Security of Open-Source Learning Management Systems (LMS)

Kamal EL AFOUI, Mohammed BERRADA, Said HRAOUI

Laboratory of Artificial Intelligence, Data Science & Emerging Systems (LIASSE), National School of Applied Sciences (ENSA), Sidi Mohamed Ben Abdellah University (USMBA), Fez – Morocco.

Abstract:

The evolution of computer technologies in education has propelled the widespread adoption of Learning Management Systems (LMS). However, amidst the competitive landscape and evolving terminology, ensuring the security of these systems remains paramount. This study conducts a comprehensive analysis of security measures in open-source LMS, employing robust methodologies for data collection, participant selection, and analysis. Through biannual benchmarking analyses, market trends among leading LMS providers such as Canvas, Brightspace, Moodle, and Blackboard Learn are identified, shedding light on shifts in market dominance and growth patterns. The conclusion underscores the urgency of bolstering security measures in open-source LMS, advocating for continuous vigilance and adaptation to safeguard educational institutions and learners in the digital age.

Keywords: *Learning Management Systems (LMS); Open source; Security; Vulnerability; Recommendations.*

I. Introduction:

The integration of computer technologies in educational practice dates back several decades to the onset of the 'information revolution.' In the 1980s, there were debates about the significance of computers in education [1]. However, in the 1990s, personal computers, educational software, and the World Wide Web experienced explosive growth, making computer-assisted pedagogy a prominent feature in education.

This development led to the rapid emergence of Learning Management Systems (LMSs) - comprehensive learning platforms that support various aspects of education, from administrative tasks to course delivery and assessment. Some researchers [2] attribute the emergence of LMSs to basic "training management systems," which later evolved into comprehensive "e-learning platforms," while others [3] highlight the role of integrated learning systems as predecessors to modern LMSs.

However, there is no universal consensus on the exact scope of the term "Learning Management System," which is often used interchangeably with "course management system." In this context, attempting to establish a singular, all-encompassing definition of an LMS or differentiating it from a CMS is considered unproductive. As a result, both terms are frequently used interchangeably. This publication aims to provide an "ostensive" definition of an LMS, covering a wide range of commercial and open-source LMSs and related technologies used in higher education institutions. However, the focus is primarily on LMSs used in academic settings rather than those used for corporate training purposes.

Currently, there are numerous LMS solutions available for higher education from commercial providers. For example, the dominant player in the United States is Blackboard Corporation, which captures approximately 57 percent of the educational market. Alternatively, institutions can choose open-source alternatives like Moodle or Sakai without incurring licensing costs. Proprietary in-house e-learning platforms developed by some institutions, particularly for-profit schools, are not addressed in this publication.

As the LMS market matures, some users consider transitioning from their current LMS to a different product. These transitions are usually motivated by cost reduction or dissatisfaction with the existing system.

All LMS products, whether commercial or open-source, offer similar functionalities, including administrative tasks such as student registration and assessment, as well as content management. Typically, LMSs leverage advanced relational database software, such as Oracle, Microsoft SQL Server, or MySQL for open-source systems, to enhance data security through various login roles such as instructor, student, or guest.

Section One, "Learning Management Systems (LMS): An Overview," begins with a comprehensive overview by Anthony Pina, focusing on LMSs commonly used in academia, with a particular emphasis on commercial products. Dr. Pina introduces key features present in most LMSs and presents a comparative analysis of prevalent products, setting the stage for Section Two, which explores selecting an appropriate LMS platform.

The section concludes with a chapter by Wolfgang Hommel, addressing security and privacy concerns within the e-learning environment. Dr. Hommel approaches security and privacy management from a systemic viewpoint, considering the complex distributed nature of e-learning environments that are susceptible to various security risks. Successful security measures are discussed within the context of popular open-source LMSs like OLAT and Moodle, with an analysis of how Federated Identity Management could enhance secure communication between e-learning entities. This chapter aims to guide developers, system administrators, and network administrators in seamlessly integrating a newly adopted LMS into existing infrastructure.

Fig 1: *Structure of the thesis*

II. Literature review:

Learning Management Systems (LMS) have become widely used in colleges and universities. Some popular LMS platforms include Blackboard, Desire2Learn, Sakai, Canvas and Moodle [4]. The popularity of these systems is seen as evidence of the institutionalization of e-learning in higher education [5]. According to Harrington and colleagues, the adoption of LMS in higher education has been faster and more widespread than any other innovation [6]. While technology-delivered instruction has a long history, the current generation of LMS is still relatively new, entering its second decade [7].

From a technical standpoint, a learning management system (LMS) is a server-based software program that interfaces with a database containing information about users, courses, and content. An LMS is similar to other systems designed for e-commerce, human resources, payroll, and student records. What sets an LMS apart is its instructional nature. It provides a seamless environment for learning and teaching activities, without being limited by time and space boundaries [8]. Face-to-face courses that use an LMS for required or supplemental activities are often referred to as web-enhanced courses [9].

Learning management systems are known by different names in the literature, including course management systems, virtual learning environments, and e-learning courseware [10]. Some authors distinguish between course management systems and learning management systems (e.g., [11], [12]), while others argue that the term "course management system" should be abandoned due to potential confusion with content management systems (CMS) [13]. Despite these minor controversies, the majority of U.S.-based journals and other media tend to use the terms "learning management system" (LMS) and "course management system" (CMS) interchangeably. In Europe and Asia, the term "virtual learning environment" (VLE) is more commonly used.

Fig 2: *Learning Management Systems (LMS)*

2.1. Learning Management Systems (LMS):

While the goal of a CMS is to store and distribute content, the goal of a learning management system (LMS) is to "simplify the administration of learning/training programs within an organization" [14]. LMS allow a learner to launch eLearning. LMS help manage the interactions between the learner and the eLearning and other related resources. LMS help learners plan and monitor their progress in their learning journey.

