A Study of Security Impacts and Cryptographic Techniques in Cloud-based e-Learning Technologies

Lavanya-Nehan Degambur, Sheeba Armoogum, Sameerchand Pudaruth
ICT Department, University of Mauritius, Moka, Mauritius

***Abstract*—e-Learning has transposed the perception of teaching and learning considering knowledge delivery and knowledge acquirement. Today, e-learning participants access and upload their materials at any time and at any place since e-learning technologies are typically hosted on the cloud. Cloud computing has embellished the base platform for the future of e-learning, however, security and privacy remains a major concern. Cloud-hosted e-learning technologies as they are accessed over the internet suffer from the same risks to information security aspects namely availability, confidentiality, and integrity. In such a context, data authenticity, privacy, access rights and digital footprints are vulnerable in the cloud. Research in this domain focuses on specific components of cloud and e-learning without covering a holistic view of applied cryptographic techniques and practical implementation. Hence, aiming at the various security aspects and impacts of cloud-based e-learning technologies, this paper puts forward reviewing the various cryptographic techniques used to secure data across the whole end-to-end cloud-based e-learning service spectrum using systematic review and exploratory method. The results obtained define several sets of criteria to evaluate the requirements of cryptographic techniques and propose an implementation framework across an end-to-end cloud-based e-learning architecture using multi-agent software.**

Keywords*—e-Learning; cloud computing; data management; pseudonymization; data deduplication

I. Introduction

In a world where the internet is the most potent communications enabler, humanity has transcended orthodox teaching and learning ways and made them global with e-learning where information, communication and digital technologies are utilized to ease the learning process. The e-learning concept has offered an effective educational tool that is accessible from anywhere to anyone encompassing professionals, scholars, teachers, and students by combining the virtues of the internet and the wisdom of knowledge. The efficacy of e-learning is improvised by enhancing the training of teachers, curriculum developments, assessments reforms and infrastructure optimization in a holistic manner. e-Learning has enriched the economic growth in various countries and has reduced the digital divide between countries, societies, and communities. The introduction of e-learning technologies in patriarchal or male-supremacist communities allows the emancipation of girls without bypassing societal norms. Underserved students can make use of this method to study at their own pace and improve their participation abilities and cognitive growth. Hence, through the dissemination of programs, gender gaps can be narrowed across the whole human diaspora. The recent COVID-19 pandemic has increased the demand for e-learning platforms since traveling has been inhibited owing to recurrent lockdowns. Thus, to be fully transformative, e-learning should be integrated formally into curriculum creation and teacher training and informally into the habits of students [1]. Cloud computing platforms have diversified the conceptualisation of delivering education using modern e-learning methods. However, this base platform for the future of e-learning is vulnerable to security threats and privacy issues.

A. Modern e-Learning Technologies

Modern e-learning involves the delivery of courses to people in an automated or virtualized form such as videos and interactive methods or via formal teaching from teachers in a personal form via the internet using digital technologies [1, 2]. Virtual learning leans on the visual acumen of protagonists to help the users present and understand topics, study at any time anywhere without teacher intervention, the ability to edit, update and share materials without prior notification and synchronization between teachers and students. Moreover, it can provide an increased number of courses without logistical investment; increase the number of students owing to the flexibility, and cost-effectiveness of such learning. Using the virtualized form, or virtual learning, students and teachers can share a variety of resources, topics and materials and present them in a customizable and personalized format to ease teaching and comprehension. Whereas in a personal form or personal learning, students and teachers have a personal space on a single-use instance or continuous use instance and use their materials to learn and improve skills and teach respectively. Features of personal learning are the ability of users to manage teaching sessions and learning materials in learning platforms, multi-user interaction during e-learning sessions and performance and goal setting per user profile.

Modern e-learning is cloud-based whereby the e-learning platforms are hosted on the cloud instead of hardware and software being installed, run, and administered on the learning provider's premises. The educational materials in today's e-learning are virtualized in cloud infrastructures and it is up to the cloud service providers to guarantee the uptime of the services available to e-learning protagonists. Cloud-based e-learning platform has triumphed due to the abilities of remote access, cost efficiency, open research-oriented environments, ability to analyze and provide insights about the behaviors of protagonists, the disintegration of geographical barriers and time constraints.

However, where information is present, dangers to information are omnipresent and information traveling on the

internet is constantly exposed to security threats. Since e-learning systems are diversified, there is a variety of resources and consumers of those online resources. Collaboration, interconnectivity, and information sharing are the pillars of e-learning systems so that data and the information it induces must be protected to maintain confidentiality, integrity, and availability. Information security issues in e-learning include data manipulation, confidentiality compromises and fraudulent authentications as e-learning developments always lean towards interoperability between learning environments, heterogeneous devices, multi-technology applications, and academic discoveries. Cloud computing readily provides this unified interconnected requirement for successful e-learning technologies.

