Towards The Development of A Secure Cloud-Based E-Learning System for Post COVID-19 Academic Institutions

RAJI FUNSHO ISAIAH[1], OKEYINKA ADEREMI ELISHA[2], ADAMU ABUBAKAR ISAH[3], JAMILU MAIPAN-UKU[4]

[1,2,3,4]*Department of Computer Science, Faculty of Natural Sciences, Ibrahim Badamasi Babangida University, Lapai, Niger State, Nigeria*

Abstract- ***The emergence of COVID-19 poses a threat to humanity, as this pandemic has forced many global activities to close, including educational activities. As a measure to reduce the spread of the COVID-19 virus and also ensure that students are not left without studying, education institutions have been forced to switch to e-learning using available educational platforms, despite the challenges facing this sudden transformation. Study have shown that the cheapest means to get affordable implementation of e-learning is through the use of cloud computing. However, data stored on the cloud suffers the risk of breach of confidentiality especially when Cloud Service Provider (CSP) choose to be dishonest. In this paper, the preliminary development of a secure cloud-based e-learning system is presented. The cloud-based e-learning system features security layer where data to be stored/retrieved on/from the cloud is encrypted/decrypted using a proposed cryptosystem. The system is capable of addressing real-world security challenges in cloud-based e-learning system.***

Indexed Terms- ***COVID-19, cloud computing, lightweight cryptosystem, e-learning, time complexity***

I. INTRODUCTION

The traditional way of teaching-learning where teacher presents the learning material to a group of students in a classroom requires that both teacher and the student must be physically present for teaching and learning to take place[1]. Although the traditional method of teaching and learning has the advantage of immediate feedback, it has many drawbacks. Some of the drawbacks of traditional teaching and learning include, inability to provide support for interactivity, inability to provide location dependent education, a student who could not take part in some lesson would also miss the training material, inflexibility of the method and a host of others. Learners have already lost interest in traditional way of imparting knowledge [2] and the emergence of COVID-19 prompted the strong support of the authorities in educational institution for e-learning. Specifically, the challenges posed by the emergence of COVID-19 which led to the closure of most educational institutions prompted the authorities to suggest adopting alternatives to traditional learning methods in emergencies to ensure that students are not left without studying and to prevent the epidemic from spreading. The traditional educational methods were replaced by e-learning when the COVID-19 virus appeared because social gatherings in educational institutions are considered an opportunity for the virus to spread. E-learning became the best option available to ensure that epidemics do not spread, as it guarantees spatial distancing[3].

The main components of e-leaning are computer technology and the Internet [4].Web-based education, digital learning, interactive learning, computer-assisted teaching and internet-based learning are commonly referred to as E-learning [5]. E-learning environments offer interactive features that increase the student's motivation for the learning process. E-learning is flexible when considering time, location, and health issues. It increases the effectiveness of knowledge and skills by enabling access to a massive amount of data, and enhances collaboration, and also

strengthens learning sustaining relationships [6]. However, the inadequate infrastructure becomes a major problem in the implementation of e-learning. Institutions that want to implement e-learning may have difficulties in the procurement of required infrastructure such as server/PC, storage, and network [3]. Besides inability to procure required infrastructure, not all of the institutions have the professional staff for designing and developing systems to manage e-learning systems. In addition, institution has to employ instructional designer who are the required experts for designing teaching materials. It is also noteworthy that institutions have to bear the cost of implementing and maintaining e-learning system. The thought of cutting the cost of infrastructure procurement and human resources for development and maintenance process of e-learning systems brought about the ideal of cloud computing where resources (hardware and software) are delivered as a service over a network (typically the Internet). With cloud computing technology, learners can access their tools from any computer, regardless of platform, as long as the computer is able to connect to the cloud.

Although cloud computing come as a solution which reduces the cost of designing, and implementing e-learning. It has among others a major drawback of vulnerability to security attacks. On one hand, transmission of educational material among the participants in the e-learning system using internet exposes the material to security attacks[2]. Cloud itself is a public place, if the cloud service provider decided to be dishonest, information stored on the cloud may be exposed to the unauthorized users. A good example of the vulnerability of cloud-based e-learning system to the cybersecurity attack is the security attack which lead to the closure of Abraham Lincoln's Namesake College (an institution that has existed for 157 years) in Illinois [7] in the year 2022. Many cloud-based e-learning systems have been designed. However, many of the existing systems either failed to consider the issue of security or consider access rights control as security measure without considering security of the data stored on the cloud. In this research work a secure cloud-based e-Learning platform through which students or learners could study offline and online is developed. The security of the proposed e-learning is achieved by developing a fast and secure cryptosystem for securing the e-learning materials being stored in the cloud so as to prevent unauthorized access even if the cloud service provider (CSP) decides to be dishonest.