LMS are "software that automate[s] the administration of training events" [15]. The automation of administrative functions via LMS can lead to considerable time, personnel, and resource savings. An LMS has significant administrative functions, which help an organization to "target, deliver, track, analyze, and report on…. learning" [14]. These robust administrative functions enable organizations to track completion of mandated training, currency of professional certifications, and mandatory human resource related programs[16].

LMS integrate tools to manage the tracking of learners and the content along with appropriate work flow processes. This combination of tools and processes allows an LMS to support the delivery and management of learning and tracking the results. As [17] explains, learning management systems "enable companies to plan and track the learning needs and accomplishments of employees, customers, and partners".

Every LMS should have the ability to display a catalog, register learners, track learner progress, and provide reports. LMSs must be capable of handling various delivery modes, such as online, instructor-led, self-paced, collaborative, facilitated, nonfacilitated, and others [18].

LMSs are either installed on an organization's intranet or hosted off-site by service providers. When using service providers, LMSs are accessed through either an extranet, which is a private network that uses Internet protocols and public telecommunication systems to share a business's information externally, or the internet, which consists of interconnected networks using TCP/IP protocols [19].

The internet is external to a corporate intranet. [20] emphasizes that a learning management system uses Internet technologies to manage the interaction between users and learning resources, whether the LMS is operated internally or externally to a corporation.

Figure 3 illustrates the relationship of the components that make up a learning management system. An LMS has the capability to manage learners and their records, as well as the learning process. Within an LMS, users interact with their learner data and learning management information. The learning content is not part of this configuration.

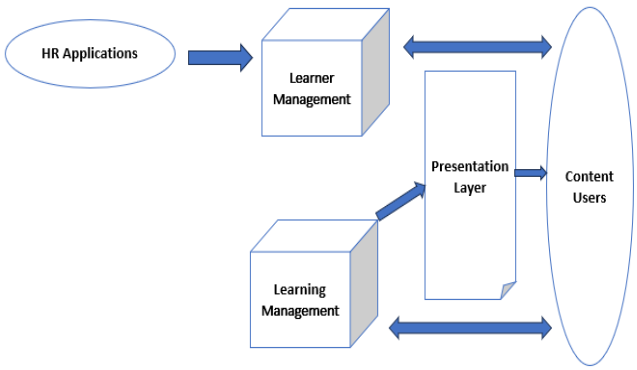


Fig 3: *LMS Components*

Some LMS focus on content management, but it is not their primary focus. According to [20], LMS vary from vendor to vendor in terms of their features, but they all have core capabilities. These include an online course catalog, an online registration system, competency assessment, eLearning launch and tracking, learning assessment, learning material management, customizable reporting, collaborative and synchronous learning tools, and integration with other enterprise applications. The goal of LMS is to manage the processes related to training and education delivery and administration. LMS are structured around the course rather than course content. Collaborative tools within LMS allow learners to work together using internet, intranet, and extranet technology coupled with CMS. The next section will describe the combination of content and learning management via the LCMS.

2.2.Types of LMS:

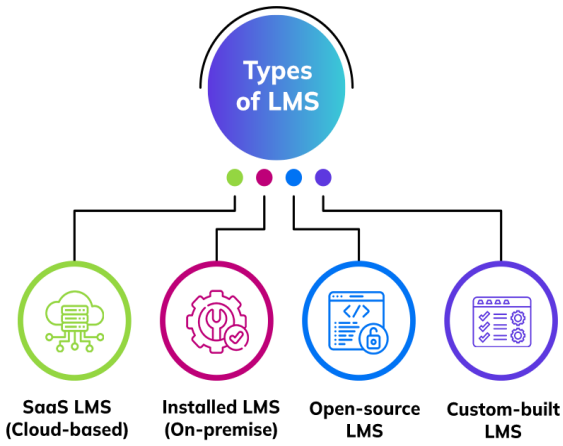


Fig 4: *Types of LMS*

Your breakdown of the four types of Learning Management Systems (LMS) provides a comprehensive overview of the options available to organizations. Here's a summary of each:

- **SaaS LMS (Cloud-based):** This option offers quick setup and easy access, making it suitable for organizations looking for convenience and scalability. However, customization options may be limited, and it's crucial to choose a provider that offers tailored solutions to meet specific needs, such as Disprz LMS.
- **Installed LMS (On-premise):** On-premise LMS solutions provide greater control over data and system management, which can be beneficial for organizations with strict data security requirements. However, they often come with high upfront costs and ongoing maintenance responsibilities, requiring dedicated IT resources.
- **Open-source LMS:** Open-source LMS platforms offer flexibility and customization options, as they are community-driven and allow for collaboration to improve the system. While they provide extensive customization possibilities, setting up and maintaining them may require technical expertise, and comprehensive vendor support may be lacking.
- **Custom-built LMS:** Tailored to specific organizational needs, custom-built LMS solutions offer unparalleled customization and control. However, they come with significant development costs, ongoing maintenance challenges, and potential compatibility issues as technology evolves. Additionally, reliance on a small team for maintenance can pose risks in case of turnover or resignations.

