CBES: A framework for Cloud-based E-learning System at SaaS Level

Ahsan Ahmed[1,*], Mohd Anul Haq[2], Niranjan Polala[3], Vuppu Shankar[4], Jayadev Gyani[2]

a.ahmed@mu.edu.sa, m.anul@mu.edu.sa, pnr.cse@kitsw.ac.in, vs.csn@kitsw.ac.in, je.gyani@mu.edu.sa

[1]Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah 11952, Saudi Arabia
[2]Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Al-Majmaah 11952, Saudi Arabia
[3]Dept of CSE, Kakatiya Institute of Technology & Science, Warangal, Telangana, India
[4]Dept of CSE (Networks), Kakatiya Institute of Technology & Science, Warangal, Telangana, India

***Corresponding Author:** a.ahmed@mu.edu.sa

Summary
Today, as we are living in the era of the Internet, the word "cloud" revolves around everyone. Cloud Computing is the concept that is implemented to provide high computing inexpensive infrastructure and software available on demand. The usage of cloud-based e-learning systems is increasingly becoming popular day by day and is gaining demand around the world. Almost all private and public educational institutions are adopting cloud computing for managing their learning resources. It provides easy anywhere easy access to its users but still the policies or methods to secure the cloud are still not developed properly. Truth worthiness is becoming critical for the future usage of Cloud-based e-learning systems (CBES). The paper discusses different advantages and weaknesses issues related to a CBES and finally proposed a framework that overcomes the different challenges for CBES at the SaaS level, thus increasing the levels of acceptance of using the CBES.

Keywords:
e-learning; Cloud Computing; Security; Cloud Policies; IAAS, PAAS, SAAS, CBES

1. Introduction

The changing world of Information Technology in this 21st century has a great impact on education. The future of tomorrow's technology directly depends on the adoption of technology by the students of this current era. The advancement of science and technology has changed the process of teaching and learning by creating many alternate methods for the same. The traditional way of teaching-learning does not support interactivity. Therefore, learners are losing interest in a traditional way of imparting knowledge, and it is no more in demand. E-Learning is an approach to learning by using electronic gadgets like computers, mobiles, laptops, iPad, etc. E-learning environments offer interactive features that increase the student's motivation for the learning process. It involves many to many interactions between its users by using the standards of web 2.0 and web 3.0. Almost all the university around the globe are transforming their traditional classroom-centered education into e-learning education by adopting cloud-based e-learning systems on their premises. Educational stakeholders (students and teachers) are getting more engaged in their teaching-learning process by adopting an e-learning environment that offers different learning styles. The e-learning system provides many advantages over the traditional education system. Better management of educational content, user performance, user assessment, cost-effective, more interactive, offers a variety of courses, user's attendance, user's authentication, availability of online experts, schedule flexibility, real-time 24 x 7 operations, a large number of audiences, increase knowledge retention, efficient in term of time, more freedom to ask questions, self-paced learning, pre-notification/alert, quick approach to the resources and easy access across borders. Nowadays, e-learning methodologies like gamification are used to improve the pedagogy in teaching-learning institutions.

Cloud Computing is the latest technology that offers dynamically highly scalable resources (hardware, operating environment, software) 24/7. It is a new internet-based technology that brought down the price of hardware infrastructure, software tools, and data processing and storage. Software in cloud computing is used to automatically aggregate computing resources and manage them [2-4]. The development of service-oriented architecture led to the development of cloud computing (SOA). Cloud computing may be summed up as a group of services that various consumers can request from a cloud service provider.

Manuscript received November 5, 2022
Manuscript revised November 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.11.92

Three different sorts of layers make up the cloud architecture: SAAS (Software as a Service), PAAS (Platform as a Service), and IAAS (Infrastructure as a Service). Through a web browser, SAAS offers its users on-demand access to various software. An illustration of SAAS services is Google App [5]. Cloud computing in PAAS offers system software and computer platforms as a service. By utilizing software and platform-level resources including operating systems and application platforms, PAAS provides the client with an electronic environment for constructing cloud infrastructure [6]. Bungee Connect is a notable example of a PAAS that offers a full range of tools for managing the software development life cycle.

