Terbit *online* pada laman : http://teknosi.fti.unand.ac.id/

Jurnal Nasional Teknologi dan Sistem Informasi

| ISSN (Print) 2460-3465 | ISSN (Online) 2476-8812 |

Study Kasus

Design and Build an Assessment Platform by Inserting *Moodle-Based Cryptographic Methods*

*Deden Pradeka [a, *], Anugrah Adiwilaga [b], Devi Aprianti Rimadhani Agustini [c], Adi Suheryadi [d], Rizki Nuriman [e]*

[abce] *Department of Computer Engineering, Universitas Pendidikan Indonesia, Jl.Dr.Setiabudi No.229, Isola, Kec.Sukasari, Kota Bandung, Jawa Barat 40154*
[d] *Department of Informatics Engineering, Politeknik Negeri Indramayu, Legok, Kec. Lohbener , Regency Indramayu , West Java 45252*

INFORMASI ARTIKEL

Article History:
Accepted by the Editor: 09 November 2023
Final Revision: 05 Januari 2024
Published *Online* : 07 Januari 2024

KATA KUNCI

Cyber Security,
Cryptography,
Platform Assessment.

KORESPONDENSI

Email: dedenpradeka@upi.edu*

A B S T R A C T

The use of digital platforms in the learning process is increasing, especially in the context of assessment activities. In this context, it is essential to realize that digital platforms can be subject to attack or fraud by irresponsible parties. It is due to the presence of sensitive data and/or restricted to a limited number of authorized persons. Therefore, the protection of data and its security in using digital platforms is very important. To enhance this layer of security in data protection, cryptographic methods play a crucial role in maintaining information security. By applying cryptographic methods to learning platforms for assessment purposes, we can increase the security and integrity of the data involved in the assessment process. This research aims to produce a plugin that can be used on a Moodle-based Learning Management System (LMS). This plugin will provide an additional activity in the form of an assessment activity with an essay exam type. When this plugin is used, all questions and answers will be encrypted into text that is difficult to understand by unauthorized parties when an attack attempt occurs. In this way, the learning platform for assessment purposes can safeguard and protect data from access by irresponsible parties.

1. INTRODUCTION

Currently, the variety of learning methods is increasing, especially with the implementation of Distance Learning (PJJ) using a digital platform or Learning Management System (LMS), which is caused by the impact of the COVID-19 pandemic [1]. This development is triggered by technological advances that make information and communication systems more accessible, as well as internet networks that permeate various aspects of life worldwide, including the world of education, which has felt its positive impact [2] [3]. In addition, the COVID-19 pandemic has also accelerated the revolution in education in the use of information technology, making the transfer of knowledge easier and faster during the learning process [4] [5].

The use of digital platforms in the learning process is not only for face-to-face purposes but also as an option for conducting assessment activities. Therefore, this widespread use must be balanced with reliable cybersecurity. The confidentiality of platform user data, such as exam questions, is noteworthy because of the potential for attacks or fraud by irresponsible parties. Therefore, maintaining the security of data, information, and platforms is a shared responsibility and awareness.

In dealing with these issues, the development of a platform assessment system that integrates cryptographic methods is one solution. Cryptography plays an important role in maintaining the confidentiality of data and information. Cryptography is the method or art of converting data or messages into a specific form or code, so that unauthorized people find it difficult to know the original data or message [6].

https://doi.org/10.25077/TEKNOSI.v9i3.2023.264-270

Bishop (1989) predicted that education in the future would become more flexible, open, and accessible to anyone, regardless of gender, age, or previous educational experience [7]. In line with this vision, Blended Learning is an innovation combining classroom learning with online media with technology support, also known as digital learning or e-learning [8] [9].

Digital learning is a learning method delivered through electronic media via the Internet. In addition, a Learning Management System (LMS) is a platform used to produce materials online. In addition, LMS is also used to manage classes, exercises, exams, or assessment platforms and develop interactions between teachers and learners [10].

With the use of online media for learning methods and the creation of specialized platforms for assessment activities [11], in addition to the positive impacts generated, threats to data in e-learning systems also arise [12]. Several important information or assets in e-learning systems become targets for irresponsible parties, including 1) Content or data in the e-learning system; 2) Personal data of users; 3) Information sent or received; 4) Network connection; 5) Bandwidth. Privacy, content, and web application protection alone cannot overcome this threat. Based on data from the Sysadmin, Audit, Network, Security (SANS) Institute, there are several common errors in software, especially in e-learning systems, including 1) SQL injection at 7%; 2) Cross Site Scripting at 39%; 3) information leakage at 32%; 4) insufficient transport layer protection at 4%; 5) fingerprinting at 4%; and HTTP response splitting at 3%. [13] [14].

