Postprint of : Bhat S. A., Alyahya D., Dar M. A. , Shah S., Edge-Computing based Secure E-learning Platforms, 2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Jeju Island, Korea, Republic of, 21-24.02.2022, pp. 324-328, DOI: 10.1109/ICAIIC54071.2022.9722680

Edge-Computing based Secure E-learning Platforms

Sameer Ahmad Bhat[1,2], Dalia Alyahya[3], Muneer Ahmad Dar[4] and Saadiya Shah[4]

[1]Graduate Studies and Research, Gulf University for Science and Technology (GUST), Kuwait.
[2]Dept. of Multimedia Systems, Gdansk University of Technology, Pomerania Gdansk, Republic of Poland.
[3]Dept. of Instructional Technology, King Saud University (KSU), Riyadh, Saudi Arabia.
[4]National Institute of Electronics and Information Technology (NIELIT), Jammu & Kashmir, India.
Email(s): bhat.s@gust.edu.kw, dmalyahya@ksu.edu.sa, muneer@nielit.gov.in, shah.saadiya@gmail.com

***Abstract*—Implementation of Information and Communication Technologies (ICT) in E-Learning environments have brought up dramatic changes in the current educational sector. Distance learning, online learning, and networked learning are few examples that promote educational interaction between students, lecturers and learning communities. Although being an efficient form of real learning resource, online electronic resources are subject to threats and vulnerabilities on the internet. Authentication, access and storage of data is a major concern among many organizations implementing E-learning platforms. This study provides a literature review of past five-year research studies, and proposes Edge-computing based solution to the currently existing authentication and data access problems that prevail in the current E-learning management systems using cloud services for data storage. The study guides researchers towards enabling Edge-computing based E-learning platforms to support low power computing devices running Elliptic Curve Cryptography for secure access and authentication.**

***Index Terms*—E-learning, Cryptography, Edge-Computing, Cloud Computing, Cryptography, ECC, ECDH, Instructional Technology**

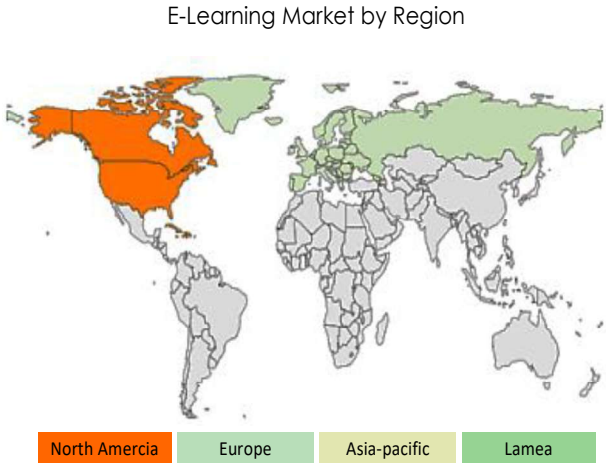

Fig. 1. Asia-Pacific would exhibit the highest CAGR of 17.4% during 2021-2030 [28].

I. Introduction

Rapid E-Learning technology progression is currently shaping the methodology of how the teaching and learning practices are carried out in today's educational environments [1]. The report by [28] states that "COVID-19 pandemic is expected to positively impact the growth rate of the e-learning market, owing to increase in adoption of digital technologies among various schools, colleges and universities across the globe and growing government support for improving e-learning platform across various developing nations of Asia-Pacific and LAMEA countries". Previously valued at $197.00 billion in 2020, the global e-learning market size is projected to reach at level of $840.11 billion by 2030, thereby registering a CAGR of 17.5% from 2021 to 2030 . While several definitions of eLearning have been proposed, generally agreed definitions state that eLearning employs computers and several other instruments of information communication technology (ICT) to enable support to and facilitate in the ongoing teaching and learning processes [2]. With focus on augmented technologies and boom in information access, E-learning has been widely accepted as an essential platform of learning since it allows learners to acquire knowledge and skills ubiquitously, whilst in the physical absence of a mentor(s) or teacher(s) [3] Typically, E-learning makes use of computing technologies, primarily connected over an intranet or Internet, to deliver information and instructions to individual learners [21]. While this broader definition is interesting, E-learning in this context is referred to as training delivered via network technology. Here the term 'training' refers to planned efforts that increase job-related knowledge and skills [4].

