EduChain: CIA-Compliant Blockchain for Intelligent Cyber Defense of Microservices in Education Industry 4.0

Md Arafatur Rahman, *Senior Member, IEEE*, Mohd Saharudin Abuludin, Ling Xi Yuan, Md. Shohidul Islam, and A. Taufiq Asyhari, *Senior Member, IEEE*

***Abstract*—Massive data handling requirement in education Industry 4.0 has attracted interests in the research of microservice architectures due to their scalability, resilience, and elasticity characteristics. This development has been challenged by extensive data exchange required by a set of independent microservices to build a complete application, which could result in increasing risks and exposure to the security and privacy breaches of the data. It is imperative to see that educational data are highly sensitive, critical for ascertaining educational attainment and facilitating credentials for qualification verifications. This article puts forward a new proposal of devising a security and privacy-preserving design mechanism of data transactions in educational microservices leveraging the blockchain technology. The design comprises three phases, namely the blockchain framework, data sending–receiving, and confidentiality-integrity-availability over a secured platform with each phase having detailed mechanisms for algorithm implementation. The proposal is shown to exhibit favorable performance in terms of time cost of publishing, throughput, and latency, and shown to have high survey acceptance in terms of confidentiality, integrity, and availability with approximately 10% improvement from prior blockchain adoption.**

***Index Terms*—Blockchain, data handling, education, industry 4.0, microservices, security.**

Manuscript received February 23, 2021; revised May 1, 2021 and June 9, 2021; accepted June 19, 2021. Date of publication June 29, 2021; date of current version December 6, 2021. This work was supported by the University Malaysia Pahang under Grant RDU210310. Paper no. TII-21-0804. *(Corresponding author: Md Arafatur Rahman.)*

Md Arafatur Rahman is with the School of Mathematics and Computer Science, University of Wolverhampton, WV1 1LY Wolverhampton, U.K. (e-mail: arafatur.rahman@ieee.org).

Mohd Saharudin Abuludin, Ling Xi Yuan, and Md. Shohidul Islam are with the Faculty of Computing, University Malaysia Pahang, Kuantan 26300, Malaysia (e-mail: mohdsaharudin@gmail.com; lingxiyuan@hotmail.com; msi.ice.ru@gmail.com).

A. Taufiq Asyhari is with the School of Computing and Digital Technology, Birmingham City University, B4 7XG Birmingham, U.K. (e-mail: taufiq-a@ieee.org).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2021.3093475.

Digital Object Identifier 10.1109/TII.2021.3093475

I. Introduction

THE recent emergence of Industry 4.0 has motivated the development of a robust data platform that revolutionizes information processing across educational institutions worldwide. This is relevant to serve the growing scale and complexity of the end-educational-stakeholder applications that are built on top of the massive data being exchanged. A key requirement herein is to have an accessible and scalable data platform while maintaining the authenticity and integrity of data transactions in order to promote universal trust on the educational environments.

To address this, there is an interesting direction on the usage of microservice architecture and design to develop a variety of scalable and resilient system applications for the education industry. Departing away from a sole single cloud solution for academic data accessibility, microservices can be considered to achieve distributed and integrated network infrastructure over the existing operations of a monolithic structure [1]. Herein, scalability is of paramount importance whereby network end-users can exploit resource-constrained devices, and the number of computing devices can be flexibly tailored and expanded, independent from the end-user applications and services provided. However, dealing with such a distributed system paradigm comes with a multitude of challenges, driven by the spread characteristics of the processing units and the need of frequent data exchanges across the platform. These make a significant proportion of the current microservice solutions difficult to guarantee data confidentiality, integrity, and availability (CIA) [2] in the existing infrastructure to minimize feasible distrust in network activities and the responsibility of fault-finding infrastructure to protect network end-users. It also remains a question how guaranteeing CIA to highly sensitive educational data could impact the overall system performance from the quality of services experienced by the end-users.

Growing interests in blockchain technology could pave a way for addressing the challenge of instrumenting CIA features to the microservices in educational platforms. It has been shown in recent research that blockchain policy can be used to identify the fake information circulating in the networks. Seeing how Industry 4.0 could provide state-of-the-art technologies [3] for intelligent real-time data access in the educational industry, a blockchain-based educational information system [4] can address collaboration of students, instructors, and administrations

1551-3203 © 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Universiti Malaysia Pahang. Downloaded on January 05,2022 at 04:36:38 UTC from IEEE Xplore. Restrictions apply.

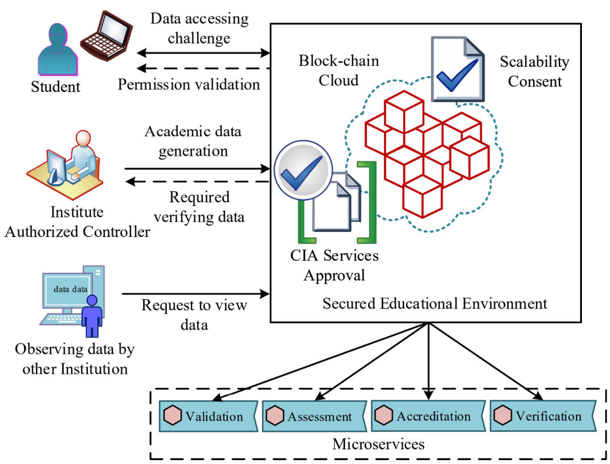

Fig. 1. Basic structure of secured educational framework.

as well as provide academic data certifications. A highly reliable blockchain-based intelligent resource management [5] is required in the educational sector to enrich the learning productivity and assure the learning sustainability for academic data certifications. Blockchain enables greater data protection and collaborates secure data sharing to build cyber defenses in an intelligent way equipped with embedded algorithmic processing.