B. Cloud-Computing and e-Learning

One exclusively pays the cloud services to fit and enhance business needs, administer infrastructure optimally and reduce operational costs. A wide-scale pooling of computing and networking resources such as processing, memory, storage, and bandwidth, all available on-demand, achieves this. Accessing those resources requires flexibility because resource distribution needs to be precise and fast to cater to rapid fluctuations in demand without service disruption or quality deterioration [2, 3]. Cloud-based e-learning platforms use cloud computing service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) that are deployed in three deployment models named public cloud, private cloud and hybrid cloud. IaaS provides the physical IT infrastructure and architecture of the system that the clients will use and allows the clients to control only the infrastructure resources provided to them, not the underlying cloud infrastructure hosting the IaaS.

PaaS provides services in terms of the operating system, hosting software and application development lifecycle-software using which the customers can develop their applications that are run on virtual machines, which abstracts the platform from the underlying physical infrastructure. SaaS offers software applications as services over the internet as compared to usual software packages bought by individual clients [4]. The end-user can hence use the cloud service provider's applications hosted on the cloud from anywhere at any time without catering for the management and control on the underlying platform or infrastructure. The public cloud deployment model delivers the cloud services readily available to the public while private cloud services by an organization are made available only to that organization and selected protagonists. Hybrid cloud computing is a mix of public and private cloud deployments to create an automated, unified, and fault-tolerant environment that offers modulated services based on user usage and requirements.

Accordingly, cloud-hosted e-learning technologies depend on the internet-connected cloud resources to function. However, both the cloud-based e-learning technology and e-learner are under constant threats by being connected with the internet. The COVID-19 pandemic has induced a rapid growth in cloud-based e-learning usage but this has also amplified attacks on such technologies. The main security concerns to cloud computing are browser security, authentication, privacy, duplication, and availability while those of e-learning are user authentication and authorization, data confidentiality and blocking, denial of service and flooding attacks. Thus, the similitude between security concerns of cloud computing and e-learning can be easily observed [2, 3].

This study aims to conceptualize how e-learning services are provided by cloud technologies, discover the various cyber security issues that impact cloud-based e-learning technologies, study the state of art cryptographic techniques used to address the issues in several aspects of cloud-based e-learning technologies, find discrepancies in application and implementation of such cryptographic techniques and finally propose solutions to those problems. The proposed approach will be beneficial for the research community to identify the set of criterias to evaluate different cryptographic techniques.

This paper is structured as follows: Section 2 relates the literature review on the security impacts upon the usage of e-learning and cloud computing technologies. Section 3 describes the research methodology used to perform the study. Section 4 analyses the findings and provides results and Section 5 concludes the paper.

II. Literature Review

In this section, a detailed review is provided on the security impacts on the usage of e-learning and cloud computing technologies and the different cryptographic techniques applied along with the entire end-to-end cloud-based e-learning service architecture.

A. e-Learning Technologies Security Aspects, Impacts and Threats

Security threats on e-learning are the problems that can adversely influence the safety of e-learning end users and their data and also apply to user authentication, authorization, and confidentiality. If the usernames and passwords given to users to log onto the e-learning platforms are compromised, users may lose the ability to use the e-learning platforms and may risk their personal, professional, and confidential transaction information being accessed and misused by unauthorized parties. Compromised systems may be vulnerable to blocking attacks whereby an attacker attacks a user's e-learning content and access e-learning material and flooding attacks whereby an attacker bombards the e-learning platform with bogus requests using an account so that the user loses access time [2]. In addition to user authentication, concerns are raised for user operation process tampering to damage data patterns and social behavior deduction through patterns to impede user privacy.

According to the study in [2, 5], Short Message Service texts (SMS) can be used as two-factor authentication to complement usernames and passwords and prevent unauthorized access; biometrics such as fingerprints, iris recognition, or voice recognition can be used with attribute-based cryptography; digital signatures can be used to authenticate identity and integrity of data and also non-repudiation of transactions; access control lists and processes can be applied to the server and user resources access to customize access mechanisms. SaaS security by default is used to secure e-learning applications. Hence, the whole system infrastructure of servers and storage must be considered in terms of security impacts. To reduce threats, the authors

recommended including server, disaster recovery, and safety and management aspects.

Aside from user authentication and authorization, private information protection, and data integrity protection; raising awareness, learning resources authenticity, seamless access, location privacy, digital rights, and usage anonymity should also be catered for e-learning security. Doing so will fulfill basic security criteria such as availability, integrity, confidentiality, authenticity, non-repudiation, and accuracy. Maitra and Bhatia [6] used vulnerability scanners such as Netsparker and N-Stalker to test e-learning platform vulnerabilities and proposed methodologies to ensure security. Both scanners identified the following vulnerabilities: SQL injection, cross-site scripting, directory traversal, BREACH attack, JavaScript library vulnerabilities, CRIME SSL/TLS attack, HTTP response splitting/CRLF injection, file inclusion, HTTP parameter pollution, HTTP authentication, and insecure cookies. According to Maitra and Bhatia [6], e-learning platform security can be accomplished in two proposed approaches: hierarchical and distributed. The hierarchical approach involves applying security in a top-down centralized manner across components while distributed approach applies different security models for every different component in the e-learning system while allowing interaction.