2.3.Features of an LMS:

[4] Identified the most common features of an LMS by categorizing them as pedagogical tools for:

- Content creation;
- Communication tools;
- Assessment tools;
- Administration tools.

a) **Content creation** and display tools allow instructors to generate course content within an embedded text/HTML editor or upload documents, spreadsheets, presentations, images, animations, audio, or video into the LMS. Hyperlinks can point to websites or documents outside the LMS. Assignments or drop boxes provide a place for students to submit materials assigned by their instructors for grading and feedback. Instructors can organize content into folders and subfolders and use the content release feature to display or hide folders and individual content items, giving the instructor control over when content is viewable by students.

b) **Communication tools** found in an LMS allow instructors to incorporate student-instructor and student-student interaction into the course. Asynchronous (non-real-time) tools include course announcements, student web pages, email to instructors and class members, threaded discussion boards, wikis, blogs, and file sharing. Synchronous (real-time) tools found in a typical LMS include text chat, whiteboard, and a sharable web browser. Groups of students can be placed into virtual teams or groups, which may include text chat, threaded discussion, and file sharing ability that can be seen only by the members of the group and the instructor.

c) **Assessment tools** provide instructors with several ways to test, survey, and track student achievement and activity in the course. Common tools include a test/assessment manager for creating and deploying exams, a generator for creating different types of questions (multiple choice, true/false, essay, short answer, matching, etc.), and question pools or test banks to store questions that can be used for multiple exams. Questions in an exam (and choices in a multiple-choice question) can be randomized and can be displayed one at a time or all at once. Instructors can give a time limit for exams and can specify the type and amount of feedback that students receive for correct and incorrect answers. Exams can be graded, ungraded, or delivered as anonymous surveys with aggregated results. An electronic grade book for managing student assignments and displaying student grades is a feature of virtually every LMS and is the most highly valued LMS feature by students [21]. Less valued by students, but highly valued by instructors, is the ability to track student activity within an LMS, including logins, time spent, and specific areas visited.

d) **Administrative tools** for instructors include control panels with the ability to manage the settings for the content creation, communication, and assessment tools, customize the look of the course, make tools, content, and resources available or

unavailable to users, manage files, and move or copy content. Administrative tools for LMS system administrators allow them to manage the creation of user accounts and courses, enrollment of instructors and students into courses, enabling and disabling of accounts and courses, and tracking activity in the system.

2.4.Add-On Components:

In addition to the standard tools provided within the LMS, most vendors offer additional products that can be integrated with the system. A common tool offered by many LMS vendors is an e-portfolio, a personal storage area allotted to individual students that resides apart from the online courses. The e-portfolio allows students to archive the assignments and projects created in their courses for use in later courses, meeting graduation requirements, or perusal by potential employers. The e-portfolio has become popular with teacher education programs and is gaining popularity in other disciplines[22].

2.5.LMS Advantages:

Before learning management systems became widely available, the delivery of online instruction required faculty or instructional designers to master Hypertext Markup Language (HTML) or web page authoring programs [23].

Turning in assignments generally involved e-mailing the professors, while assessment was done manually, with the results often entered into spreadsheets. Delivery of content online was limited, as publicly available websites were not protected from copyright violation by fair use guidelines [24]. The major advantage of the LMS is that it brought content delivery, communication, assessment, and administration of online instruction into a single secure platform that could be accessed by anyone on the Internet [4], [8].

2.6.LMS Limitations:

The LMS is not without limitations and disadvantages. According to Ioannu and Hannafin (2008), users often found the systems to be slow, confusing, and more focused on administrative needs rather than student needs. Another complaint was that the LMS interface was dull and rigid compared to more engaging online social environments like MySpace, Facebook, and YouTube [26]. Siemens (2004) suggested that the LMS interface should be simplified and made more intuitive. Lane (2008) discovered that current systems primarily served as a repository of materials and did not support sound pedagogical practice. Piña, Green, and Eggers (2008) also expressed concern about the lack of instructional design guidance and tools for the development of rich multimedia-based instruction. While some teaching tools exist within an LMS [4], they do not include tools to guide instructors in the design of online instruction and sound pedagogical practice [26].

2.7.Open source LMS:

As commercial LMS companies grow larger and as their products become more complex and expensive, many schools, colleges, and universities are questioning whether their needs can be better met by open-source products, rather than by a commercial system. Open source has financial and programmatic appeal [27]. For those who subscribe to a social constructivist point of view where reality is constructed from the collective experiences of groups [28], open source also has a philosophical appeal. In an open-source environment, the source code of the product is made available to the user without charge. Software licensing fees, which can be substantial, are eliminated. Open-source software frees the user from a contractual agreement with a specific vendor. A program or system based on open-source software may be customized and branded according to a user or institution's needs and desires--rather than to a vendor's current priorities. In the case of learning management systems, there exists a vibrant and active community of developers for Moodle and Sakai, the two most popular systems, and for several others.

This would include server hardware and software, server administration, database administration, programming, and technical support that would otherwise be supplied by the vendor of a commercial system. To leverage the advantages of being able to customize the LMS (a primary "selling" point for open-source software), an institution running Moodle would require in-house expertise in MySQL and PHP programming, while Sakai would require Java programmers.

Operating a customized and institution-specific LMS has its potential pitfalls. While the 2006 shipment of a bug-laden WebCT Vista product proves that commercial releases sometimes occur hastily [29], commercial learning management systems are typically field tested before public release and tend to be backed by a warranty and contractual obligations of customer support and downtime limitations. Open-source code carries no guarantee or warranty.

a) Moodle:

Moodle (Modular Object-Oriented Dynamic Learning Environment) has been available to the public since 2002. It is a product of the research and development of a small educational technology company in Australia that wanted to provide an alternative to commercial learning management systems. Unlike an LMS from a commercial vendor, the system is developed and supported by a strong and active community of developers, users, and administrators that keeps the software and supporting documentation updated and continuously evolving. The product has been downloaded millions of times and 1.5 million current installations [30] serve over 200 million users. Moodle is available as open-source software under the Free Software Foundation GNU General Public License and is based upon the open-source MySQL database and PHP scripting language. The software can be downloaded for free from its web site at the URL http://moodle.org. Users can install Moodle on a stand-alone computer or server, or the software can be installed across an enterprise or distributed across a department or institutional server farm. Finally, its ease of installation, testing, and adoption has contributed to making Moodle the fastest-growing LMS in the world [31].