Looking at the CIA issues surrounding the educational microservices and the blockchain potential in providing data confidentiality and security, this article puts forward a proposal of designing a CIA-compliant blockchain technique as part of the wider cyber-defense framework for securing educational microservices. Focusing on applications that define the framework components, we investigate ways of blockchain integration with the microservices, namely data validation, assessment, accreditation, and verification, which particularly handle sensitive cloud data using a set of independent operations running through a lightweight blockchain system. The system is envisaged to provide confidentiality and integrity for different types of academic information, such as registration data, certificates, transcript, etc., as part of the CIA triad services, and aims to maximize its availability through provision of lightweight computational blocks. This is captured in the framework shown in Fig. 1.

We refer to this proposed framework as *Educhain*, which executes the entire process of obtaining confidentiality and security of academic information. Educational data can be accessed and stored by registered students or authorized user in this platform. Strangers who are not registered in the desired educational institutions cannot access academic information herein; but, they can request to view a specific information. Blockchains are incorporated to build the user trust, whereas the microservices can enhance data accessibility and achieve scalability. Combining the two is anticipated to ensure data security due to the follow-up of data block transactions and eliminate risky activities through secured handling of academic data. In a nutshell, this work contributes to the following.

1) We propose a secure framework that serves a set of educational microservices for secured data handling exploiting blockchain technology.
2) We incorporate CIA features to the system design that integrates blockchain and educational microservices.
3) We examine the scalability of the proposed framework via numerical testing and quantitative investigation.
4) A comparative analysis is conducted to validate the proposed proposal by measuring the performance of our system in contrast to a variety of methods with blockchain structure.

The rest of this article is organized as follows. In Section II, we describe some closely related works. The overall methodology is discussed in Section III. Section IV explains the results and discussion of proposed system. Finally, Section V concludes this article.

II. Related Work

In this section, some concepts or strategies have been reviewed related to blockchain, microservices in different sectors, CIA, advanced driven designs for Industry 4.0, and intelligent cyber defense to present our proposed model. The CIA-based blockchain is a prominent issue for intelligent cyber defense on any platform.

A. Microservices in Various Sectors and CIA Security Strategy

Coulson *et al.* [6] developed a prototype based on microservice for web application by autoscaling process and evaluated it for prediction using supervised machine learning. Wang *et al.* [7] mentioned an elastic scheduling model that can solve task scheduling of different microservices in cloud-based computing resources. Mena *et al.* [8] described the microservices concept for the application of software architecture on IoT devices to acquire data and to maintain the module configuration. Chen *et al.* [9] developed virtual war room model to handle the behavior of microservice applications, including data tracing and fault analysis. In software industry, Akbulut and Perros [10] executed the performance analysis of hardware behavior, time of query response, and rate of packet loss for microservices sketch patterns to reduce infrastructural risks. Chen *et al.* [11] constructed a microservice-based framework on the properties of heterogeneous and dynamic edge-clouds that could solve the optimization problem of microservice-based deployment using deep-integration learning process.

Pinheiro *et al.* [12] proposed a solution of blockchain cloud networks and smart contracts to monitor the integrity files where the system protocol provided CIA, decentralization, and automation analysis for the generated results through symmetric encryption. Kumar *et al.* [13] suggested a CIA security solution to protect the VANETs architecture to avoid intrusion by applying end-to-end certification and authentication in where data are transferred in the encrypted form to verify communication entities. Cha *et al.* [14] recommended a framework based on CIA using blockchain strategies and key escrow encryption systems to address security issues in data supply chain management on large-scale storage data in the untrusted environment. Tohidi and Vakili [15] proposed an authenticate lightweight design

Authorized licensed use limited to: Universiti Malaysia Pahang. Downloaded on January 05,2022 at 04:36:38 UTC from IEEE Xplore. Restrictions apply.

to make a secure conjunction between the neighborhood network gateway and smart grid control center for data transfer to compress the data using lossless compression and Merkel hash tree algorithm to achieve CIA, which diminishes the data transmission, computational, and cloud expenses. Halabi and Bellaiche [16] presented a broker-based structure to handle the cloud security SLAs through CIA features protection against vulnerabilities and threats in cloud.

B. Advanced Driven Designs for Industry 4.0

To enhance the quality of emerging IoT technology and to optimize cloud computing, including cyber security, Industry 4.0 is an ongoing industrial revolution. Kalør *et al.* [17] investigated the complexities of network slicing and the protocols of industrial communication for utilization, incoherence, and authenticity to manage various requirements in Industry 4.0. Jiang *et al.* [18] performed network behavior analysis and feature extraction using big data for Industry 4.0 usage. In particular, He *et al.* [19] proposed a replacement algorithm based on locality-aware to make a most effective cloud computing for efficient manufactory of Industry 4.0. Li *et al.* [20] developed blockchain-based FeneChain that could investigate and operate the energy trading activities to build an industrious environment for Industry 4.0. Moreover, Li [21] studied the "education supply chain" and configured the educational system in the context of interactions of global institutions for Industry 4.0.

C. Blockchain-Based Intelligent Cyber Defense

Shen *et al.* [22] presented blockchain-based vehicular social network model, including certificate authority, for a position-based confidentiality-preserving protocol service. Milne *et al.* [23] developed a trusted cyber-physical scheme using distributed ledger and blockchain mechanism to achieve integrity, device detection, and authentication. In edge-AI permitted IoT, Lin *et al.* [24] mentioned blockchain-based knowledge market framework through distributed P2P mode using consensus and cryptographic mechanism to produce knowledge tradable for effective and secure knowledge exploration. Besides, Yazdinejad *et al.* [25] presented cluster architecture where SDN controllers with blockchain are applied on IoT network to provide advanced routing protocols and to remove POWs for increased protection. Choi *et al.* [26] developed an innovative model with blockchain and fabricated RPS prototype in order to monitor the data-integrity as PoM and identified cyber-attacks in real time of PLCs due to PoW network associated with lot of nodes.

Unlike the earlier published studies cited in this article, herein a CIA authorized blockchain design has been proposed that generates a new secure data handling scheme with validated microservices in any educational institution to meet the aim of implementing multipurpose high-performance model.