Computing and storage infrastructure are referred to as IAAS. Data centers, networking tools, and bandwidth set aside for storage are all included. IAAS allocates the resources for the services that are used by the users and therefore IAAS makes use of a load balancer for balancing the load on the server [7]. One of the better examples of IAAS that offers highly scalable processing capacity is Amazon's EC2. The amount that each user utilizes for each of the three services determines how often they are paid. It lessens the user's burden associated with purchasing and establishing the data center for their businesses. Along with the three-layered architecture, cloud deployment models are of four types as follows: public, private, community, and hybrid cloud [8]. These deployment models are shown in Fig 1. A public cloud is a concept where the cloud resources are accessible to users via open API and set up outside of the corporate firewall. A cloud service provider (CSP) is responsible for offering a public cloud's services to different clients. Sun Cloud, IBM's Blue Cloud, Amazon Elastic Compute Cloud (EC2), Windows Azure Services Platform, and Google AppEngine are a few examples of public clouds. In a hybrid cloud, the infrastructure is split between an internal business data center and external cloud providers [9-10]. In the hybrid cloud model, resources from the private and public clouds are coordinated. These clouds are still separate entities, but they are linked together so they can benefit from various deployment options. By using a "hybrid cloud" architecture in their computing environments, businesses and individuals can lessen their reliance on outside services while enjoying fault tolerance and rapid utilization. A hybrid cloud design requires both on-premises hardware and cloud infrastructure, including local and remote servers. Having a virtualization environment with its own servers is referred to as a private cloud. In a private cloud, an individual entity's network hardware or a private channel is used to sustain IT services [11]. The network's communication in a private cloud is managed by servers or private channels. This can be carried out by the organization itself, shared with a third party, or occasionally hired out for a specific purpose exclusively. This structure is used by organizations that want their data or infrastructure under their own control. Industry sectors including banking and healthcare, government organizations, and corporate divisions like HR, and consumer services may require the additional security offered by the private cloud due to regulatory obligations as well as the processing of sensitive data. However, because it requires significant capital assets, it is not correctly a cloud service. Unlike a private cloud, which only thinks about one company, a community cloud thinks about a wider range of things. This deployment plan could be seen as the same as an intranet, a private cloud, an extranet, and a public cloud. The cloud is a shared resource that is taken care of by a group of companies that work together as a logical community. The goal, policy, compliance factors, and safety measures are all set by the group. The community cloud can be run by a third party from outside the community or by groups from within the community.