Data in the form of text sent through digital assessment platforms are vulnerable to potential tampering from those who seek to access the contents of the data quickly, as digital platforms often do not apply additional layers of security, such as encryption, during the data transmission process [15]. Therefore, the idea of an assessment platform combined with cryptographic methods makes the integrity and security of the data in the transmission process more secure, as the encryption process is done before the data is transmitted to increase the security layer. It is implemented through a plugin that can be applied to the Moodle Learning Management System (LMS) platform. This plugin is used to run assessment activities securely through a digital platform.

There are previous studies that can be a reference for researchers in carrying out this research. The research titled "Studi Pustaka Tentang Kerentanan Keamanan *E-learning* dan Penanganannya" is a type of literature review research that discusses security vulnerabilities associated with using e-learning or digital learning. The use of these platforms often has security gaps that hackers can exploit, and this research provides solutions to overcome these vulnerabilities according to the types of attacks that hackers can carry out [16].

The research conducted by Azlin with the title "Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64" aims to improve data security, especially in the context of passwords. Using the Base64 algorithm in the developed application allows the implementation of an encryption process that converts text files into random characters. In addition, the application can also perform a decryption process to restore the text file to its original form. The application could encrypt and decrypt text files with more than 100,000 characters without changing their integrity [17].

The research on "Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang" aims to increase data security from access by irresponsible external parties. An additional layer of security can be provided through the implementation of this algorithm, as external parties who attempt to know the original text must know the key and the type of algorithm combination used in the encryption process. This research also tested the effectiveness of using the Base64 algorithm by conducting a series of trials using 20 different methods. The results showed that the data was successfully secured and could not be hacked by external parties [18].

Research on "Penerapan Kombinasi Algoritma Base64 Dan Rot47 Untuk Enkripsi Database Pasien Rumah Sakit Jiwa Prof. Dr. Muhammad Ildrem" aims to improve the security of patients' data so that irresponsible parties do not misuse it. In this study, researchers combined two algorithms, namely ROT47 and Base64, to produce an adequate algorithm that can be appropriately implemented to maintain hospital patient data security [19].

Based on the explanation above, the problem with the system used as a case study in the research is that the current system still has concerns about maintaining the security of personal data. So, a system must be evaluated to solve these problems and reduce the potential use of data by unauthorized people; therefore, this research raises the topic of designing a platform assessment by inserting a Moodle-based cryptography method. The results of this research can be utilized to add a layer of security in assessment activities using a digital platform.

2. METHOD

The research method applied in this study used the Design and Development Research (D&D Research) approach. This approach has two main characteristics, namely (1) it produces a product and (2) the product is produced through a research process. The D&D Research approach is a development of the waterfall model that allows the development of information systems to be more systematic and sequential, with the following stages [20].

1) Communication (Project Initiation & Requirements Gathering).
   The Planning stage describes the estimated technical tasks to be performed, risks that may arise, resources required for system development, expected work products, implementation schedule, and monitoring of the development process..
2) Planning (Estimating, Scheduling, Tracking).
   The planning stage explains the estimated technical tasks to be carried out, risks that may arise, resources required for system development, expected work

products, implementation schedule, and development process monitoring.

3) Modeling (Analysis & Design).
This stage focuses on designing and modeling the system architecture, including the design of data structures, software architecture, user interfaces, and program algorithms. The goal is to deeply understand the big picture of the work to be done.

4) Construction (Code & Test).
The Construction stage involves translating the design into machine-readable code or language. Once the code has been created, the system and code are tested to detect and correct any possible errors.

5) Deployment (Delivery, Support, Feedback).
The Deployment stage includes software delivery to customers, periodic maintenance, repair, evaluation, and development based on the feedback provided. The goal is to keep the system running and developing according to the needs and goals set.

The advantages of applying this research method are:

- It means that the system can be ensured to be suitable because each process is carried out in stages.
- Errors that are likely to occur can be minimized.

For more details, see Figure 1.

The data collection method used is observation, which analyzes the needs of the existing assessment platform system at the University of Education Indonesia Campus in Cibiru. The data observed includes information about students, lecturers, and exam types.