III. Overview of Educhain Model

This section introduces the blockchain-based CIA authorized cloud architecture and builds a new secure data handling model in any educational institution to meet the aim of implementing multipurpose high-performance structure using the microservices design, named Educhain model, which is shown in Fig. 2. Driven by data transaction needs, a stateless microservice does not hold session state within requests, but a stateful microservice contains session data for multiuse case. The CIA of academic information in this model can build data satisfactions and validations among the stakeholder of the educational institution. This framework can build more user trust on CIA of academic data in network activities as a professional service against forged institutions' websites. As the necessity of the blockchain-based secure educational data usage is increasing rapidly, scalable solution is also a key factor as well. The main design views for this platform based on several phases are presented as follows.

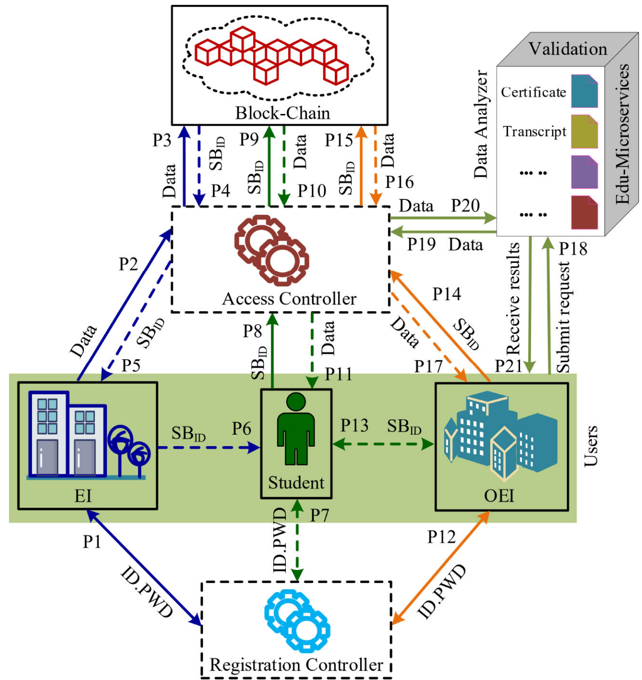

Fig. 2. Educhain model.

A. Phase-1: Overview of the Educhain Model

The proposed approach is basically designed by four modules, such as user role, registration control, access control, and secured data storage, whose operations are discussed below.

1) User's Role and Functionality: The user's role and functionality of the Educhain model is controlled by education institution (EI), other EI (OEI), and student. EI is the key data provider and generator of all academic information within the cloud of blockchain-based educational system network on behalf of its own students. EI cannot generate own public keys but it can generate or update educational information of their students in the blockchain using the student's public key (P_k) and create a set of session keys for each unique transaction as main functionality without sharing that information with outsiders.

OEI is the key data recipient of secured academic information in the blockchain. As the main functionality, it is not only able to create user's public key, add or update the user academic data but also keeps total viewership of the academic data with

Authorized licensed use limited to: Universiti Malaysia Pahang. Downloaded on January 05,2022 at 04:36:38 UTC from IEEE Xplore. Restrictions apply.

the permission of the registered student to read and verify the educational records from the blockchain network. A student is the initial and key participant of own academic information in the blockchain-based educational system, who has the right to create a unique identity and view its respective data. The main functionality of the students is to create their own public key (P_k) and digital identity to be paired with their education record as owner. A student has no right to key in other educational data without its own data but grant other parties total viewership of its data.

2) Registration Control: In this case, the registration control module primarily allows the students to create their own unique digital identity with their own public key. When a student wants to register to an educational institution by this framework, it generates unique blockchain student identity with password and issues digital ID and password PWD to student securely. Also it stores this information in the Educhain data storage. The public key generation is based on the Rivest–Shamir–Adleman (RSA) public key cryptosystem for the enforcement of integrity. All instances of academic record creation in the blockchain must be done with the creation of a valid RSA public key beforehand.

3) Access Control: The access control module permits all parties to interact with the blockchain-based secure educational system and access the information from blockchain-based database. The participants of the blockchain must have an intermediary module, such as access control, to interact with the blockchain to ensure the usability, availability, and security of the system. All methods of interaction, such as adding records, viewing records, or sharing records, must be securely executed through the access control module of this platform.

4) Secured Data Storage: The secure data storage module of the blockchain-based educational system is specifically designed for all parties to securely store their data under the full confidentiality and integrity. Moreover, it is based on a blockchain method of check-and-balance where all transactions are cross referenced by the SHA256 hash generated. All addition of records will generate a bi SHA256 of the new and previous record. Any tampering of data can be checked and verified by the sequencing of each SHA256 hash. A break in the sequence indicates data tampering and justifies that the chain after the break or fork should be declared null and void.

B. Phase-2: Data Sending and Receiving Mechanism With Data Analysis

Data analyzer is designed to analyze the lightweight eduservices with validation support in Educhain system. Applying validation techniques, it enables automated data analysis to analyze eduservices, such as certificates, transcripts, etc., in the blockchain-based education model. The operations of the proposed method happen sequentially through the process of sending and receiving in the Educhain model. There are three types of users in this system, such as EI, student, and OEI, wherein only EI is allowed to send data to Educhain. As illustrated in the diagram of Fig. 2, the mechanism for sending and receiving data in this platform is briefly presented as follows.

Processes 1, 7, and 12: All users must provide valid user id (ID) and password (PWD) to use the system. Otherwise, they need to register with the registration controller (RC). Once authenticated, they can instruct the access controller (AC) to access to the Educhain. Only AC can access Educhain directly.

Process 2: Once authenticated, EI can send data of specific student to the AC. All data will be encrypted at this phase.

Process 3: The encrypted data will be sent to Educhain for storing purposes.

Process 4: The Educhain will store the data in the block. A unique id, SBID will be created for the student block. The student block id, SBID will return to the AC.

Process 5: EI will store the SBID received from AC and store it in their database for their reference.

Process 6: A student will get their SBID by the EI as requested. They can use it to access their block in the Educhain.