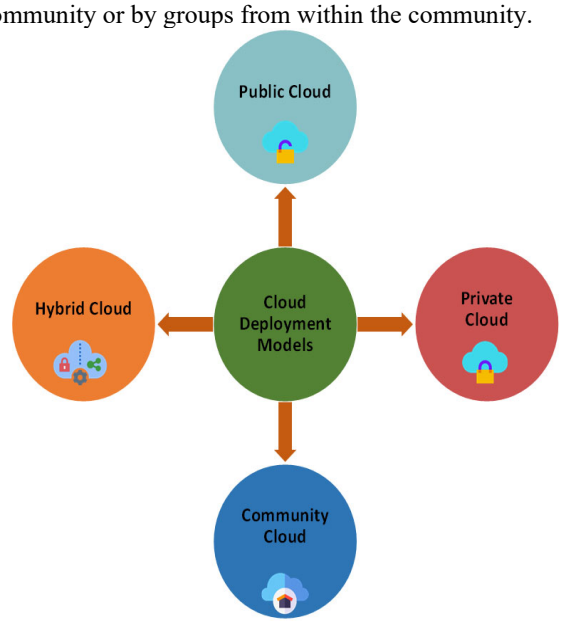

Figure 1: Four types of Cloud deployment models

Cloud-based e-learning is an indication of technology development for educational institutions that have many benefits over the traditional way of teaching-learning. It has increased the interest of teachers and learners in the usage of technology for the teaching-learning process. Many institutions do not have enough infrastructure for implementing e-learning systems. These institutions have an opportunity to adopt CBES to cater to their need. Indeed, a CBES has many challenges like hardware cost, software cost, server configuration, maintenance cost, and finally reliability and security of important data is a major issue for adopting the CBES. Despite these shortcomings it also has its advantage like 24 x 7 availability, fast accessibility, better performance, reduced cost, retain standards, and efficient management of resources.

Now security is a major concern that criticizes the usage of CBES. The application and data deployed on the remote server can crash anytime without prior notification.

As several educational institutions are adopting CBES, it has become a critical issue for the cloud service providers to design an SLA (service level agreement) about feature availability and security of the services, cloud services providers are providing. In this research paper, a detailed description of different cyber-attacks is discussed and a framework to overcome these threats is proposed.
The paper has six sections including an introduction as follows: Section I presents an introduction to e-learning and Cloud Computing with its various deployment model. Section II discusses the literature review. Section III depicts the architecture of CBES. Different threats to CBES are discussed in section IV. Section V explains the proposed security framework for CBES at SaaS Level, Section VI highlights the conclusion and future work respectively.

2. Literature Review

In recent years, various scholars suggested their idea about e-learning systems, cloud computing (CC) technology, and their integration with respect to the enhancement of users' teaching-learning experience. This section highlights attention on a few recent studies done for e-learning systems utilizing cloud computing with and without security aspects. In the year 2014, A. K. Mohammed discussed the e-learning model using problem-solving places (PSP) for enhancing the user's teaching-learning experience [1]. The e-learning architecture using the PSP module when implemented using Cloud Computing (CC) technology requires a study and adoption of some application type-specific security framework and features. The current research study proposes a framework at the SaaS level that will complement the enhancement of the PSP-based e-learning system's user teaching-learning experience in a secure and efficient manner. Wenjuan Li introduced a cloud security framework based on the trust module. A trust entity is a type of cloud service which aids in boosting the transaction rate in a cloud environment. To protect its users, this trust-based process develops various security measures. Customers, who are the cloud's stakeholders, can have faith in a variety of cloud providers, and suppliers can have faith in their clients as well [12]. The trust-based model was based on several characteristics, including domain name, trust level, service kind, etc. The values of these attributes serve as the sole foundation for cloud users' reputations.

The methodology suggested by Duralraj guarantees data availability and offers a way to shield critical data from attackers. To propose a solution in the form of security measures connected to CBES, this study identifies various security vulnerabilities in the cloud service delivery paradigm. The many attacks on e-learning service delivery methods put forth by various researchers were discussed. Involved problems, security requirements, and threats were also considered. This examination of e-learning models encourages users to use a secured internet layer to access their cloud-based data [13]. Multiple criteria like security, performance, migration, availability, cost, and accountability were presented by Gyani [14] to evaluate the Quality of service (QoS) of various cloud providers. The criteria such as trust value, generation time, domain name, etc. are totally relied upon by cloud service providers. False reputations for cloud stack owners can result from using these parameters incorrectly or fraudulently, hence this approach cannot be regarded as a secure way to embrace cloud services.