b) Sakai:

Sakai, arguably the second most popular open-source LMS, is quite different from Moodle. Founded in 2004, Sakai was developed by a consortium of leading research universities as an open-source alternative to home-grown or commercial learning management systems. Participating institutions included M.I.T., Stanford, Indiana, Michigan State, and U.C. Berkeley. Unlike Moodle, which is built on a MySQL/PHP stack, Sakai is based on the Java language platform, similar to Blackboard. Situating itself as a competitor to both the home-grown and commercial LMS, the Sakai interface and feature set closely resemble those of Blackboard and other commercial LMS, with tools for content creation, communication, assessment, and administration [4].

c) Blackboard:

As of the close of the 2000s-decade, Blackboard, Inc. was clearly the dominant, market-leading commercial LMS vendor for both K-12 and higher education. Formed in 1997, the company grew rapidly by merging with CourseInfo in 1999 and by buying a number of LMS and non LMS companies, including MadDuck Technologies (the makers of Web Course in a Box), CampusWide by ATT in 2000, Prometheus in 2002, SA Cash in 2003, WebCT in 2006, NTI Group in 2008, and Angel Learning in 2009 [32]. These acquisitions have generated more than just an LMS lineup, they have created a more comprehensive product line that also includes systems for conducting various campus business transactions, and for inter-campus communications and emergency alerts.

d) Canvas:

Canvas was created in 2011 by Instructure, UTAH (USA) and deployed from 2012 in universities and schools of UTAH. The open-source solution has been distributed alongside the proprietary Instructure offer in SaaS mode.

e) Other Open-Source Systems:

Beyond the United States and Canada, there are numerous open-source LMS used by schools, colleges and universities, business and industry. Here are a few of them: Claroline: Belgium eFront: Greece Docebo: Italy Dokeos: Belgium ILIAS: Germany OLAT: Switzerland There are many more LMS. It is inappropriate to cover any in detail. Links to all of the above and additional LMS can be found here (see LMS Companies and Organizations).

2.8.Security in LMS:

An LMS is a critical part of an organization's IT infrastructure, used to store, manage, and process information in the form of training or education resources for either internal or external distribution[33]. It is vital therefore that this information remains accurate, confidential, and available when required [34]. Given the dependence on information technology in today's society, the availability of IT systems can be as critical as the information itself. Recent worldwide events have sparked interest in disaster recovery, with many companies realizing the implications of information loss and unavailability on their ability to work, and the possible cost in terms of damaged reputation or lost revenue (Disaster Recovery. Encarta. © 2005 Microsoft Corporation). IT availability can be seriously compromised through hacking, both in terms of site defacement or more serious attacks, such as DoS (Denial of Service) which can lead to partial or complete inaccessibility of the system in question. High-profile incidents such as the recent defacement of the US Army LMS have focused attention on LMS security and prompted urgent inquiries into the protection of such systems[35].

2.9.Vulnerabilities in LMS:

Since all systems have some degree of vulnerability, it is important to know what kind of vulnerabilities are present in LMS. In general, there are various types of vulnerabilities in LMS as it deals with information and information exchange. First, it is the vulnerability at the operating system level. Sometimes certain tools do not function well with the existing operating system in use by an organization. This will cause the tools not to function properly and some errors might occur which will disrupt the learning process. LMS might require additional plug-ins to be installed. However, if the plug-ins have security issues, they can be exploited by hackers to gain control of the system or do a malicious attack. Another issue is when there is a mismatch between what the LMS system provides and the security policy of the organization. Some features in LMS might be disabled as it is not in line with the organization's security policy. This will cause functionality problems and sometimes be unstable. In some cases, the LMS might not have a policy that dictates what are the security measures that exist in its environment. This will make it hard for the administrator to identify security settings or identify a security breach in its environment. If an LMS has a lot of different security measures, it might confuse the administrators and might lead to them forgetting to check or missing certain security settings. In addition to that, some vulnerabilities are related to the database and network security procedures of the LMS. This will be the prime target for attacks hoping that there might be unsecured data that can be exploited. Usually, the data might have a wide range of subject matter from general information to personal information and sometimes it might also contain sensitive information. If there are chances of data loss, it can disrupt the learning process and will also have a legal impact. A good example of this happened to U-Grad using its WebCT Classic Vista where a security breach caused the loss of names, social security numbers, and also credit card information of about 1800 students and alumni. Last but not least, there are various security bugs in the LMS applications. Built-in security measures in LMS might seem to be sufficient, but there are chances that there might be insecure features in the applications that can be exploited. This will have a wide range of impacts and might cause data loss or damage. [36]

2.10. Recommendations for Securing LMS:

Utilize encryption for all sensitive information. This will make it troublesome for interlopers to abuse the information. A safe channel should consistently be utilized by the director, student, coach, and chairmen when transferring and getting to sensitive data. Information that ought to consistently be encoded incorporates secret words, messages, and individual information from the student database. Continuously store the learning management system on an integrated server environment and guarantee that the security settings giving admittance to the student database permit the least openness to the information. Remember to disable the automatic cache of pages with individual or sensitive information. Standard execution of weak point evaluations on software applications and system components, especially the operating system, DBMS, and application server. This is probably the best approach to recognizing the presence of known weaknesses.
Through patching, the machine-based technical weaknesses, the technology can significantly forestall unauthorized admittance to or harm done to applications, whether it is the abuse of bugs in the application or a hidden assault on a weak distant host. The operating systems of the server and client machines ought to be updated on a standard timetable. At the point when security-related bugs are found, they can generally be forestalled utilizing patches delivered by the operating system or software vendor. This will make it harder for assailants to exploit or directly attack the operating system or other applications. Always use firewalls between the student/customer and employees on the internal network and the server. This will keep the assailant from a distant assault on the student/customer's machine. A powerful firewall can stop the spread of worms and bugs from the student/customer to the internal network or server. Finally, always make backups for the system as a great step towards recovering from an assault or unexpected data loss. This involves the irregular backup of the state of the system as disk images and the scheduled backup of data on the system to either removable media or through the network to another storage area. [37] [38] [39].