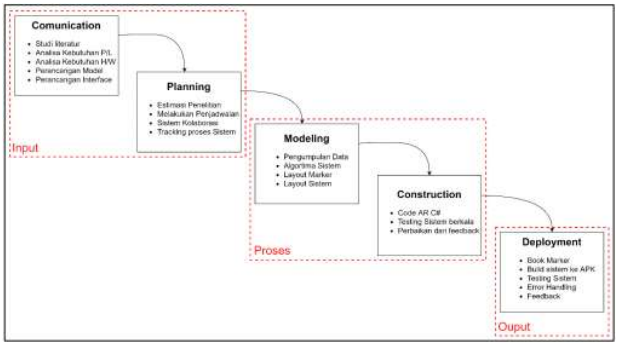

Figure 1. Stages of Waterfall Model Research

3. RESULTS

The research that has been done produces a Moodle-based platform assessment. In addition, the main result of this research is a plugin that can be used on the Moodle-based assessment platform. When used, the feature contained in the plugin adds a layer of security to the assessment activity by encrypting the essay and answer forms.

1. Entity-Relationship Diagram (ERD) Customization

The plugin developed for the quiz activity in the assessment platform generates a new database that stores all encrypted student question-and-answer data. Therefore, this new database is linked to the course database on Moodle LMS. As shown in Figure 2, the database structure and Entity-Relationship Diagram (ERD) illustrate how the entities in the database are connected.

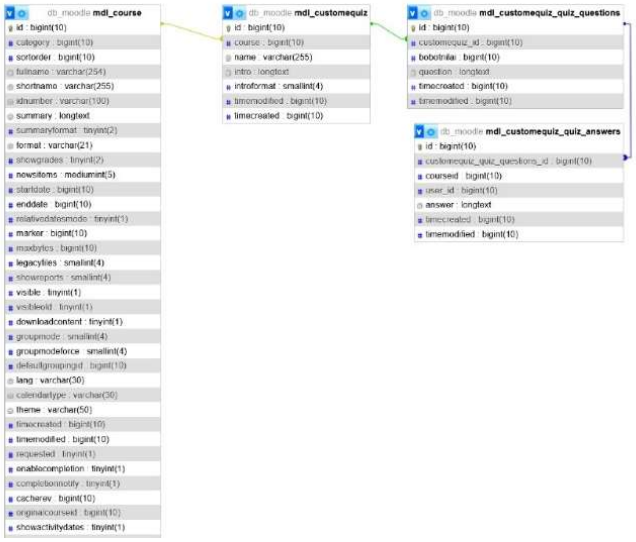

Figure 2. Entity-Relationship Diagram (ERD)

2. Activity Quiz Increase

Using the plugin created on the Moodle-based assessment platform adds a new activity option called "Cryptography-

https://doi.org/10.25077/TEKNOSI.v9i3.2023.264-270

Based Moodle Plugin for Essay Exams," as seen in Figure 3. When this activity is selected and used, the data, such as questions and answers from students, will be encrypted.