Process 8: Once authenticated, a student can send an instruction to the AC to fetch their data in the Educhain by providing their SBID.

Process 9: AC will interact with the Educhain to fulfill the student request.

Process 10: Educhain will look for student's data in the blockchain with the SBID as a reference and return it to AC.

Process 11: AC will pass encrypted data to the student as earlier request. Students can view their data after decryption.

Process 13: One of the advantages of this model is that the student can permit other people or institution to view their data at a certain period as long as they have their SBID.

Process 14: Once authenticated, OEI will send a request to view data by sending the SBID to the AC.

Process 15: AC will interact directly with the Educhain to fulfill the OEI request.

Process 16: Once found, data will send to AC in encrypted form.

Process 17: The AC will pass the data to OEI, and after the data decrypted, OEI can view the data.

Process 18: All users submit their requests to data analyzer for data validation.

Process 19: Data analyzer will interact with AC for the lightweight services validation to fulfill the user's requests.

Process 20: AC will permit data analyzer to ensure the analyzing data validation.

Process 21: Data analyzer will send the feedback to the users over their requests about eduservices.

C. Phase-3: CIA on Secure Educational Platform

Academic data security is ensured by exploiting CIA services through AC to get high performance of data accessibility for which the following aspects are discussed.

1) Confidentiality: Generally confidentiality assessments protect the sensitive data from unrecognized access and misconduct. So, academic data can be accessed by registered and permitted users in education system. Different levels of access ensure that only valid users can have legal permission to ensure the ability distribution and prevent the conflict of interest. A detailed of the enforcement of confidentiality can be found

Authorized licensed use limited to: Universiti Malaysia Pahang. Downloaded on January 05,2022 at 04:36:38 UTC from IEEE Xplore. Restrictions apply.

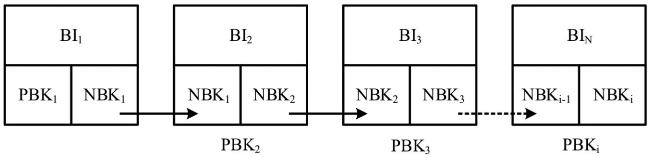

Fig. 3. Building blocks of Educhain.

in the encryption and decryption Algorithms 1 and 2 where the using notations are public key (P_k), session key (S_k), raw educational data (D), cipher (cip), utf-8 encoding (u), base 64 encoding (64), common 128-b advanced encryption standard (AES), encrypt-then-authenticate-then-translate (EAX), EI, student (STD), and other educational institution (OEI).

Encryption algorithm utilizes a dual hybrid cryptosystem where the raw educational data are paired and encrypted together with the RSA public key to form the cipherdata and the session key. This dual hybrid system ensures that trust and anonymity are embedded into a trustless ecosystem. The right to confidentiality is enforced with a failsafe system where all tridata are required to decrypt the educational data. The tridata encompass the RSA public key, the session key, and the identifying data, where in most cases can be set by the unique student ID. The absence of any one of these data would trigger a fail-safe, as described in the decryption algorithm. In order to break the confidence cycle, the malicious entity is required to possess all tridata or decipher all two layers of RSA and AES algorithm and reverse the SHA256 hash to get to the raw data. In any case where one of the sensitive data is leaked to the public via a malicious entity either from EI or OEI, the student still maintains the ultimate right of confidentiality without exposing any other sensitive information.

Algorithm 1: Academic Data Encryption and Sending to Educhain System.

Initialization of variables
P_k, $D = raw$(CGPA, ID, Cert)
$D = raw$ (CGPA, ID, Cert)
$D(u) = D$ is encoded in $utf - 8$
$S_k = Enc(rand + P_k)$
$S_kcip = encrypt\ AES(P_k + S_k)$
$Dcip(u) = encrypt\ EAX(S_k + D)$
$Dcip(u) = enc$(CGPA, ID, Cert)
$Dcip(64) = Dcip$ is encoded to base64
Encrypted $Dcip(64)$ is sent to the Blockchain by EI
$S_kcipher$ sent to STD

2) Integrity: Academic data on the blockchain platform and network cannot be deleted or altered once it has been added to the blockchain. Integrity measures defend data from unrecognized transaction. Due to its immutability factored in by the block to block hashing method, all information keyed into the blockchain shall have their integrity instilled in place. A detailed description of the enforcement of integrity can be found in the block creation process of Fig. 3

$$NBK_i = \text{Hashing}(BI_i, PBK_i) \tag{1}$$

Algorithm 2: Academic Data Decryption and Retrieving From Educhain System.

Initialization of variables
P_k, $S_kcipher$, $Dcip(64) = enc$(CGPA, ID, Cert)
Encrypted $Dcip(64)$ is retrieved from the block-chain
$S_kcipher$ retrieved from STD
$Dcip(u) = Dcip(64)$ is decoded back to $utf - 8$
$S_k = Decrypt\ S_kcip\ AES(P_k + S_kcip)$
if $S_k \neq (P_k + S_kcip)$
else
Decryption failed, invalid pairing of P_k and S_kcip, Process is terminated
if
$D(u) = Decrypt\ EAX(Dcip(u) + S_k)$
if $D(u) \neq (Dcip(u) + S_k)$
else
Decryption failed, invalid S_k and P_k is used, Process is terminated
if end
$D = D(u)$ is decoded back to raw data
$D = raw$(CGPA, ID, Cert)
D can be retrieved by OEI

where NBK_i is ith number of previous blocks, PBK_i is ith number of first blocks, and BI_i is storing ith block number and data in the blockchain

$$PBK_i = \begin{cases} NULL & \text{if } BI_1 \text{ is the first block} \\ NBK_{i-1} & \text{otherwise} \end{cases}. \tag{2}$$

PBK_1 is the first block known as the Genesis block, which should be $NULL$ in value at all times according to the blockchain engineer. The consecutive block, Block PBK_2 shall be determined by the hash of BI_2, which is populated by the academic data and NBK_1, which is the hash output of the former block, PBK_1. Therefore, each block is chained backward by the former block's hash output, NBK_{N-1} and chained forward by the block's new hash output NBK_N.