III. Methodology:

3.1. Description of the Study:

In an educational context, Learning Management System (LMS) is a web-based application to support the learning process [40]. It's a new trend that many institutions use LMS for teaching and studying. Since the high cost of proprietary software, open source LMS becomes an attractive solution. Using the same reasoning that more users can make the software better, we can assume that open source LMS has a better chance to be more secure than other open-source software. An experiment is needed to confirm this assumption [41]. A study about security in open source LMS will open a new perspective for learning data security. This can help institutions determine whether it's safe to use open source LMS for the learning process. This study will also help open source LMS developers enhance their software security since there's little chance that they do something for security if there's no strong demand from open source LMS users. [42]

Open-Source Learning Management Systems or open-source software in general is not well known for being secure. The fact that many eyes make all bugs shallow (with Linus law) assumes that open-source software should be more secure than proprietary software [43]. But on the other hand, open-source software is not immune to the increasing number of security threats. This issue comes with the implication of increasing number of users and various interests on open-source software [44]. For example, students who use open-source software for learning and lecturers who use this software to support the learning process [45]. This condition implies that there's a special requirement to enhance data security for learning institutions.

3.2. Data collection:

Data was collected through the examination of LMS software and respective security documentation, as well as information and opinions given by LMS developers [46]. The primary source of data was the developers themselves who have intimate knowledge of their software from a higher level, in addition to those responsible for the security of the software. The research team contacted these individuals by various means such as email, instant messaging, and voice over IP [47]. Data was collected through direct questioning and also informal discussion with the developers. This gave insight on the security concerns for the ten LMS as well as the security concerns regarding open-source software in the IT industry [48]. Periodic contact was maintained with some developers over the duration of the project in order to keep current with new developments regarding the LMS.

3.3. Participants:

Knowing the software developers of open-source Learning Management Systems (LMS) created this software in their leisure time, mostly by individuals who have regular jobs, educators and students whose learning has been a catalyst in making them motivated to increase the use of technology [49]. They create this software for various personal reasons; some to improve the learning experience of their students, some to help themselves in their study, and others to fulfill their spare time by doing something beneficial. All of their various reasons have led to the development of many various types of open source LMS, in many programming languages, with different platform requirements [50]. We chose to define our population as software developers who have a teaching background in formal or informal education, and students whose learning has a catalyst which motivates them to increase the use of technology. Due to the vast number of different LMS available, we had decided to use a sampling of certain types to best suit our study [41]. This research was conducted using a case study of the Learning Management System (LMS) "Moodle"; this had been chosen due to its popularity in many different countries, various age group users and has given us access to its recent and older versions.

3.4. Procedure:

Because open-source systems are usually much more customizable than closed-source systems, people will often alter the code base to fit their needs. While this is a desirable feature in that it allows the system to meld to the specific needs of an institution, it also introduces great potential to inadvertently create security holes. And finally, if there is one thing that the open-source community is known for, it is being open and sharing ideas. This sense of community and shared developments leads to a great number of new features; however, many may not get a thorough examination before

being implemented into a system. All of these are reasons why an assessment of open-source system security is vital. [51]

3.5. Data Analysis :

During the manual examination, the majority of the actions and the outcomes were noted to help with validation and to give an understanding into the measure of examination that was completed. At first, the procedures included interfacing with the application as a non-authenticated client. This was to imitate a hacker assault that might be done on an application that has quite recently been published to the web. This is done so that the vulnerabilities discovered may be averted before the genuine arrival of the application. An endeavor was made to record every single conceivable information entry point which might be an establishment for SQL Injection and Cross Site Scripting assaults. This should facilitate a more focused examination on key areas of the application. Any vulnerabilities discovered were evaluated for their discernible effect on the functionality of the application. This is so an engineer testing the same or similar issue may consider it to be a need to alter and therefore, there might be fewer vulnerabilities of this sort in future applications. [52]

3.6.Validation and Reliability:

The aim of this part of the research was to evaluate the security reliability and security validity of the OSS LMS in use or which administrators were intending to use. However, we experienced some practical difficulties in trying to separate these two methods. In all cases our intent was to test safety-of-security. An improvement to this method would have been to use the SSE method only as a reliability test by introducing known vulnerabilities and assessing whether the tool detects those that are known to exist through CVEs. Step tests are often used as a means of assessing the validity of a tool compared to a gold standard. Unfortunately, in security assessment there is often no gold standard and we would never be able to conduct these tests without risking our ability to compromise a system due to functional equivalence with commonly used malicious activity. Given the uncertainty over many security diagnoses it seems that assessment of test-retest reliability, inter-rater reliability and internal consistency may be the best way forward for future security assessment tool validation. A study into factor analysis would also be very interesting in this area.