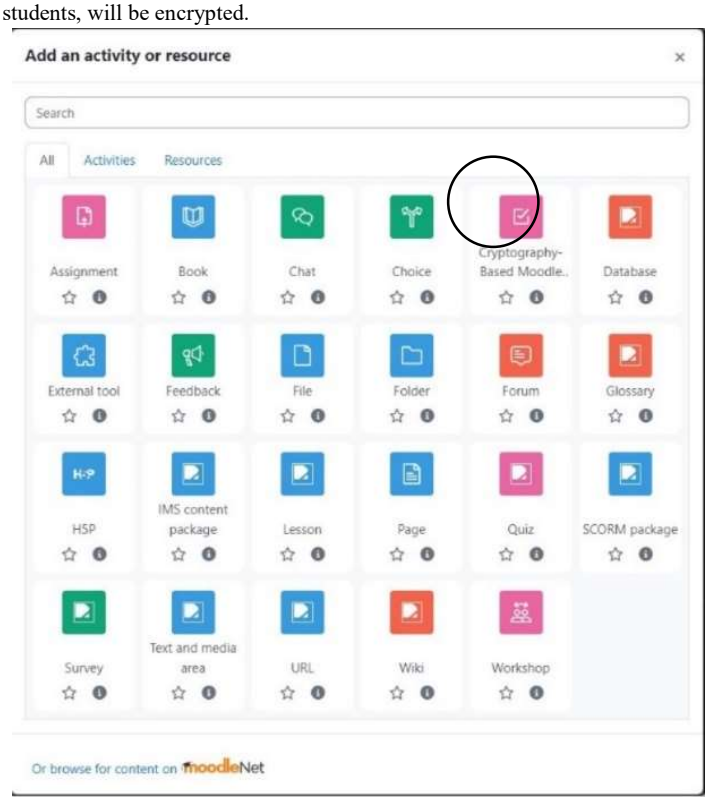

Figure 3. Select Page Activity

3. Page for filling out and submitting student questions

The encrypted essay exam question is decrypted when the student accesses the question, as shown in Figure 5. The result is displaying the question in a sentence form that the student quickly understands without displaying the encrypted question data. When students submit their answers after answering the question, the encryption will again be performed to store the answers in the database.

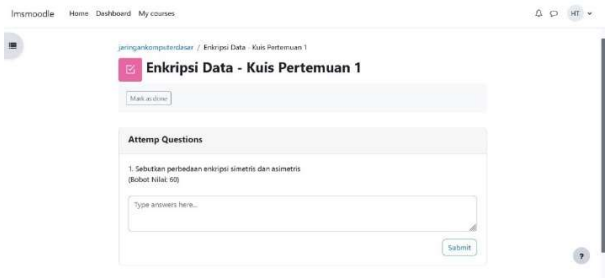

Figure 4. Student Question and Answer Submit Pages

After students submit their answers, the answer encryption process is done from the client side, which is referred to as client-side encryption. Thus, during the transmission of student answer data to the database, what is sent is the ciphertext resulting from the encryption process, and the ciphertext will be stored in the database.

4. DISCUSSION

4.1. Analysis System

This research decided to use Moodle as the supporting medium of the various Learning Management Systems (LMS) and other platforms available to support assessment activities. Moodle was chosen because it is a comprehensive and easy-to-use platform for assessment purposes. In addition, in 2018 and 2019, Moodle was ranked in the top 20 best LMS based on user experience, and until 2023, the Moodle platform maintained a user satisfaction score of 98% [21]. In addition, Moodle is also an open-source platform.

Moodle provides various teaching and learning activities, including assessment activities such as quizzes or exams. In the context of this research, which focuses on developing an assessment platform specifically for quizzes or essay exams, cryptographic methods are applied to maintain data security, such as exam questions and answers from students taking the exam. Moodle, as an open-source platform, allows the results of this research to be implemented as a Plugin that can be used on Moodle-based platforms.

Various algorithms can be used to implement cryptographic methods, and one of them is the Base64 algorithm, which is used in this research for the encryption and decryption process. The Base64 algorithm is an encoding and decoding method in ASCII format that is based on a 64-bit base number system. It

is one of the methods used to encode binary data [22]. The use of this algorithm aims to ensure good functionality in the development of assessment platforms with cryptographic methods. Previous researchers have widely used the Base64 algorithm, and have proven successful in the encryption and decryption process, producing ciphertext or encrypted text that is difficult to understand by people not experienced in cryptography [23].

4.2. Design System

The designed system can be used by 2 (two) actors, namely teachers and students. The teacher acts as an assessment implementer, while the student acts as an assessment participant. The following is a flowchart of the system that has been presented in Figure 5.

.

