IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 9, September 2021

DOI: 10.17148/IARJSET.2021.8932

Use of Open-Source Technologies in the Educational Environment of Higher Education Institutions

Rahul B. Deshmukh

Assistant Professor, Department of Mathematics, Sant Rawool Maharaj Mahavidyalaya,

Kudal Sindhudurg Maharashtra

Abstract: The higher education sector is undergoing a time of extraordinary transition. Universities are adopting, or at least grappling with, plenty of new technology and teaching approaches, including a range of applications, portals, and remote teaching tools that support online and hybrid learning environments. The goal of this article is to examine cybersecurity of digital education in India, as well as the existing platforms on the industry for e-learning systems, of which the Moodle framework is the most popular. Finally, the authors make recommendations for using LMS MOODLE to organise students' self-study, as well as protecting participants' individual data and ensuring cyber security within the system.
.

Keywords: OSS, cyber security, cybercrime, Moodle, e-Learning, education**.**

I. INTRODUCTION

E-learning is one of most recent disciplines that is adding to the massive amount of data being generated. E-learning is the process of acquiring new information and skills via the use of electronic gadgets. Distance learning has become more popular in recent years as a result of the global development of technology and the explosion in information availability. One aspect of the e-learning process is distance learning, which allows people to share information across geographical barriers and limits. In simpler terms, e-learning is the use of electronic technologies to provide access to educational curricula outside of a traditional classroom.[1] Data generated by online learning platforms and learning management systems (LMSs)[2] as part of e-Learning scenarios is one source of data expansion. According to statistics, online course portals such as Coursera, edX, and Udacity have a total of more than million students, with much more than courses provided by many universities. Throughout the literature, more complex and technical definitions of e-learning are provided.
The authors of [3], for example, divide the definitions into four basic categories:
i) The technological features of e-learning are the emphasis of this category.
ii) This category focuses on resource accessibility rather than the outcomes of any accomplishment.
iii) This category focuses on the communication and interaction tools used by the parties involved.
iv) This category considers e-learning as a new way of learning or an upgrade on an existing educational model, focusing on the educational aspects of the technology.

The higher education sector is undergoing a time of extraordinary transition. Universities are adopting, or at least grappling with, plenty of new technology and teaching approaches, including a range of applications, portals, and remote teaching tools that support online and hybrid learning environments.[4] Universities face new difficulties, demands, and hazards as the structure of classrooms and the student experience evolves. Many of these developments and challenges have been brought to light by 2020, including the COVID-19 pandemic. Colleges have become more dependent on remote learning technologies as they have been forced to discontinue in-person instruction. Simultaneously, financial strains have increased as students delay applications or demand rebates and refunds for lessons taken in their rooms. Universities are confronted with ever-increasing dangers and decreasing financial margins.

Prior to the effects of COVID-19, higher education networks were a high-value target for cyberattacks, but the widespread use of remote and online learning significantly increased the quantity and intensity of cyberattacks on institutions. In fact, cyberattacks on educational institutions have increased at a higher rate than any other sector. In light of this, cybersecurity is more critical than it has ever been. Large credential combo lists offered and traded on World Wide web marketplaces, as well as a proliferation of login services across new technologies like Zoom, Meet, and other third-party education

DOI: 10.17148/IARJSET.2021.8932

partners, are driving an increase in data attacks. The attack surface on schools has grown exponentially, and there is no turning back now.

II. METHODOLOGY

Today's organisations facing a growing number of cybersecurity challenges, but cybercriminals find higher education to be particularly appealing.

- **Personal Data**: Universities have a lot of sensitive, personal information like financial records, medical history, and Social Security numbers that can be sold on the open market.
- **Research**: Many universities and colleges are still using legacy systems that can be easily exploited, which attracts attackers because of the sensitive nature of emerging research projects.
- **Outdated System & Large, untrained user networks**: Many users in colleges and universities are simply unaware of security issues, allowing malware to infiltrate their networks unwittingly via personal applications or systems.

