Nonce++$
13. **if** ($Df = 1$ and get_PoW == FALSE) **then**
14. return ($Nonce - 1$, out)
15. **else**
16. return 0

(Continued)

Algorithm 4: Continued

17. **enf if**
18. **end while**
19. **enf if**
20. **End**

Algorithm 5: Proofing of mined block by *MS* unit

1. **Input** mB, Pl
2. **Output** Verify *out* is correct $\rightarrow$ *verified*
3. **Begin**
4. $Calculate\ (\ ) \rightarrow MkH$
5. $Extract\ (HB) \rightarrow Nonce$
6. $Compute\ (out) \rightarrow out_{veri}$
7. **if** $(out_{veri} = out)$ **then**
8. return (*verified* == TRUE)
9. **else**
10. return (*verified* == FALSE)
11. **end if**
12. **End**

5 Performance and Security Evaluation

In this section, we first evaluate the performance of the proposed mechanism in terms of execution time, throughput, and power consumption. We then analyze the security and authentication strength of the proposed mechanism. We conduct simulation experiments using the network simulator NS-2 [47] on the Linux platform. The NS-2 is an open-source simulation tool widely used in research to simulate various network scenarios. The proposed mechanism uses Ganache Cli [48] to validate transactions. It can simulate the interactions of Ethereum in a way that is close to the real Ethereum blockchain, which is a well-known decentralized blockchain platform, and without the high costs of operating a real Ethereum. The testing machine has an Intel Core i3-4005U CPU, 1.7 GHz, 3 MB Cache, and 4 GB memory. To simulate the proposed architecture, we use the default parameters summarized in Table 3. In the implementation, we ran the simulation for about 30 min during which 3,000 learning transactions were performed, and the average result was measured over 35 simulation runs of the proposed mechanism.

Table 3: Simulation parameters utilized in the proposed mechanism

Parameter	Value
Channel	Wireless
Radio range/Mobility type	Random
Propagation	Two-ray channel
Protocol	Mac 802.11
Speed of members	4/6/8/10 m/s

(Continued)

Table 3: Continued

Parameter	Value
Number of students/instructors/ universities/*MS*	400/200/20/20
Simulation time	900 s
Traffic type	Constant bit rate
Covered area	10 km × 10 km
Packet size	32–512 bytes
Packet length to blockchain	32 bytes
PreBH	8 bytes
Trns counter	8 bytes
B	160 bytes
HB	80 bytes

The performance results of the proposed architecture during the simulation are then compared with other authentication mechanisms that do not use distributed networks or blockchain technology. These authentication mechanisms use a third-party, cloud-based authentication discussed in [49,50] and use centralized authentication servers as presented in [51,52] that apply a certificate-based solution to establish authentication between user devices with restricted resources.

The four key factors used for the evaluation of the proposed architecture are as follows:

- Throughput: defines the total number of learning transaction requests that are processed among the affiliated universities.

- Response time: represents the elapsed time for recording or updating learning transactions between students or instructors and *MS* units in affiliated universities.

- Power consumption: calculates the consumed power by users' IoT devices to record transactions in the blockchain.

- Security and authentication analysis: evaluates the security and authentication during communication in the proposed architecture.

5.1 Performance Evaluation

In this subsection, we first compute the throughput performance to determine the total number of learning transactions that can be carried out by affiliated universities in one second using the proposed blockchain-based architecture. Then, the throughput results of the proposed mechanism are compared with the centralized-based authentication solutions that use cloud-based and certificate-based authentication as shown in Fig. 5. The results indicate that the proposed mechanism was able to achieve higher throughput: the average throughput was 3,326 Mbps compared to 2,463 Mbps and 2,288 Mbps for cloud-based and certificate-based authentication mechanisms, respectively. This is because a distributed network comprising affiliated universities is used in the proposed mechanism, rather than the centralized authentication methods, which incur computation and communication overheads for simultaneous communication requests. The authentication efficiency is correlated with the number of connected devices. When the number of authentication devices increases, it requires

multiple transfers for identification and authentication data to the centralized authorization servers to verify the identity and authenticity of users, thereby increasing the overhead incurred by the network and authentication server. This decreases the authentication efficiency and increases the response time. Fig. 6 shows the processing time required by the proposed mechanism to authenticate and respond to learning requests using various concurrent IoT devices compared to the time required by centralized cloud-based and certificate-based authentication mechanisms.