This hash chaining from a transaction to the next block is implemented with the SHA256 one-way hashing method, which enforces the integrity of the whole blockchain. Whenever there is a discrepancy between the hash codes, it is produced an evidence of data tampering either by substitution or modification. For such incident, the chain of integrity is broken and the transaction should be nullified. This process guarantees that each submission of records has the integrity of both system and user that stored data of the blockchain is logically true.

3) Availability: The deals of availability preserve data timely and do not allow interrupted access in the process. The blockchain is accessible only through ac module to ensure a streamlined query process and users have an equal right to access blockchain resources for getting entire facility from online. Table I shows three categories of users with different access levels those who can communicate with Educhain through ac while sending and receiving data. As a result, an independent streamlined access of the blockchain network is provided

Authorized licensed use limited to: Universiti Malaysia Pahang. Downloaded on January 05,2022 at 04:36:38 UTC from IEEE Xplore. Restrictions apply.

TABLE I
USER ROLES IN EDUCHAIN

Access Level	Student	EI	OEI
Owner	✓	x	x
Create	x	✓	x
Update	x	✓	x
Allow sharing	✓	x	x
Read	✓	✓	✓

equally to all users across the board encompassing OEI, EI, and students. The only prerequisite is that access to data availability is granted only to individual participants, as long as they have the correct credentials. Students can view and share their data if they have their public key, session key, and unique ID. EI can add data into the blockchain using authorized public key of the student. OEI can view data using session key and unique ID by the student permission.

D. Phase-4: Scalability on Academic Data

The Educhain model can solve the concerns of data scalability by the multinode technique, multitransnational block, and lightweight web structure to handle large user data transactions or current user workloads. In Algorithm 3, the using notations are time (T), time limit ($Tlim$), block index/block length ($BlockIdx$), timestamp ($Tstamp$), chain length ($content$), block (B), and transaction (Tx).

Algorithm 3: The Data-Block Transaction of Educhain System.

if $(BlockIdx == 0)$ **then**
  Create Genesis Block, B_0
  Initialize default value in Genesis Block
end if
if (pending $Tx \neq 0$) **then**
  Create New Block, B_n
  Block Pooling:
  for $(T = 0, T < Tlim, T{+}{+})$ **do**
    Create New Transaction, Tx_{n+1}
    Add data to Tx (author, content, chipherdata)
    Add timestamp to transaction
  end for
end if
Generate $SHA256$ hash of B_n
if ($SHA256$ hash of $B_n \neq B_{n-1}$) **then**
  return error
else
  Add B_n to $BlockIdx$
end if
check integrity of $BlockIdx$
if (error == None) **then**
  share $BlockIdx$ to connected nodes
else
  raise error
end if
get latest block information from connected nodes

Block pooling, as described in the algorithm earlier, involves the processing of several transactions at once in a concurrent block as opposed to the conventional method of hashing and chaining each transaction in a singular block. In the algorithm, a new block B_n is created at which time a transaction Tx_n+_1 is executed. Once this process occurs all submitted transactions to the node within time $Tlim$ would be accepted and processed as a single block. All contents and data in the block B_n would be hashed by SHA256. Once the block is verified and secured, it would be added to the local blockchain $BlockIdx$. The hashes of each block B_n would be further checked. If there are no errors, $BlockIdx$ would be sent and published to all connected nodes. When all other nodes accept $BlockIdx$, the confirmation status would be sent back to the local machine. It increases the efficacy of the blockchain to process more transactions with a shorter time and computing resources.

IV. RESULTS AND DISCUSSION

There are two aspects: performance analysis and feasibility analysis of our edusystem have been mentioned in this section. So, quantitative exploration has been conducted to know the user's perception of academic data handling before and after the implementation of blockchain technology.

A. Performance Analysis

Educhain is designed to conduct against the other two algorithms, such as Eduleger and DVF, for measuring the performance of our blockchain-based system using a local blockchain server, a remote blockchain server, and a client server. To measure the performances of this system, data sizes in kilobytes (KB) from 10, 20, 30, 40, to 50 KB are used depending on the key metrics, such as the average time in milliseconds (ms), the throughput in kilobits per second (kb/s), and the latency in milliseconds (ms) as well as a number of clients (from 1 to 5) are used depending on the throughput in kb/s, which are shown in Fig. 4(a)–(d).

The first performance test is the time cost on a publishing transaction, which is the duration of each algorithm to post a single data block in its respective blockchain database. This measures the variances and the broad average under different load capacity. According to the results, the experiment is started from 10 KB and 73.01 ms for Eduledger, 51.82 ms for Educhain, and 48.05 ms for DVF. At the minimum load point, it provides the shortest average time for DVF. As the data load increases, the average time of Eduledger and DVF rose sharply from 95.75 to 214.2 ms (+118.45 ms) for the former algorithm and 75.75 to 224.2 ms (+148.45 ms) for the latter algorithm 20 and 40 KB where DVF overtook Eduledger at the 40 KB. The average time at 30-KB data load of Educhain has changed significantly from 120.56 to 202.4 ms. To find the expected results, Eduledger reached the peak point by the longest average time 299.86 ms as to 50 KB where Educhain took 263.21 ms and DVF took 257.01 ms. However, Educhain has performed more consistently; but DVF has fluctuated throughout test due to crossing top and below of the threshold of Educhain's trendline at 40 and 50 KB, respectively.

Authorized licensed use limited to: Universiti Malaysia Pahang. Downloaded on January 05,2022 at 04:36:38 UTC from IEEE Xplore. Restrictions apply.