II. MOTIVATION

The existing e-learning systems such as [8] and [9] did not consider security issue while [2] failed to take into consideration that cloud service provider where learning material are stored for easy access can become dishonest and thereby breach the confidentiality of the data stored on the cloud. Hence, existing e-learning system are still vulnerable to security attacks. A cloud-based e-learning system that employs the use of cryptographic techniques to encrypt data before they are stored on the cloud and also requires that decryption key be provided by the potential users who access the content of the cloud can solve the infidelity problem that may arise from Cloud Service Provider (CSP) since only the user who has access to decryption key can have access to the stored data. The quest to solve the infidelity problem of cloud service providers prompted this research work.

This paper is structured as follows: Section 2 presents related literature. In Section 3, architectural designs, system design and discussion of the implementation of the designs are presented. Experimental results and discussion of the results are presented in section 4 while Section 5 gives the conclusion.

III. RELATED WORKS

In this section related works on the existing cloud-based e-learning system is presented. The prediction made by Weiser in 1991 that there will be proliferation of computational resources where access to information at any place and time is possible [10] has indeed come to pass. There is now a wide range of computational devices such as mobile phones, personal digital assistants (PDAs), palmtops or laptops capable of wireless communication over the internet. Educational systems all over the world have seized the opportunity brought by this technological development to improve the way of disseminating knowledge. With these developments in technology, new avenues for learning outside of the traditional classroom, including asynchronous and distant

learning are now possible. However, educational institutions are now more defenseless to a broad range of cybersecurity risks because of this digital revolution. Cybersecurity attacks have been very rampant this days as the availability, confidentiality, and integrity of sensitive data are being jeopardized due to exposure to the unauthorized users[11]. Post COVID-19 era have witnessed more cases of breach of confidentiality[12] and privacy intrusion. Protecting sensitive data in e-learning environment is therefore very essential. Various techniques put up by researchers for protecting data on transit or storage include cryptography, steganography, watermarking, and a host of other measures.

REVIEW OF RELATED WORKS ON EXISTING CLOUD-BASED E-LEARNING SYSTEMS

The problem solving places (PSP) e-learning architecture for enhancing user's teaching-learning experiences proposed by[8] is not suitable for cloud-based e-learning unless the security measures are integrated into the architectural designs. [2] Proposes a framework at the Software as a Service (SaaS) level to complement the enhancement of the PSP-based e-learning system's user teaching-learning experience in a secure and efficient manner. However, the approach only consider security against unauthorized accesses. The security of the data stored on the cloud is not considered, consequently, if the cloud service provider who possess access right to the data on the cloud decided to be dishonest, confidentiality of the data stored on the cloud may be compromised.

A cloud security framework based on the trust module was introduced by [13]. A trust entity is a type of cloud service which aids in boosting the transaction rate in a cloud environment. Various security measures were developed for the purpose of protecting its users. Customers, who are the cloud's stakeholders, can have faith in a variety of cloud providers, and suppliers can have faith in their clients as well. The trust-based model was based on several characteristics, such as domain name, trust level, service kind, etc. The values of these attributes serve as the sole foundation for cloud users' reputations. The major drawback of this approach lies on the fact that if the CSP decide to be dishonest, the security of the system cannot be guaranteed.

The influence of the COVID-19 pandemic on Croatia's e-learning systems was examined by Ivan in 2021 [12]. Using the findings as a basis, a methodology for cyber threats detection which includes establishing a theoretical basis on Distributed Denial of Service (DDoS) and flash crowd event traffic, defining a laboratory test-bed setup for data acquisition, development of DDoS detection model, and testing the applicability of the developed model on the case study was proposed. Through prompt DDoS detection and other socioeconomic benefits like the creation of a focused study area, the application of the suggested methodology can enhance the effectiveness of the teaching process. Although this approach address the network anomalies, it did not address the security of the data stored on the cloud.

The design and implementation of cloud-based e-learning platform for scientific subjects where three core science subjects (physics, chemistry and biology) were used as test bed for in the research work, PHP (Hypertext pre-processor) programming language was used for server-side scripting, Action script and Macromedia-Flash were used for media content authoring and MySQL as the back-end database[9] proved to be an elegant application. However, the authors did not consider how the content of study material stored on the cloud can be secure from privileged users such as Cloud Service Provider (CSP).