Academic or non-academic organizations, or even industry experts cover knowledge management and virtual collaboration in their definition [22]. E-learning in this case is described to broadly include any system that generates and disseminates information and is designed to improve learners' performance [5]. Alternatively, E-learning is also considered as a disruptive technology since it transforms practices of how learning is approached in an educational context [6]. In the times of CoVID-19, most of the education systems are in future envisioned to change entirely with the development of newer innovate E-Learning platforms, in particular the quality e-education services and supporting processes.

E-Learning systems mainly have five significant participants – Authors, Students, Managers, Teachers and System Developer (System Administrators). Apart from that, unauthorized users, basically hackers may attempt to gain illegal access to the E-learning systems to steal critical resources [7]. In present E-learning systems, managers or instructors communicate with learners, and share resources that require elevated security and

secure data communication methods and protocols, thereby prevent unauthorized and unprecedented access to services by unrecognized users. Hackers can alter or modify E-Learning resources such as learning materials, certificates, question papers, lecture materials, mark sheets etc. [8]. To leverage the IoT features in the E-Learning systems, the study by [24] highlights vital security issues that significantly influence the ways, how IoT layered architectures are structured, and how the vulnerabilities exhibited by the Cloud networking services severely pose threats data and information security. Apparently, vulnerabilities as such lead to inefficient and nonfunctional service thereby expose critical information to the malevolent users. This could pose a severe threat to the E-learning systems, and E-learning data management teams must highly secure the E-learning system resources [9].

From our literature review, we observe the different definitions of E-learning. For example, the definition by [10] finds four dimensions Fig. 2 to define the concept of E-learning:

- Technology-driven: Use of technology to deliver learning and training programs;
- Delivery-system-oriented: The delivery of a learning, training, or education program by electronic means;
- Communication-oriented: Learning facilitated by the use of digital tools and content that involves some form of interactivity, which may include online interaction between the learner and their teacher or peers; and
- Educational-paradigm-oriented: Information and communication technologies used to support students to improve their learning.

II. Current Trends – Encryption Standards in E-learning

Though being efficient, online e-learning resources available on the internet are prone to threats and vulnerabilities on the internet. E-learning systems as such must satisfy the basic concepts of data security – integrity, confidentiality and availability [11]. Confidentiality – aims to ensure privacy to data and information. Data and information, both are kept secret and private, and prevented from unauthorized access by people, application processes or any hardware devices. Integrity – aims to ensure originality, correctness, and accuracy of data and information by preventing it from any accidental losses, or intended malicious attacks to update or modify the original content. Data and information must remain in original structure and format. Availability – aims to ensure access to reliable data, information, and communication in a timely manner to authorized users. Non-repudiation assures that user who carry out operations in a system, cannot deny their actions. For example, if a user deletes his/her learner's results, and then denies the act, then the system should provide necessary log files pertaining to operations carried out by the user, so as to back track or trace performed operations on the system. Moreover, tamper-proof and reliable log files must be retained, and system auditing allows to fulfil this requirement. A digital signature is a countermeasure for non-repudiation.

Typical encryption algorithms applied to secure file systems are: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, Chaos Approach. Based on review

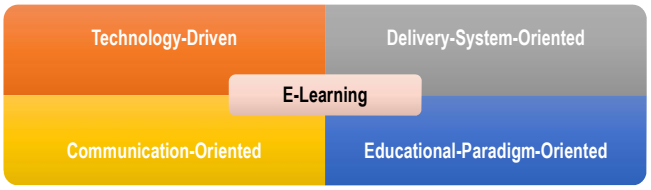

Fig. 2. Sangrà et al. [10]

of literature it is found that each of these algorithm is giving varying performance as context changes and there are some constraints observed among few of these algorithm. Various algorithms have been used to encrypt data in E-learning systems. For example, Ambalika Ghosh at al. [12] propose an object-oriented modelling approach, and implement International Data Encryption Algorithm (IDEA) to show how privacy and confidentiality of information, communicated between a teacher and student at the time of displaying marks scored for a course can be achieved. IDEA is a symmetric-key block cipher, and operates on 64-bit blocks using a 128-bit key and consists of a series of eight identical transformations. IDEA, as an encryption–decryption technique can protect roll number or marks for any changes made by the hackers.