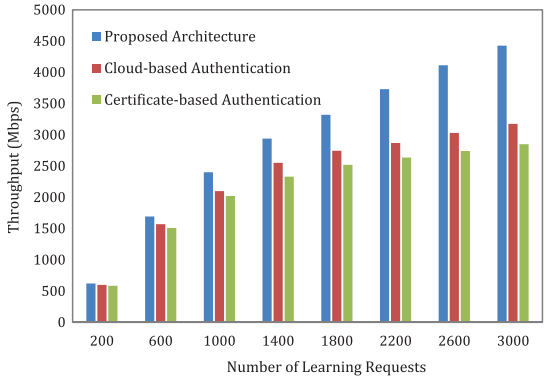

Figure 5: Comparison of throughput for processing various requests using the proposed mechanism *vs.* the centralized cloud-based and certificate-based authentication mechanisms

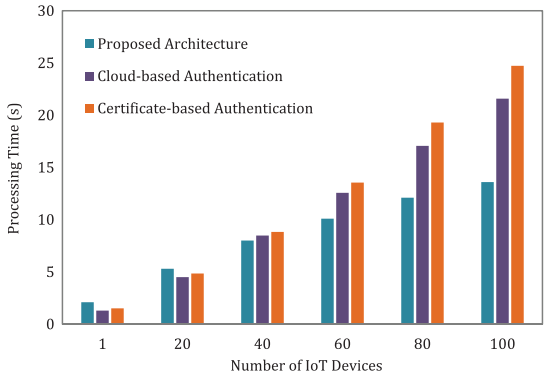

Figure 6: Comparison of processing time for a varying number of IoT devices using the proposed mechanism *vs.* the centralized cloud-based and certificate-based authentication mechanisms

The results show that the proposed decentralized authentication architecture requires a shorter response time than the centralized authentication methods when the number of connected devices is small. The response time increases rapidly when the number of devices increases. This is because the overhead of operating a distributed authentication protocol in the blockchain is greater when the network scale is small. In contrast, the authentication efficiency improves dramatically when the number of network devices increases [53].

Next, we calculate the total execution time that the proposed mechanism takes to record learning information of various sizes. This total time (Υ_t) is defined by the time taken to transmit the amount of learning data, the symmetric encryption time for the learning data, the asymmetric encryption time for encrypting the symmetric key, and the total amount of time spent by the university's MS on recording

learning data into a block as given in Eq. (1).

$$\Upsilon_t = T\,(\text{Trns}) + T(Enc\ \ (Trns)) + T\,(Enc\ \ (Sk)) + T\,(MS\ \ (Trns)) \tag{1}$$

Fig. 7 shows the average execution time that the proposed architecture takes to record learning information of different sizes ranging from 10 KB to 10 MB compared to the execution time taken by the centralized cloud-based and certificate-based authentication mechanisms. We have also calculated the power consumed by user devices when transmitting or updating learning information in the blockchain. The total power consumption (φ_P) is calculated by multiplying the time required by the users' IoT devices (in Eq. (1)) with the power consumption (H_E) associated with the devices as given in Eq. (2). Fig. 8 shows the average power consumption in megajoule (mJ) for different transactions in the proposed mechanism against the centralized cloud-based and certificate-based mechanisms. The results indicate that our mechanism can achieve 45% less power consumption compared to other mechanisms.

$$\varphi_P = T\,(\text{Trns}) \times P\,(H_E) + T(Enc\ \ (Trns)) \times P\,(H_E) + T\,(Enc\ \ (Sk)) \times P\,(H_E) + T\,(MS\ \ (Trns)) \times P\,(H_E) \tag{2}$$