Although e-assessment, the use of integrated information technologies to support assessment processes across all stages in its life cycle in e-learning [7] has proliferated, it has faced three main threats: identity misuse, disclosure of information, and fraudulent alteration. During an e-assessment session, identity misuse may happen if an attacker uses the identity of the real e-learning user being assessed; sensitive and private data transmitted may lead to the disclosure of confidential information Since e-assessment and e-learning data are stored in databases, they can be subject to alteration which is problematic to students and teachers in terms of data integrity. Those issues can be analyzed and tackled in two perspectives namely the educational perspective by considering learners and teachers scenarios and problems and using the technical architectural perspective to secure the information system running the e-assessment solutions [7]. According to [8], the e-learning system, as well as the underlying infrastructure, should be evaluated for threats and risks to secure the subsequent technological solutions analysis and security policy audits by financial institutions and payments.

Cloud-based m-learning extends the e-learning by expediting the delivery of educational activities, materials, and contents that can be readily performed and accessed at any time at any place via the internet using mobile devices. Since mobile devices are exposed to operating system vulnerabilities, mobile web browser vulnerabilities, untrusted applications, application collusion, spyware, malware attacks, data leaks, jailbreaks, and personal user malpractices; cloud-based m-learning is posed to vulnerabilities. These vulnerabilities can be analyzed in a three-tiered architecture comprising of mobile device tier, network platform/provider tier, and cloud tier. Malicious push advertisements and SMS's can be sent using mobile devices to perform distributed attacks. Vulnerabilities due to network tier threats are inherent to the service provider such as internet protocol vulnerabilities, Man-In-The-Middle (MITM) attacks, and malicious server agents. Generally, the cloud platforms are vulnerable to DNS/web spoofing, in-house unauthorized access, malware injection attack, authentication, and MITM attack, side-channel attack, virtual machine escape, and Denial of Service (DoS) attacks [9]. Conventionally, cloud-hosted applications are affected via attacks like cross-site forgeries and SQL injections; viruses and e-learning modules from session hijackings and riding affect Learning Management Systems (LMS). Besides, cloud data storage is susceptible to obsolete and insecure cryptographic storage and data duplication.

B. Cloud Computing Security Aspects, Impacts and Threat

Security concerns related to cloud computing are associated with basic security on aspects of data such as transmission, storage, and recovery, availability of applications, services, and data authentication demands, and browser security [2]. From a customer perspective and owing to the abstract nature of cloud and lost physical control, the following five main security threats have been obtained: data exposure to unauthorized antagonists, unauthorized access, data loss, manipulation and induction, Service Level Agreement (SLA) violation and privacy breaches. Data exposure and unauthorized access affect the data confidentiality requirement; data loss and data manipulation breaches data integrity requirement; privacy breaches antagonizes privacy preservation requirement while SLA violation goes against both data confidentiality and integrity.

Threats faced by e-learning users and providers are mostly internet-based where the Denial-of-Service (DoS) and Distributed DoS (DDoS) are omnipresent threats to the availability of such services. Rahman et al. [5] subsequently explored the different attacks on cloud-based e-learning platforms. Firstly, the web browser, which is the user's gateway to the e-learning platform exposed an ideal target for an attack. Phishing attacks eventuate when during the authentication process the user access has not been verified and certified. However, backdoor channel attacks negate authentication to prevent trusted users from accessing their confidential data, and virtual machine attacks involve seizing vulnerabilities in virtualization platforms to detach the physical resources to the virtual resources and reroute data access towards hackers. Nevertheless, insider attacks involve people familiar with the e-learning service provider getting access to the system through knowledge of system policies and architectures. Third-party cloud providers outsource cloud resources among themselves to provide high availability; however, this can be detrimental to user data privacy if policies, procedures, and contracts are not clearly defined. To prevent theft, unauthorized induction, and dissemination, they suggest disposing of the imperfect and redundant data from the cloud and physically.

Since cloud computing is provided in three distinctively different service models, each of them has its own security requirements which should be analyzed. In SaaS, security impacts are about data security, network security, data integrity, data segregation, and data breaches. Security issues regarding PaaS affect data location, and privileged access while those in IaaS are web service attacks, SLA attacks, DDoS, MITM attacks, and DNS security. Data location

vulnerabilities arise because it is unknown where data is stored and processed physically when users are accessing the applications on the platform [10]. Whereas privileged access vulnerabilities occur as a consequence of cloud providers potentially having all possible access rights to data residing on their platforms and any breach on the cloud provider side cascades onto the data.

To use a cloud service over the internet, the cloud provider runs web service protocols that are exposed to attack using XML signatures breaking security between a user's browser and the cloud service. Since SLAs are the legal bindings to service delivery between providers and users, attacks are possible against SLAs to exploit undefined metrics and hence defy quality, availability, performance, and reliability of resources. DDoS attacks deny important services from running by unleashing a tremendous number of requests, which are difficult to be handled by the attacked service. Usually, a Master controls several Slave bots to launch a DDoS on the Target cloud IaaS server. MITM attacks, a subcomponent of eavesdropping, happen when the attacker positions itself between the cloud user and the cloud IaaS server to hear and retrieve communication and even falsify the connection [10]. Besides, DNS attacks occur when vulnerabilities in domain name services are exploited to prevent the resolution of the IaaS cloud environment's domain names to the correct IP addresses. Both the cloud users' and the providers' packets can then get rerouted to prevent access, provoke a DoS, compromise credentials, falsify connections or clone queries and requests.