OBSERVATIONS FROM THE REVIEW OF RELATED WORKS

It is observed from the review of related works on the existing cloud-based e-learning systems that the emphasis of the researchers has been on the detection of the anomalies in network security and prevention of the unauthorized access to the materials stored on the cloud. However, no effort has been made on the protection of the data stored on the cloud against privileged users such as CSP. The study of the existing lightweight cryptosystems also reveals that the existing techniques are not time and memory conservative. Hence, this research work, proposes a cloud-based secure e-learning system that employs a newly designed cryptosystem to secure data stored on

the cloud against attacks from the privilege cloud users.

IV. METHODOLOGY

In this section, a detailed description of the proposed secure cloud-based e-learning system is presented.

ARCHITECTURAL DESIGN OF THE PROPOSED CLOUD-BASED E-LEARNING

The proposed cloud-base e-Learning architecture is adapted from 5 layered cloud-based e-learning architecture proposed by [14]. Security layer is added to the existing 5 layers which make the proposed architecture have six layers which include (i) Infrastructure layer (ii) Platform layer (iii) Application layer (iv) Security layer (v)Access layer and (vi) User layer. The purpose of adding security layer is to ensure that privilege users such as cloud service provide cannot access the data stored on their cloud unless it has access to the encryption key. The following discusses the purpose of each layer in the proposed architecture.

(i) Infrastructure layer: Infrastructure layer contains architecture that supports virtual machine, cloud platform, virtual repositories and physical infrastructures such as servers, network devices, storage, buildings and other physical facilities. The layer shares Information Technology (IT) infrastructure resources and connects huge system pool together to provide services.

(ii) Platform layer: This layer hosts the operating system where e-Learning application will be running and other software that ensure the proper running of the application layer.

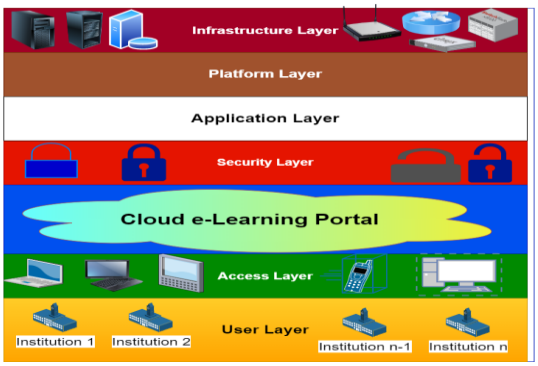

Figure 1: architectural design of the proposed secure cloud-base e-Learning system.

(iii) Application layer: This layer is a specific e-learning application that is utilized for sharing learning resources and interaction among users that includes synchronous or asynchronous discussion and chatting.

(iv) Security layer: The security layer is responsible for data security in the cloud. In this layer courseware that is to be stored on the cloud by an authorized user (instructor) are encrypted. When an authorized user (student/instructor) accesses the information from the cloud, the information has to be decrypted using the right decryption key before it becomes useful. The purpose of introducing this layer is to prevent privilege users (such as cloud service provider) who have access privilege to the cloud from using their privilege access to expose the contents stored in the cloud to unauthorized users. The design of the security layer is extensively discussed in section 3.

(v) Access layer: This layer is in charge of managing access to cloud e-learning services which is available on the architecture such as: types of access devices and presentation models. This study adopts the concept of multi-channel access which enables a variety of available services that are accessible through a variety of devices (such as mobile phones, smartphones, computer, etc.) and a variety of presentation models (such as mobile applications, desktop applications, and others). The purpose of the adoption of this concept is to increase the availability of devices that can access the services available on the cloud-based e-learning architecture used.

(vi) User layer: the user layer consists of various educational institutions

The system design is based on the proposed architectural design and the system flowchart in Figure 2.

DESIGN OF THE SECURITY LAYER OF THE PROPOSED CLOUD-BASED E-LEARNING SYSTEM

A cryptosystem is proposed for data security in the proposed e-learning system. This section details the architectural design of the proposed cryptosystem.
The components of the architectural design of the proposed cryptosystem comprises of key generation algorithm, block manipulation module, Encryption module, the Encryption Process and the Decryption process as shown in Figure 4.