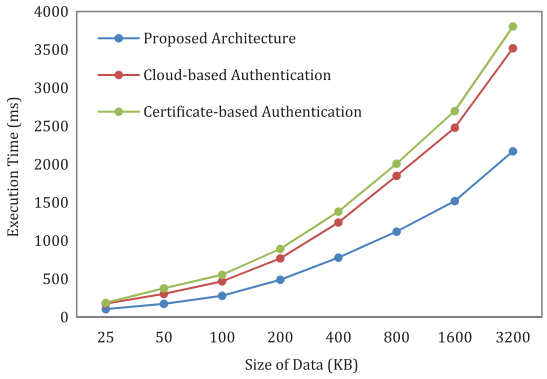

Figure 7: Comparison of execution time for recording data of varying size

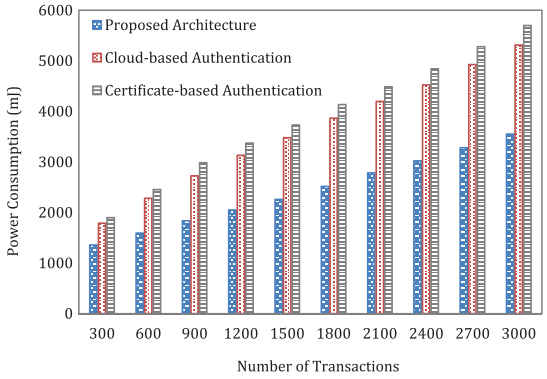

Figure 8: Comparison of power consumption in the proposed mechanism versus the cloud-based and certificate-based authentication mechanisms

In addition, the results show that the proposed mechanism performs better than others when recording data of varying sizes and processing transactions in the blockchain. It can also increase the battery life of resource-constrained IoT devices. This is because the proposed mechanism has significantly lower authentication overheads than the centralized authentication mechanisms, which require additional re-authentication procedures when a student moves to other universities or transmits new learning transactions. Additionally, using lightweight encryption algorithms, the proposed mechanism requires less time to encrypt information when a student is fully or partially enrolled at a university. The proposed scheme only requires re-encrypting the symmetric key *Sk* associated with the ciphered transactions without having to re-encrypt all transactions with the new keys of the new affiliated universities, thus taking a constant time to encrypt or decrypt the *Sk* regardless of transactions size.

5.2 Authentication Evaluation

In the proposed architecture, we focus on the authentication process during communication between users' devices in a distributed university network. In traditional authentication schemes, the repeated movements of students or instructors between universities require frequent registration and authentication processes to ensure continuous secure communication. Furthermore, since different universities apply separate protocols, these traditional methods require re-approval between the parties for the continuity of authentication, which consumes much time and effort. In the proposed architecture, students do not require repeated registration and re-authentication when moving between different universities, thereby reducing the time required for re-authentication.

The proposed architecture performs the authentication between the student IoT devices and their associated *MS*, and between the *MS* units at the communicated universities. The *MS* authenticates its connected users' devices based on the identical user IDs and the ability of *MS* to successfully decrypt the *Sk* corresponding to each device. To ensure the security of the ID and the key pair stored on the user's device from possible physical attacks, the identifiers must be stored encrypted in the device.

The network efficiency during communication is determined by the total amount of learning data that reaches the maximum processing rate at each university. Fig. 9 compares the average authentication delay time of a transmitted learning packet with the network utilization ratio between the proposed mechanism and the centralized cloud authentication mechanism. According to the results, when a network load is low, the effect of the proposed mechanism on the network is slight. However, when the learning transactions increase and student mobility between universities also increases, the network load increases but with less impact on the network efficiency with our mechanism compared to the centralized mechanism.

5.3 Security Analysis

This section presents an analysis of the security provided by the proposed mechanism. It defines an attack model that includes attacks commonly targeting blockchain-based IoT networks [54], and its ability to resist them and fulfill the security requirements for secure communication in a distributed university network.

5.3.1 Attack Model

The following defines an attack model through which an attacker can obtain important learning information for a student or instructor.

- Brute force attack: An attacker tries all possible key values on a ciphertext fragment until an intelligible plaintext translation output is obtained.

- Eavesdropping: A passive attack in which the attacker exploits an insecure communication between devices to acquire a student's confidential learning information.
- Network traffic-analysis attack: An attacker analyzes the information intercepted during communication between user devices, so that the attacker can obtain the information needed to authenticate one user device to another.
- Man-in-the-middle attack: An attacker places themself between two communicating parties (e.g., student's device and the *MS*) and impersonates a legitimate student's device by sending a response message that is acquired by impersonating the legitimate recipient.
- Collusion attack: A group of users colludes by combining their decryption keys and creating a legal key that allows access to learning data that they cannot access individually.