Finally, COVID-19 has made it considerably easier for threat actors to access higher education networks. After all, the majority of students and staff now access to institutional networks remotely – from potentially insecure wireless networks – and communicate using digital tools. Higher education has very distinct cybersecurity requirements than other sorts of enterprises. [5] Campuses are divided into public spaces (areas where anybody can go), semi-public spaces (classrooms and faculty offices), and guarded areas from a physical standpoint. The network surface is large at the network layer, spanning everything from student accommodation to administrative offices and learning labs. Each of these ecosystems contains a diverse collection of mismanaged and untrustworthy equipment. Cyberattacks have always had the purpose of extorting money and resources from their victims. Cybercriminals utilise a variety of tactics to acquire access to these resources, including socially engineered assaults such as phishing, spear phishing, and spoofing, to deceive users into handing over their log-in credentials or other personal information that can be used to breach a system.

Another widely utilised strategy in higher education is hacking, which is the practise of detecting and exploiting holes in a system or network to get access to data.[6] It frequently entails breaking into a computer system and extracting contents using a password-cracking algorithm. In particular, over 80% of hacking-related incidents involved password breaking or the exploitation of stolen or lost user credentials. Is there anything that can help? It's free and open source. For a variety of reasons, open-source choices are particularly appealing in higher education. For starters, they're free, so we don't have to jump through budgetary hoops when we need tools. Second, there is frequently a cultural match. Because many institutions have a history of adopting open source, they may already have open-source expertise on hand, removing one of the most major adoption obstacles in many businesses.

Universities are caught in an expensive arms race as they try to buy new tools and adapt their methods to resist the next adversary attack, which boosts higher education's cybersecurity operational protection and response.[7] Meanwhile, the attackers figure out how to get past the tools, switch tactics, and assault different targets. The race will be costly for universities regardless of the outcome. They will suffer financial damages if they lose a fight. If they win a battle, it suggests they put a lot of money into a good security programme. In surveys and interviews, CISOs[4] cited eight major challenges they're dealing with today. Phishing, User education, Cloud security, High-profile information security strategy, Next-generation security technology planning, Identity and access management, Governance over data security, Unsecure personal devices

