Journal of Cyber Security
DOI:10.32604/jcs.2021.022112

Tech Science Press

Article

Securing Fog Computing For E-Learning System Using Integration of Two Encryption Algorithms

Hind A. Alshambri[1,*] and Fawaz Alassery[2]

[1]Department of Information Technology, Taif University, Al-Hawiya, Taif 21974, Saudi Arabia
[2]Department of Computer Engineering, Taif University, Al-Hawiya, Taif 21974, Saudi Arabia
[*]Corresponding Author: Hind A. Alshambri. Email: S44080243@students.tu.edu.sa

Received: 14 September 2021; Accepted: 23 September 2021

Abstract: Currently, the majority of institutions have made use of information technologies to improve and develop their diverse educational methods to attract more learners. Through information technologies, e-learning and learning-on-the go have been adopted by the institutions to provide affordability and flexibility of educational services. Most of the educational institutes are offering online teaching classes using the technologies like cloud computing, networking, etc. Educational institutes have developed their e-learning platforms for the online learning process, through this way they have paved the way for distance learning. But e-learning platform has to face a lot of security challenges in terms of cyberattacks and data hacking through unauthorized access. Fog computing is one of the new technologies that facilitate control over access to big data, as it acts as a mediator between the cloud and the user to bring services closer and reduce their latency. This report presents the use of fog computing for the development of an e-learning platform. and introduced different algorithms to secure the data and information sharing through e-learning platforms. Moreover, this report provides a comparison among RSA, AES, and ECC algorithms for fog-enabled cybersecurity systems. These Algorithms are compared by developing them using python-based language program, in terms of encryption/decryption time, key generations techniques, and other features offered. In addition, we proposed to use a hybrid cryptography system of two types of encryption algorithms such as RSA with AES to fulfill the security, file size, and latency required for the communication between the fog and the e-learning system. we tested our proposed system and highlight the pros and cons of the Integrated Encryption Schemes by performing a testbed for e-learning website scenario using ASP.net and C#.

Keywords: Fog computing; information security; integrated encryption; RSA; AES; ECC; e-learning systems

1 Introduction

E-learning where students use the web and other Internet technologies to enhance learning and teaching experiences. E-learning users often focus on the benefits one gets from e-learning based on its purpose, which is teaching and learning. Several e-learning institutions began ICT adoption with no care plan and understanding the related security concerns. E-leaning is the new method in which e-learning ultimately depends on the Internet for functionality. The Internet has become a venue for the e-learning environment. E-learning development has led to subsequent new ways of learning, as well as opportunities in learning. The new learning methods have become part of human lives hence helping students excel in their learning [1].

The world's education systems have witnessed unprecedented disruptions this year due to the Coronavirus pandemic. Most of the world's schools and universities have closed their doors to more than 1.5 billion students, according to recent figures released by the UNESCO Institute for Statistics. Education experts agreed that education after COVID 19 will not be the same as before, especially with the emergence of a highly automated infrastructure that uses cloud computing and artificial intelligence systems. There are expected major and structural changes in education patterns, methods, trends, and policies, whether at the general or university education level. Signs of these shifts are already emerging. One of the most prominent transformations in education in the post-COVID 19 era, and we have begun to touch on some of them. It is a strongly rising trend towards the use of advanced technologies to create more portals and platforms for the various stages of education, especially after these technologies proved their effectiveness in the early spread of the pandemic.

Over time, e-learning systems have received much interest because of their wide application in distance education. A vast data amount has continuously been shared among the students, examiners, and teachers who need to exchange these data privately. E-learning being supported by the Internet, has attracted an equal measure of illegal activities like security threats, and its outcome has affected the potential of information sharing and management. The e-learning systems need to be secure so that the sharing process is protected against several security attacks. The exam contents such as quizzes, answer sheets, and tests. Security of the e-learning systems will attract authentication mechanisms for the users as well as the fog server or trusted servers, the session ley establishment protocols that set up the keys needed for specific periods like exams, seminars, or classes. There will always be a need for maintaining the trust level and authentication level, which enable regular legitimacy checks for the students. To ensure the security reliability of e-learning systems, the process of analysis of security is done to define the advantages and disadvantages of security schemes [2].

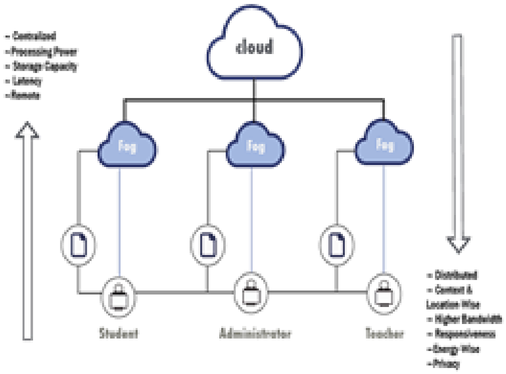

Figure 1: The use of fog computing in e-learning

The new promising model of computing is fog computing where it expands cloud computing to the edge of networks, offering applications that are closer to consumers and that are closer to end-users. Although such applications are profusely available these days, they still lack what are so-called features of data security. Developers do not have adequate options that can be comprehensively checked. Data encryption is considered one of the most common techniques utilized and used to ensure the security of data and the privacy of data. Two phases of the adaptive dynamic scalable model are then suggested, in which the device dynamically selects an encryption method based on the frequency of access of the encrypted data. In the event of regular access to data, the adopted model will then choose the appropriate and effective algorithm with reduced additional complexity. Over the next stage, by deciding the size of the encryption key, the model will use a customizable technique to estimate the security level required. To automatically encrypt more sensitive data, a stronger code is again used by the crypto algorithm. and a smaller code can be used to secure common or even less important information to protect the fog node from cryptographic exhaustion. Therefore, Cloud storage a cost-effective solution for delivering services to process, analyze, and store data. One of the problems that make it a challenge to ensure adherence to some of the specifications of IoT systems, including location-based services, usability, and reduced power, is the cloud computing network architecture. To provide low latency, location-aware wireless communication, fog computing aims to follow a heterogeneous range of devices such as laptops, routers, mobile phones, etc., that are distributed in various geographical locations as fog nodes.