C. Cryptographic Techniques in e-Learning Technologies

To secure e-assessment in terms of personal data protection and hosts and network protection, the TeSLA system proposed transport layer security (TLS) using authorization certificates, public key infrastructure, and pseudonymization. TLS allows every entity to mutually authenticate with its peers and create tunnels secured with data encryption and integrity checks using X.509 certificates instead of passwords. TeSLA's PKI manages certificates employing different certificate authorities (CA), revocation lists, three-layered security procedures, and 4096 bits RSA (Rivest–Shamir–Adleman) keys for Certification Authority (CA) certificates [7]. Identity management and data protection are achieved with pseudonymous credentials adapted from attribute-based signatures utilizing randomized TeSLA IDs generated per user so that the full identity of a user remains anonymous.

In contemplation of securing cloud-based m-learning architecture, each tier is secured in a top-down hierarchical manner starting with mobile devices with multi-client authentication, multiple firewalls, and network and exchange servers. Authentication and authorization protection, identity and key management, backup and disaster recovery, anti-replay techniques, state-of-the-art encryption, and protection as a service are solutions to protect the cloud infrastructure tier. Lastly, the network tier is protected using next-generation firewalls and application access authorization [9].

To secure and authenticate data storage in e-learning systems, hash tables and hash trees have been proposed to ensure data integrity for the transmission, storage, and processing of authentication data between a user and the e-learning system. Encryption is performed on authentication information before transmission and a linear dimensional reduction transformation projects user data and verification data into lower dimensions to preserve relative vector distances and authentication correctness. To secure authentication data integrity, InterPlanetary File System (IPFS) is proposed to store data on a Merkle Directed Acyclic Graph (DAG) file structure, which combines a Merkle tree and a Guided Ring graph. IPFS uses SHA-1, SHA-256, and BLAKE2 cryptographic hash functions to guarantee immutability and immunity to DDoS attacks on the authentication process [11].

To protect multi-agent e-learning platforms' access control and ensure trust and reputation, a combination of Role-Based Access Control (RBAC) inspired models called Trust-Based Access Control (TrustBAC) and Trust Satisfaction and Reputation (T-SR) have been proposed by Asmaa and Najib [12]. Trust levels between users/actors/agents can usually be generated by using user credentials, results of past user interactions, user characteristics, and the context in which those actions occurred [12]. This allows conditions to be created to define safety rules to be applied in access control processes, simplify the generation of trust value, and trust establishment.

Cyber-trust provides legal significance to a public exchange of documents over the network in e-learning environments and hence helps counteract cyber-attacks and cyber-espionage. Network Time Synchronization (NTS) provides standardized cyber-trust assurance for e-learning systems by using three layers of trust criteria expanded to the public internet cyberspace together with an independent Network Time Synchronization source. The three layers of trust criteria are the basic factors that combine to granularly model what a legal user should be and are based on five trust characteristics targeted, subjective, measurable, dynamics, and conditionally passed [13]. Independent Network Time Synchronization source is used because in-built time synchronization modules and synchronization subnets based on network time protocol can be compromised which can threaten end-user and e-learning platform private keys and digital signatures while also endangering the whole public key infrastructure used to secure the communication.

Ali and Zafar [14] recommended that, for e-learning security, DoS attacks and unauthorized logins can be handled by single sign-on authentication. Data evaluation issues at login and on course contents are solved using trust certificates and biometrics. Architecture challenges concerning data transmission channels and access controls are catered for using virtualization technologies and encrypted SSL/TLS channels via the web administration console.

D. Cryptographic Techniques in Cloud Computing

Challenges to data exposure are intercepted with the use of convergent encryption, homomorphic encryption, and proxy-re-encryption. Identity-Based Cryptography (IBC) and Attribute-Based Cryptography (ABC) serve as potential cryptographic solutions for unauthorized access [3]. However, data loss and manipulation are mitigated using Proof of Data Possession (PDP) and Proof of Retrievability (POR) while Privacy breaches' cryptographic solutions are searchable

encryption and are achieved using Private Information Retrieval (PIR). PDP checks if remote cloud servers have outsourced data using a challenge-response protocol. A client using PDP can check if a file is stored and is available on a cloud server in its original form using a four-step procedure: pre-process, challenge, proof, and verification. POR verifies data integrity and data recoverability in case of failure by adding sentinels in data. The data owner can send a challenge to the cloud server using randomly selected sentinel positions in the data and as a response, the corresponding sentinels must be sent back. If it is not the case, the data are suspected to be modified or deleted.

Searchable Encryption allows a cloud server to search encrypted data using information that the data owner or client has previously provided. This is called a trapdoor [3]. The cloud host hence does not know the exact query nor the data that matches the query thus providing confidentiality with searching ability. The data owner or a cloud client can receive the data locally and decrypt it while saving bandwidth. There are two types of searchable encryptions: symmetric and public keys. PIR schemes provide clients with the ability to request data from cloud servers without revealing which item is being retrieved to the storage itself hence protecting curious cloud providers. PIR is available in two schemes: computation PIR (cPIR) which provides privacy from computationally linked servers and information theoretic PIR (itPIR) which provides privacy for computationally independent servers.