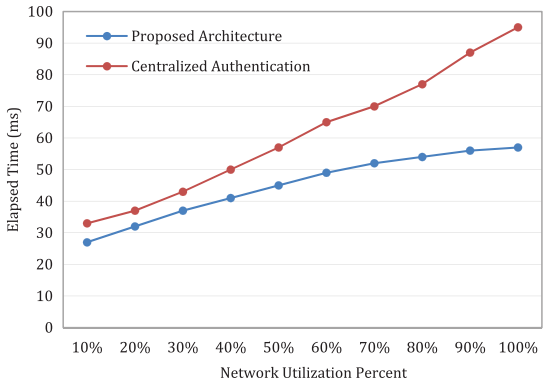

Figure 9: Comparison of authentication efficiency with network utilization in the proposed mechanism *vs.* the centralized cloud authentication

5.3.2 Resistance to Attack

Each proposed architecture must satisfy security requirements such as authentication, integrity, and availability, which are more targeted [55]. In the proposed dedicated architecture for a distributed university network, the confidentiality of learning records is protected against unauthorized users and untrusted storage. Only authorized students, instructors, or staff can access authenticated learning records. In addition, all learning data is transparently encrypted and stored in the blockchain, and it would be very difficult to retrieve plaintext without the proper keys used in the encryption. Integrity guarantees that learning transactions are delivered to the target university without being modified by an adversary during transmission. Furthermore, the integrity of the learning blocks in the blockchain is protected, and any unauthorized change to block data will be detected. Finally, the availability ensures that learning data is available to authorized parties whenever it is required.

In many cases, the attacker needs to join a university network or access the *MS* of an affiliated university using malicious attacks or a blocked or fake ID to acquire learning information, or tamper with students' academic credentials or records. In the proposed attack model, we consider the targeted attacks on a university whereby an attacker can access or modify the sensitive learning information of a student.

With the proposed work, the learning transactions are encrypted by symmetric encryption and the symmetric key *Sk* is encrypted by public key encryption. When the *MS* is required to read the learning record of a student, the private key must be obtained first to decipher the *Sk* and then decrypt the student record. Assuming that, using a brute-force attack, an attacker succeeds in obtaining the

Sk for a transaction packet that he is not authorized to access, the attacker is still unable to retrieve the *Sk* values for other users' devices using the brute-force attack as there is no means of guessing the random values of *ID*, *MAC*, and *Nonce*. The exchange of learning transactions between a student's device and *MS* starts after the device is authenticated and the identity of a student is verified. Upon authentication, the student receives the key pair (*Pk*, *Ptk*).

Consider the situation where an attacker eavesdrops on the transmitted transactions, and succeeds in obtaining the student's key pair. The attacker needs to know the values of the student *ID* and the device's MAC address in order to calculate the *Sk* and decrypt the transactions. Even if the attacker succeeds in retrieving the values of the encryption keys using a man-in-the-middle attack, the attacker is still unable to compute the high randomness blockchain parameters, such as *MkH*, *Ts*, *PreBH*, and *Nonce*, used in blockchain cryptography.

During the communication between *MS* units at affiliated universities, only the recipient *MS* can receive the student's key pair to decrypt *Sk* and then the learning record. Other universities that do not have the proper *Ptk* key will not be able to decrypt the student learning record. As the mechanism discloses cryptographic keys only to the trusted universities of authenticated users, non-affiliated universities, and unauthorized users cannot obtain them. Moreover, since the user's *ID* is associated with the generated cryptographic keys, it is useless to attempt to create transactions using different keys. In addition, illegal users or unaffiliated universities are unable to obtain encryption keys using collusion activities. Thus, the proposed mechanism is collusion resistant.

According to the evaluation conducted in this section, we conclude that our proposed architecture can provide robust protection against attacks such as the brute-force, eavesdropping, man-in-the-middle, and collusion attacks considered in the presented attack model. In addition, the proposed architecture can achieve the desired security requirements of authentication, integrity, and availability with superior levels of efficiency and less power consumption. The proposed distributed architecture does not require much time for the authentication process, unlike the centralized authentication systems which require multiple repetitions of the authentication process. Moreover, the proposed work does not significantly increase the communication overhead and has less negative impact on the network efficiency.