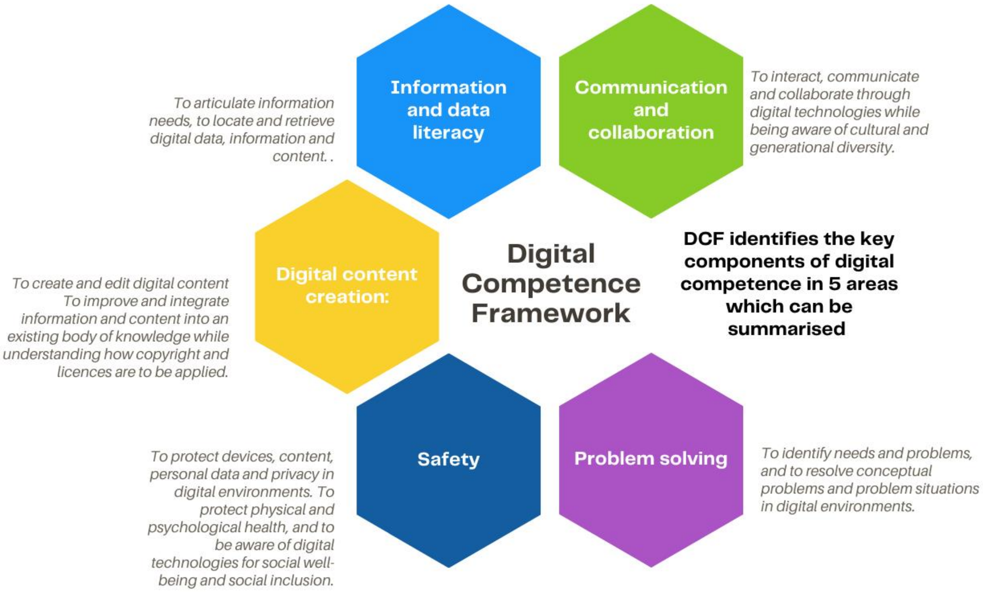
III. RESULTS AND DISCUSSION

3.1 Open-Source Software (OSS)

All efforts to improve that technologies produced in research environments are eventually deployed and employed operationally are referred to as technology transition. There is now a newer strategy to technology migrating based on open source software (OSS)[8] In many circumstances, OSS techniques have the potential to improve technological transfer. OSS techniques, on the other hand, only work when they are well implemented. OSS is described as software for which the human-readable source code is available for everyone to use, study, reuse, modify, enhance, and redistribute.

Using an OSS approach can facilitate and speed up technology transition, as detailed more below. Many researchers and government programme managers, on the other hand, aren't sure how to employ an open-source strategy to help with technology transformation. This covers research on establishing secure cyber infrastructure, core parts of cyber systems, information security user protection and education, cybersecurity research infrastructure, and cyberspace technology evaluation and transition.

The Digital Competence Framework, or DCF, (Fig 1) is a framework for improving citizens' digital skills. To be digitally proficient nowadays, one must be knowledgeable in all areas of DCF.


Information and data literacy
To articulate information needs, to locate and retrieve digital data, information and content. .
Communication and collaboration
To interact, communicate and collaborate through digital technologies while being aware of cultural and generational diversity.
Digital content creation:
To create and edit digital content To improve and integrate information and content into an existing body of knowledge while understanding how copyright and licences are to be applied.
Digital Competence Framework
DCF identifies the key components of digital competence in 5 areas which can be summarised
Safety
To protect devices, content, personal data and privacy in digital environments. To protect physical and psychological health, and to be aware of digital technologies for social well-being and social inclusion.
Problem solving
To identify needs and problems, and to resolve conceptual problems and problem situations in digital environments.

3.2 Open-Source Learning Management System

Many studies suggest that traditional teaching methods, such as using books and static figures, are ineffective in conveying complex scientific concepts. As one of the quickest trends in today's education, the current emerging media technology revolution has supplemented the traditional face-to-face learning process with various e-learning communities to assist in preparing the students for more in-depth in interactive educational contexts, which could lead to enhanced learning opportunities in both online as well as on mixed-learning courses. Institutions all over the world used commercial learning and teaching applications to keep instructors and students in touch 24 hours a day, seven days a week. Licensing for those commercial applications could be prohibitively expensive. Licensing such educational systems could cost a lot of money for many institutes. OSS may be the best solution for such a cost problem. There are other open-source applications available that are designed to handle a variety of difficulties, but Moodle is the most robust open-source tool.

3.3 Moodle View

Moodle is an open-source programme that is both user-friendly as well as flexible. LMS stands for Learning Management System, which is an online interactive platform for electronic or Online Interactive environment (OIE) and virtual learning environment (VLE), both of which have a large social framework for education support and are a competitive alternative to several commercial applications. The word Moodle stands for Modular Object-Oriented Dynamic Learning Environment, which is mostly useful to computer programmers. Martin Dougiamas designed Moodle[9], who has extensive experience in both education and computer engineering as a revolutionary e-learning technology that allows educators to easily create and share online courses. Moodle was created as a cheaper alternative to the expensive systems on the market. It has a wide range of features and a relatively short learning curve, making it a popular tool among universities for creating online dynamic web-based teaching and learning environments. It can be used as a stand-alone online teaching and learning environment or as a substitute to face-to-face formal learning.