Key Generation Algorithm
The key generation algorithm will ensure that both the sender of the information and the recipient of the information generate the same secret key without the knowledge of the public. Elliptic Curve Diffie-Helman (ECDH) key exchange algorithm whose process is illustrated in Figure 3 and the design presented in Algorithm 1 is employed in the key generation algorithm

Algorithm 1: Key Generation Module

Keygeneration (curvename, G, n, a, b)
START
A randomly selected number n_s where n_s is in interval 1 to $n-1$ and n is the order of subgroup of the elliptic curve (curvename) points, generated by the generator point G of the elliptic curve curvename whose equation is given by $Y^2 = X^3 + aX + b$ where a and b represents the constants in the equation of the elliptic curve curvename
GENERATE public key $p_s = n_s * G$. p_s is calculated after performing point doubling and point addition operations on the point G, n_s number of times. Basically, $n_s * G = \{G \oplus G \oplus G \ldots \oplus G\}_{n_s\ times}$ where $\oplus$ is point addition operator.
Steps 2 and 3 are repeated twice as sender and recipient are involves. Thus, for the sender n_s and p_s are generated as private and public key respectively while for the recipient n_r and p_r are generated as private and public key respectively.
Calculate the shared secret key SSK by both the sender and recipient using the publicly available key of the other user. The sender calculates the SSK using the equation
$SSK = n_s * p_r = n_s * n_r * G$
The recipient calculates the SSK by using the publicly available sender's public key
$SSK = n_r * p_s = n_r * n_s * G$
Return SSK
STOP

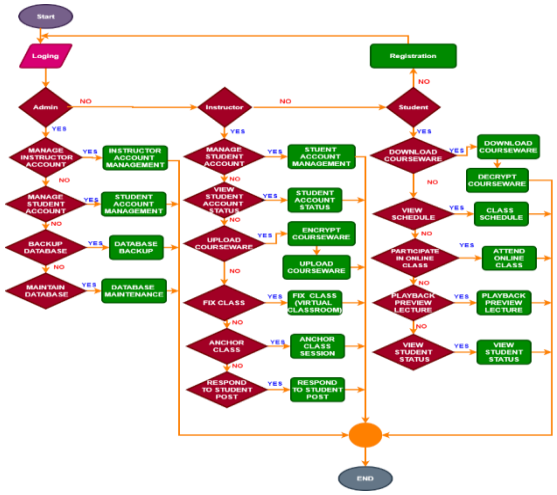

Figure 2: System flowchart of the proposed secured cloud-based e-learning system

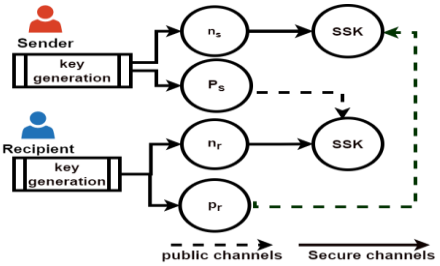

Figure 3: Key generation Process in the proposed Cryptosystem

Block Manipulation Module: The purpose of this module is to eliminate the use of substitution box (S-box). The module accepts a block of binary data of n bits and SSK generated from Algorithm 1 as input. Bit grouping, bit permutation and exclusive-or (XOR) function are applied to achieve non-linearity, confusion and diffusion properties. Figure 3a depicts the block manipulation module of the proposed

cryptosystem. The design of the block manipulation module is presented in Algorithm 2.

Encryption Module: Encryption module is applicable to both encryption and decryption processes. The encryption module is responsible for transforming the input plaintext/ciphertext into unreadable/readable form. Figure 3b depicts the encryption module in the proposed cryptosystem. The encryption module takes shared secret key SSK, the hash value hashval, and the plaintext/ciphertext inpdata as input and produces ciphertext/plaintext outdata as output. Algorithm 3 represents the design of encryption module.

Encryption / Decryption Process: The encryption process is responsible for transforming the plaintext data into ciphertext data while the decryption process transforms the ciphertext data into plaintext data. Both processes use encryption module to achieve their goals. Figure 3c and 3d depict the encryption and decryption processes in the proposed cryptosystem. The sender carries out encryption process while the recipient carries out decryption process. Algorithm 4 and Algorithm 5 represent the design of encryption and decryption processes respectively.