Fog Computing vs. Cloud Computing

On-demand computing service delivery is known as cloud computing. We can also use services over the Internet for data storage capacity. Everyone could gain connections to everything from applications to storage from a cloud service provider without possessing any network infrastructure or any storage systems. However, fog computing is considered a decentralized infrastructure or method of computing where computing resources are located between the cloud or some other data center and the data source. Fog computing is a model that delivers services on edge networks to user requests. Fog layer devices normally perform network-related operations such as routers, gateways, bridges, and hubs. Moreover, Table 1 shows the main differences between fog computing and cloud computing.

Table 1: Difference between fog and cloud computing

Feature	**Cloud computing**	**Fog computing**
Latency	High	Low
Capacity	Data on cloud computing does not decrease while transferring or sending it	Data on fog computing decrease when sending it to cloud computing
Responsiveness	Time to response is low	Time to response is high
Security	Less security than fog computing	High security
Speed	Depend on the VM connectivity	Higher speed
Data integration	Data integration on multiple data	Data integration on multiple data and devices
Mobility	Limited mobility	Mobility supported
Location Awareness	Partially supported	Supported
Number of server nodes	Number of server nodes are few	Number of server nodes are more
Geographical distribution	Centralized	Decentralized and distributed
Location of service	Service provided within the Internet.	Service provided at the edge of the local network
Working environment	Specific data center building with air conditioning systems	Outdoor or indoor
Communication mode	IP network	Wireless communication WALN, WIFI, 3G, 4G, 5G, etc.
Dependence on the quality of core network	Requires strong network core	Can also work in weak network core

In short fog computing offers more suitable services for the e-learning process so it is the need of the day. On the other hand, due to extended fog computing nodes, this system is more vulnerable to cyber threats. To secure the institutional as well as student data a well-designed algorithm is required. In this regard, three algorithms RSA, AES, and ECC passed through comparison. Unconditional security in terms of cybersecurity can only be achieved through symmetric as well as asymmetric encryption [2]. Now, most of the global network security organizations are using RSA, AES, and ECC algorithms for data encryption/decryption in terms of security.

2 Related Work

2.1 E-Learning Services Growth and Development

Technological use for supporting learning and teaching began in the 1980s. This happened at the time when computers were disseminated for personal use. The emphasis on electronic-enabled learning was designed to help the learners understand the functionality of the computer systems, but currently, the technological perspective has become just a means through which learning, and teaching can be facilitated.

This method was important in facilitating long-distance education based on the traditional education model or training. Before 1983, teachers used dominant teaching tools that were widely available for interaction and instructions that took place in a class setup. Between 1984 and 1993, the technological innovations provided the multimedia that was important in dynamic presentations and breaking the classroom interactions. Between 1994 and 2000, web infancy provided the introduction of emails, streaming of videos, and media players, which provided the earners and teachers the ability to access notes and learning materials. Finally, 2001 and beyond provided the next-generation web, which provided advanced website designs, high bandwidth, and rich streaming of media hence revolutionizing the educational means of delivery and interaction [3].

2.2 Importance of E-Learning

E-learning offers everyone an opportunity to learn. The aspect of learning anytime and anywhere enhances life-long learning and the ability to eliminate the problems that are related to distance learning. E-learning flexibilities provide the students with the core motivation factors which help in choosing the student’s course. Technology use for learning provides the ability for improved learning quality, improved access to training and education, reduced education cost-effectiveness. E-learning is a well-designed, engaging, affordable, learner-centered, interactive, flexible, easily accessible, and efficient means of meaningfully distributing and facilitating an e-learning environment. E-learning enhances access to learning materials and helps the students in widening access to some limited resources through the elimination of barriers that are socio-economic-based or individual so that learners can lead their life-long learning. Improved communication links and better access to learning by the learners to improve participation because e-learning platforms allow learners to communicate with their peers or have private forums that can influence their learning positively. E-learning provides fast delivery of assessments so that the lecturers provide fast feedback, and the students contribute to the feedbacks with ease [4].

2.3 Information Security in E-Learning

E-learning depends on information and communication technologies meaning that networks, storage, and retrieval capabilities and the sharing and distribution of information will be essential. This fundamental equipment led to several security risks that often compromise information due to loss of confidentiality, integrity, or availability. There has been an emphasis on the content and technological challenges that deter the successful implementation of security in e-learning environments. Security is essential because, in e-learning, information that is derived from user data is the key assets of the organization. Some of the security concerns in e-learning include confidentiality and user authentication. learning functionality has expanded so that information needs to be protected to avoid the loss of availability, integrity, and confidentiality.

The operations and security threat to e-learning has similar characteristics with other electronic services, and the approaches used for management could have similar features. For the organizations to protect and optimize their investment returns in their learning technologies, then the systems, content, and services must be interoperable, manageable, usable, and durable. This is because the high-cost barriers or the greater task levels need to be done, but the security aspects are still intangible in the cyber world [5].

2.4 E-Learning Management Mechanisms

Diverse management mechanisms are helpful in the mitigation of risks, avoiding or limiting the risks through the implementation of appropriate means of security. Not every threat shall be avoided but rather the associate problems can be eliminated. The management mechanisms that are introduced must consider the negative effects of the actual tasks of the system. Security management mechanisms shall assist in protecting the tasks of the e-learning systems, the organization and structuring of the systems will help in ensuring the flexibility and functionality of the system is well done. The system complexity, physical interconnections, user acceptance, and usability, and possible side effects which could affect other system components must be dealt with in an e-learning system to ensure that the services provided through them are working as expected [6].

2.5 E-Learning Service Goals

There is always a need for security consideration in e-learning systems. There exists no absolute security for the e-learning systems, but the objectives of the systems will help in realizing how security shall be deployed. This shall include the needs like architecture, security concepts, implemented features, and the programming languages used in making the system. The objectives must seek to satisfy the following: first is the e-learning systems criteria of identification whereby the interdisciplinary field shall be easily extracted, and specific issues examined with the respect to mutual influence on the research aspects. Secondly, the threats analysis and case studies demonstration should be realized whereby the criteria and the dependencies must consider the beginning of the threats analysis and expose them before they affect the e-learning systems. Finally, it must develop recommendations to ensure technical manageability and technical deployment usability [4].