The influence of the COVID-19 pandemic on Croatia's e-learning systems was examined by Ivan in 2021. Using the findings as a foundation, a research technique was suggested to create a cyber-threat detection model that considers the particulars of using e-learning systems in emergencies and separates flash crowd events from anomalies in the communication network. The suggested methodology comprises developing a DDoS detection model, designing a laboratory testbed configuration for data collecting, verifying the applicability of the generated model to the case study, and establishing a theoretical foundation for DDoS and flash crowd event traffic. Through prompt DDoS detection and other socioeconomic benefits like the creation of a focused study area, the application of the suggested methodology can enhance the effectiveness of the teaching process [15]. Sheikh in the year 2013, proposed a framework for confirming the security measures and capabilities asserted by cloud providers regarding the dependability of cloud services. The providers' security controls are expressed as trust properties that were authorized by some trustworthy authorities. Both, hard and soft trust was incorporated into the proposed hybrid model. Hard trust is attained by validating the trust properties through digital certificates. The entity's business practices, and prior experience are used to evaluate the soft trust [16]. By filling the system with false values, cloud service providers can defraud the system, give their clients a bad reputation, and enhance the popularity of unsecured cloud services. To avoid drawbacks, the system must not involve such types of parameters. This research paper proposed a framework at the SaaS level that overcomes the various difficulties in adopting CBES. Thus, increasing the levels of security for e-learning systems.

3. Architecture of CBES

Cloud computing infrastructure can be used in different ways for e-learning systems in the education field. But most of the time, this combination meets the needs of educational institutions in terms of virtualization of resources, centralization of data storage, scalability, low operating costs, and availability of e-learning systems. This

means that the majority of CBES share a similar architecture [17]. This framework incorporates not just the cloud management system but also all the hardware and software computer resources and services available in the cloud for the purpose of e-learning. Fig 2 depicts the usual architecture of a CBES. The CBESs are three-layered. Cloud Management System Layer 1. It is the interface of an e-learning system t which users interact. This layer has numerous management subsystems that integrate e-learning into cloud computing. Actors can contribute content, create new courses, and collaborate using their browsers instead of course design and management tools. Virtual machines that provide cloud services make up the second layer. It offers SaaS, PaaS, and IaaS. Software is used online. They don't need software, hardware, or upgrades. The third and final layer is called the Physical Hardware Layer, which contains the system's physical architecture. This layer is the information infrastructure, and it contains all the resources that are utilized. It also serves as a representation of the fundamental computing capabilities of students, including the physical memory, CPU, etc. The pool of physical hosts is a dynamic resource that can be scaled up. This indicates that new physical hosts can be added to increase the amount of processing power that is made available for cloud middleware services.

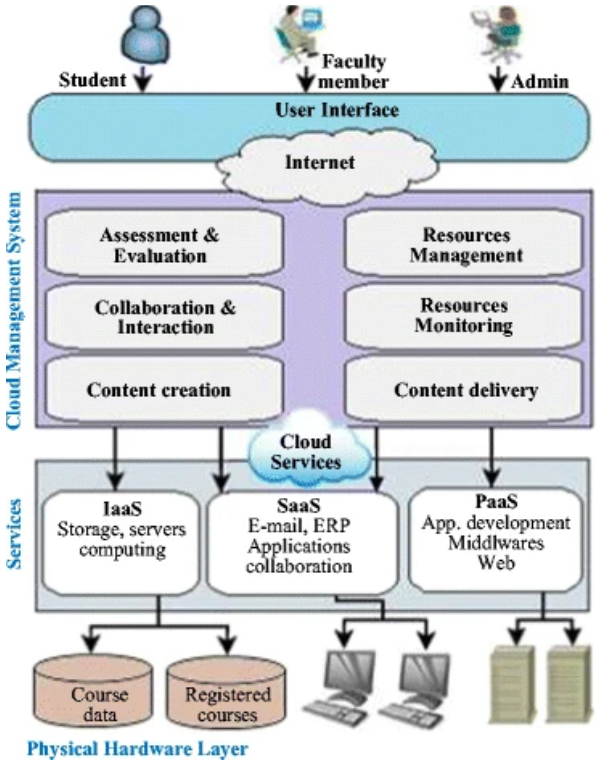

Figure 2: Common architecture of CBES [18]