6 Conclusion and Future Work

Securing learning data, and authenticating learners and their resource-constrained IoT devices have become an important concern, especially for e-learning systems. Universities use different protocols to identify and authenticate students in distance learning settings, which makes the interaction and migration of students or instructors between universities a difficult process that requires frequent registration and re-authentication procedures to ensure continuous secure communication. Centralized authentication methods are unable to achieve wholly secure and efficient communication in a distributed network. In this paper, we proposed a security architecture that provides a decentralized device authentication method and guarantees the security of learning records in a geographically distributed university network. The proposed architecture is based on blockchain technology. It considers the resource limitations of IoT devices, thereby allowing devices to securely communicate and exchange sensitive learning data, and ensure secure communication between different affiliated universities. It also enables students and instructors to easily migrate and join multiple universities in the network using their already-established identity, without the need for user re-authentication. The proposed work improves authentication efficiency by implementing hybrid lightweight encryption

algorithms and hash functions to facilitate the learners' IoT devices to securely transmit and share learning data whithin the learning enviroments.

The efficiency of the proposed architecture was evaluated, and the results demonstrated its ability to effectively increase throughput of learning requests by about 40% of the centralized authentication mechanisms. It can also significantly reduce the communication overhead and response time by about 26% while increasing the number of users' IoT devices. In addition, the authentication efficiency is improved by about 27%, while the power consumption of IoT devices is reduced by about 35% compared to cloud-based authentication. The security analysis shows the ability of the proposed architecture to resist well-known attacks, such as brute-force, eavesdropping, man-in-the-middle, and collusion attacks, which mainly affect the security requirements of learning data.

Although the proposed scheme can achieve efficient authentication over the distributed universities, one main limitation is that the e-learning data can only be shared by affiliated universities in the network, and the user cannot share learning data directly with another user, which must be done through the associated MS units. In future research, we intend to solve this limitation and extend the proposed architecture for application in other IoT scenarios. Moreover, we plan to explore the possibility of enhancing its security and performance of the architecture using artificial intelligence techniques.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] T. Y. Lam and B. Dongol, "A blockchain-enabled e-learning platform," *Interactive Learning Environments*, vol. 30, no. 7, pp. 1229–1251, 2022.

[2] R. Setiawan, M. M. Devadass, R. Rajan, D. K. Sharma, N. P. Singh *et al.,* "IoT based virtual E-learning system for sustainable development of smart cities," *Journal of Grid Computing*, vol. 20, no. 3, pp. 1–30, 2022.

[3] C. I. Silvestru, A. C. Firulescu, D. G. Iordoc, V. C. Icociu, M. A. Stoica *et al.,* "Smart academic and professional education," *Sustainability*, vol. 14, no. 11, pp. 6408, 2022.

[4] R. Raimundo and A. Rosário, "Blockchain system in the higher education," *European Journal of Investigation in Health, Psychology and Education*, vol. 11, no. 1, pp. 276–293, 2021.

[5] M. Wang, Y. Lin, Q. Tian and G. Si, "Transfer learning promotes 6G wireless communications: Recent advances and future challenges," *IEEE Transactions on Reliability*, vol. 70, no. 2, pp. 790–807, 2021.

[6] E. Fazeldehkordi and T. M. Grønli, "A survey of security architectures for edge computing-based IoT," *IoT*, vol. 3, no. 3, pp. 332–365, 2022.

[7] S. Medileh, A. Laouid, R. Euler, A. Bounceur, M. Hammoudeh *et al.,* "A flexible encryption technique for the internet of things environment," *Ad Hoc Networks*, vol. 106, pp. 102240, 2020.

[8] A. Rashid and A. Masood, "Zone of trust: Blockchain assisted IoT authentication to support cross-communication between bubbles of trusted IoTs," *Cluster Computing*, pp. 1–18, 2022.

[9] O. A. Khashan, "Parallel proxy re-encryption workload distribution for efficient big data sharing in cloud computing," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conf. (CCWC)*, Nevada, USA, pp. 0554–0559, 2021.

[10] R. Ch, D. J. Kumari, T. R. Gadekallu and C. Iwendi, "Distributed-ledger-based blockchain technology for reliable electronic voting system with statistical analysis," *Electronics*, vol. 11, no. 20, pp. 3308, 2022.