2.6 Complexity and Character of E-Learning Systems

E-learning systems will go a long way in supporting the learning process. Several constructivist theories of learning will cause the demand for a high degree of freedom which includes comes mechanisms of evaluations and implementations can only be solved by dynamic web-based systems. An increase of the interactivity of the systems will raise the elements of integration which may slow the systems or use several security loopholes. The flexibility of the teacher while using the e-learning system is important to ensure effectiveness and efficiency for both the learner and the teacher. Therefore, all these must be well managed to ensure that the e-learning system is well balanced to deal with every challenge while ensuring that the systems are running smoothly [3].

2.7 E-Learning Security

E-learning environment security needs to avoid such threats as modification, interception, fabrication, and interruption. Security research has provided policies, identity, and intellectual property as ways to provide security to the e-learning environment. Avoiding attacks in e-learning environments requires control of access as the main way. Controlling access can be done through authentication and authorization, which identifies the legal user process that helps in overcoming illegal application use. Systems that are heavily secured are often difficult to access by legitimate users meaning that there is a need for balanced access and security. Access control by use of some technology devices is often considered inadequate because the attacks do not come from the outsiders but rather from the insiders also. The proper supervision of how information is handled is an important aspect that ensures vulnerabilities or loopholes are not created so that the management of information security is successful and consequently ensures e-learning security is implemented well [6].

2.8 Fog Computing Architecture

Cloud fog computing offers a decentralized form of applications and on-demand services that are useful in the management and analysis of big data on the network edge. Fog computing offers storage, controlling, processing, and networking. The fog layer assists in service as the intermediaries in the middle of the cloud and the device being used. Fog-enabled systems need vital architectural needs that can apply to several vertical markets. There has not been a standard for fog computing architecture; therefore, it can be classified as the device layer, the fog layer, and the cloud layer [7]. Fog architecture classification contains the data layer, the core network, and the service layer, and the device layer having communication technologies. The core layer can provide the management, network, and others to its end-user. They include fog nodes like base stations, routers, bridges, gateways, and switches, which are helped by the computing resources, and the local servers, which contain cameras, embedded computing, controllers, and smart phones. The network connection is important in deploying the fog nodes wherever they are required. Infrastructure owners provide data centers that are accountable for the multi-tenant virtualization infrastructure useful for flexibility, and improved operation power and storage, including other services that help in the sharing of needs with the user demands [8].

2.9 Security Needs for Fog-Enabled E-Learning Systems

Fog-enabled systems are getting applied in many fields of life because their networks are smart and are anticipated to be naturally remote for communication of wireless connection for communication with other fog done. Wireless communication mediums have vulnerable network attacks through eavesdropping and the like. Often, the most vital security features concerning data security include integrity, confidentiality, and availability. Integrity describes the completeness of data and the accuracy of the data [9]. Data availability and its resources ensure that network services provisioning, as well as the data determined for authorized users when needed. Fog-enabled systems without these decisions cannot do the things that are helpful because it lowers the chances of compromise by the attackers. Another system's security factor includes the lack of standardized security, and several system devices are made by diverse vendors, and the device's security is lacking in the accepted standards of these industries. This is because several system security errors single out the fact that no single framework has been agreed upon [10].

2.10 Fog Computing Security Challenges

Several weaknesses are depicted while protecting computing frameworks and storage from unauthorized access. Fog-based architectures are often considered more secure compared to cloud architectures because of numerous causes, which include lower dependencies on the Internet and the likely information as well as storage exchanges amid the cloud and the users in non-real-time. The fog-enabled systems use diverse interconnection networks of every partaking device like the wireless and mobile core networks, which makes them probable attack points [11]. Network monitoring is important in the detection of anomalies and detection of security vulnerabilities. This means that analysis of the most critical layers is important for the fog-enabled systems whereby the core-infrastructures are done by similar individuals who manage the locations of the system. Virtualization infrastructure in the data centers is possible to be incorporated to help in the deployment of the network edge while the biggest threats of the e-leaning systems attack the virtual machines [12].

From the real world, data centers include virtualization server's hub together with other managerial service controls, but based on security perspective, the entire network edge of the data centers are at risk as they include public APUIs, which cause the provision of services to the connected users as well as the other web applications. The challenges of fog security are shared into core-network and service-level security, device-level security, as well as data center level security [13].

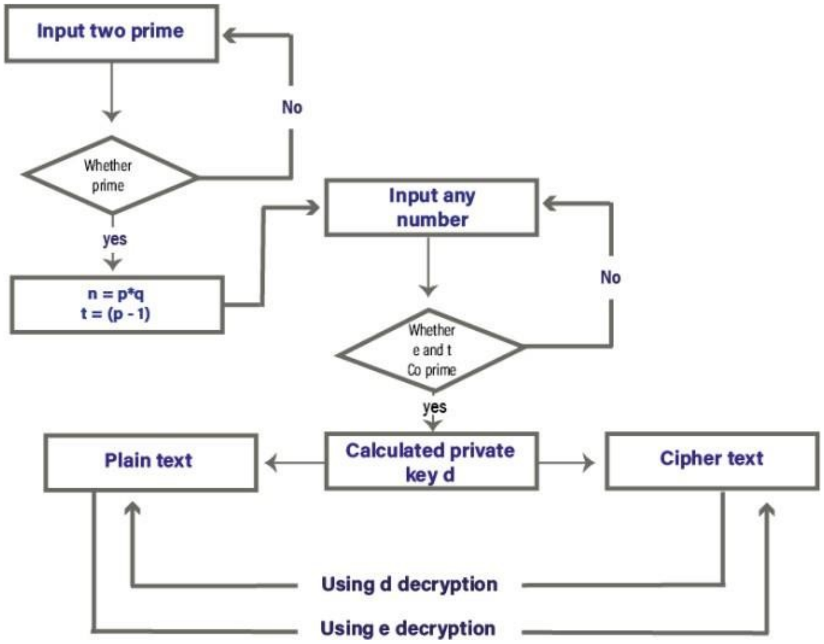

Figure 2: Encryption/Decryption on RSA

2.11 Algorithm Suggestion for Fog-Enabled E-Learning Systems

Fog enables e-learning platforms that cannot allow a third party to do encryption/decryption for data security for fog nodes. Fog computing must be installed a well-designed algorithm to ensure a secure communication process. Each fog node would be factory customized with a shared as well as a cryptographic algorithm that enables direct and secure communication among nodes. Without considering the distance between the network nodes or other security protocols. These algorithms are capable to perform independent encryption and decryption at different nodes for the key generation process [14].