Convergent encryption, a content hash keying cryptosystem, both protects data outsourced to the cloud and ensures client-side data duplication so that the storage can host only one copy of a file regardless of the number of users accessing it. In client-side deduplication, convergent encryption provides two levels of encryption, symmetric data encryption level, and asymmetric key encryption level. At the data encryption level, an enciphering key, K, is derived from the data itself using a one-way hash function and used to encrypt the data so that the same data encrypted by several users will produce the same encrypted data, which will be stored only once [3]. At the asymmetric key encryption level, the depositor uses the recipient's public key and asymmetric encryption to encrypt the key K, to be shared alongside user metadata.

Homomorphic encryption algorithms allow third parties to perform deterministic computations on encrypted data to ensure privacy preservation [3]. Homomorphic mechanisms also allow private queries whereby the client sends an encrypted query and the cloud server replies with an encrypted response without looking at the query itself. A user can also save encrypted data on the cloud and then have the cloud server retrieve only some files that when decrypted satisfy some conditions without the server having decrypted the data. To provide data secrecy against cloud providers, proxy re-encryption algorithms usage has officiated the cloud storage outsourcing storage clouds use proxy re-encryption algorithms to provide data secrecy against cloud providers [3]. If a cloud entity wants to access cloud data from a depositor, the cloud server must first re-encrypt the data using the cloud entity's public key and the server's public master key while considering privileges granted.

To secure user data storage and access on the cloud, Pavani et al. [15] performed a comprehensive review of several types of Attribute-Based Encryption (ABE) where each user is identified by a set of attributes. For key policing, by assigning a range of attributes to each user within a control tree, Encryption Key Policing attributes (KP-ABE) are used in general. En route towards the use of non-monotonic access structures, that used control doors such as NOT operations in the control framework, the Expressive Main Regulation ABE (EKP-ABE) which is an expanded version of Key-Policy ABE (KP-ABE) has been proposed. To protect the user's privacy, Ciphertext-Policy ABE (CP-ABE), an inverse iteration of KP-ABE uses a series of attributes for the user's private key to feed the cyphertext to an access framework. To integrate multiple data domains and associated processes, Hierarchical Attribute Dependent Encryption (HABE) ensured data consistency and accuracy throughout the system.

To protect user revocation, Multi-Authority ABE (MA-ABE) uses secured encryption that processes encryption using global public parameters. Additionally, for file protection, File Hierarchy ABE (FH-ABE) encryption scheme is used where files are protected based on the layered entry layout. Pertaining to encryption where users encrypt data based on attributes induced by measuring user's characteristics and corresponding assigned weights, Ciphertext-Policy Weighted ABE (CPW-ABE) was suggested as an efficient ABE. Moreover, to prevent the disclosure of data owners' and data users' sensitive data, Policy Hidden ABE (PH-ABE) has been used [16]. Multi-level ABE (ML-ABE) allows data to be encrypted through multi-level access control schemes whereby users can access only parts of data. Partially hidden access policies are maneuvered to hide the private information attributes and fully hidden ABE policies are used to hide private information and their values.

Policy Hidden Outsourced ABE (PHO-ABE) allows a user to delegate the decryption process execution to a semi-trusted server but keeps the ability to verify decrypted data correctness. To perform user authentication, Attribute-Based Signatures (ABS) have been proposed whereby the user must hold a set of attributes satisfying an access policy to sign a message. An attribute authority generates user attributes and private keys, and a verification entity verifies generated signatures [16]. Multiple Authority ABS (MA-ABS) allows multiple authorities to manage attributes and private keys. Attribute-Based SignCryption (ABSC) logically combines ABE and ABS in one-step to provide fine-grained and granular access control, authentication of data origin, and data confidentiality.

There is a certain cryptographic method, the location-based encryption method, which allows encryption and decryption to be possible only at a specific location using location details to generate cryptographic keys. Relatively, a hybrid algorithm, comprising of both the symmetric Advanced Encryption Standard (AES) algorithm to encrypt data and the asymmetric Rivest-Shamir-Adleman (RSA) algorithm to encrypt the AES private key for key exchange are used to protect data [17]. The fast computation of symmetric algorithms and the high security of asymmetric key pairs prevent HTTP-centric brute force attacks while guaranteeing secure key exchange.

Cognitive cryptography is used for intelligent data management which involves managing strategic, confidential, and secret data, following protocols to verify every information holder, managing semantic information that data contains, and managing data at all the operational levels of the organization entity. In cognitive cryptography, data are secured using unique personal information from biometrics and using semantic information that distinctly identifies individual features of a participant [18]. The cognitive cryptographic protocol involves concealing and encrypting data by splitting and distributing it among a selected group of secret and trusted entities that are identified and verified using their biometric characteristic information and their selected personal features' semantic description.

The review indicates that there are significant research gaps given the security impacts and issues on cloud-based e-learning platforms. e-Learning technologies deal with end-user data such as personal information, location, behavioral patterns, digital footprints, and intellectual properties such as applications, notes, videos, and research. Since cloud computing deals with the transmission, storage, processing, and access of this e-learning data, the analysis and recommendations cover a broad view and multiple aspects of the entire cloud-based e-learning service.