Dougiamas decided to make Moodle a licensed open-source version so that users could use, edit, add features, and share the software without changing or eliminating the original licence and copyrights. Moodle was originally created for the Linux operating system, but it is now compatible with a variety of operating systems, including Windows and Mac. Moodle's first version was launched in 2002. Following the initial release, numerous programmers all around the world began investigating and scrutinising the Moodle code, adding and removing features as needed, and resolving any flaws that were discovered. Many colleges around the world have adopted Moodle to create customised instructional environments to that course. Table 1 shows the list of top 10 countries prepared from registered sites in 242 countries.

Table 1: Top 10 Countries Using Moodle (Moodle.com)

Country	Registered sites
Spain	14,291
United States	13,828
Mexico	10,130
Germany	10,098
Brazil	9,083
India	7,601
Indonesia	6,695
France	6,364
Colombia	5,841
Russian Federation	5,694

Source : https://stats.moodle.org/

Instructors can create courses in academic contexts by selecting course options such as the course format, course title, start and end dates, and so on. Instructors can just use Moodle to develop self-contained online courses by managing web-based content such as course segments, lessons, and focused technology. They can also utilise technology to supplement their traditional courses to help students understand complex topics with minimal face-to-face interaction, or to enrich their existing courses.

3.4 Features of Moodle- Following figure Fig. 2 shows features of Moodle.

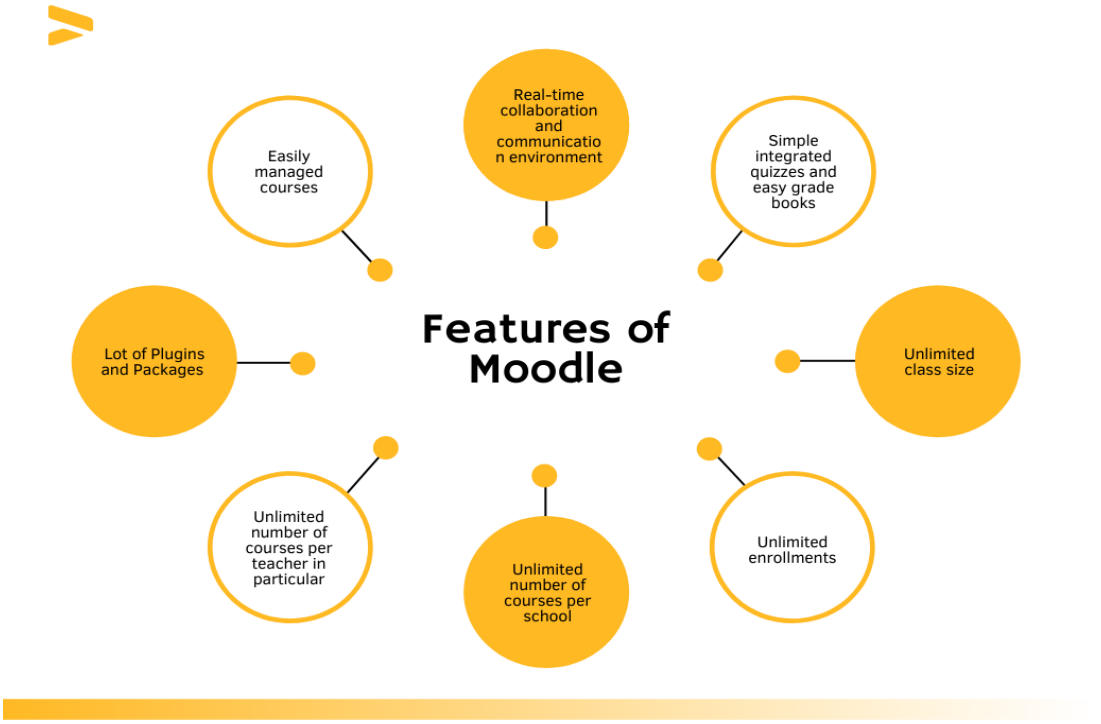

Real-time collaboration and communicatio n environment
Easily managed courses
Simple integrated quizzes and easy grade books
Lot of Plugins and Packages
Features of Moodle
Unlimited class size
Unlimited number of courses per teacher in particular
Unlimited number of courses per school
Unlimited enrollments