3 Methodology

The use of technology in learning offers the potential to improve the quality of learning, improve access to training and education, and reduce the cost-effectiveness of education. Lack of hardware and software security designs and limited resources makes e-learning systems vulnerable to various malicious attacks. Cloud computing technology is one of the technologies that helped in instructional operations, due to its flexibility and scalability, which means that it can accept large numbers of students. On the other hand, cloud computing suffers from data latency problems, bandwidth, and some security Issues, so fog computing has been used to reduce these problems.

Fog computing is one of the new technologies that facilitate control over access to big data, as it acts as a mediator between the cloud and the user to bring services closer and reduce their latency. Fog computing provides a decentralized form of applications and services on demand that are useful to manage and analyses big data at the edge of the network. Fog computing supplies storage, control, processing and networks. Fog computing provides storage, control, processing, and networks. There is a need for effective security mechanisms that do not deplete the storage, computation, and power of the e-learning system devices. Fog computing is an extension of cloud computing, so it inherits some of the problems of security and privacy, and this increase concerns in the process of exchanging data and files in e-learning.

In e-learning, privacy and safety in communication are considered the biggest concerns of users, so most research suggested using encryption techniques to secure the information sent and received between the user and the fog. There are two types of encryption techniques which are symmetric and asymmetric encryption. In asymmetric encryption, two types of encryption keys, private and public, are used. The most popular algorithms for asymmetric encryption are RSA and ECC, which are the most commonly used, especially with IoT devices, as they are highly optimized and secure. Asymmetric encryption is complicated not only because of the number of keys used but also because they do not encrypt files of large sizes. As for symmetric cryptography, the same key is used in encryption and decryption, and it is considered more secure than asymmetric encryption. In symmetric encryption, data is encrypted in blocks. This helps encrypt large files. To overcome the limitations in asymmetric encryption and to take advantage of symmetric encryption features in encryption of high-volume files, we suggested using hybrid encryption which combines asymmetric encryption with symmetric key ciphers.

This research aims to compare the most encryption algorithms that are used to provide more secure communication between fog computing and the E-learning system. The algorithms that have been chosen RSA, ECC, and AES, these algorithms will be tested based on the following matrices: key size, encryption/decryption time, and key generation.

The research will be divided into three phases as follows:

Phase 1: This section of the research will overview the general aspect of RSA, ECC, and AES encryption algorithms

Phase 2: This section of the research will compare the results of the algorithms codes. Based on the outputs, deciding which algorithm is best for securing the system and faster. The goal is to measure the performance matrices of key size, execution time, and key generation.

Phase 3: We aim to combine two algorithms to secure the communication between end-users and fog nods. This paper proposes the use of integrated cryptographic schemes, which are schemes that take advantage of symmetric and asymmetric encryption and key derivation algorithms to provide secure encryption over the public key.

4 Problem Statement

Confidentiality has always been one of the biggest obstacles to virtually all cloud computing, particularly with concerning confidential information. To ensure data security, safety protocols should be rigorous enough, but resources and processing time are costly. In the fog computing climate, the need for data protection is as relevant as in any other, but a restricted, resource in the Fog Computing Environment is opposed to strong security measures. Scalable safety provides a way to allow efficient use of the finite resources of the fog computing world by specifically stating that the performance of cryptography should be correlated with the quality of the encryption keys, the more sensitive the data is, and the higher the degree of security intensity should be used. In the fog computing climate, this paper offers an active, elastic, and scalable paradigm for protecting data stored and sensitive information. Studies suggest that RSA, ECC, and AES -based encryption and decryption algorithms can use for independent and self-contained devices for security purposes [13]. The following section gives a brief introduction to these algorithms.

4.1 First Option: RSA

Rivest-Shamir-Adleman (RSA) algorithm is used in modern computers for encryption and decryption of messages. RSA is the most widely studied and used asymmetric approach of the cryptographic algorithm due to its simple and well-designed mechanism. Because of these features, most of the Secure Socket Layers (SSL) providers use this algorithm as a baseline to compare the capabilities of other algorithms. However, RSA needs a longer key length so not suitable in terms of storage capacity, current standards include 1024- and 2048-bit keys for encryption through this algorithm. RSA encryption algorithm is based upon the selection and multiplication of two prime numbers through constituent factors [15]. Each factor (prime number) should produce two keys, which are referred to as public and private keys. And each key can decrypt the message using its complementary key.

RSA Key Generation:

RSA cipher system model, R, and S stand for two prime numbers where A is an integer with no common factor between R and S.

$a^{((r-1)*(s-1))} = 1\,mod(r*s)$

The user where he receives the encrypted file needs to decrypt it by construct two large prime numbers denoted r and s. The product of r and s is denoted n = r * s.

In practice, R and S should be the same length and N is their product which should be 200 numbers or more.

$\mathbf{r = 7, s = 17,}$ **and** $\mathbf{n = rs = 119}$.

The sender then selects an integer e that has a multiplicative inverse modulo called encryption exponent. In this example, the receiver will choose e = 5 which has a multiplicative inverse modulo.

$(r-1)(s-1) = (7-1)(17-1) = 6*16 = 96$

The sender will find decryption exponent D where it constructs the multiplicative inverse of e modulo (r-1)(s-1).

Now the sender has the public key which consists of two numbers n and e. The public key will be available to anyone who might want to send an encrypted message to the receiver.

```
     keyPair = RSA.generate(15360)
pubKey = keyPair.publickey()
print(f"Public key:
     (n={hex(pubKey.n)},  e={hex(pubKey.e)})")
pubKeyPEM = pubKey.exportKey()
      print(pubKeyPEM.decode('ascii'))
```

RSA Encryption:

Now if User A wants to send message m to User B, then

$C = m^e\ mod\ n$

```
     f = open('Myfile.txt', 'rb')
msg = f.read()
     #print(msg)


     encryptor = PKCS1_OAEP.new(pubKey)
encrypted = encryptor.encrypt(msg)
     print("Encrypted:", binascii.hexlify(encrypted))
```

RSA Decryption:

If User B wants to read User A message, he shall decrypt it using the private key (d,n).