4. Various Threats to CBES

In the last few decades, ICT has changed quickly, which has led to a lot of new learning opportunities and challenges. The expansion of the computing environment in every industry has resulted in an increase in security risks. There is potential for cyber-exploitation of eLearning platforms because they serve as an open gate, allowing a wide variety of cyber dangers to target the eLearning systems [19]. Many learning institutions would like to adopt cloud technology, but they are mostly worried about the security models offered by various cloud service providers. However, despite all vendors' assurances that their cloud infrastructure is highly safe and fully protected against various threats and vulnerabilities, end customers are still hesitant to move their sensitive data to the cloud. It has been found that most cloud service providers are using cloud services for storage rather than computing. As storage is becoming cheaper day by day, most service providers are offering storage as a service that is being consumed by the community at large. Hosting information at service providers and computing at the service providers' end is a major setback to the cloud computing industry today due to a lack of security. As many security issues have been observed in today's cloud-based e-learning environment. Here in this section, various possible threats encountered during CBES API access requests are discussed as depicted in Fig 3.

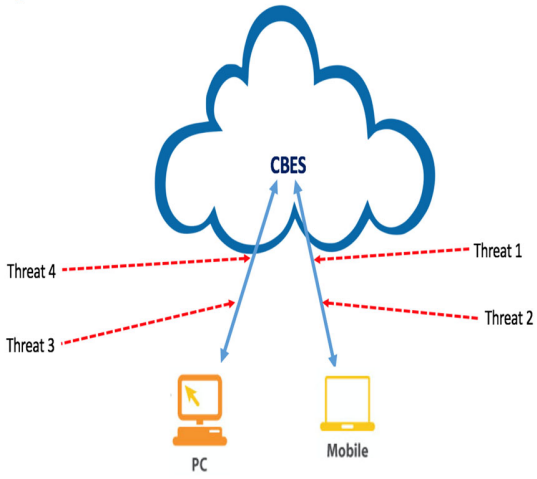

Figure 3: Various threats encountered by CBES

Threat 1- SQL injection: This technique is used to hack any web page. This type of attack has been used to breach security measures and steal sensitive users' information from e-learning systems. As the name suggests, these kinds of attacks rely on the idea that predefined logical expressions within a predefined query can be modified by inserting operations that always result in true or false results. Web forms with accompanying CGI scripts that fail to properly validate user input are a common vector for this

type of injection. Not only can these injections occur in character fields, but also in numbers and dates. If the application does not restrict numeric data for numeric fields, then SQL clauses such as "where" and "having" can be modified in the same way. It targets the dynamic website databases by injecting some unwanted malicious SQL code along with SQL queries.

Threat 2- Cross Site Script (XSS) – The attacker injects malicious script into the vulnerable webpage hosted on the server. The malicious script bypasses the web server and is saved into the database. The victim (the user requesting the data from the server) receives an unwanted response from the server.

Threat 3- Virus/Worms: These are harmful programs that come through a network or domains. They can damage or destroy the information that is very crucial for an organization. It is not limited to just information damage, but it will destroy the system itself by gradually reducing its performance to zero. Trojan, viruses, and malicious programs can wipe out the whole cloud-based e-learning environment.

Threat 4- Data compromise: The data compromise during the request and response access for a webpage is an important process that cannot be overlooked. Negligence in this process will lead to the leaking of important data.
Various threats encountered by CBES are highlighted in Table 1 along with their possible solutions.

Table 1: Threats and their solutions

Threats	Possible Outcomes
Threat 1	Make use of programming function for cleaning unnecessary SQL code
Threat 2	Escape all the URL characters that are vulnerable to a webpage. Filter the HTML attributes. Quoted values must be used with caution in JavaScript programs. Putting important data in CSS property values can be harmful and must be taken into consideration.
Threat 3	Use antivirus software to remove unwanted harmful programs from the system and network. A firewall can be used as a defense mechanism against the virus.
Threat 4	Various data encryption technologies like SSL and TLS can be used for data privacy and security while communicating over the network.