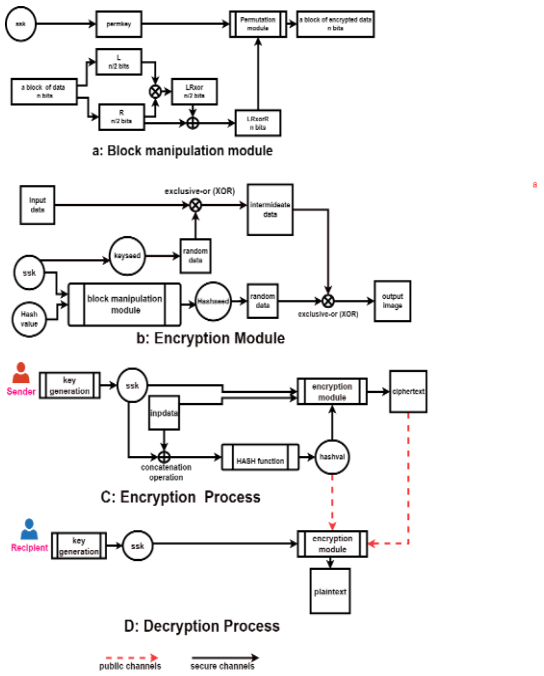

Figure 4: Architectural design of the proposed binary file lightweight cryptosystem

Algorithm 2: Block Manipulation Module

Inputs:

Block: array of binary digits of size n

SSK: Shared Secret key between the sender and the receiver

START

Accept a block of data block of size n bits

Accept the share secret key SSK

DIVIDE the block of data of n bits into two equal parts L and R each of size (n/2) bits such that $L = block\left[1 \ldots \frac{n}{2}\right]$ and $R = block\left[\frac{n}{2} + 1 \ldots n\right]$

COMPUTE $xorbit[i] = L[i] \otimes R[i] \quad for\ 1 \le i \le \frac{n}{2}$ where $\otimes$ represents the exclusive-or(XOR) operator

COMPUTE $xorbitR = xorbit \oplus R$ where $\oplus$ represents the concatenation operator

GENERATE an array $permkey[1 \ldots n]$ of random integers using SSK as seed

COMPUTE $encbits[i] = xorbitR[permkey[i]] \quad for\ 1 \le i \le n$, where encbits represents the array of bits of the encrypted block

STOP

Algorithm 3: Encryption Module

Inputs:

inpdata: the text to be transformed it may be plaintext or ciphertext

SSK: Shared Secret key between the sender and the receiver

hasval: the hash value computed from the concatenation of the plaintext and SSK

Output:

outdata: the transformed text it may be ciphertext or plaintext

1. START
2. ACCEPT inpdata, SSK and hasval as input data
3. COMPUTE the size of inpdata in bits as dsize
4. GENERATE a random number kseed using SSK as the seed
5. GENERATE array of random bits $randata[1 \ldots dsize]$ using kseed as seed
6. COMPUTE hashseed using SSK and hasval as input to Algorithm 2
7. GENERATE array of random bits $hashrandata[1 \ldots dsize]$ using hashseed as seed

8. COMPUTE
$interdata[i] = randata[i] \otimes inpdata[i] \quad for\ 1 \le i \le dsize$
where $\otimes$ represents the exclusive-or(XOR) operator
9. COMPUTE
$outdata[i] = hashrandata[i] \otimes interdata[i] \quad for\ 1 \le i \le dsize$
where $\otimes$ represents the exclusive-or(XOR) operator
10. STOP

Algorithm 4: Encryption process

Inputs:
inpdata: plaintext to be transformed to ciphertext
SSK: Shared Secret key between the sender and the receiver

Output:
hashval: the hash value computed from the concatenation of the plaintext and SSK
ciphertext: encrypted data
START
ACCEPT inpdata and SSK as input
COMPUTE $catdata = inpdata \oplus SSK$ where $\oplus$ is the concatenation operator
Pass the numerical representation m of catdata into a hash function to produce an hashed message $hashval = hashfunction(m)$
COMPUTE ciphertext using inpdata, SSK, and hashval as input to Algorithm 3
STOP

Algorithm 5: Decryption process

Inputs:
inpdata: ciphertext to be transformed to plaintext
SSK: Shared Secret key between the sender and the receiver
hashval: the hash value computed from the concatenation of the plaintext and SSK
Output:
plaintext: decrypted data
START
ACCEPT inpdata, hashval, and SSK as input
COMPUTE plaintext using inpdata, SSK, and hashval as input to Algorithm 3
STOP

3.3 DESIGN AND IMPLEMENTATION OF THE PROPOSED CLOUD-BASED E-LEARNING SYSTEM

This section gives the details of the choice of programming language used for the implementation, input and output design, hardware and software requirement for the implementation of the proposed e-learning system.