$M = C^d mod\, n = m^{ed} mod\, n = m$

```
decryptor = PKCS1_OAEP.new(keyPair)
decrypted = decryptor.decrypt(encrypted)
print('Decrypted:', decrypted)
```

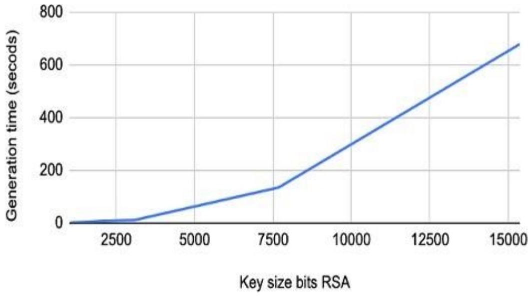

Figure 3: Key generation time *vs.* key size bits RSA

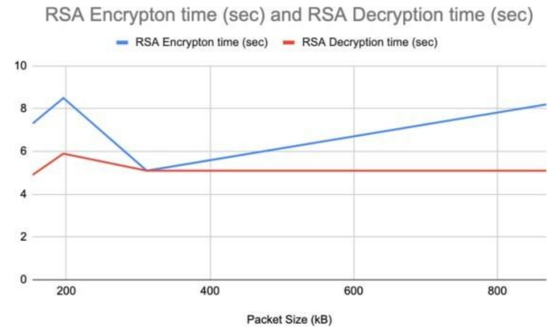

Figure 4: Encryption/Decryption time RSA

4.2 Second Option: AES

Advanced Encryption Standard (AES) algorithm is based upon Rijndael cipher. This algorithm was first introduced by the National Institute of Standards and Technology in 2001 and approved by U.S. Federal Government as a successor of DES. AES is based upon the symmetric data encoding and decoding scheme and shared secrete key for cybersecurity. AES algorithm uses a block of 128-bit data along with 10–14 repetitive cycles (according to the key length) of addition, subtraction, and permutations. Among the symmetric algorithms, AES is an extensively studied, well-tested, and applied algorithm. AES is a powerful algorithm in terms of processing power, time, the key length in comparison to other symmetric asymmetric algorithms. This algorithm is based upon simple and quick running on an 8-bit processor in rounds and variations in each round introduce security [1]. AES algorithm is a very simple and easy to install in hardware components that are being extensively used in the latest processing machines.

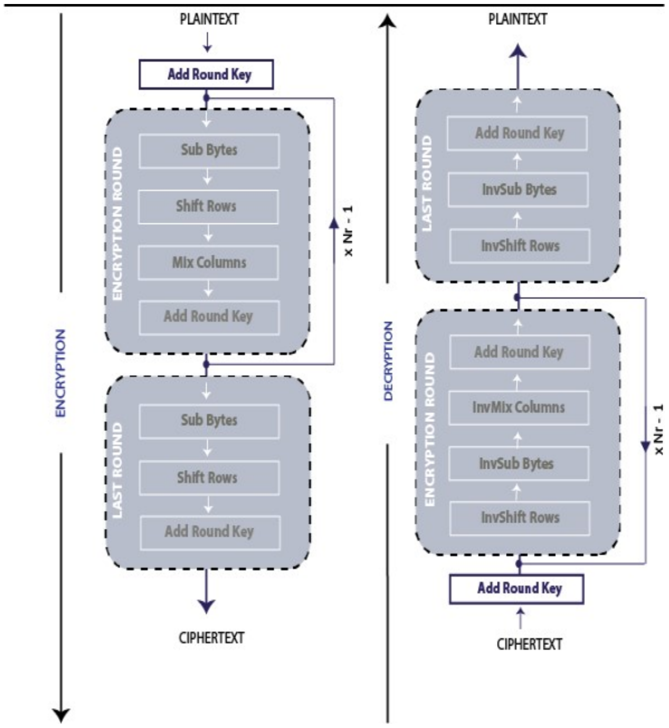

Figure 5: Encryption/Decryption on AES

AES Key Generation:

In AES the key is generated using a key derivation function (KDF).

```
 # generate a random salt salt =
get_random_bytes (AES.block_size)
 # use the KDF to get a private key from the password   private_key
= hashlib.scrypt
      (password.encode(), salt=salt, n = 2^14, r = 8, p = 1, dklen = 32)
```

AES Encryption:

The AES take the message and the encryption key as input and produces an encrypted text with the initialization vector (IV). Encrypting on AES takes the plain text, the round key as input, and generates the ciphertext with IV.

```
# Encrypt the plaintext with the given key:
#   ciphertext = AES-256-CTR-Encrypt(plaintext, key, iv) iv =
secrets.randbits(256) plaintext = open('Myfile.txt', 'rb')
plaintext = plaintext.read()
aes = pyaes.AESModeOfOperationCTR(key,
pyaes.Counter(iv))
ciphertext = aes.encrypt(plaintext) print('Encrypted:',
binascii.hexlify(ciphertext))
```

AES Decryption:

First, initialize the same parameters as in the encryption and use the key and the IV from the encrypted message to decrypt it.

```
# Decrypt the ciphertext with the given key:
#   plaintext = AES-256-CTR-Decrypt(ciphertext, key, iv)
```

```
 aes = pyaes.AESModeOfOperationCTR(key, pyaes.Counter(iv))
decrypted = aes.decrypt(ciphertext)    print('Decrypted:', decrypted)
```

4.3 Third Option: ECC

Elliptic Curve Cryptography (ECC) is another asymmetric cryptographic algorithm. This algorithm is based upon the use of modified form discrete logarithm as these variants are applied in an elliptic group, to achieve more security. The market has started using ECC replacing RSA algorithm, as ECC leads ahead in terms of key size as well as processing requirements [1]. However, careful utilization of ECC is mandatory to ensure security against potential cyber threats.

This algorithm's working is dependent upon the selection of elliptical curve with fixed coefficients and variable or selection of prime curve with limited non-negative values. The values of the curve help to choose public and private keys for encryption purposes.