III. Methodology

This section demonstrates the methodology used for reviewing the literature of e-learning and cloud computing security and also on the analysis of the identified concerns. An empirical study was performed using qualitative techniques and systematic review as the research instruments for the technical analysis of documents. A systematic review was employed in selecting and critically appraising research relevant to the domain. The documents focus on e-learning technologies, cloud computing, information security, security impacts, and cryptographic techniques on e-learning and cloud computing. These technical documents have been reviewed to learn about how cloud-based e-learning technologies work and about the latest advancements in security aspects and cryptographic techniques in cloud computing and e-learning. The development of cryptography in the recent years related to the theme of cloud-based e-learning is evaluated from the literature using chronological and thematic methods. The results are categorised thematically based on functionalities, security aspects and different cryptographic techniques. Based on the evaluation, several criterias have been thematised to propose an implementation framework in which a critical appraisal has been performed on these findings in order to formulate recommendations based on different scenarios.

IV. Results and Discussion

Following the study of the state of art in cryptographic techniques applied to cloud-based e-learning systems, the following observations have been made:

1) The entire end-to-end high-level architecture of the cloud-based e-learning service that includes the end-user, the administrators, the internetwork, and the cloud service including servers and storage must be considered when analyzing the cyber security threats faced and the cryptographic techniques used to protect the various aspects of information.

2) The aspects that require protection are Confidentiality, Integrity, Availability, Authenticity, Accuracy, and Non-Repudiation.

3) We propose to use a hybrid form of hierarchical and distributed approaches to break down each component of the end-to-end cloud-based e-learning system in a top-down manner and analyze each component separately.

4) The end-to-end cloud-based e-learning system can be broken down into three tiers, namely, User Tier, Network Tier, and Cloud Tier.

5) The user tier consists of the end-user devices and services accessed by a web browser or an e-learning application. End users can be students, teachers, or administrators.

6) The network tier consists of the internetwork services provided by a network provider or an internet service provider. Usually, TLS/SSL and IPSec VPN technologies are used to secure the connection.

7) The Cloud tier embodies the server and storage infrastructure that is broken down based on IaaS, PaaS, and SaaS service models. The cryptographic techniques specifically used in the Storage component of the Cloud Tier are also analyzed as an independent entity aside from service models.

8) Each tier has its functionality and security aspect requirements, which are fulfilled by cryptographic techniques.

9) Several criteria have been extrapolated from information gathered and are considered when using cryptographic techniques to fulfill the requirements.

*10)*While the use of cryptographic techniques has been theorized and implemented in some capacity, no explicit method or framework has been defined for their implementation across the whole cloud-based e-learning spectrum.

A. Cryptographic Techniques Tabulation

These ten observations exhibit several inferred criteria, and the different cryptographic techniques used in the User Tier and the Cloud Tier as tabularized below. The Cloud Tier includes the Storage, IaaS, PaaS, and SaaS cloud computing services. Table I depicts the functionality of end-user devices and security aspect requirements when accessing a web browser or an e-learning platform that uses cryptographic techniques.

Table II represents the Storage Cloud Tier to analyze the storage component of cloud-based services to protect the various aspects of information.

Table III depicts the IaaS Cloud Tier that explores the security aspects of the running applications and different workloads in the cloud.

Table IV illustrates the PaaS Cloud Tier to analyze the security aspects of developing and managing application functionalities and the corresponding cryptographic techniques.

TABLE I. USER TIER

Functionality	Cryptographic Technique	Security Aspect
1. Access Control and Trust Establishment	• TrustBAC model • TSR Model • PKI	Confidentiality Integrity Availability Authenticity Non-Repudiation
2. Authentication	• Biometrics driven ABC	Confidentiality Integrity Authenticity
3. Course Content Security	• Trust Certificates	Confidentiality Integrity Authenticity Non-Repudiation
4. E-Assessment	• Location-Based Cryptography • Pseudonymization	Confidentiality Integrity Availability Authenticity Accuracy
5. Usage Anonymity	• Pseudonymous credentials (ABC) • Location-Based Cryptography	Confidentiality Accuracy
6. Anonymous Search	• Searchable Encryption	Confidentiality Accuracy
7. Anonymous Retrieval	• PIR	Confidentiality Availability Accuracy
8. Client-Side Deduplication	• Convergent Encryption	Confidentiality Integrity Availability Accuracy
9. Client-Side Availability Check	• PDP	Confidentiality Availability Accuracy
10. Client-Side Integrity and Recoverability Check	• POR	Confidentiality Integrity Availability

TABLE II. STORAGE TIER

Functionality	Cryptographic Technique	Security Aspect
1. File System Security	• IPFS hash functions (SHA-1, SHA-256, and BLAKE2)	Confidentiality Integrity Availability Accuracy
2. Data Deduplication	• Convergent Encryption	Confidentiality Integrity Availability
3. Data Privacy Preservation	• Homomorphic Encryption	Confidentiality
4. Data Secrecy	• Proxy Re-encryption	Confidentiality
5. Data Availability Check	• PDP	Confidentiality Availability Accuracy
6. Data Integrity and Availability Check	• POR	Confidentiality Integrity Availability Accuracy
7. Anonymous Search	• Searchable Encryption	Confidentiality Accuracy
8. Anonymous Retrieval	• PIR	Confidentiality Accuracy
9. Data Signing	• ABSC	Integrity Authenticity Non-Repudiation
10. Intelligent Data Management	• Cognitive Cryptography	Confidentiality Integrity Availability Authenticity Non-Repudiation Accuracy