[11] A. Khashan, R. Ahmad and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Networks*, vol. 115, pp. 102448, 2021.
[12] A. K. Yadav, A. Pandey and S. Singh, "Significance and impact of blockchain technology in education system," in *Advances in Mechanical Engineering*, Singapore: Springer, pp. 597–605, 2021.
[13] S. Nakamoto and A. Bitcoin, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, pp. 21260, 2008.
[14] U. Khalid, M. Asim, T. Baker, P. C. Hung, M. A. Tariq *et al.,* "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Computing*, vol. 23, no. 3, pp. 2067–2087, 2020
[15] R. Fotohi and F. S. Aliee, "Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT," *Computer Networks*, vol. 97, pp. 108331, 2021.
[16] K. Kumutha and S. Jayalakshmi, "Blockchain technology and academic certificate authenticity—A review," *Expert Clouds and Applications*, vol. 209, pp. 321–334, 2022
[17] R. Himanshu, "An overview of blockchain technology: Architecture and consensus protocols," *Smart City Infrastructure: The Blockchain Perspective*, pp. 293–315, 2022.
[18] G. Caldarelli and J. Ellul, "Trusted academic transcripts on the blockchain: A systematic literature review," *Applied Sciences*, vol. 11, no. 4, pp. 1842, 2021.
[19] A. Iftekhar, X. Cui, Q. Tao and C. Zheng, "Hyperledger fabric access control system for internet of things layer in blockchain-based applications," *Entropy*, vol. 23, no. 8, pp. 1054, 2021.
[20] S. Xie, Z. Zheng, W. Chen, J. Wu, H. N. Dai *et al.,* "Blockchain for cloud exchange: A survey," *Computers & Electrical Engineering*, vol. 81, pp. 106526, 2020.
[21] Y. Wang and H. Chen, "Blockchain: A potential technology to improve the performance of collaborative emergency management with multi-agent participation," *International Journal of Disaster Risk Reduction*, vol. 72, pp. 102867, 2022.
[22] U. Chelladurai and S. A. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 1, pp. 693–703, 2022.
[23] M. Javaid, A. Haleem, R. P. Singh, S. Khan and R. Suman, "Blockchain technology applications for industry 4.0: A literature-based review," *Blockchain: Research and Applications*, vol. 2, no. 4, pp. 100027, 2021.
[24] F. Jamil, M. Ibrahim, I. Ullah, S. Kim, H. K. Kahng *et al.,* "Optimal smart contract for autonomous greenhouse environment based on IoT blockchain network in agriculture," *Computers and Electronics in Agriculture*, vol. 192, pp. 106573, 2022.
[25] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi, M. Khemakhem *et al.,* "Hierarchical blockchain-based multi-chaincode access control for securing IoT systems," *Electronics*, vol. 11, no. 5, pp. 711, 2022.
[26] P. Bhaskar, C. K. Tiwari and A. Joshi, "Blockchain in education management: Present and future applications," *Interactive Technology and Smart Education*, vol. 18, no. 1, pp. 1–17, 2020.
[27] A. Alammary, S. Alhazmi, M. Almasri and S. Gillani, "Blockchain-based applications in education: A systematic review," *Applied Sciences*, vol. 9, no. 12, pp. 2400, 2019.
[28] G. Chen, B. Xu, M. Lu and N. S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, no. 1, pp. 1–10, 2018.
[29] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *European Conf. on Technology Enhanced Learning*, Lyon, France, pp. 490–496, September 2016.
[30] BEN: Providing borderless blockchain education. [Online]. Available: https://blockchainedu.org/
[31] C. Knowles. Sony Global Education Looks to Revolutionise Education with Blockchain Tech. [Online]. Available: https://futurefive.co.nz/story/sony-global-education-looks-revolutionise-education-blockchain-tech