Choice of Programming Language
Python programming language was used for the simulation of the proposed cryptosystem. However, only design consideration is considered in the case of the proposed secured cloud-based e-learning system.

Input Design
The user (admin, instructor, or student) interaction with the system begins with the login form to collect the user's login credential and validates against the database. The credential are verified and validated by determining the roles each user can play in session. After a successful access to the system the application presents a portal which serves as the dashboard to the user. From here, the user can continue interaction with the system based on the predefined role. New users can find a link to a register and login to the system.

Output Design
The system presents information to users based on their roles. New users can get a confirmation or error message during the course of registration. The student can view or download courseware or participate in a live virtual classroom anchored by the instructor. The instructor can view report of number of student participating in the class session and also responds to questions or comments. The outputs are presented through monitor/display screen for softcopy, speakers for audio output, and printer for hard copy.

Implementation Requirement
This section discusses the requirement for the successful implementation of the proposed e-learning system. Hardware and software requirements are discussed.

Hardware Requirement

The cloud service provider that can be used for the hosting of the proposed e-learning system must have high computational capacity (Central processing unit (CPU)) in order to be able to handle large client requests and multimedia processing and large volume of storage devices in measure of terabyte (TB) to host large media files, large bandwidth to handle traffic or high contention. However, the clients/users (the admin, instructors and students) accessing the solution should have the following minimum requirements

- A multimedia ready personal computer (PC), mobile phone, or Personal Digital Assistant (PDA).
- A small dedicated server (not compulsory)
- Digital Camcoder/Camera to capture video
- Headset/Speaker to play sounds
- A modem/DSL for internet connection
- A microphone to capture audio

Software Requirement

The cloud provides the software platform for the running of the application. However, the user/client system should have the following:

- Windows, linux, or machintos operating system,
- Browser with flash player
- Macromedia flash for media processing

plaintext	'Several attempts have been made by researchers to overcome the weaknesses of conventional Playfair ciphers. A 6 × 6 matrix was proposed by[20] instead of 5 × 5 the conventional playfair cipher. The construction of the matrix key is similar to that of conventional technique but with a larger set of alphabets. This matrix is large enough to accommodate numerical digits (0 to 9) in addition to 26 English alphabets in the classic technique. In addition, the I/J was counted as two separate letters and each is placed in separate cells in order to avoid ambiguity at decryption time. Similarly, [9] proposed a 7 x 4 matrix key Playfair cipher where two symbols and were added to create a one-to-one correspondence between plaintext and ciphertext A DNA and Amino Acids-Based Playfair Cipher algorithm where the user is capable of using any combination of alphabets, numbers, special characters, or even spaces in a plain-text was proposed by [21].'
Encrypted text	b"\xddXN|\xee\xb6E\xc8~4\x95J\x9d\xf1\x88\x06\xa7!\xd3wd\x8d\x03\x0b\x14\xf9\xac\xdf\xd8& \x89\xe4f_Yi\xaa,\xb8u\\\xa4\xb8\x03\x92*\xfb\xbc\xe1V\x87\x01\xa6@\x81\x13\xa7@\x8c\x08__\x9fY\x8d\x83\xe4\xa6\xd0bthb\xb7\x9b\x00?\xe8\x99\xc2(\xf3AJ\xe1sb!\x07\xf9!)\xdf\xcd\x83^#\x1c\xa9\xf8\x8b\xe1\x99Lw$\xd8fO\xbb\x1b\xf0\xf1\xc5\xb4\xef8\xf9U\xf2\x1a\x9f \xb3\xd6\x9c\x186\xbfo\xfa\xcc`\xe7\x82KP\x8bw\xa7\xe69\xd2}\xbd\xfbY\x0b\x83\xb8s\xfb\ xef\xd8\xa2):`\x12.\xb9\xa0\xa1\xe83\xa8\x9a\xc6\xf1i*\'\xeeo\xb2)C\x8b)\xea&\x90\xb2\xbc\ x17g\xa3\x94s\x1e\xe0\xff\xbfd\xa9\xf7\xb2\xd2\xa2*\xd1\x87>\x02\xb5#\xe5\xce3\xd1\xa3N \x82\xe4\xa3\x144\x86\xa3XJ\xfat\x83\x0c\x97\xefK\xb3wv\xa5\xd5W\xba\xd2\xee\xbdoJ\x8 e\x85g]\xaeh\xf7\xe7\xc9\xc4\xae\xd0\x9dhcKI\x1e\n\xd8\xed\xc2g\x04\x1e\xd6\xddVoKS\x0 e\xf0im\x98\xf3\xbd\xe0\x93\x08\xd4`\xffxH\x9e\x1d\xba)\xf9\|!Y^\xd8\x01\xe3\x98\x84\xb2\ xecaB\xf4\xad\xa3\xd4\xbf\xca\xcf\xbe\xbbq\x01\x01\xfcd*\xfc\x97cdu\xd2\x8d\x01\xd0ZYC WYY\xb1,,\x07:\xcd\xb6YS\xb9:(B\x1b\xa8\xea\xb1\xee\xb3\xa3,v\t\xc7#\xc8\x94\x06\xbf\xb d\xca\xeb:\x1c_m\xd7\x1546}F\x1egh\xe2\xb4\x88W\xd0\x00\x08\x8ca\xc4U\xa5\x92M\x149 \x86\xacx\x1e\x1e\xc7%\x81\xdcL4\xdcN\x9bd\xea\xf4\xaa\xf1\x85\xf2\x01\x80\xe2\xd6I{y8\ x8d\xb3G\xc44_\xb4\x8b\x871G\xca\xaa\xec\x9b\x04\x8afG\xa0\xad+\xf5\x05\xbf\x96\x9e\x1 3\x9c\x14\xda(\xf1z~O\xfd\x0e\xb7H\xc9\xff\xf7Sl\x8b\n\r[I\x12&\xea(\xe2\x97\x8c(\xf4aI\xd 6\xc7$\x0c\x9fp\xc3,o\xf1\x08\xfc;W\xb3\x8cH\rS\x91[\xd7\x968\xbf\x06\xab\x1e\x02"\x9b|,\ xc8\x81\xb1\x86\x14\xb0\x14<\xfd\xc7u\x90|}\xdfy\x0f'
Decrypted text	b'Several attempts have been made by researchers to overcome the weaknesses of conventional Playfair ciphers. A 6 \xc3\x97 6 matrix was proposed by[20] instead of 5 \xc3\x97 5 the conventional playfair cipher. The construction of the matrix key is similar to that of