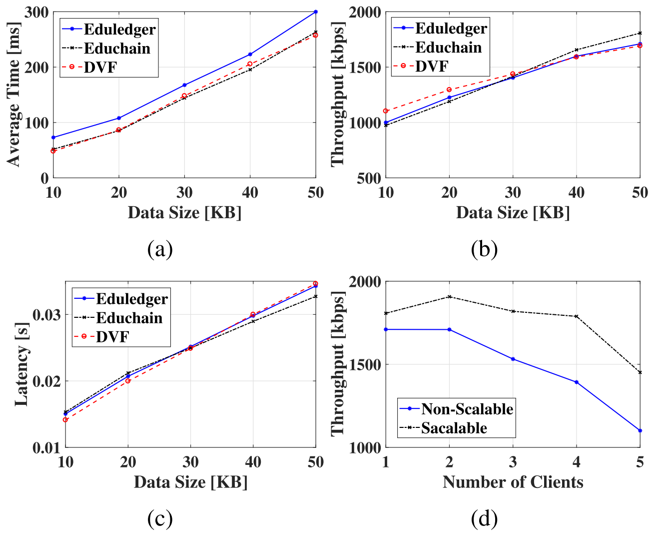

Fig. 4. Analysis on (a) time cost of publishing transactions, (b) throughput per algorithm, (c) latency per algorithm, and (d) throughput per client.

The second performance test is the throughput of data transactions, which measures the average speed of each algorithm to process the data block stream to the respective blockchain database. This will observe the variability between each algorithm under different load capacities for the benchmark performance. According to the demonstration of this test, it is started from 10 KB with 1000.22 kb/s for Eduledger, 973.71 kb/s for Educhain, and 1102.43 kb/s for DVF. DVF's algorithm yielded the highest throughput at the minimum load point. Due to the data load increases, the throughput of Eduledger and DVF rose steadily but Educhain has shown a sharp increase from 1145.35 kb/s at 20 KB to 1711.09 kb/s at 40 KB overtaking both Eduledger and DVF. All algorithms leveled off and peaked between 40 and 50 KB where Educhain produces the highest throughput 1807.11 kb/s as the best scalable performance and DVF shows the lowest result.

The third performance test is to determine the latency per data size where it measures the average delay of each algorithm to send and receive a variable data block to their respective blockchain server. This will allow for observation of the latency difference among algorithms under different load capacities as benchmark performance. According to the presentation of this work, it started from 10 KB with 0.01505 ms for Eduledger, 0.01532 ms for Educhain, and 0.01412 ms for DVF. At the minimum load point, DVF's yielded the best shortest duration of latency. Between 10 to 30 KB, the duration of latency of all algorithms rose in tandem with their respective position, DVF at the lowest rate increase to 0.02547 ms, seconded to Eduledger at 0.02566 ms followed by 0.02575 ms. All algorithms followed the same trendline until they intersected at 30 KB. At 30 KB, the respective latency of each algorithm is 0.02566 ms (Eduledger), 0.02575 ms (Educhain), and 0.02547 ms (DVF). If increase in latency, Educhain ended the experiment with the latency of 0.03272 ms as lowest rate followed by Eduledger at 0.03429 ms and DVF at 0.03462 ms. It can be observed that DVF yields the best result in terms of latency at loads below 30 KB; however,

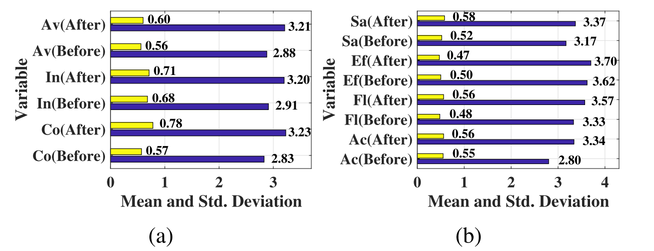

Fig. 5. Analysis on user evaluations for (a) confidentiality (Co), integrity (In) and availability (Av), (b) accountability (Ac), flexibility (Fl), effectiveness (Ef), and satisfaction (Sa).

Educhain has the overall commandment of latency above 50 KB. A low latency algorithm is preferred to prevent time and data loss. Therefore, these show favorable scalability behavior for the Educhain.

The last performance test is to measure the throughput of multiple clients to blockchain server for the scalable integrated Educhain format in comparison to the nonscalable integrated Eduledger format. It measures the average throughput of client from each algorithm to send a data block to their respective blockchain server. We are interested in observing the differences in throughput per client between each algorithm under a single load capacity fixed at 50 KB.

For these test observations, at one client, Eduledger started from 1710.03 kb/s and Educhain started from 1807.11 kb/s. Educhain has slowly reached its peak for three clients up to 1990.71 kb/s but, it decreases mildly until 1923.83 kb/s with four clients before falling sharply to 1451.36 kb/s with five clients. Eduledger has shown a continuous uptrend from one client to two clients. Next, the trend reverses to a steady downtrend until it reaches 1426.93 kb/s at four clients and it resumes with a sharp decline to 1100.96 kb/s at five clients. Clearly, Educhain has shown the scalable and improved results with higher overall throughput at every level as compared to Eduledger.

B. Feasibility Analysis

The system exploration consists of 21 items based on seven criteria: confidentiality, integrity, availability, accountability, flexibility, effectiveness, and satisfaction, where each criterion containing three items are adapted with some modification from Rahman *et al.* [27], which utilizes the Likert-type scale of four scales starting from 1=strongly disagree to 4=strongly agree, measuring the perception or opinion of a different factor in academic data handling, which are represented in Fig. 5(a) and (b). There are two sessions where the first session will be a 15-min briefing about the existing academic data handling system and the second session will be another 15-min briefing about blockchain-based academic data handling system.

1) User Perception Toward CIA: For the confidentiality in academic data handling, the acceptability of existing method provides m= 2.83 and SD = 0.57, whereas the user perception after implementation achieves m = 3.23 and SD = 0.78. Most users have affirmed that the proposed method can ensure better integrity with m = 3.20 and SD = 0.71 compared to conventional

Authorized licensed use limited to: Universiti Malaysia Pahang. Downloaded on January 05,2022 at 04:36:38 UTC from IEEE Xplore. Restrictions apply.