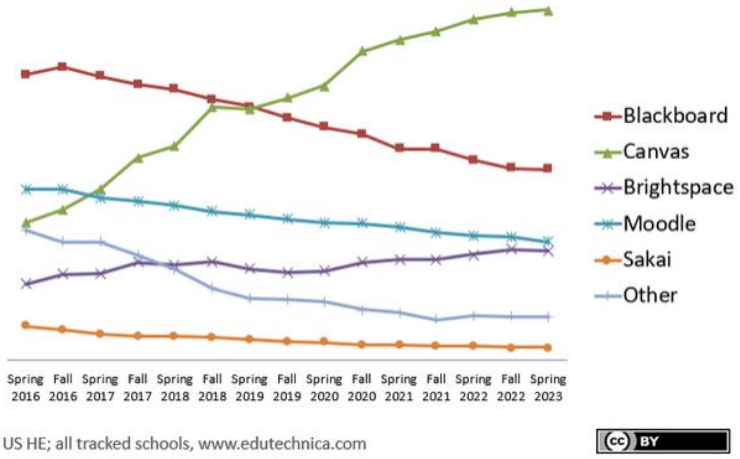
3.7.Reproducibility:

A description of the data collection was the next topic of discussion. It was expressed that the nature of this study required the acquisition of data by way of experimentation and implementation of different LMS. Lists of both intrusive and non-intrusive methods were provided. These methods were to come later in the form of security assessments, each type being implemented on different LMS. Our sample was that of different open source LMS. The intrusive methods were to prove difficult, as they were typically executed as applications to Higher Education Learning Management Systems. (However, due to the highly relative nature of security, testing on comparative systems is likely to provide similar results). Finally, a collection of security-related data was to be carried out on LMS users and administrators, in the form of surveys and interviews. This data as a whole was to compose case studies of specific LMS, each consisting of a compilation of documents that display evidence of an LMS security level at a particular time and environment. This method was chosen finally because reproducibility would be easier, in that the same methods could be implemented at a later time to compare different results. This would be possible due to the specific nature of LMS security and the sometimes sporadic and unannounced changes in the software of a particular LMS.

IV. Results:

For the past decade, Client Stat has conducted biannual benchmarking of Learning Management System (LMS) market share data in the United States. Our spring analysis captures shifts occurring over the winter break, while the fall analysis highlights changes over the summer period. Consistent with historical trends, this year's analysis reveals fewer alterations during the winter compared to the typical fluctuations observed during summer.

The data indicates a noticeable deceleration in the pace of change overall, suggesting a trend towards greater stability in the LMS landscape.



Instructure Canvas maintains its dominant position in the market, boasting a market share nearly double that of its closest competitor in terms of the number of institutions utilizing it, and over double in terms of the number of enrolled students. The influence of Canvas in the educational landscape continues to expand steadily.

D2L Brightspace also demonstrates notable growth, steadily closing the gap with Moodle, which has been experiencing a prolonged, gradual decline. Brightspace has surpassed Moodle in terms of student enrollments, securing the third position by this metric.

Meanwhile, Blackboard Learn's decline persists, albeit at a decelerating pace, aligning with broader industry trends.

	Blackboard Learn	D2L Brightspace	Instructure Canvas	Moodle	Sakai	Other
Institutions	735	422	1364	449	50	143
	22.8%	13.1%	42.3%	13.9%	1.6%	4.4%
Enrollments	4,203,530	2,292,883	8,662,284	1,404,259	316,105	675,196

Spring 2023, 500+ FTE students (3222 schools as of spring 2023), www.edutechnica.com

V. Discussion:

The discussion of the security of Open-Source Learning Management Systems (LMS) in the context of the provided market analysis involves several key points:

- **Dominance of Canvas and Security Implications:**

  Canvas, as the dominant player in the LMS market, must prioritize security due to its widespread usage and influence in educational institutions. With a large user base, Canvas becomes an attractive target for cyberattacks, necessitating robust security measures to protect sensitive data and ensure uninterrupted learning experiences.

- **Growth of D2L Brightspace and Security Considerations:**

  The notable growth of D2L Brightspace positions it as a significant contender in the LMS market. As Brightspace gains traction, it must address security concerns to maintain its momentum and instill confidence among users. Strengthening security features and regularly addressing vulnerabilities will be essential to sustaining its growth trajectory.

- **Decline of Moodle and Security Challenges:**

  Moodle's prolonged, gradual decline raises questions about its ability to adapt to evolving security threats and meet the changing needs of educational institutions. A declining user base may lead to reduced investments in security, potentially exposing remaining users to greater risks. Moodle must prioritize security efforts to reverse its decline and regain trust among users concerned about data protection.

- **Persistent Decline of Blackboard Learn and Security Implications:**

  Blackboard Learn's ongoing decline aligns with broader industry trends, potentially reflecting dissatisfaction with its features, including security capabilities. As Blackboard Learn continues to lose market share, maintaining adequate security measures becomes crucial to prevent further erosion of trust and ensure the protection of user data.

- **Trend Towards Stability and Security Challenges:**

  The trend towards greater stability in the LMS landscape may suggest a maturation of the market, but it also presents security challenges. As LMS platforms solidify their positions, they must prioritize security to safeguard against potential threats and maintain the trust of users who rely on these platforms for teaching and learning.

VI. Conclusion:

With the rapid proliferation of distance learning, schools confront the difficult problem of choosing and managing an appropriate technological environment that fits their budget, technical resources, curriculum, pedagogy, and profile of the student body. In this context, the book is intended to fill the gap in the current literature on the interaction between LMSs, supporting technologies, and relevant teaching methodologies. This book is intended for administrators, faculty, subject specialists, and all those looking to launch a new or to expand an existing distance learning program. In particular, it covers commercial and open-source LMSs as well as technologies used for synchronous and asynchronous course delivery, and it offers a comprehensive discussion of factors influencing the transition from one LMS to another. The reader will also find coverage of virtual labs, electronic portfolios, and technological solutions related to the problems of plagiarism, student tracking, assessment, and security of e-learning environment.