Nikhilesh Barik et al. [13] propose framework implementing unique authorization with a Two-Level Access Control (TLAC). Shared secret key encrypts a service request and public key infrastructure guarantees the confidentiality of message during transmission. If any document was altered by the malicious users, the receiver would get the different digests for the original message. So the integrity and non-repudiation is achieved by using digital signature. In case deletion of any documents from the managers' side, it is possible to trace back with archived log files. Tamper proof mechanism may be used to solve the problem.

Ahmad Baihaqi et al. [14] have implemented AES 256- bit for document encryption, RSA 2048-bit for digital signature, and SHA 256 bit for message digest in PHP and JavaScript programming language. The study designs a Secure Electronic Learning System (SELS) application that supports basic security features – confidentiality, integrity, authentication, and non-repudiation.

Chuyang Li et al. [8] propose Blockchain technology based solutions to problems in online education, wherein it is used for e-learning assessment and certification. The study also proposes a network structure using combined public and the private Blockchain. New network structure using combined public and private Blockchain eliminates limitation of a single node role in traditional single-Blockchain systems with high flexibility, and it also fully retains the security and credibility of the Blockchain technology.

Karima et al. [15] propose a plug-in named EL-Security checker that enable controlling, verifying and eliminating attacks in e-learning platforms. The study proposes a solution that analyzes, verifies and checks authentication attacks. A new layer, called El-Security Layer is formulated to control and verify authentication vulnerabilities, affecting the e-learning system. Module to module communication is established using the Request-Response model.

Jegatha Deborah L et. al [16], propose a simple mutual authentication dialogue between the students and the server. The online examination system develops a secure system to distribute and collect the question papers and answers scripts to and from the students, respectively. At the end of examination, each student submits it response back to the server. S. Kanimozhi et. al [17] have implemented a cloud-based e-learning system employing access control mechanism that prevents illegal user access to the resources of cloud. The study discusses key management schemes in combination with access control technique to secure share content and enable protection to e-learning environment. Findings show that cloud services are secure, flexible, and scalable in cloud-based e-learning.

Priyanka Saxena et al. [18] propose an intuitive authorization mechanism implementing customized set of rules and authorization key-based mechanisms that increases the level of security. The study develops a new system built with training machines to: a) identify unauthorized user accesses, and b) prevent theft or mal-processes if any user is authenticated by other means. Post to authentication, authorization is carried out using modified role-based access control. Key encryption uses SHA256 hash generation working one way only, and cannot be reversed by anybody in the system, though by users who leak the key.

We conducted a literature review of articles published over the past five years. From the review, we observe that most of the research studies have focused on developing frameworks and improving content organization in E-learning systems. However, just few research studies have attempt to provide an insight into the security issues prevailing in the E-learning systems.

A. Problem Statement

Qualitative analysis of recent articles referenced in the prior section shows that:

- the basic security mechanisms have been implemented mostly on server side, and clients are expected to own their devices with medium to high level of computational power, in order to access available E-learning resources online.
- Authentication mechanisms employ encryption algorithms to allow users gain access to the E-learning systems. Encryption algorithms typically used are computationally expensive in terms of required hardware resources. For example, algorithms, such as Rivest–Shamir–Adleman (RSA) may offer secure solutions that are often difficult to comprise, these in turn demand high speed computational devices for efficient operation.
- The power of Edge-computing [19] has been overlooked completely to process data locally, and mostly cloud servers are employed for access to data and storage.