TABLE III. IAAS TIER

Functionality	Cryptographic Technique	Security Aspect
1. Access Control and Trust Establishment	• NTS-based Cyber Trust	Confidentiality Availability Authenticity Non-Repudiation Accuracy
2. Virtual Machine and Block Data Deduplication	• Convergent Encryption	Confidentiality Availability Authenticity
3. Storage Replication for Disaster Recovery	• PHO-ABE	Confidentiality Availability Accuracy
4. Virtual Machine Encryption	• MA-ABE	Confidentiality Availability Accuracy

TABLE IV. PAAS TIER

Functionality	Cryptographic Technique	Security Aspect
1. Authentication of different types of users	• HABE	Confidentiality Availability Authenticity
2. User-based Encryption	• CPW-ABE	Confidentiality Availability Accuracy
3. Data Replication between Cloud Providers for High Availability	• PHO-ABE	Availability Accuracy

Table V describes the SaaS Cloud Tier to inspect the security aspects of ready-to-use cloud-hosted application functionalities and the corresponding cryptographic techniques.

TABLE V. SAAS TIER

Functionality	Cryptographic Technique	Security Aspect
1. Authentication, Authorization, and Access Control	• RBAC • KP-ABE • CP-ABE	Confidentiality Availability Authenticity
2. File Storage Encryption	• FH-ABE	Confidentiality Accuracy
3. Policy-Based Encryption	• PH-ABE	Confidentiality Accuracy
4. Object Storage Encryption	• ML-ABE	Confidentiality Accuracy
5. File Level Replication	• PHO-ABE	Confidentiality Availability Accuracy
6. File Signing	• ABSC	Integrity Authenticity Non-Repudiation Accuracy

B. Criteria Definition

The criteria below define what cryptographic techniques need to provide and what can be used to measure and evaluate the application of cryptography in fulfilling the requirements previously mentioned. The criteria consider the security needs of end-users of cloud-based e-learning technologies while entirely leaving the implementation specifics upon the cloud-based e-learning provider.

1) Authentication Criteria: The authentication mechanism should use cryptographic personalized based on the attributes of the users so that third-party attributes do not define the key generated per user.

2) Access Control Criteria: Access control and trust establishment cryptographic techniques should be used granularly based on user identity and attributes following the principles of least privilege and separation of privileges principle.

3) Pseudonymisation Criteria: Cryptographic techniques should ensure that a user's e-learning activity and data cannot be used for traceability and inference basis.

4) Anonymous Searching Criteria: Cryptographic techniques should ensure that any e-learning user can perform searches on encrypted data stored on the cloud without revealing what the original data is, to protect intellectual property and integrity.

5) Anonymous Retrieval Criteria: Cryptographic techniques should ensure that any e-learning user can retrieve encrypted data and part of encrypted data on the cloud without revealing what the original data is, to protect intellectual property and integrity.

6) Anonymous Storage Criteria: Cryptographic techniques should ensure that any e-learning user can store encrypted data stored on the cloud without revealing what the original data is.

7) Deduplication Criteria: Cryptographic techniques should ensure that data is not duplicated when stored on the cloud, whether at the source client-side or the destination cloud side.

8) Replication Criteria: Cryptographic techniques should ensure the high availability of data stored on the cloud through replication without revealing what the original data is.

C. Proposed Implementation Framework

The application and implementation of the above cryptographic techniques along the end-to-end cloud-based e-learning architecture can be done in a holistic and guided software framework as follows:

1) A multi-agent system consisting of software agents could be installed on all users' devices including computers, smartphones, and tablets to perform various activities based on each user's roles and attributes.

2) Administrators could manage cryptography applied to cloud storage and each of the cloud service models of IaaS, PaaS, and SaaS.

3) Students could encrypt, decrypt, sign, authenticate, manage keys, choose ciphers, verify certificates and signatures and check e-assessment cryptography features based on the roles, privileges, and attributes they have been assigned.

4) Since high-end and computationally intensive cryptographic techniques have been proposed, the underlying cloud infrastructure could be provisioned with adequate resources such as Graphical Processing Units (GPU), virtual GPUs (vGPU), and memory, to handle both Cloud Tier cryptographic processes and to sustain client-side ones that could be outsourced to them via the agents.

5) The locally installed software agents could use the available end-user device resources to perform calculations if the device can support such activities using inbuilt technology such as trusted platform modules in the case of computers and laptops or encryption chips for smartphones.

6) The local agents could interface with web browsers installed on the end-user devices and provide access to the e-learning services through a web portal without affecting user experience or adding ambiguity.

7) If the e-learning platform being accessed provides a VPN to the end-user to access its services, the software agent could be the local endpoint of the VPN to the user, providing both token generation and authentication interface and web access to the service via web browser integration.

8) The software agent could also automatically or interactively install security certificates in the web browsers to which it is integrated.

9) The software agent could be integrated into the cloud service management console provided to the administrators by cloud providers via their application programming interfaces.