5. Proposed Security Framework for CBES at SAAS level

In this section, the proposed security framework for Cloud based e-learning system (CBES) at the SaaS level is discussed. The framework provides enhanced security features at the SaaS level during the transaction request initiated from CBES for cloud access. Fig. 3 shows the security framework architecture for CBES at the SAAS level. The transaction request will require data exchange between CBES and SaaS cloud service. Authentic users get access to the service for which they are authorized. The authentication and authorization module checks the privileged access for the users. Following access control, data privacy and data integrity are maintained by implementing Public Key Infrastructure.

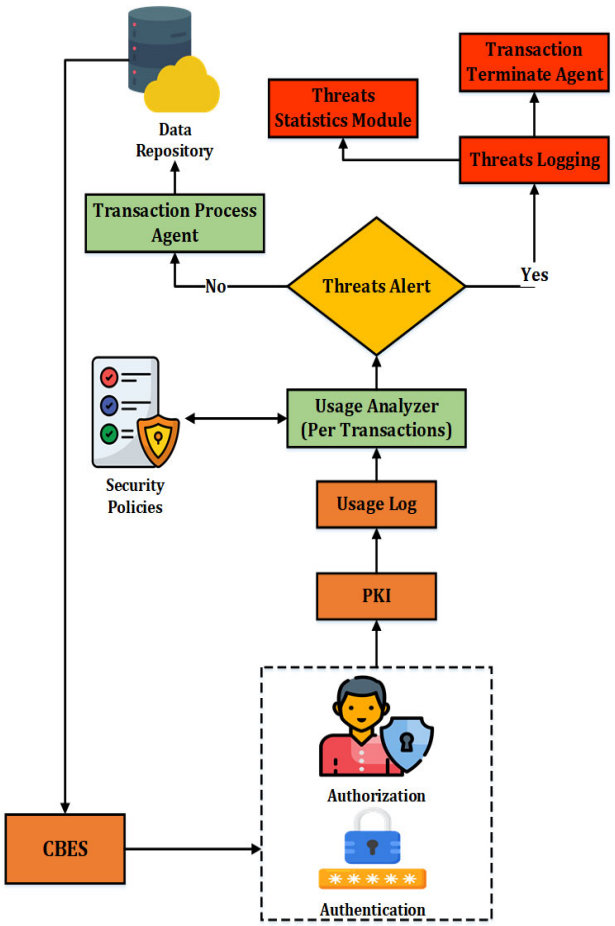

Figure 3: Security framework architecture for CBES at the SAAS level

For each cloud service transaction request, the usage analyzer based on the security policies inspects the usage log for the presence of any possible threats. There are two scenarios:

Scenario 1: When a threat is encountered by a usage analyzer, a threat alert message is generated that eventually prevents the further processing of that specific transaction. It logs the specific threats for future statistical analysis and terminates the transactions with the help of the transaction terminate agent program.

Scenario 2: When no threat is encountered by the usage analyzer, the transactions are successfully processed, and the data exchange is successful between CBES API and CBES repository at the SaaS level.

6. Conclusion and Future Work

It cannot be denied that cloud computing provides supercomputing services with a low-cost budget, but its security is the main barrier to adopting the services by its users. The acceptability of CBES is significantly influenced by cloud security. Once the security of the CBES will enhance, the user's experience and acceptance of CBES will be enhanced eventually. This paper suggests the Cloud security framework at the SaaS level to enhance the currently available security features by introducing a unique usage analyzer module for effective threat management. The future work will include implementing and security testing the proposed framework at different cloud layers. Also, the implementation of the proposed framework will be in accordance with the ICT standards to be adopted by all cloud-based e-learning systems around the world.

References

[1] A. K. Mohammed and A. Ahmed, "E-learning Environment with Problem Solving Places for Teaching and Learning of Algorithm Oriented Concepts", *IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies –ICCICCT, Noorul Islam University, India*, pp. 17-20, 10-11 July, 2014.