Research conducted by the Sloan Consortium and the National Center for Education Statistics indicates that online student enrollments is the fastest growing sector of higher education, increasing at a rate ten times higher than total college and university enrollments [53]. The vast majority of these online courses are being delivered via learning management systems, one of the true success stories in the long history of technology use in education [7]. The LMS's first decade has been one of fierce competition, with companies appearing, disappearing or bought by other companies. A few companies have emerged currently as dominant players; however, the history of technology is populated with companies, such as WordStar and WordPerfect, which once dominated their respective domains and later disappeared[54].
New research is showing that the emergent wave of minority users are favoring mobile technologies over desktop and notebook computers and are adept at using the advanced features of these technologies for both entertainment and communication [25]. Angel and Desire2Learn have made their systems capable of display on iPods and PDAs and the other LMS manufacturers are following suit. It is likely that as both LMS and mobile device technologies advance, current challenges, such as screen and input device size, will become a thing of the past.

The security of Open-Source Learning Management Systems remains a critical consideration amidst the evolving dynamics of the LMS market. Dominant players like Canvas must uphold high security standards, while challengers like Brightspace need to prioritize security to sustain their growth. Platforms experiencing decline, such as Moodle and Blackboard Learn, must address security concerns to regain competitiveness and ensure the protection of user data. Overall, the trend towards stability underscores the importance of robust security measures to safeguard educational institutions and learners in an increasingly digital learning environment.

Acknowledgment:

This paper and the research behind it would not have been possible without the exceptional support of my supervisors, Mohammed Berrada and Said Hraoui. Their enthusiasm, knowledge and exacting attention to detail have been an inspiration and kept my work on track. Kamal EL AFOUI, my colleague at National School of Applied Sciences, have also helped over our researches and answered with unfailing patience numerous questions about the topic.

References:

[1] Cuban, L. (1986). Teachers and Machines: The classroom use of technology since 1920. New York: Teachers College Press.

[2] Mallon, D., Bersin, J., Howard C., & O'Leonard, K. (2009). Learning Management Systems 2009. Executive Summary. Bersin and Associates Research Report.

[3] Bailey, G. D. (Ed.). (1993). Computer Based Integrated Learning Systems. Englewood Cliffs, NJ: Educational Technology Publications.

[4] Dabbagh, N., & Bannan-Ritland, B. (2005).*Online learning: Concepts, strategies, and applications*. Upper Saddle River, NJ: Pearson Prentice Hall.

[5] Piña, A. A. (2008a). How Institutionalized is Distance Learning? A Study of Institutional Role, Locale and Academic Level. *Online Journal of Distance Learning Administration*, *11*(1).

[6] Harrington, C. F., Gordon, S. A., & Schibik, T. J. (2004). Course management system utilization and implications for practice: A national survey of department chairpersons. *Online Journal of Distance Learning Administration*, *7*(4).

[7] Piña, A. A. (2008b). *Distance Learning and the Institution: Foundations, Importance and Implementation*. Saarbrücken, Germany: VDM Publishing.

[8] Ullman, C., & Rabinowitz, M. (2004). Course management systems and the reinvention of instruction. *Technological Horizons in Education Journal*. Retrieved May 11, 2009, from http:// www.thejournal.com/articles/17014

[9] Schmidt, K. (2002). The web-enhanced classroom. *Journal of Information Technology*, *18*(2).

[10] Gibbons, S. (2005). Library course-management systems: an overview. *ALA Library Technology Reports, 41*(3).

[11] Ceraulo, S. (2005). Benefits of upgrading to LMS. *Distance Education Report, 9*(9).

[12] Watson, W. R., & Watson, S. L. (2007). An argument for clarity: What are learning management systems, what are they not, and what should they become? *TechTrends, 51*(2).

[13] Piña, A. A., Green, S., & Eggers, M. R. (2008). *Learning management systems: Lessons from the front lines.* Paper presented at the annual Technology in Education (TechEd) Conference, Ontario, CA.

[14] English, P. (2001, April). What the future holds for e-learning. Retrieved February 2, 2004, from http://www.futuremedia.co.uk/elearning_guide_thefutureofelearning.php

[15] Hall, B. (2002b). Six steps to developing a successful e-learning initiative: excerpts from the e-learning guidebook. In Allison Rossett (ED.) The ASTD E-Learning Handbook. New York: McGraw-Hill.

[16] Hall, B. (2002a). Learning management systems 2002. Retrieved March 1, 2004, from http://www.brandonhall.com

[17] Robbins, S. R. (2002). The evolution of the learning content management system. Retrieved February 25, 2004, from http://www.learningcircuits.org/2002/apr2002/robbins.html

[18] Singh, H. (2001). Learning content management systems. Retrieved November 20, 2003, from http://www.internettime.com/Learning/lcms/

[19] GetNewWise. (2004). Glossary. Retrieved February 25, 2004, from http://www.getnetwise.org/glossary.php

[20] Rosenberg, M. J. (2001). e-Learning. New York: McGraw-Hill.

[21] Kvavnik, R., & Caruso, J. (2005). *ECAR study of students and technology 2005: Convenience, connection, control and learning*. Boulder, CO: EDUCAUSE Center for Applied Research.

[22] Burnett, M. N., & Williams, J. M. (2009). Institutional uses of rubrics and e-portfolios: Spelman College and Rose-Hulman institute. *Peer Review, 11*(1).

[23] Hill, J. R., Wiley, D., Nelson, L. M., & Han, S. (2004). Exploring research on internet-based learning: From infrastructure to interactions. In Jonassen, D. H. (Ed.), *Handbook of research on educational communications and technology* (2nd ed.). New York: Simon and Schuster/Macmillan.

[24] Piña, A. A., & Eggers, M. R. (2006). *Teaching, administering and supporting blackboard, webct and desire2learn*. Paper presented at the annual Technology in Education (TechEd) Conference, Pasadena, CA.

[25] Ranie, L., & Keeter, S. (2006). *How Americans use their cell phones*. Washington, DC: The Pew Research Center.