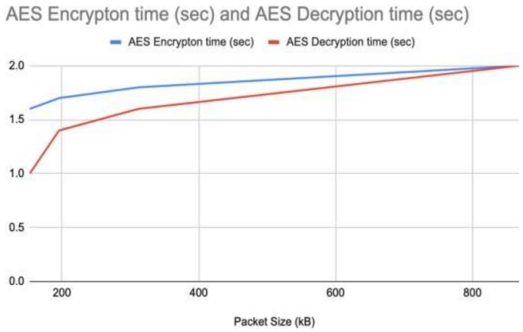

Figure 6: Encryption/Decryption time AES

ECC Key Generation:

Public and private keys in elliptic curves are generated by securely generating a random integer in a certain range.

- Search for elliptic curve E (F), the F represents a finite field.
- Find the point Q on E (F).
- Choose the pseudo-random number x, 1≤ x ≤ (n – 1).
- Find P = x Q
- Get the ECC key pair (p,x).

```
curve = registry.get_curve('brainpoolP256r1') def
compress_point(point): return hex(point.x) + hex(point.y % 2).
privKey = secrets.randbelow(curve.field.n)
pubKey = privKey * curve.g

print("private key:", hex(privKey))
print("public key:", compress_point(pubKey))
```

ECC Encryption:

Encrypting in ECC, the sender chooses a random positive integer x and uses it to encrypt the plain text consisting of the pair of points. the receiver gets the ciphertext = {xG,(plain text) + x(B's public key PB) }.

```
def ecc_calc_encryption_keys(pubKey):
   ciphertextPrivKey = secrets.randbelow(curve.field.n)
ciphertextPubKey = ciphertextPrivKey * curve.g
   sharedECCKey = pubKey * ciphertextPrivKey     return
(sharedECCKey, ciphertextPubKey)
```

```
(encryptKey, ciphertextPubKey) =
ecc_calc_encryption_keys(pubKey)
```

```
print("ciphertext pubKey:",
compress_point(ciphertextPubKey))
print("encryptionkey:", compress_point(encryptKey))
```

ECC Decryption:

Decrypting in ECC the receiver gets the two points of the curve where he will multiply the first point with his private key. Then subtracts the product of the multiplication with the second point: Plain text (PT) + x (B‘s public key PB) – nB(xG) = PT + x(nBG) – nB(xG) = PT Where only A knows the value of X.

```
def ecc_calc_decryption_key(privKey, ciphertextPubKey):
 sharedECCKey = ciphertextPubKey * privKey     return
sharedECCKey
```

```
 decryptKey = ecc_calc_decryption_key(privKey, ciphertextPubKey)
print("decryptionkey:", compress_point(decryptKey))
```

```
privKeyHex = privKey.to_hex() pubKeyHex =
privKey.public_key.to_hex() print("Decryption private
key:", privKeyHex) decrypted = decrypt(privKeyHex,
encrypted) print("Decrypted:", decrypted)
```

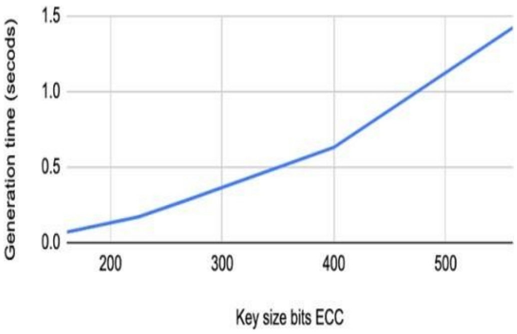

Figure 7: Key generation time *vs.* key size bits ECC

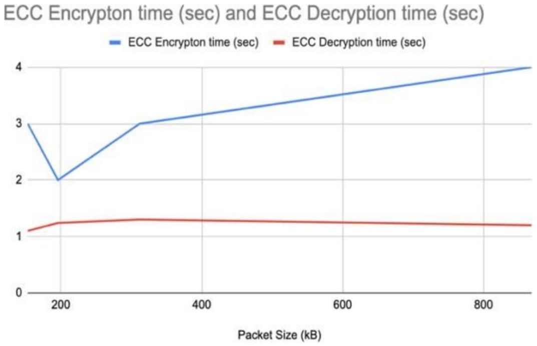

Figure 8: Encryption/Decryption time ECC

4.4 Comparison between RSA, AES and ECC

The RSA, ECC, and AES algorithms introduced in this study are discrete protocols that are aimed to provide higher levels of security. Fig. 9 introduces the key length requirement of RSA, AES, and ECC algorithms.

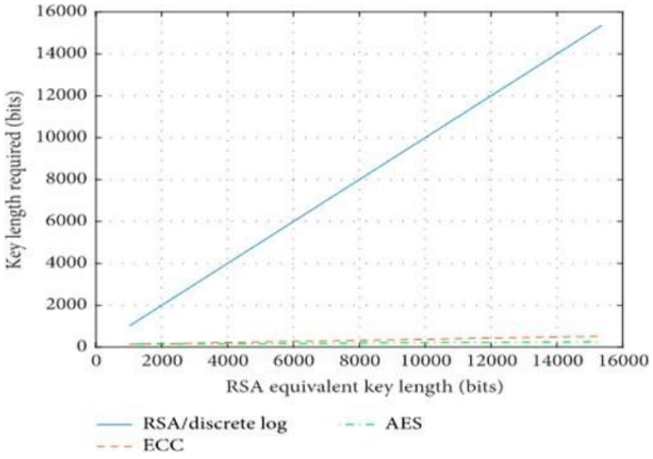

Figure 9: Key length required by algorithms

To obtain the same scale of security offered by 2048 bits of RSA only 112 bits of AES are required. In terms of key length, ECC and AES provide a much better approach than RSA. But this ratio relatively parallels in the case of ECC and AES. To use longer key length RSA would require wider bandwidth for public key transfer. While no extra bandwidth is required either in the case of AES or ECC implementation.

In terms of storage RSA needs 4n number of bits per private message, ECC needs 2n and AES needs only n number of bits per private message or secretes shared over the network [2]. These requirements exclude the bits required for overhead and indexing value.

