JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VIII No 2, April 2022, hlm. 147 - 152 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v8i2.1381
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

PROJECT-BASED LEARNING ON CRYPTOGRAPHIC USING LMS

M. Syaifuddin[1], Amrullah[2*], Rico Imanta Ginting[1], Mochammad Iswan[1], Juniar Hutagalung[1]
[1]Sistem Informasi, STMIK Triguna Dharma
[2]Fakultas Ilmu Komputer, Universitas Muhammadiyah Sumatera Utara
email: [*]amrullah@umsu.ac.id

Abstract: Cryptography is one of the important subjects to learn because the content of the discussion discusses data security. Data security has a very important role considering that most transaction activities are carried out on the internet. Many platforms offer virtual transactions, such as motorcycle taxis, online marketplaces, and banking. For transacting on the internet, reliable data security is needed to maintain the security of user data from internet crimes (cybercrime). For cryptography learning to produce students who understand cryptography in-depth, this learning is carried out independently. One of the lessons to improve independent skills is a project approach. With project-based learning, students will be actively involved in completing projects given by the lecturer. To facilitate interaction and monitor projects completed by students, an LMS (Learning Management System) was created. The lecturer will later upload the student projects through the LMS, and if the student wants to work on the project, they can download it from the LMS.

Keywords: Cryptography; LMS; Online transactions

Abstrak: Kriptografi merupakan salah satu mata pelajaran yang penting untuk dipelajari karena isi bahasannya membahas tentang pengamanan data. Saat ini, keamanan data memiliki peran yang sangat penting, mengingat sebagian besar aktivitas transaksi dilakukan di internet. Banyak platform yang menawarkan transaksi virtual, seperti ojek online, pasar online dan perbankan. Dalam bertransaksi di internet dibutuhkan keamanan data yang handal untuk menjaga keamanan data pengguna dari kejahatan internet (cyber crime). Agar pembelajaran kriptografi menghasilkan mahasiswa yang memahami kriptografi secara mendalam, maka pembelajaran ini dilakukan secara mandiri. Salah satu pembelajaran untuk meningkatkan kemampuan mandiri adalah dengan pendekatan project. Dengan pembelajaran berbasis project, mahasiswa akan terlibat aktif menyelesaikan project yang diberikan dosen. Untuk memudahkan interaksi dan monitor project yang diselesaikan mahasiswa, maka dibuat LMS (Learning Manajement System). Setiap project mahasiswa nantinya akan di unggah oleh dosen melalui LMS dan mahasiswa bisa mengunguh project di LMS
Dengan menambahkan LMS dan pembelajaran yang berbasis project pada pembelajaran kriptografi menunjukkan hasil belajar yang lebih baik. Hal ini dapat dilihat pada hasil tinjauan dilangan dengan penyelesaian sebuah soal dan hasil ujian akhir mahasiswa.

Kata kunci: Kriptografi; LMS; Transaksi Online,

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VIII No 2, April 2022, hlm. 147 - 152 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v8i2.1381
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

INTRODUCTION

Currently, the presence of the internet has penetrated. It is widely used by the community for various purposes and needs, both in business fields such as online motorcycle taxis, online markets, banking, etc. With the help of the internet, all forms of communication and transactions are easier and can reach areas difficult to reach. With the widespread and increasing use of the internet, development and research is currently being carried out on the use of the internet in helping activities and routines and human work [1] [2].

With the increasing use of the internet, it is necessary to pay attention to the security side of user data. This is because user privacy data on the internet can be easily accessed and obtained, which can later be misused by others to commit fraud or to harm others. Data security is needed to ensure that data usage on the internet is safe, reliable, and strong [3]. With reliable data security, users are no longer worried about private data confidentiality when using the internet [4].

One of the security techniques used is data encryption [5]. Encryption is one of the fields of data security by changing the contents of the data into new data whose contents can only be understood and understood by the intended person or the owner of the decryption key [4].

Encryption and decryption are a discussion of the security field in cryptography. Maintaining information and ensuring that the information received is safe and that there is no data change when the data is sent is a top priority in communicating.