[26] Ioannou, A., & Hannafin, R. (2008). Deficiencies of course management systems: Do students care? *Quarterly Review of Distance Education*, *9*(4).

[27] Stewart, B. (2007). Why Athabasca chose moodle. *Distance Education Report, 11*(3). Changing Course Management Systems: Lessons Learned Changing Course Management Systems: Lessons LearnedChanging.

[28] Driscoll, M. P. (2007). Psychological theories of instructional design. In Reiser, R. A., & Dempsey, J. V. (Eds.), *Trends and issues in instructional design and technology* (2nd ed.). Upper Saddle River, NJ: Pearson Merrill/Prentice-Hall.

[29] Chasen, M. (2009). *Future of blackboard and angel*. Keynote presentation at the Angel User Conference, Chicago, IL

[30] Valade, J. (2002). *PHP & MySQL for dummies*. New York: Wiley.

[31] Cole, J., & Foster, H. (2007). *Using moodle* (2nd ed.).

Sebastapol, CA: O'Reilly Media.

[32] Blackboard, Inc. (2009).*Blackboard media center press releases*. Retrieved June 10, 2009, from http://www.blackboard.com/Company/MediaCenter/Press-Releases.aspx.

[33] Bradley, V. M. (2021). Learning Management System (LMS) use with online instruction.International Journal of Technology in Education (IJTE), 4(1), 68-92.https://doi.org/10.46328/ijte.36

[34] Odeh, A. & Keshta, I. (2021). Impact of COVID – 19 pandemic on education: Moving towards e-learning paradigm. International Journal of Evaluation and Research in Education (IJERE), 11(2). http://doi.org/10.11591/ijere.v11i2.21945

[35] DO Okumu, RO Omollo - Journal of Computational …, 2022 - ojs.bonviewpress.com. Human Firewall Simulator for Enhancing Security Awareness against Business Email Compromise. bonviewpress.com

[36] H Ibrahim, S Karabatak - 2020 8th International …, 2020 - ieeexplore.ieee.org. A study on cybersecurity challenges in e-learning and database management system. researchgate.net

[37] OL van Daalen - Computer Law & Security Review, 2023 - Elsevier. The right to encryption: Privacy as preventing unlawful access. sciencedirect.com.

[38] MJ Khan - World Journal of Advanced Research and Reviews, 2023 - wjarr.com. Securing network infrastructure with cyber security. wjarr.com

[39] A Razaque, N Shaldanbayeva, B Alotaibi, M Alotaibi… - Electronics, 2022 - mdpi.com. Big data handling approach for unauthorized cloud computing access. mdpi.com.

[40] S. Basaran and R.K.H. Mohammed, "Usability evaluation of open source learning management systems," in International Journal of …, 2020. semanticscholar.org

[41] P. A. Ukhov, D. A. Borshchenko, D. D. Kabanov, et al., "Customization of open-source solutions on the example of the LMS Moodle distance learning platform," Journal of Physics: Conference Series, 2021. [Online]. Available: iopscience.iop.org. iop.org

[42] M. K. Asamoah, "ICT officials' opinion on deploying open source learning management system for teaching and learning in universities in a developing society," E-learning and Digital Media, 2021. sagepub.com

[43] B. Bhushan, P. Sinha, K. M. Sagayam, and J. Andrew, "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions," Computers & Electrical Engineering, vol. 93, 2021, Elsevier. [HTML]

[44] M. Manulis, C.P. Bridges, R. Harrison, V. Sekar, et al., "Cyber security in new space: Analysis of threats, key enabling technologies and challenges," Journal of Information Security, vol. 2021, Springer, 2021. springer.com

[45] S. Xie, Z. Zheng, W. Chen, J. Wu, H.N. Dai, "Blockchain for cloud exchange: A survey," Computers & Electrical Engineering, vol. 86, Elsevier, 2020. henrylab.net

[46] R. Rabiman, M. Nurtanto, and N. Kholifah, "Design and Development E-Learning System by Learning Management System (LMS) in Vocational Education.," Online Submission, 2020. ed.gov

[47] A. H. Duin and J. Tham, "The current state of analytics: Implications for learning management system (LMS) use in writing pedagogy," Computers and Composition, 2020. [HTML]

[48] J. P. Widodo, L. Musyarofah, et al., "Developing a Moodle-based learning management system (LMS) for slow learners," Jurnal Inspirasi Pendidikan, vol. 12, no. 1, pp. 1-10, 2022. unikama.ac.id

[49] V. Shurygin, N. Saenko, A. Zekiy, E. Klochko, et al., "Learning management systems in academic and corporate distance education," in International Journal of Emerging Technologies in Learning (iJET), 2021. learntechlib.org

[50] S. Pinilla, A. Cantisani, S. Klöppel, W. Strik, "Curriculum development with the implementation of an open-source learning management system for training early clinical students: An educational design research," in Adv. in Med. Educ. Pract., vol. 2021, Taylor & Francis, 2021. tandfonline.com

[51] J. R. Howe, "Open-Source Tools to Bridge the Cybersecurity Budget Gap in Small Businesses and Local Governments," 2020. [HTML]

[52] H. Hanif, M. H. N. M. Nasir, M. F. Ab Razak, A. Firdaus, et al., "The rise of software vulnerability: Taxonomy of software vulnerabilities detection and machine learning approaches," Advanced Computer Applications, vol. 181, Elsevier, 2021. [HTML]

[53] Allen, I. E., & Seaman, J. (2007). *Online nation: Five years of growth in online learning*. Needham, MA: The Sloan Consortium.

[54] Bergin, T. (2006). The proliferation and consolidation of word processing software: 1985-1995. *IEEE Annals of the History of Computing*, *28*(4).