Fig-2: Features of Moodle

In addition, Moodle provides several benefits like 24/7 access from anyplace within the world to its learning platform, Download and upload course material as well as audio, video, .doc, docx, PDF, image, and so on, Link to resources anyplace on the net, simply produce designing courses while not have to be compelled to learn hypertext mark-up language data, Access files/papers/resources by a laptop, give the possession to the course content, Manage course content from year to year and never lose any work, Handle secure payments through using online Gateway. The goal of this article is to examine cybersecurity of digital education in India, as well as the existing platforms on the industry for e-learning

systems, of which the Moodle framework is the most popular. There are suggestions for improving the establishment and digitization education as well as suggestions for completing tasks within the Moodle system.
Also, in this article were studied aspects of teaching and learning management systems application on based on this framework and to establish the recommendations on how to improve students' self-study process at academic institutions. In conclusion the authors make recommendations on the organisation of students' self-study based on LMS MOODLE. The Moodle Learning Management System allows tutors to create teaching materials, courses, work programs, lectures, presentations, audio - video files, any images, texts, and modules for recording and controlling students' learning activities, among other things.

The course is broken into sections by topic using theme structuring. Each study week of the course is represented by a different segment on the calendar. The course author edits the course content. It's simple to add multiple features to an e-course, such as lectures, tasks, forums, glossaries, and so on. There is a website for each course where you can see the most recent course modifications. As a result, the Moodle system gives instructors the tools they need to deliver course materials, teach theoretical and practical lessons, and coordinate individual and group student learning activities. Assessments are done on various scales based on the tutor's work programmes for the various educational fields. Because Moodle-based testing is the most common form of knowledge control in remote learning, the test tasks include a variety of question kinds (multiple choice, short answers, yes/no, and so on). Moodle has a number of features that make it simple for users to process test results. Test results can be statistically analysed using the system. The Moodle LMS includes a wide range of connectivity modules for educational process participants, including questionnaires, surveys, glossaries, practical (laboratory) courses, seminars, workbooks, chat, forums, tests, Wikis, and tasks.

3.5 Legal Support for the LMS MOODLE Application

I have identified a number of associated legal difficulties into the educational and technological components of the LMS MOODLE application for organising students' self-study. We categorise them under the following categories:
1. Ensuring that personal data is protected and that LMS MOODLE participants are properly authenticated
2. Ensuring LMS MOODLE cyber security and protecting intellectual property rights
3. A local rule based on the LMS MOODLE for the arrangement of students' self-study.

The type of discipline speciality and the substance of professional competence that students are meant to gain throughout their self-study, as well as the student's legal standing, all play a role in the legal resolution of the aforementioned concerns. Given the legal significance of the aforementioned aspects, one of the most pressing issues that must be addressed during the electronic self-study process is ensuring the privacy of LMS MOODLE users.
The legal basis for the issues identified in this study includes various requirements linked to ensuring the protection of students' personal data that must be imposed on the teacher and the LMS MOODLE administrator. These responsibilities include the following:
1) To ensure that a minimum sufficient set of personal information about students is processed via LMS MOODLE in order to organise self-study.
2) To ensure the confidentiality of the information regarding each student's results and the content of their works, unless their agreement to the handling of personal data specifies otherwise.
3) to approve the mechanism for processing the personal data of LMS MOODLE participants (usually by the Academic Boards of higher educational establishments)
4) To making it impossible to identify LMS MOODLE members in any other way, develop a secure password for them.