[2] U. Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", *Ist International Conference on Parallel, Distributed and Grid Computing*, pp. 211-216, 2010.

[3] A. Ahmed, A. R. Khan and S. Ahmed, "Collaboration of Knowledge Network and E-Learning System with Social Sites for Teaching-Learning," *Fourth International Conference on Advances in Computing and Communications, India,* pp. 147-150, 27-29 August, 2014. doi: 10.1109/ICACC.2014.41

[4] A. R. Khan, A. Ahmed and S. Ahmed, "Collaborative web based cloud services for E-Learning and educational ERP," *Recent Advances in Engineering and Computational Sciences (RAECS), India*, pp.1-4, 6-8 March, 2014. doi: 10.1109/RAECS.2014.6799644

[5] A. Bhardwaj, "Cloud Security Assessment and Identity Management", *Proceeding of 14th International Conference on Computer and Information Technology, Dhaka, Bangladesh*, pp. 1-6, 22-24 December, 2011.

[6] W. Wu, "E-Learning Based on Cloud Computing", *International Journal of Emerging Technologies in Learning*, Vol 16, No. 10, pp. 4-17, 2021. doi.org/10.3991/ijet.v16i10.18579.

[7] P. Hendradi, M.K. Abd Ghani, S.N. Mahfuzah, U. Yudatama, U., N.A. Prabowo and R.A. Widyanto, "Artificial Intelligence Influence in Education 4.0 To Architecture Cloud Based E-Learning System", *International Journal of Artificial Intelligence Research*, 4(1): 1-9, 2020. doi.org/10.29099/ijair.v4i1.109

[8] R. Nazir, Z. Ahmed, Z. Ahmad, N.N. Shaikh, A.A. Laghari and K. Kumar, "Cloud Computing Applications: A Review", *EUDL, EAI Endorsed Transactions on Cloud Systems*, 20(17): 5, 2020. doi.org/10.4108/eai.22-5-2020.164667

[9] S. Sengupta, "Cloud Computing Security- Trends and Research Directions", *IEEE World Congress on Services*, pp. 524-531, 2011.

[10] S. Ramgovind, M.M. Eloff and E. Smith, "The Management of Security in Cloud Computing", *IEEE conference on Information Security for South Africa*, pp. 1-7, 2010. doi.org/10.1109/ISSA.2010.5588290

[11] R. Alvarez, T. Mirzoev, A. Gowan, B. Henderson and S.E. Kruck, "Learning laboratories as services in private cloud deployment", *Journal of Computer Information Systems*, 59(4), pp. 354-362, 2019. doi.org/10.1080/08874417.2017.1368422

[12] W. Li, L. Ping and X. Pan "Use Trust Management Module to Achieve Effective Security Mechanisms in Cloud Environment", *IEEE International Conference on Electronics and Information Engineering*, pp. VI14-VI19, 2010.
doi.org/10.1109/ICEIE.2010.5559829

[13] M. Durairaj and A. Manimaran, "A Study on Security Issues in Cloud based E-Learning", *Indian Journal of Science and Technology*, Vol 8(8), pp. 757-765, 2015. http://dx.doi.org/10.17485/ijst/2015/v8i8/69307

[14] J. Gyani, A. Ahmed and M. A. Haq, "MCDM and Various Prioritization Methods in AHP for CSS: A Comprehensive Review", *IEEE Access*, vol. 10, pp. 33492-33511, 2022.
doi.org/10.1109/ACCESS.2022.3161742

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

[16] S.M. Habib, V. Varadharajan and M. Mühlhäuser, "A Trust-aware Framework for Evaluating Security

Controls of Service Providers in Cloud Marketplaces", *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 459- 468, 2013. doi.org/10.1109/TrustCom.2013.58