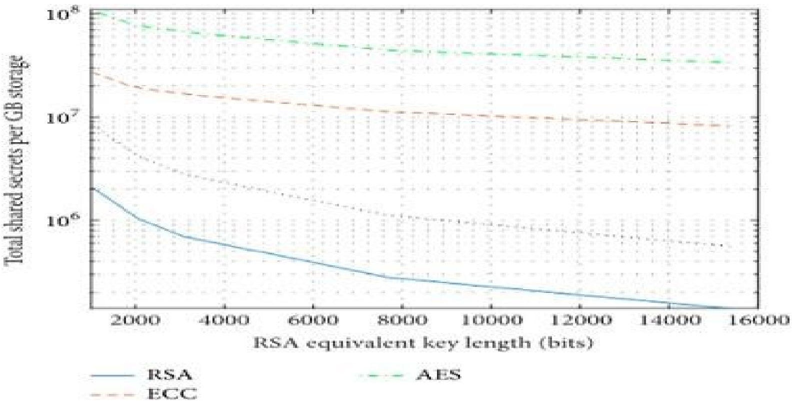

Figure 10: Storage requirement by algorithms

As it is evident from Fig. 8 that a single GB of data traveling through the network needs a greater number of bits for secrete sharing in the case of RSA rather than AES and ECC.

Encryption and decryption parameters and requirements of different algorithms are dependent upon system architecture, software, hardware components, and their optimization. Generally, AES offers the quickest encryption and decryption algorithm being the symmetric cipher. On the other hand, ECC provides improved key pair generation as compared to RSA, as RSA needs several huge orders as compared to the smaller key used in ECC. In addition to bit requirements there arise manufacturing problems too [15]. A huge sharing of public keys is required only for 1 GB of secure data transfer.

Table 2: Comparison between RSA, AES and ECC

Parameters	AES	RSA	ECC
Cipher type	Symmetric	Asymmetric	Asymmetric
Development	2001	1978	1985
Key length	128,192,256	Key length depends on number of bits on a module	Smaller but effective key
Rounds	10.12.14	1	1
Block size (bits)	128	Variable block size	Stream size is variable
Level of security	Excellent security	Good level of security	Highly secure
Encryption speed	Faster	Average	Very fast

5 Integrated Encryption Schemes (IES)

In the coming years, with the increasing dependence on the e-learning system, which requires low latency and support for mobility and geographical distribution. As cloud computing has difficulty meeting e-learning system requirements, it appears that the fog computing platform meets these requirements. The use of fog computing has been proposed to extend the cloud computing model to the edge of the network and place the resources so that they are close to the users, thus helping to quickly provide service to users. Cloud computing can be used for data sharing and storage services. Thus, data owners can store their confidential data in several fog nods. This data is encountered in fog nodes and to keep its confidentiality and availability close to users, which may cause further challenges to data sharing security.

In this section, we will present a method for sharing data in E-learning based on a fog environment. The proposed method seeks to excel at sharing data in cloud computing. To improve system performance in general and security aspects in particular. To solve the problem, we suggest transferring data between fog nodes and secure sharing, keeping in mind security challenges. By combining some encryption techniques, which are symmetric and asymmetric encryption technology. Combining more than one encryption algorithm to provide less processing time and better response than cloud systems. Low latency, data availability, and confidentiality are the reasons why education has adopted fog computing and the combination of the two types of encryption may bring all these advantages to the user.

Asymmetric encryption, which is the most commonly used ECC, RSA which is the most preferred due to the smaller keys, short signatures, and better performance. The use of asymmetric encryption alone in communication between fog computing and e-learning is more complicated than symmetric encryption, not only because there are two types of keys, but it also cannot encrypt or decrypt large files. Asymmetric encryption is also much slower than symmetric, so AES encryption is 1000 times faster than RSA. The main reasons for using fog computing in e-learning are the enormous amount of information and its pressure on the cloud, which leads to poor data access and protection, and therefore asymmetric encryption alone, if used for data security, does not meet these conditions. To overcome the limitations of asymmetric encryption such as not encrypting files of any size and also preserving the features in them, a modern approach to using asymmetric encryption has been proposed. Hybrid encryption combines the two types of encryptions and achieves the best features for the communication between fog nods and the system.

To secure the communication between the end-users and fog nods this paper proposes using integrated encryption schemes, which are schemes that take advantage of both symmetric and asymmetric cipher benefit and key derivation algorithms to provide secure encryption on the public key. Integrated encryption schemes use RSA or ECC asymmetric encryption algorithms to encapsulate the symmetric encryption key and later use symmetric encryption like AES to encrypt the file. Examples of integrated ECIES and DLIES schemes.

IES Encryption:

In integrated encrypted schemes there are three
keys: -Asymmetric (public and private key)-
Symmetric key.

In the encryption phase, there are two types of objects that needs to be encrypted: the file and the symmetric key.

1. The file will be encrypted by using a symmetric key, also known as DEM. Which is an encrypted block contain encapsulated data.
2. The symmetric key used for the file encryption will be encrypted by using the public key of the user. This is known as KEM which is an encrypted block contain encapsulated symmetric key.

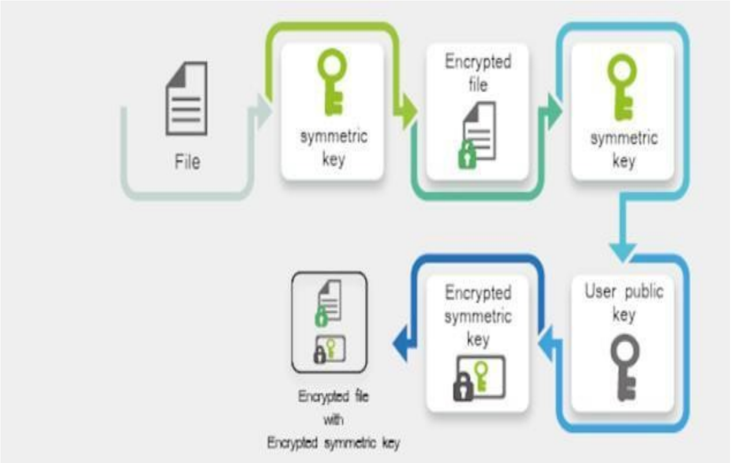

Figure 11: Encryption process in integrating two types of Algorithms

IES Decryption:

When the encrypted blocks arrive, there are two types of objects that needs to be decrypted: File and the symmetric key.

1. At first the KEM which contains the symmetric key needs to be decrypted by the user's asymmetric private key, to use the symmetric key in the next phase.
2. The second block DEM will be decrypted by the output symmetric key from the KEM block, to decrypt the file.