	conventional technique but with a larger set of alphabets. This matrix is large enough to accommodate numerical digits (0 to 9) in addition to 26 English alphabets in the classic technique. In addition, the I/J was counted as two separate letters and each is placed in separate cells in order to avoid ambiguity at decryption time. Similarly, [9] proposed a 7 x 4 matrix key Playfair cipher where two symbols and were added to create a one-to-one correspondence between plaintext and ciphertext A DNA and Amino Acids-Based Playfair Cipher algorithm where the user is capable of using any combination of alphabets, numbers, special characters, or even spaces in a plain-text was proposed by [21].'

V. RESULTS AND DISCUSSION

Simulation of the proposed cryptosystem for securing data to be stored on the cloud of the proposed cloud-based e-learning was carried out on a laptop with the following specifications:

Processor Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz 2.40 GHz
Installed RAM 4.00 GB (3.86 GB usable)
Device ID 11E0C8DD-31FB-4E73-AC83-7B34FE5EBE7A
Product ID 00331-10000-00001-AA962
System type 64-bit operating system, x64-based processor

The Scientific Python Development Environment, Copyright © 2009-2020 Spyder was used throughout the development and analysis.

SIMULATION RESULTS OF THE PROPOSED CRYPTOSYSTEM

Samples of plaintext are encrypted using the developed cryptosystem and the resulting encrypted data are decrypted to ascertain whether the plaintext can be obtained from the encrypted data. A sample of the results obtained is presented in Table 2. Note, for the purpose of visual inspection, the encrypted and decrypted data is represented in byte form.

Table 2: Sample of plaintext, encrypted text, and decrypted text using the proposed cryptosystem

By visual inspection, it can be seen from Table 2 that the encrypted text is completely different from the input plaintext and the output decrypted text. It can also be seen from Table 2 that the plaintext and decrypted text are similar. These results reveal that the proposed cryptosystem is capable of preventing the unauthorized person from having access to the content of the data stored or on transit. Also the result reveals that authorized user who has the key can obtain the complete contents of the encrypted data stored or on transit.