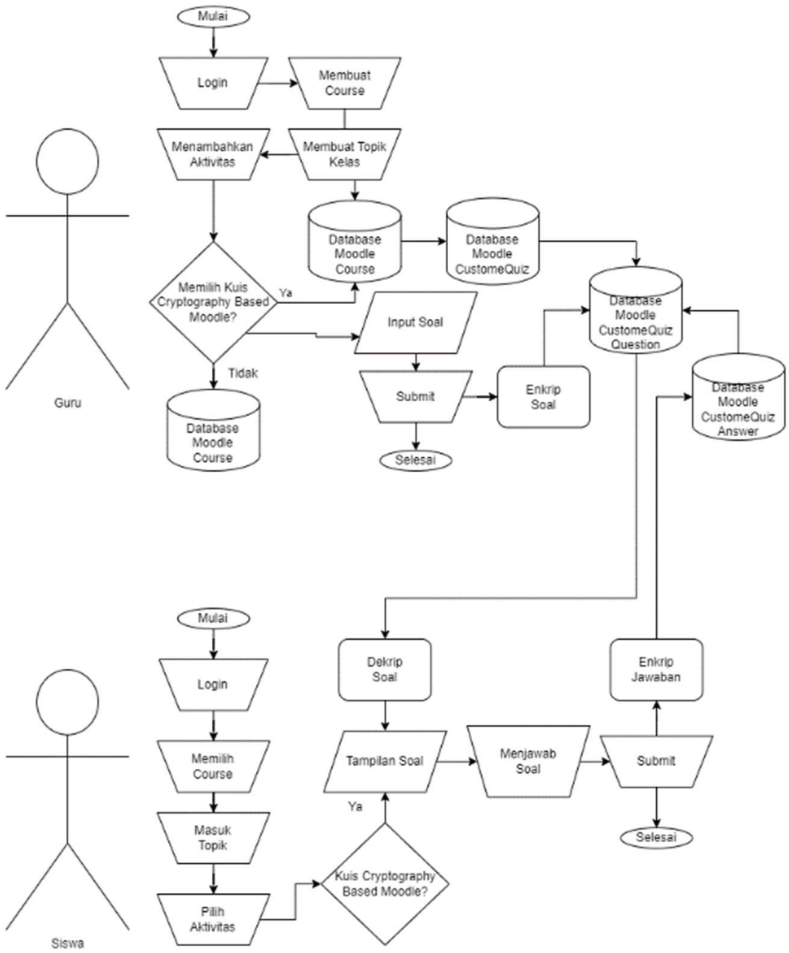

Figure 5. System Flowchart

4.3. Implementation System

The system implementation begins by applying the data obtained from the observation, which includes information related to lecturers, students, and subjects, for the assessment platform. Each actor has access to the subjects available on the assessment platform. After logging in, the teacher can create an activity for assessment activities, as illustrated in Figure 3. Meanwhile, students can access activities that have been provided by the teacher, as shown in Figure 4.

4.4. Testing System

System effectiveness testing is carried out using the black box testing method using a tool called Wireshark. This tool can be used to monitor and analyze data traffic traveling through the network without requiring internal knowledge of encryption implementation details. This test focuses on the level of security and performance of the encryption process and the ability to protect the data sent, namely questions and answers that have been submitted. The test results are presented in Figure 6 and Figure 7.

In Figure 6, it can be seen that the student answer data captured using Wireshark can be read and accessed easily. It shows that the data does not have an adequate encryption layer. However, in Figure 7, an effective encryption process has been applied because when Wireshark accesses the student answer data, the data is converted into an unreadable format that is difficult for unauthorized parties to understand.

 https://doi.org/10.25077/TEKNOSI.v9i3.2023.264-270

Therefore, using encryption has improved data security and protected the confidentiality of student answers during the transmission process over the network.