10) Finally, the administrators could implement and administer the PKI that governs the certificates being used using the software agent.

V. Conclusion

The use of cloud computing and its service models to deliver e-learning technologies, followed by the impact on cyber security aspects and threats was reviewed systematically. The innovative cryptographic techniques used in cloud computing and e-learning have been presented in terms of authentication, access control, pseudonymization, data storage, and access. It was observed that instead of a holistic approach to cryptography, only specific aspects of cloud-based e-learning were focused on and that no explicit implementation guidelines nor framework currently exist. As a result, this comprehensive review provides a holistic tabulation of cryptographic techniques for cloud-based e-learning. It also defines a set of criteria that can be used to evaluate whether the existing cryptographic techniques are fulfilling the requirements as needed. Finally, a framework is proposed to implement cryptographic techniques in a unified way across an end-to-end cloud-based e-learning architecture using multi-agent software. The empirical results are considered in the light of some limitations to the existing literature in cryptography

for cloud-based e-learning technologies. For future work, a theoretical framework will be implemented via a holistic approach using different cryptographic techniques. This will lead the pathway to practical implementations of the framework.

REFERENCES

[1] A. Chopra and A. Chopra, "Security Threats and Remedies in E-Learning System," International Journal of Computer Science and Telecommunications, vol. 7, no. 7, pp. 6-10, 2016.

[2] M. S. Malhi, U. Iqbal, M. M. Nabi, and M. A. Malhi, "E-Learning Based on Cloud Computing for Educational Institution: Security Issues and Solutions," International Journal of Electronics and Information Engineering, vol. 12, no. 4, pp. 162-169, 2020.

[3] N. Kaaniche and M. Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms," Computer Communications, vol. 111, pp. 120-141, 2017.

[4] M. Bosamia and A. Patel, "An overview of cloud computing for e-learning with its key benefits," International Journal of Information Sciences and Techniques, vol. 6, pp. 1-10, 2016.

[5] A. Rahman, S. Sarfraz, U. Shoaib, G. Abbas, and M. A. Sattar, "Cloud based E-Learning, Security Threats and Security Measures," Indian Journal of Science and Technology, vol. 9, no. 48, pp. 1-8, 2016.

[6] M. Bhatia and J. K. Maitra, "E-Learning Platforms Security Issues and Vulnerability Analysis," In: International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES), Lucknow, India, pp. 276-285, 2018.

[7] C. Kiennert, P. Rocher, M. Ivanova, A. Rozeva, M. Durcheva, and J. Garcia-Alfaro, "Security Challenges in e-Assessment and Technical Solutions," In: 21st International Conference on Information Visualisation, London, UK, pp. 366-371, 2017.

[8] S. Ramjan, "E-Learning Security for Collaborative Academy in Area of ASEAN Community," In: 12th International Conference on eLearning for Knowledge-Based Society, Thailand, pp. 23.1-23.8, 2015.

[9] O. Adejo, I. Ewuzie, A. Usoro, and T. Connolly, "E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure," International Journal of Information Technology and Computer Science, vol. 4, pp. 1-9, 2018.

[10] M. Durairaj and A. Manimaran, "A Study on Security Issues in Cloud based E-Learning," Indian Journal of Science and Technology, vol. 8, no. 8, pp. 757-765, 2015.

[11] L. Q. Huan, D. Nyugen, H. Pham, and N. Huynh-Tuong, "Authentication in E-Learning Systems: Challenges and Solutions," Science and Technology Development Journal - Engineering and Technology, vol. 3, no. 1, pp. 95-101, 2020.

[12] A. Kassid and N. El Kamoun, "Towards a new access control model based on Trust-level for E-learning platform," Journal of Information Assurance and Security, vol. 11, no. 6, pp. 302-310, 2016.

[13] D. Melnikov, V. Petrov, N. Miloslavskaya, A. Durakovskiy, and T. Kondratyeva, "Cybertrust in e-Learning Environment based on Network Time Synchronization," In: 8th International Conference on Computer Supported Education, Setubal, Portugal, pp. 402-407, 2016.

[14] R. Ali and H. Zafar, "A Security and Privacy Framework for e-Learning," International Journal for e-Learning Security, vol. 7, no. 2, pp. 556-566, 2017.

[15] V. Pavani, P. S. Krishna, A. P. Gopi, and V. L. Narayana, "Secure data storage and accessing in cloud computing using enhanced group-based cryptography mechanism," in: Materials Today: Proceedings, 2020.

[16] S. Belguith, N. Kaaniche, and M. Hammoudeh, "Analysis of Attribute-Based Cryptographic Techniques and their Application to Protect Cloud Services," Transactions on Emerging Telecommunications Technologies, e3667, pp. 1-13, 2019.

[17] N. S. M. Shamsuddin and S. A. Pitchay, "Location-Based Cryptographic Techniques for Data Protection," Malaysian Journal of Science, Health & Technology, vol. 4, pp. 65-68, 2019.

[18] M. Ogiela and L. Ogiela, "Cognitive cryptography techniques for intelligent information management," International Journal of Information Management: The Journal for Information Professionals, vol. 40(C), pp. 21-27, 2018.