TABLE II
T-TEST RESULT

Criteria	Method	Mean	SD	Sig(p)
Confidentiality	Before After	2.83 3.23	0.57 0.78	0.0046
Integrity	Before After	2.91 3.20	0.68 0.71	0.0248
Availability	Before After	2.88 3.21	0.56 0.60	0.0158
Accountability	Before After	2.80 3.34	0.55 0.56	0.0001
Flexibility	Before After	3.33 3.57	0.48 0.56	0.0413
Effectiveness	Before After	3.62 3.70	0.50 0.47	0.4654
Satisfaction	Before After	3.17 3.37	0.52 0.58	0.0852

practice with $m = 2.91$ and SD $= 0.68$ for user perception in academic data handling. It is incontestable that users believed that the proposed method could ensure data availability as the revealed findings as $m = 3.21$ and SD $= 0.60$ compared to their perception on the recent method as $m = 2.88$ and SD $= 0.56$. The confidentiality, higher integrity, and availability of their data will be increased with the implementation of the proposed method due to exhibit a desirable attitude of users.

2) User Perception Toward Accountability, Flexibility, Effectiveness, and Satisfaction: On the accountability of academic data handling, from the observation, most users affirmed that the proposed method is a better way ($m = 3.34$ and SD $= 0.56$) compared to the current method ($m = 2.80$ and SD $= 0.55$). For the user perceptions on academic data handling, the majority of users agreed that the flexibility of proposed method ($m = 3.57$ and SD $= 0.56$) is much better compared to the current method ($m = 3.33$ and SD $= 0.48$) if implemented. Users believed the proposed method of academic data handling is more effective compared to the current method ($m = 3.62$ and SD $= 0.47$). Thus, they consented more to this method ($m = 3.70$ and SD $= 0.50$) from their perception. Analysis of user satisfaction opinions in academic data handling provides ($m = 3.37$ and SD $= 0.58$) on proposed method compared to current method as ($m = 3.17$ and SD $= 0.52$). Most users expect a reliable and effective academic data handling system, such as this, for better outcomes and satisfaction to avoid risky activities for the long term.

3) T-Test Result: It has been tested to exhibit whether there is any significant difference between the conventional method and exploiting blockchain-based proposed method in academic data handling to validate the hypothesis of the work. The T-test results are shown in Table II for p-value $p < 0.05$, which are evaluated to compare the mean values of two groups and observed the significant differences for proposed system compared to the existing systems. User perception toward several features of this system is measured to utilize the Likert-type scale of four scales ranging from 1 (strongly disagree) to 4 (strongly agree). We have obtained the mean values of the proposed method in term of confidentiality, integrity, availability, accountability, flexibility, effectiveness, and satisfaction given by 3.23, 3.20, 3.21, 3.34, 3.57, 3.70, and 3.37, respectively, which is better than conventional methods. We have noticed that the differences between both approaches are significance since $p < 0.05$ as governed by Cronbach alpha rule of thumb except the significance of two features (effectiveness and satisfaction) in which the $p > 0.05$.

V. CONCLUSION

Motivated by the need of digitalization in the education Industry 4.0, we studied a new framework of secured data handling by exploiting blockchain technology to guarantee CIA of highly sensitive educational data delivered via a set of microservices. We developed systematic mechanisms to aid in the development and implementation of the framework though specifications of functional units of the blockchain-enabled platform. We then demonstrated the desirable performance of the system using standard metrics, such as time cost of publishing transactions, throughput, and latency. To provide further validation, we performed user acceptance testing around CIA features and needs. This later investigation revealed the significant need of incorporating blockchain technology for flexible, reliable, and secured handling of sensitive academic data.

REFERENCES

[1] Y. Gan and C. Delimitrou, "The architectural implications of cloud microservices," *IEEE Comput. Architecture Lett.*, vol. 17, no. 2, pp. 155–158, Jul.–Dec. 2018.
[2] M. Warkentin and C. Orgeron, "Using the security triad to assess blockchain technology in public sector applications," *Int. J. Inf. Manage.*, vol. 52, 2020, Art. no. 102090.
[3] S. Karadayi-Usta, "An interpretive structural analysis for Industry 4.0 adoption challenges," *IEEE Trans. Eng. Manage.*, vol. 67, no. 3, pp. 973–978, Aug. 2020.
[4] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.
[5] H. Yang, A. Alphones, W.-D. Zhong, C. Chen, and X. Xie, "Learning-based energy-efficient resource management by heterogeneous RF/VLC for ultra-reliable low-latency industrial IoT networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5565–5576, Aug. 2020.
[6] N. C. Coulson, S. Sotiriadis, and N. Bessis, "Adaptive microservice scaling for elastic applications," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4195–4202, May 2020.
[7] S. Wang, Z. Ding, and C. Jiang, "Elastic scheduling for microservice applications in clouds," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 1, pp. 98–115, Jan. 2020.
[8] M. Mena, A. Corral, L. Iribarne, and J. Criado, "A progressive web application based on microservices combining geospatial data and the Internet of Things," *IEEE Access*, vol. 7, pp. 104577–104590, 2019.
[9] H. Chen, P. Chen, and G. Yu, "A framework of virtual war room and matrix sketch-based streaming anomaly detection for microservice systems," *IEEE Access*, vol. 8, pp. 43413–43426, 2020.
[10] A. Akbulut and H. G. Perros, "Performance analysis of microservice design patterns," *IEEE Internet Comput.*, vol. 23, no. 6, pp. 19–27, Nov./Dec. 2019.
[11] L. Chen *et al.*, "IoT microservice deployment in edge-cloud hybrid environment using reinforcement learning," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2020.3014970.
[12] A. Pinheiro, E. D. Canedo, R. T. DeSousa, and R. D. O. Albuquerque, "Monitoring file integrity using blockchain and smart contracts," *IEEE Access*, vol. 8, pp. 198548–198579, 2020.
[13] G. Kumar, R. Saha, M. K. Rai, and T.-H. Kim, "Multidimensional security provision for secure communication in vehicular ad hoc networks using hierarchical structure and end-to-end authentication," *IEEE Access*, vol. 6, pp. 46558–46567, 2018.
[14] S. Cha, S. Baek, and S. Kim, "Blockchain based sensitive data management by using key escrow encryption system from the perspective of supply chain," *IEEE Access*, vol. 8, pp. 154269–154280, 2020.