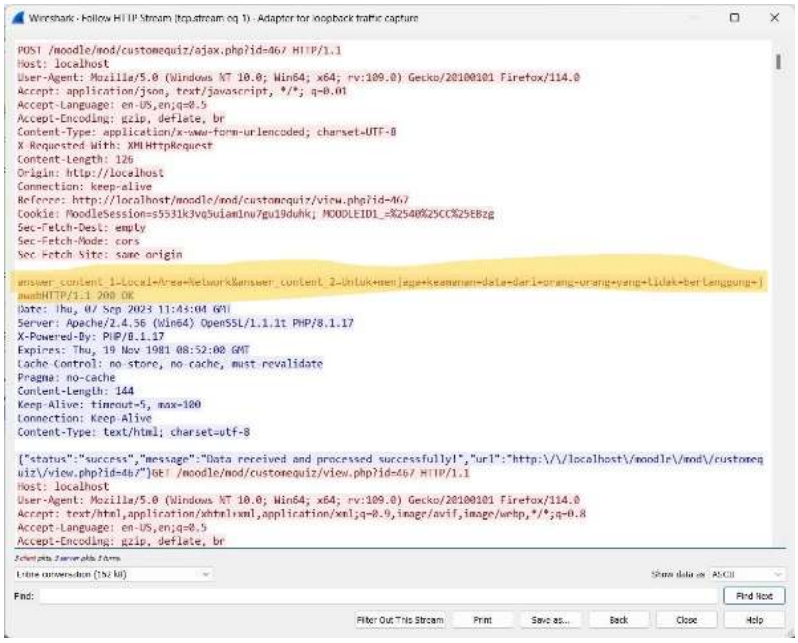

Figure 6. Test Results on Essay Test Creation Before Using Plugins

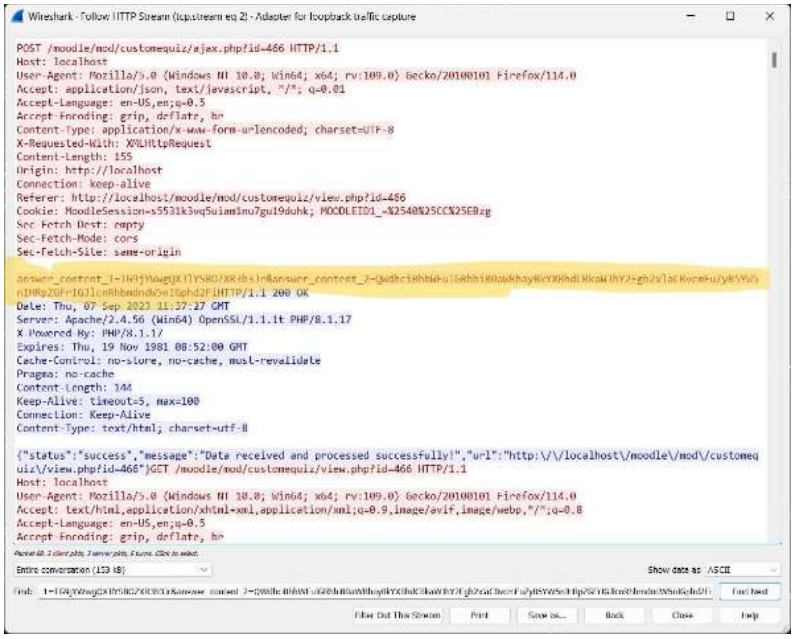

Figure 7. Test Results on Creating Essay Exams After Using Plugins

5. CONCLUSION

The Base64 algorithm has successfully supported the creation of plugins for developing assessment platforms. It is proven through the encryption and decryption process that is successfully implemented on essay exam questions and student answers when using the plugin that has been created. Testing with the black box method also shows that the assessment platform system can run according to design and function as expected.

However, it is essential to note that the cryptographic algorithm used in this research is a commonly used algorithm, and online tools are available to perform decryption with ciphertext input or text that has been encrypted. Therefore, there are still potential loopholes for irresponsible parties to commit fraud.

Overall, this research has improved the integrity of the assessment platform. With the implementation of cryptographic

methods, the security level of the assessment platform increases one step further compared to assessment platforms that do not use cryptographic methods. Therefore, this system can be further developed by applying more robust cryptographic algorithms so that the platform for assessment activities can be more effective in preventing potential fraud from irresponsible parties.

ACKNOWLEDGEMENT

Thank you to Universitas Pendidikan Indonesia for funding this research through LPPM research grant 2023.

BIBLIOGRAPHY

[1] A. Widyasari, M. R. Widiastono, D. Sandika dan Y. Tanjung, "Fenomena Learning Loss sebagai Dampak Pendidikan di Masa Pandemi Covid-19," *BEST JOURNAL (Biology Education, Science & TEchnology),* vol. 5, no. 1, pp. 297-302, 2022.

[2] J. Kristiyono, "Budaya Internet: Perkembangan Teknologi Informasi Dan Komunikasi Dalam Mendukung Penggunaan Media Di Masyarakat," *Jurnal SCRIPTURA,* vol. 5, no. 1, pp. 23-30, 2015.

[3] G. Subroto, "Peran Dan Tantangan Tik (Internet) Dalam Pembangunan Pendidikan Indonesia," *Jurnal Teknodik,* vol. 19, no. 2, pp. 119-134, 2015.

[4] R. Raja dan P. C. Nagasubramani, "Impact of modern technology in education," *Journal of Applied and Advanced Research,* vol. 3, no. 1, pp. S33-S35, 2018.

[5] M. Siahaan, "Dampak Pandemi Covid-19 Terhadap Dunia Pendidikan," *Jurnal Kajian Ilmiah (JKI),* vol. 1, no. 1, pp. 73-80, 2020.

[6] R. A. Joseph dan V. Sundaram, "Cryptography and steganography–a survey," *International Journal of Computer Technology and Applications,* vol. 2, no. 3, pp. 626-637, 2011.