III. Secure E-learning Systems

In the following sub-sections, we propose solutions to the previously stated challenges. The first part addresses the need to reduce the processing load on the authentication server. The second and the third part address the need to reduce computational complexity of security mechanism, as well as to ensure local availability of data.

A. Light weight Cryptography

Despite more appealing features, researchers, techno-savvy and educated class of smartphone users are highly concerned about the security of data stored in either smartphones or other mobile devices such as laptops or Tablet computers, and the way how confidentiality is ensured when such mobile devices exchange data with each other or communicate over a network susceptible to intruders. Typically, learners employ such low power computational devices to gain access to E-learning resources, and this requires encryption of authentication and authorization data. Symmetric encryption algorithms such as DES, 3DES, ADES, and others, and asymmetric encryption algorithms which include RSA, Diffe-Hellman, ECC, and others, are traditional encryption algorithms [20]. Data encryption by these algorithms show low operability, posing obstacles in subsequent data processing.

To ensure, low power computational devices are supported, we propose Elliptical Curve Cryptography (ECC) as the best possible solution since it offers the same level of encryption/decryption with just a key size of 210 bits compared to the level of security offered by RSA that uses a long key size of 2048 bits (see Table I). Encryption key used in ECC conceals secret data so prevent an unidentified user to decipher its contents. The enciphering process of hides the plain text data, and the encryption process results cipher text as its output. While in engaged in communication, the encipherer decodes the message to be communicated and generates a cryptogram. The cryptogram is transmitted and sent to the recipient.

Elliptic Curve Cryptography (ECC) as an asymmetric, public key cryptographic technique, allows communicating devices to generate two keys – a public key and a secret key called the private key. The public key is distributed to all the devices, and the private key is hidden and kept secret by the client encrypting or decrypting the message [23].

Definition 1 (Elliptic Curves). Let P represents the field of characteristic $\neq 2, 3$, then an elliptic curve $\mathbb{G}_P$ defined over the P consists of the set of elements $(x, y) \in P^2$, that satisfy the eq(1), which is the short Weierstraß equation of an elliptic curve.

An Elliptic curve $\mathbb{G}$ over $\mathbb{G}_P$ is a set of all solutions $(x, y) \in \mathbb{P} * \mathbb{P}$ to an equation

$$y^2 = x^3 + cx + d \tag{1}$$

where $(a, b) \in P$ satisfy the relation $-16(4a^3 + 27b^2) \neq 0$, represents quantity $\triangle$, the discriminant of eq(1). $\triangle \neq 0$ denotes the singularity of the curve $\mathbb{G}_P$.

The elliptic curves $\mathbb{G}_P$ consists of elements called points. Fig. 3 and Fig. 4 show the elliptic curves defined over the two finite fields F_{1021} and F_{16381}.

IV. Edge-Computing enabled Authentication and Data access

Edge computing (EC) is an extension of cloud computing with its own characteristics that are different than the

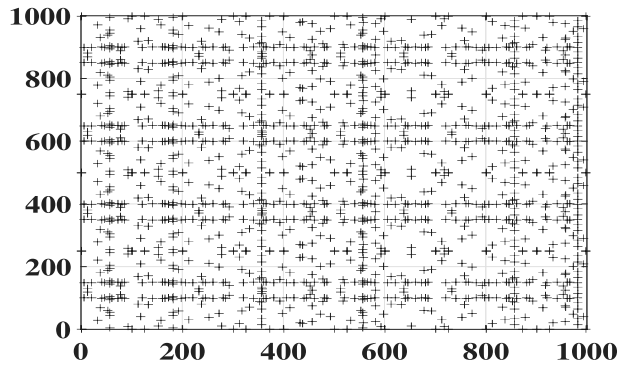

Fig. 3. $G_{P_{1021}} : y^2 = x^3 - 3x + 3$ [23]