The topic of cyber security is another crucial feature of LMS MOODLE members' personal data protection. To address this issue, cyber dangers to the participants and components of the LMS MOODLE should be recognised, and a system of legal and technological tools for dealing with cyber security concerns should be devised. As a result, the university authorities will be responsible for guaranteeing the cyber security of LMS MOODLE and its users when it is used to organise self-study. These include, for example, the creation and approval by the Academic Boards of a procedure for organising students' self-study, the preparation of methodological specific suggestions for ensuring the cyber security of a modular, Moodle environment, instructions for organising technical information protection in the effective system, and so on.

IV. CONCLUSION

Due to the lack of a definite policy on digitalization of higher education, it is necessary to combine efforts to develop some policy on ICT-based education transformation with a fixed strategic vision, clear markers, and proper management of this policy regardless of changes in administration and individual performers, to remove legislative, institutional, and other barriers that obstruct this policy. Develop a plan for Internet educational institutions to have broadband access, encourage the adoption of digital documentation and digital services in the education sector, recommend the execution of educational projects in data security, cybersecurity, personal information protection, and digital user rights in distance learning, and introduce new professions and disciplines related too. Independent work, which is defined in the paper as a way for preparing training sessions in the Moodle system, is an important feature in the preparation of training sessions in the Moodle system. Simultaneously, the widespread use of the Moodle system for the purpose of coordinating students' autonomous work necessitates the resolution of challenges relating to educational, technological, and legal elements of the relevant information system's use. Applying these ideas to improve the Moodle system's efficiency will assist to ensure the security of users of the relevant system and relevant digital assets, as well as the system's overall cyber security.

V. REFERENCES

[1] A. Moubayed, M. Injadat, A. B. Nassif, H. Lutfiyya, and A. Shami, "E-Learning: Challenges and Research Opportunities Using Machine Learning Data Analytics," *IEEE Access*, vol. 6, no. July, pp. 39117–39138, 2018, doi: 10.1109/ACCESS.2018.2851790.

[2] M. E. Dawson and I. Al Saeed, "Use of open source software and virtualization in academia to enhance higher education everywhere," *Cutting-Edge Technol. High. Educ.*, vol. 6, no. PARTC, pp. 283–313, 2012, doi: 10.1108/S2044-9968(2012)000006C013.

[3] A. Sangrà, D. Vlachopoulos, and N. Cabrera, "Building an inclusive definition of e-learning: An approach to the conceptual framework," *Int. Rev. Res. Open Distance Learn.*, vol. 13, no. 2, pp. 145–159, 2012, doi: 10.19173/irrodl.v13i2.1161.

[4] B. Al Kurdi, M. Alshurideh, and S. A. Salloum, "Investigating a theoretical framework for e-learning technology acceptance," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 6484–6496, 2020, doi: 10.11591/IJECE.V10I6.PP6484-6496.

[5] D. A. Wheeler, "Using an Open Source Software Approach for Cybersecurity Technology Transition," 2015.

[6] J. Maranga, M. J. Maranga, and M. Nelson, "Emerging Issues in Cyber Security for Institutions of Higher Education Innovation Methodologies in Information Technology View project Computer Security View project Emerging Issues in Cyber Security for Institutions of Higher Education," *IJCSN-International J. Comput. Sci. Netw.*, vol. 8, no. 4, 2019, [Online]. Available: www.IJCSN.org.

[7] G. N. Reddy and G. J. U. Reddy, "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies," no. September, 2014, [Online]. Available: http://arxiv.org/abs/1402.1842.

[8] D. Maughan, D. Balenson, U. Lindqvist, and Z. Tudor, "Crossing the 'valley of death': Transitioning cybersecurity research into practice," *IEEE Secur. Priv.*, vol. 11, no. 2, pp. 14–23, 2013, doi: 10.1109/MSP.2013.31.

[9] M. Pleskach, V. Pleskach, I. Zaiarna, and O. Zaiarnyi, "Modern digital challenges and technologies in the educational environment of higher education institutions," *CEUR Workshop Proc.*, vol. 2845, pp. 237–250, 2021.