[7] W. Prayitno, "Implementasi Blended Learning Dalam Pembelajaran Pada Pendidikan Dasar Dan Menengah," *Jurnal Pendidikan,* vol. 6, no. 1, 2015.

[8] L. dan K. L. Dangwal, "Blended Learning: An Innovative Approach," *Universal Journal of Educational Research,* vol. 5, no. 1, pp. 129-136, 2017.

[9] R. Shivam dan S. Singh, "Implementation of Blended Learning in Classroom: A review paper," *International Journal of Scientific and Research Publications,* vol. 5, no. 11, pp. 369-372, 2015.

[10] D. Yana dan A. , "Efektivitas Penggunaan Platform Lms Sebagai Media Pembelajaran Berbasis Blended Learning Terhadap Hasil Belajar Mahasiswa," *DIMENSI,* vol. 8, no. 1, pp. 1-12, 2019.

[11] D. G. H. Divayana, "The Implementation of Blended Learning with Kelase Platform in the Learning of Assessment and Evaluation Course," *iJET (International Journal of Emerging Technologies in Learning),* vol. 14, no. 17, pp. 114-132, 2019.

[12] W. T. Atmojo, M. E. Siregar dan K. K. Audrey, "Pengenalan Cyber Security Dalam Revousi Industri 4.0 Dan Menyongsong Era Society 5.0," dalam *Prosiding PKM-CSR*, Kabupaten Tangerang, 2021.

[13] H. F. Aldheleai, M. U. Bokhari dan H. S. Hamatta, "User Security in E-Learning System," dalam *2015 Fifth International Conference on Communication Systems and Network Technologies*, Gwalior, 2015.

[14] S. E. Prasetyo, N. Hasanah dan G. Wijaya, "Pengujian Keamanan Learning Management System TutorLMS terhadap Kerentanan Insecure Design dan Broken Access Control," *TELCOMATICS,* vol. 7, no. 2, pp. 53-60, 2022.

[15] G. E. Violettas, T. L. Theodorou dan G. C. Stephanides, "E-Learning Software Security ested for Security Vulnerabilities & Issues," dalam *2013 Fourth International Conference on e-Learning" Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity"*, 2013.

[16] R. Pramudita, S. Fuada dan N. W. A. Majid, "Studi Pustaka Tentang Kerentanan Keamanan E-Learning dan Penanganannya," *JURNAL MEDIA INFORMATIKA BUDIDARMA,* vol. 4, no. 2, pp. 309-317, 2020.

[17] A. F. Musadat dan J. Nur, "Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64," *Jurnal Informatika,* vol. 7, no. 2, pp. 1-5, 2018.

[18] T. Lovian dan I. Fitri, "Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang," *JURNAL MEDIA INFORMATIKA BUDIDARMA,* vol. 6, no. 1, pp. 692-700, 2022.

[19] R. Aulia, A. Zakir dan D. A. Purwanto, "Penerapan Kombinasi Algoritma Base64 Dan ROT47 Untuk Enkripsi Database Pasien Rumah Sakit Jiwa Prof. Dr. Muhammad Ildrem," *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan),* vol. 2, no. 2, pp. 146-151, 2018.

[20] H. S. Fuada dan D. Pradeka, "Kenal Hardware: Media Pembelajaran Pengenalan Perangkat Keras Komputer Menggunakan Teknologi Augmented Reality," *Building of Informatics, Technology and Science (BITS),* vol. 4, no. 1, pp. 247-255, 2022.

[21] L. Andre, "20 Best LMS Software solutions of 2019," All B2B, 21 08 2023. [Online]. Available: https://reviews.financesonline.com/p/moodle/. [Diakses 10 10 2023].

[22] M. S. Kurniawan, I. G. A. S. Putra, I. M. A. Maheswara, R. Y. M. N. Labamaking, I. M. E. Listartha dan G. A. J. Saskara, "Analisis Efektivitas Dan Efisiensi Metode Encoding Dan Decoding Algoritma Base64," *Jurnal Jitek (Jurnal Informatika Dan Teknologi Komputer),* vol. 3, no. 1, pp. 24-34, 2023.

[23] R. Minarni, "Implementasi Algoritma Base64 untuk Mengamankan SMS pada Smartphone," *Building of Informatics, Technology and Science (BITS),* vol. 1, no. 1, pp. 28-33, 2019.