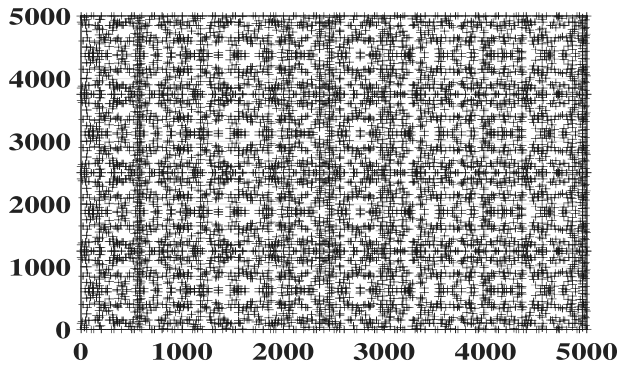

Fig. 4. $G_{P_{16381}} : y^2 = x^3 - 3x + 3$ [23]

characteristics of cloud computing. Cloud servers process large amounts of data, offer in-depth analysis on data, and even support real-time or non-real times solutions in business decision making processes. EC enables storage of data on locally available devices, mostly close to the information source, and thus the need to upload data to Cloud servers is eliminated. Bandwidth, delay, and jitter are easily controllable and improve due to the reduction of network size. In the case of E-learning, network bandwidth is significantly improved with reduced network size. EC is employed in small-scale intelligent analysis and local services, while Cloud computing supports centralized processing of large-scale data. EC extends a small-scale role compared to Cloud services and allows real-time intelligent analysis and processing of data locally on devices supporting computing at Edge networks. While being close to the source and feasible, at the edge of a networks, EC systems enable platforms that allow storage to consumer data and access features. Healthcare improvisation, Network optimization processing, and data transportation are some of services managed by EC devices currently.

Digital transformation needs intuitive solutions to drive the current processes and methodologies implemented in Industry Revolution 4.0 (IR). IR demands data sensing mechanisms implementing Industrial Internet of Things (IIoT), Blockchain, Cyber Physical Systems (CPS), Digital Twin, and high speed reliable access to internet provided by state-of-art technologies, such as 5G or 6G. These are basically the core drivers of digital transformation in industries looking forward to developing Smart systems. However their role in academics is still at infancy stage, though exceptions are there, for instance Edge Computing has significantly impact the ways in which academia and industries have emerged in the recent times, especially during CoVID-19 pandemic.

TABLE I
COMPARISON OF KEY LENGTH (IN BITS)

RSA- key	ECC - key	Proportion of RSA/ECC
512	106	5:1
768	132	6:1
1024	160	7:1
2048	210	10:1

The Internet of Things (IoT), virtual worlds, and vehicle-to-vehicle interactions are moslty realized to rely on the Cloud computing infrastructures as these enable access to end users at ease and ubiquitously [25]–[27]. EC systems basically integrate the advanced capabilites of IoT and 5G networking infrasture. As such EC systems reveal features, such as low network bandwidth requirement, portability and safety of edge devices. While functional and operative at network's edge, EC systems may expose various computational, storage, and networking services to the end users. Consumers of EC system services can access data and other system serves, whereas the edge software can be developed and managed in a short span of time compared to cloud services that often need longer times to ensure highly efficiency.

As from the literature review, typical authentication processes in E-learning systems require sending users' data to the server for authentication, and then servers respond with a validation response. With prolific users connected to a system, large authentication processes overload the server, thereby resulting in slow response times or even denial of requests by the server. Though in usual user authentication processes, the current systems may run without showcasing any serious implications, however when it comes to conducting events, such as large scale online exam, demand reliability and exhibit serious concerns.