[17] A. Fernández, D. Peralta, F. Herrera, J.M. Benítez, "An Overview of E-Learning in Cloud Computing", *Workshop on Learning Technology for Education in Cloud (LTEC'12). Advances in Intelligent Systems and Computing, vol 173.* Springer, Berlin, Heidelberg, 2012. https://doi.org/10.1007/978-3-642-30859-8_4

[18] A.E. Mhouti, M. Erradi, and A. Nasseh, "Using cloud computing services in e-learning process: Benefits and challenges", *Educ Inf Technol 23*, pp. 893–909, 2018. https://doi.org/10.1007/s10639-017-9642-x

[19] M.M. Hassan, A. Gumaei, S. Huda and A. Almogren, "Increasing the trustworthiness in the industrial IoT networks through a reliable cyber-attack detection model", *IEEE Transactions on Industrial Informatics*, pp. 6154-6162, 2020.
doi.org/10.1109/TII.2020.2970074

AHSAN AHMED earned his Master's degree in Computer Science from Jamia Hamdard University, New Delhi, India, in 2008. From 2008 to 2010, he was a research intern at CSIR's laboratory. Since November 2010, he has been working as a lecturer in the Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah, Kingdom of Saudi Arabia. He had 13 years of experience in teaching. His research interests include machine learning, web technologies, cloud computing, reputation systems and e-learning. He has presented four papers in international conferences and published eighteen research papers in reputed journals indexed by SCI under his research and other technical areas.

MOHD ANUL HAQ earned a Ph.D. from Indian Institute of Technology Roorkee, India, in 2013. He received a Master's degree in Computer Applications from UP Technical University (currently Dr. A.P.J. Abdul Kalam Technical University Uttar Pradesh) and Bachelor's Degree from HNB Garhwal University, Srinagar, Uttarakhand. The central component of his research is in artificial intelligence and machine learning. The target applications of his research are deep learning-based image classification, modeling, and forecasting. He completed several research projects sponsored by different national/international agencies. He serves as guest editor and reviewer in reputed journals including Nature, Elsevier, Springer, Techscience press, and many more. He was invited from Microsoft HQ, Redmond, to showcase his AI research projects for the AI for Earth summit in 2019.

NIRANJAN POLALA received Ph.D in CSE from Kakatiya University, Warangal in the year 2013. He received M.Tech (Computer Science and Engineering) from NIT, Warangal in the year 2001 and B.E Computer Science from Nagpur University in 1992. He authored three textbooks in the field of computer science. He published 50 research papers in various International Journals and Conferences. Presently he is Professor and of CSE in KITS, Warangal. He is a member of the ISTE and CSI.

VUPPU SHANKAR earned a Ph.D degree from Kakatiya University, Warangal, Telangana, India, 2016. He received a master degree in computer Science and Engineering from JNTU-Hyderabad, in 2005 and Bachelor's degree in Computer Technology, KITS-Ramtek, Nagpur University, Nagpur, India, in 1995. He is life member of ISTE. He is currently Professor in the Dept of Computer Science & Engineering with Network specialization, at Kakatiya Institute of Technology & Science (KITS), Kakatiya University-Warangal. His core research component is in the area of AI &ML, other research interest includes Databases, Data mining and Networking. At present, he is supervisor for UG and PG students at institute level. He is an author for chapters published in LNCS, Springer, 2013 and 2014. He published research work in various reputed journals, conferences in IEEE and Springer.

JAYADEV GYANI has been working in the Department of Computer Science at CCIS, Majmaah University, Kingdom of Saudi Arabia since 2015. He received his PhD in Computer Science from the University of Hyderabad, India in 2009 and Master's degree in Computer Science and Engineering from Osmania University, INDIA in 1994. He worked as Lecturer, Asst. Professor, Professor, and Head of the CS Department, and had a teaching experience of 25 years. His research interests include software engineering, big data analytics, distributed computing, machine learning algorithms, and their applications. He has several publications in international journals and conferences to his credit. He presented papers in conferences held in Germany, Malaysia, and Nepal. He is a member of ACM and senior member of IEEE.