Authorized licensed use limited to: Universiti Malaysia Pahang. Downloaded on January 05,2022 at 04:36:38 UTC from IEEE Xplore. Restrictions apply.

[15] H. Tohidi and V. T. Vakili, "Lightweight authentication scheme for smart grid using Merkle hash tree and lossless compression hybrid method," *IET Commun.*, vol. 12, no. 19, pp. 2478–2484, 2018.

[16] T. Halabi and M. Bellaiche, "A broker-based framework for standardization and management of cloud security-SLAs," *Comput. Secur.*, vol. 75, pp. 59–71, 2018.

[17] A. E. Kalør, R. Guillaume, J. J. Nielsen, A. Mueller, and P. Popovski, "Network slicing in Industry 4.0 applications: Abstraction methods and end-to-end analysis," *IEEE Trans. Ind. Informat.*, vol. 14, no. 12, pp. 5419–5427, Dec. 2018.

[18] D. Jiang, Y. Wang, Z. Lv, S. Qi, and S. Singh, "Big data analysis based network behavior insight of cellular networks for Industry 4.0 applications," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1310–1320, Feb. 2020.

[19] J. He, G. Jia, G. Han, H. Wang, and X. Yang, "Locality-aware replacement algorithm in flash memory to optimize cloud computing for smart factory of Industry 4.0," *IEEE Access*, vol. 5, pp. 16252–16262, 2017.

[20] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang, "Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6564–6574, Oct. 2020.

[21] L. Li, "Education supply chain in the era of Industry 4.0," *Syst. Res. Behav. Sci.*, vol. 37, no. 4, pp. 579–592, 2020.

[22] H. Shen, J. Zhou, Z. Cao, X. Dong, and K.-K. R. Choo, "Blockchain-based lightweight certificate authority for efficient privacy-preserving location-based service in vehicular social networks," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6610–6622, Jul. 2020.

[23] A. J. Milne, A. Beckmann, and P. Kumar, "Cyber-physical trust systems driven by blockchain," *IEEE Access*, vol. 8, pp. 66423–66437, 2020.

[24] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, "DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2440–2452, Jan. 2020.

[25] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," *IEEE Trans. Services Comput.*, vol. 13, no. 4, pp. 625–638, Jul./Aug. 2020.

[26] M. K. Choi, C. Y. Yeun, and P. H. Seong, "A novel monitoring system for the data integrity of reactor protection system using blockchain technology," *IEEE Access*, vol. 8, pp. 118732–118740, 2020.

[27] M. A. Rahman, V. Mezhuyev, M. Z. A. Bhuiyan, S. N. Sadat, S. A. B. Zakaria, and N. Refat, "Reliable decision making of accepting friend request on online social networks," *IEEE Access*, vol. 6, pp. 9484–9491, 2018.

Md Arafatur Rahman (Senior Member, IEEE) received the Ph.D. degree in electronic and telecommunications engineering from the University of Naples Federico II, Naples, Italy, in 2013.

He is currently a Senior Lecturer with the School of Mathematics and Computer Science, University of Wolverhampton, Wolverhampton, U.K. He was an Associate Professor with the University Malaysia Pahang, Pahang, Malaysia. He is a Co-Author of more than 100 international journals and conferences. His research interests include wireless communication, cognitive radio networks, security, and big data analytics.

Mohd Saharudin Abuludin received the M.Sc. degree in ICT from the Faculty of Computing, University Malaysia Pahang, Pahang, Malaysia, in 2020.

His main area of research interest includes blockchain in education.

Ling Xi Yuan received the B.CS. degree in computer systems and networks from the Faculty of Computing, University Malaysia Pahang, Pahang, Malaysia, in 2021.

He is currently a Technology Consultant with Ernst & Young Consulting Sdn. Bhd, Kuala Lumpur, Malaysia. He is currently exploring opportunities in the blockchain and its related industries. His current research interests include blockchain, robotic process automation, and Internet of Things.

Md. Shohidul Islam received the B.Sc. and M.Sc. degrees from the Department of Information and Communication Engineering, University of Rajshahi, Rajshahi, Bangladesh, in 2009 and 2010, respectively. He is currently working toward the Ph.D. degree in system network and security with the Faculty of Computing, University Malaysia Pahang (UMP), Pahang, Malaysia.

He was an Assistant Professor in computer science and engineering with the Central University of Science and Technology, Dhaka, Bangladesh. He is currently a Research Assistant with UMP. His current research interests include blockchain and cyber security, Internet of Things, heterogeneous network, distributed network, data security, artificial intelligence, and neural network.

A. Taufiq Asyhari (Senior Member, IEEE) received the B.Eng. (Hons.) degree in electrical and electronic engineering from NTU, Singapore, in 2007, and the Ph.D. degree in information engineering from the University of Cambridge, Cambridge, U.K., in 2012.

Since March 2020, he has been an Associate Professor in networks and communications and subsequently becoming the Head of Future Information Networks Research Cluster with Birmingham City University, Birmingham, U.K. Prior to this position, he was with Coventry, Cranfield, and Bradford Universities. He is currently the Academic Principal Investigator for the multimillion pound 5G Connected Forest project funded by the UK-DCMS. His research interests include fundamental and applied information theory with applications to communication networks, cyber-physical systems, machine learning, and statistical data analysis.

Dr. Asyhari was the recipient of several academic awards and recognitions, including nomination of the Most Innovative Use Case—5G Week Awards in 2021 and British Council's COP26 Trilateral Research Award in 2021.

Authorized licensed use limited to: Universiti Malaysia Pahang. Downloaded on January 05,2022 at 04:36:38 UTC from IEEE Xplore. Restrictions apply.