EC offers the optimized solution to overcome this problem. The resources in the EC and users of edge network are in the close proximity (e.g., location), this lead EC to enable personalized services for users, as per the current scenarios, such as location-based services. We propose a two stage authentication process Fig 5, wherein Edge manager first locally authenticates users, and then communicates authentication statistics to the main Cloud server, or other servers used in the authentication process. Many trust domains can coexist since edge computing serves as a source of distributed interactive computing environment. Assignment of an identity to each entity is essential within the trust domains and even for mutual authentication, when different trust domains coexist. Cross-domain authentication and handover authentication technologies offer support to data and privacy security of users in different trust domains and heterogeneous network

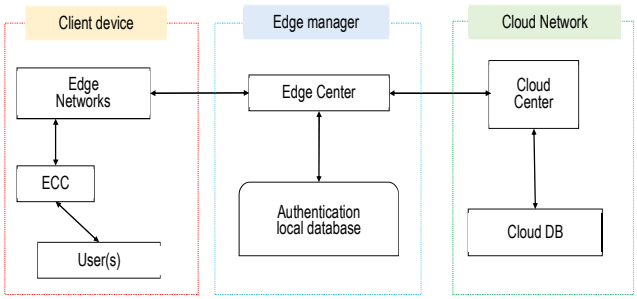

Fig. 5. Authentication process using Edge-Computing.

environments [19]. EC group specific databases can be stored locally on EC networks and then users assigned to those groups can be authenticated without the need from the actual authentication server. This would significantly reduce the load on the authentication server, and response times from the main authentication server can improve drastically.

V. Conclusions

This study provides a review of the recent security methods, prevailing in the existing E-learning management systems. Research studies of past five years are evaluated to determine the current trends and techniques that are employed to enable security in online learning platforms. Edge-computing as an emerging solution is proposed in this study, to address the challenges of authentication and data access methods in E-learning systems. We envision that Edge networks can act as proxy servers enabling local authentication and authorization to resources existing on the actual Cloud server. This would enable dual authentication as well as add a new local security layer to the existing learning management networks. In our future studies, we aim to implement the concept in a real time scenario to observe the real time characteristics of the proposed system.

References

[1] H. Lucas and J. Kinsman, "Distance- and blended-learning in global health research: potentials and challenges," Glob. Health Action, vol. 9, no. 1, p. 33429, Dec. 2016, doi: 10.3402/gha.v9.33429.

[2] R. Phillips, G. Kennedy, and C. McNaught, "The role of theory in learning technology evaluation research," Australas. J. Educ. Technol., vol. 28, no. 7 SE-Articles, Aug. 2012, doi: 10.14742/ajet.791.

[3] A. Moubayed, M. Injadat, A. Shami, and H. Lutfiyya, "Student engagement level in an e-learning environment: Clustering using k-means," Am. J. Distance Educ., vol. 34, no. 2, pp. 137–156, 2020.

[4] E. T. Welsh, C. R. Wanberg, K. G. Brown, and M. J. Simmering, "E-learning: emerging uses, empirical results and future directions," Int. J. Train. Dev., vol. 7, no. 4, pp. 245–258, Dec. 2003, doi: https://doi.org/10.1046/j.1360-3736.2003.00184.x.

[5] M. J. Rosenberg and R. Foshay, "E-learning: Strategies for delivering knowledge in the digital age." Wiley Online Library, 2002.

[6] D. R. Garrison, E-learning in the 21st century: A community of inquiry framework for research and practice. Taylor & Francis, 2016.

[7] R. Bansal, A. Gupta, R. Singh, and V. K. Nassa, "Role and Impact of Digital Technologies in E-Learning amidst COVID-19 Pandemic," in 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2021, pp. 194–202.

[8] C. Li, J. Guo, G. Zhang, Y. Wang, Y. Sun, and R. Bie, "A blockchain system for E-learning assessment and certification," in 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), 2019, pp. 212–219.

[9] A. A. Keshlaf, A. A. Alahresh, and M. K. H. Aswad, "Factors Influencing the Use of On-Line Meeting Tools," in 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, 2021, pp. 908–912.

[10] A. Sangrá, J. E. Raffaghelli, and M. Guitert-Catasús, "Learning ecologies through a lens: Ontological, methodological and applicative issues. A systematic review of the literature," Br. J. Educ. Technol., vol. 50, no. 4, pp. 1619–1638, 2019.