CONCLUSION

In this paper a preliminary prototype of an e-learning architecture where and an additional layer, namely security layer is added to the architecture proposed by [14] is presented. The purpose of adding security layer is to ensure confidentiality of the data being stored on the cloud even if the CSP chooses to be dishonest. The presented system offers a new tool for addressing real-world security challenges in cloud-based e-learning system. In future, implementation of the design of the proposed e-learning system as well its security analysis will be carried out.

REFERENCES

[1] O. K. Boyinbode and R. O. Akinyede, “MOBILE LEARNING : AN APPLICATION OF MOBILE AND WIRELESS TECHNOLOGIES IN NIGERIAN LEARNING SYSTEM,” Int. J. Comput. Sci. Netw. Secur., vol. 8, no. 11, pp. 386–392, 2008.

[2] A. Ahmed, M. A. Haq, N. Polala, V. Shankar, and J. Gyani, “CBES: a framework for cloud-based e-learning system at SaaS level,” Int. J. Comput. Sci. Netw. Secur., vol. 22, no. 11, p. 651, 2022, doi: 10.22937/IJCSNS.2022.22.11.92.

[3] A. M. Maatuk, E. K. Elberkawi, S. Aljawarneh, H. Rashaideh, and H. Alharbi, “The COVID - 19 pandemic and E - learning : challenges and instructors,” J. Comput. High. Educ., vol. 34,

no. 1, pp. 21–38, 2022, doi: 10.1007/s12528-021-09274-2.

[4] E. Aboagye, J. A. Yawson, and K. N. Appiah, "COVID-19 and E-learning: The Challenges of Students in Tertiary Institutions," Soc. Educ. Res., vol. 2, no. 1, pp. 1–8, 2020, doi: https://doi.org/10.37256/ser. 212021422.

[5] I. Yengin, A. Karahoca, and D. Karahoca, "An E-learning success model for instructors' satisfaction in the perspective of interaction and usability outcomes.," Procedia Comput. Sci., vol. 3, pp. 1396–1403, 2011, doi: https://doi.org/10.1016/j.procs.2011.01.021.

[6] K. Mukhtar, K. Javed, M. Arooj, and A. Sethi, "Advantages, limitations and recommendations for online learning during COVID-19 pandemic era.," (COVID19-S4l 36, pp. COVID19-S27-S31., 2020. doi: https://doi.org/https://doi.org/10.12669/pjms.36.COVID19-S4.2785.

[7] K. Townsend, "Ransomware Attack A Nail in the Coffin as Lincoln College Closes after 157 Years," Security Week, 2022. https://www.securityweek.com/ransomware-attack-nail-coffin-lincoln-college-closes-after-157-years/ (accessed Aug. 26, 2024).

[8] A. K. Mohammed and A. Ahmed, "E-learning Environment with Problem Solving Places for Teaching and Learning of Algorithm Oriented Concepts," in IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies –ICCICCT, Noorul Islam University, India, 2014, pp. 17–20.

[9] O. Oludipe, O. K. Fatoki, N. A. Yekini, and E. E. Aigbokhan, "Cloud-Based E-Learning Platform : From the Perspective of ' Structure ' and ' Interaction ,'" Int. J. Innov. Res. Educ. Sci., vol. 1, no. 1, pp. 1–6, 2014.

[10] E. Tuncay, Effective use of Cloud computing in educational institutions. 2010.

[11] B. Ogheneovo, F. Obukohwo, M. Dumebi, E. Bassey, R. E. Ako, and A. A. Ojugo, "Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech)," J. Sci. Technol. Res., vol. 6, no. 2, pp. 293–311, 2024, doi: https://doi.org/10.5281/zenodo.12617068.

[12] I. Cvitić, D. Peraković, M. Periša, and A. D. Jurcut, "Methodology for Detecting Cyber Intrusions in e-Learning Systems during COVID-19 Pandemic," Mob. Networks Appl., 2021, doi: doi.org/10.1007/s11036-021-01789-3.

[13] W. Li, L. Ping, and X. Pan, "Use Trust Management Module to Achieve Effective Security Mechanisms in Cloud Environment," in IEEE International Conference on Electronics and Information Engineering, 2010, pp. VI14-VI19,.

[14] N. Selviandro and Z. A. Hasibuan, "Cloud-Based E-Learning : A Proposed Model and Benefits by Using E-Learning Based on Cloud Computing for Educational Institution," ICT-EurAsia 2013, pp. 192–201, 2013.