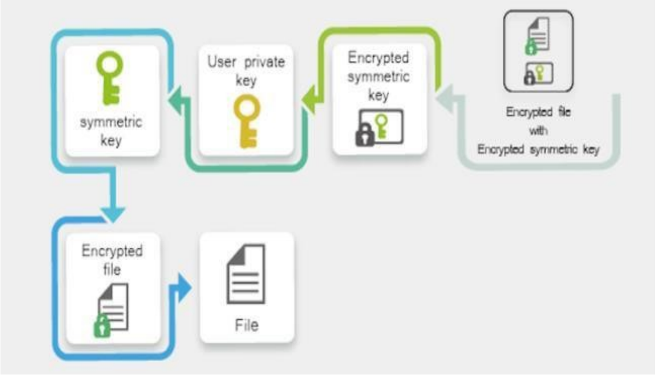

Figure 12: Decryption process in integrating two types of algorithms

6 Experimentation and Evaluation

This paper tests the reliability of the Integrated encryption Schemes in the educational activity. like lectures, exams, and other files. We used trusted servers and fog servers to test the authentication of students and teachers via Integrated Encryption Schemes. The key distribution in integrated encryption Schemes that take advantage of both symmetric and asymmetric cipher benefit and key derivation algorithms to provide secure encryption on the public key. To ensure the advantages of the proposed system and its limitations, we performed a security analysis. In this security analysis, we validate the work by performing a testbed using python, ASP.net, and WCF services.

6.1 Security Analysis for Integrated Encryption Schemes (IES)

6.1.1 Authentication

In this process, we verify the identity of only the person allowed to view files, which we have achieved by using the public key to encrypt the symmetric key (used in protecting files). Therefore, our system has prevented anyone else from accessing this key. Also, our system does not allow adding new files except by the admin of the website, whose identity is verified by our system using the password entered by him.

6.1.2 Authorization

Our system allows the student to read files only by using his private key, through which he knows the symmetric key (related to these files only) and which is specified by the system administrator only, and therefore the student cannot perform any operation other than what the system allowed him to do.

6.1.3 Confidentiality

Our system guarantees the privacy of data and its protection from attempting to unlawfully disclose its contents, as it encrypts the sent files using the AES algorithm, and it encrypts the symmetric encryption key (used in the previous process) by using RSA algorithm, and therefore no one can see the contents of this files (except for authorized persons), due to the difficulty and nearly impossibility of breaking the integrated encryption used in our system as it relies on two algorithms, each of which is one of the strongest encryption algorithms.

6.1.4 Integrity protection for data

This means not to modify the contents of the message sent from the sender to the recipient, and our system has done so by using the MD5 algorithm, which is considered one of the most important hash functions (one-way functions), which includes detecting the modification of the content or location of any bit of the message.

7 Conclusion

In short, e-learning is the need of the day and is extensively used throughout the world’s educational institutes for distance learning. These e-learning platforms need to be secured to make sure the security of confidential information regarding examinations, teachers, and the institute. But these platforms are vulnerable to threats. But a there is a need of introducing well-designed algorithms and security to minimize the risk of cyber-attacks. Fog computing enables e-learning platforms to provide extended services, but this technology makes the data more vulnerable. So, RSA, AES, and ECC algorithms can suitably be used for data encryption. No matter which algorithm is chosen depending upon the system requirements and hardware availability, it will be mandatory to ensure the provision of pre-shared secret data to factory-paired communication devices. However, secure the technology is there always a need for improvement to ensure security against future attacks and vulnerabilities.

Acknowledgment: This work was supported at Taif University by TRUSP (2020/150).

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] N. Tariq, M. Asim, F. Al-Obeidat, M. Zubair Farooqi, T. Baker *et al.,* “The security of big data in fog-enabled IoT applications including blockchain: A survey,” *Sensors*, pp. 1–33, 2019.

[2] P. Zhao, S. Sintonen and H. Kynäslahti, "The pedagogical functions of arts and cultural-heritage education with ICTs in museums–A case study of FINNA and Google Art Project," *International Journal of Instructional Technology and Distance Learning*, pp. 1–81, 2015.

[3] M. I. Ghareb and S. A. Mohammed, "The effect of e-learning and the role of new technology at university of human development," *International Journal of Multidisciplinary and Current Research*, pp. 299–307, 2016.

[4] N. Guragain, "E-learning benefits and applications," Helsinki Metropolia University of Applied Sciences, pp. 1–53, 2016.

[5] R. Ali and H. Zafar, "A security and privacy framework for e-learning," *International Journal for E-Learning Security*, pp. 556–567, 2017.

[6] N. H. P. Dai, K. András and R. Zoltán, "E-learning security risks and countermeasures," *Emerging Research and Solutions in ICT*, pp. 17–25, 2016.

[7] S. Mostafavi and W. Shafik, "Fog computing architectures, privacy and security solutions," *Journal of Communications Technology, Electronics and Computer Science*, pp. 1–15, 2019.

[8] H. J. Cha, H. K. Yang and Y. J. Song, "A study on the design of fog computing architecture using sensor networks," *Sensors*, pp. 1–16, 2018.

[9] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Integration of blockchain and cloud of things: architecture, applications, and challenges," *IEEE Communications Surveys & Tutorials*, pp. 1–29, 2020.

[10] M. Aazam, S. Zeadally and K. A. Harras, "Fog computing architecture, evaluation, and future research directions," *IEEE Communications Magazine*, pp. 1–8, 2018.

[11] T. Alam and M. Benaida, "Blockchain and Internet of Things in higher education," *Universal Journal of Educational Research*, pp. 2165–2174, 2020.

[12] J. Yakubu, S. Muhammad Abdulhamid, H. A. Christopher, H. Chiroma and M. Abdullahi, "Security challenges in fog-computing environment: A systematic appraisal of current developments," *Journal of Reliable Intelligent Environments*, pp. 1–26, 2019.

[13] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan and R. Ranjan, "Fog computing security challenges and future directions," *IEEE Consumer Electronics Magazine*, pp. 1–7, 2019.

[14] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, fog and edge computing enabled smart campuses and universities," *Applied Sciences*, vol. 9, no. 21, pp. 1–24, 2019.

[15] J. M., Zhong, H. R. Xie, D. Zhou and D. K. W. Chui, "A blockchain model for word-learning systems," *International Conference on Behavioral, Economic, and Socio-Cultural Computing*, pp. 130–131, 2018.