[11] S. Kausar, X. Huahu, A. Ullah, Z. Wenhao, and M. Y. Shabir, "Fog-Assisted Secure Data Exchange for Examination and Testing in E-learning System," Mob. Networks Appl., 2020, doi: 10.1007/s11036-019-01429-x.

[12] A. Ghosh and S. Karforma, "Object-oriented Modeling of IDEA for E-learning Security," in Intelligent Computing and Applications, Springer, 2015, pp. 105–113.

[13] N. Barik and S. Karforma, "Secure e-Learning Framework (SeLF) BT - Information Systems Design and Intelligent Applications," 2015, pp. 691–698.

[14] O. C. Briliyant and A. Baihaqi, "Implementation of RSA 2048-bit and AES 128-bit for Secure e-learning web-based application," in 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), 2017, pp. 1–5, doi: 10.1109/TSSA.2017.8272903.

[15] K. Aissaoui and M. Azizi, "El-Security: E-learning Systems Security Checker Plug-in," in Proceedings of the 2nd international Conference on Big Data, Cloud and Applications, 2017, pp. 1–6.

[16] J. D. L, K. R., V. P., B. S. Rawal, and Y. Wang, "Secure Online Examination System for e-learning," in 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 2019, pp. 1–4, doi: 10.1109/CCECE43985.2019.9052408.

[17] S. Kanimozhi, A. Kannan, K. Suganya Devi, and K. Selvamani, "Secure cloud-based e-learning system with access control and group key mechanism," Concurr. Comput. Pract. Exp., vol. 31, no. 12, p. e4841, 2019.

[18] P. Saxena and H. Sanyal, "Improved Rules and Authorization Key Processing for Secured Online Training," in 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2020, pp. 690–694, doi: 10.1109/ICECA49313.2020.9297463.

[19] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," IEEE access, vol. 8, pp. 85714–85728, 2020.

[20] Dar, M. A., Askar, A., Alyahya, D., & Bhat, S. A. (2021). Lightweight and Secure Elliptical Curve Cryptography (ECC) Key Exchange for Mobile Phones. International Journal of Interactive Mobile Technologies (iJIM), 15(23), pp. 89–103., doi: 10.3991/ijim.v15i23.26337.

[21] M. A. Dar and S. A. Bhat, "Evaluation of mobile learning in workplace iraining," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016, pp. 1468-1473, doi: 10.1109/ICACCI.2016.7732255.

[22] Askar, A. Mobile Electronic Performance Support System as a Learning and Performance Solution: A Qualitative Study Examining Usage, Performance, and Attitudes. Turkish Online Journal of Educational Technology, 17(2), (2018), pp. 76-88.

[23] Djath, L., 2021. RNS-Flexible hardware accelerators for high-security asymmetric cryptography (Doctoral dissertation, Université de Bretagne occidentale-Brest).

[24] Shah JL, Bhat HF, Khan AI. Integration of Cloud and IoT for smart e-healthcare. InHealthcare Paradigms in the Internet of Things Ecosystem 2021 Jan 1 (pp. 101-136). Academic Press.

[25] Bhat SA, Dar MA, Elalfy H, Matheen MA, Shah S (2021). A Novel Framework for Modelling Wheelchairs under the Realm of Internet-of-Things, International Journal of Advanced Computer Science and Applications(IJACSA), 12(2), (2021). http://dx.doi.org/10.14569/IJACSA.2021.0120293

[26] Belchior R, Vasconcelos A, Guerreiro S, Correia M. A survey on blockchain interoperability: Past, present, and future trends. ACM Computing Surveys (CSUR). 2021 Oct 4;54(8):1-41.

[27] Rover DT, Mina M, Herron-Martinez AR, Rodriguez SL, Espino ML, Le BD. Improving the Student Experience to Broaden Participation in Electrical, Computer and Software Engineering. In2020 IEEE Frontiers in Education Conference (FIE) 2020 Oct 21 (pp. 1-7). IEEE.

[28] Allied Market Research. https://www.alliedmarketresearch.com/e-learning-market-A06253, 2021. (accessed on: 20.01.2022).