[32] P. Ocheja, B. Flanagan, H. Ueda and H. Ogata, "Managing lifelong learning records through blockchain," *Research and Practice in Technology Enhanced Learning*, vol. 14, no. 1, pp. 1–19, 2019.
[33] P. Ocheja, B. Flanagan and H. Ogata, "Connecting decentralized learning records: A blockchain based learning analytics platform," in *Proc. of the 8th Int. Conf. on Learning Analytics and Knowledge*, NY, USA, pp. 265–269, March 2018.
[34] A. Badr, L. Rafferty Q. H. Mahmoud, K. Elgazzar and P. C. Hung, "A permissioned blockchain-based system for verification of academic records," in *2019 10th IFIP Int. Conf. on New Technologies, Mobility and Security (NTMS)*, Canary Island–Spain, pp. 1–5, 2019.
[35] R. Arenas and P. Fernandez, "CredenceLedger: A permissioned blockchain for verifiable academic credentials," in *2018 IEEE Int. Conf. on Engineering, Technology and Innovation (ICE/ITMC)*, Stuttgart, Germany, pp. 1–6, June 2018.
[36] Q. Dai and N. Zhu, "University student status management system based on blockchain," in *the Int. Conf. on Cyber Security Intelligence and Analytics*, Shanghai, China, pp. 752–757, March 2022.
[37] S. T. Siddiqui, M. Fakhreldin and S. Alam, "Blockchain technology for IoT based educational framework and credentials," in *2021 Int. Conf. on Software Engineering & Computer Systems and 4th Int. Conf. on Computational Science and Information Management (ICSECS-ICOCSIM)*, Pekan, Malaysia, pp. 194–199, August 2021.
[38] D. Shah, D. Patel, J. Adesara, P. Hingu and M. Shah, "Exploiting the capabilities of blockchain and machine learning in education," *Augmented Human Research*, vol. 6, no. 1, pp. 1–14, 2021.
[39] S. Banerjee, D. Das, M. Biswas and U. Biswas, "Study and survey on blockchain privacy and security issues," in *Cross-Industry Use of Blockchain Technology and Opportunities for the Future*, IGI Global, pp. 80–102, 2020.
[40] J. Guo, C. Li, G. Zhang, Y. Sun and R. Bie, "Blockchain-enabled digital rights management for multimedia resources of online education," *Multimedia Tools and Applications*, vol. 79, no. 15, pp. 9735–9755, 2020.
[41] Z. A. Shaikh, A. A. Khan, L. Baitenova, G. Zambinova, N. Yegina *et al.,* "Blockchain hyperledger with non-linear machine learning: A novel and secure educational accreditation registration and distributed ledger preservation architecture," *Applied Sciences*, vol. 12, no. 5, pp. 2534, 2022.
[42] D. J. Wheeler and R. M. Needham, Correction to XTEA, Comput. Lab., Univ. Cambridge, Cambridge, U.K., Draft Tech. Rep., October 1998. [Online]. Available: https://www.cl.cam.ac.uk/archive/djw3/xxtea.ps
[43] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.
[44] A. A. M. Ragab, A. Madani, A. M. Wahdan and G. M. Selim, "Hybrid cryptosystems for protecting IoT smart devices with comparative analysis and evaluation," in *Proc. of the Future Technologies Conf.*, San Francisco, USA, pp. 862–876, October 2019.
[45] O. A. Khashan and N. M. Khafajah, "Secure stored images using transparent crypto filter driver," *International Journal of Network Security*, vol. 20, no. 6, pp. 1053–1060, 2018.
[46] O. A. Khashan, "Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment," *IEEE Access*, vol. 8, pp. 66878–66887, 2020.
[47] NS-2 Simulator. [Online]. Available: https://www.isi.edu/nsnam/ns/
[48] Fast ethereum rpc client for testing and deveopment. [Online]. Available: https://github.com/trufflesuite/ganache-cli
[49] G. Sharma and S. Kalra, "A lightweight user authentication scheme for cloud-IoT based healthcare services," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 1, pp. 619–636, 2019.
[50] P. Chandrakar, S. Sinha and R. Ali, "Cloud-based authenticated protocol for healthcare monitoring system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 8, pp. 3431–3447, 2020.
[51] J. Choi, J. Cho, H. Kim and S. Hyun, "Towards secure and usable certificate-based authentication system using a secondary device for an industrial internet of things," *Applied Sciences*, vol. 10, no. 6, pp. 1962, 2020.

[52] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza and K. Wehrle, "Towards viable certificate-based authentication for the internet of things," in *Proc. of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy*, NY, USA, pp. 37–42, April 2013.
[53] M. H. Nasir, J. Arshad, M. M. Khan, M. Fatima, K. Salah *et al.,* "Scalable blockchains—A systematic review," *Future Generation Computer Systems*, vol. 126, pp. 136–162, 2022.
[54] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg *et al.,* "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55–68, 2022.
[55] O. A. Khashan, "Secure outsourcing and sharing of cloud data using a user-side encrypted file system," *IEEE Access*, vol. 8, pp. 210855–210867, 2020.