Understanding and exploring cryptography is fundamental for Computer Information Systems Study Program students, so many efforts have [illegible] facilitate learning [6]–[11]

Presenting media in assisting the delivery of learning materials received positive responses and responses from students [12]–[14], so in this study, they also presented a learning media in the form of LMS (*Learning Management System*). With the help of LMS in learning cryptography, students will be able to simulate the results of manual calculations carried out students.

To increase student independence in learning cryptography, lecturers are no longer positioned as the only source of knowledge. In this study, the lecturer only gave orders packaged in the form of a project, and later, students actively completed the project. Examples of projects that students will complete will later be uploaded to the LMS, and students can download them from the LMS.

LMS in learning can facilitate interaction between lecturers and students, especially in monitoring the results of projects carried out and completed by students. And the selection of project-based learning in cryptography learning is based on students' self-confidence. With project-based learning, students must work independently to complete projects [15].

To maintain and ensure that the projects completed by students are in the right corridor, lecturers must play an active role in guiding and monitoring projects completed by students [16].

METHOD

The method is a step or procedure prepared to achieve the planned goal. In building and developing (Research and Development) LMS (Learning Manage-

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VIII No 2, April 2022, hlm. 147 - 152 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v8i2.1381
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

ment System) in the form of CAI, a method is used, and the method used is a waterfall. Development research is research that aims to develop an existing procedure or model. Development research is often referred to as Research and Development (R & D). Development research is often referred to as research and development (R & D). The stages of the research are (1) preliminary, (2) development, (3) validation, and (4) implementation. [17]

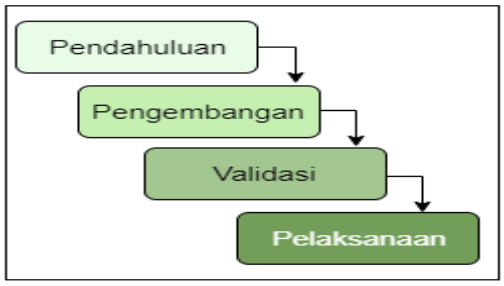

Figure 1 Stage R & D

Explanation of the waterfall model in Figure 1

1. Preliminary

An analysis of needs for knowing the goal of learning cryptography. This analysis on lecturers and students. Because of these subjects on a learning process. Analysis of the lecturers conducted material and analysis of the results of understanding the material being taught to students. This analysis will get an overview of the model and learning style that will be applied later.

2. Development

The development here consists of making LMS and designing teaching materials. In this study, the LMS was built on the web. This consideration is made because the LMS position is expected to be used anywhere and anytime.

3. Validation

Validation is the stage of asking for advice, input, and assessments related to products that experts have made. The product made in this research has been tested and is suitable for learning cryptography, which is oriented towards the final result of making a data security application.

After being declared valid and with some notes, the product is tested on a small scale with 15 students and 3 lecturers. The LMS and the teaching materials will be monitored and evaluated during the learning process. This is intended to see how effectively the product achieves the desired learning objectives.

Based on the monitoring and evaluation results, this product underwent several improvements, including an LMS that should be easier to use and the addition of a more organized task collection facility.

Products that are recommended to be repaired will be repaired. After improving the product, it was retested on a larger scale, which amounted to 25 people and 3 lecturers. In this test, supervision and reevaluation of student learning outcomes are examined. And at this stage, the learning outcomes are by the expected goals, and to realize these goals, the new LMS and teaching materials are considered to have contributed greatly to this achievement.

4. Implementation

The product was made and declared feasible to be applied to learning cryptography, then trained by lecturers who teach cryptography courses. And after the lecturer understands the truth, this product is applied in every cryptography lesson at STMIK TRIGUNA DHARMA College, majoring in Information Sys-

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VIII No 2, April 2022, hlm. 147 - 152 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v8i2.1381
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

tems Study Program.

RESULTS AND DISCUSSION

This research has produced LMS and teaching materials used in learning cryptography. The figure of this LMS is:

1. Form Register

Figure 2. Form Register

This form is used to register. This is done at the beginning if you want to use this LMS. In this form, there are two facilities, namely those for lecturers and students. Lecture facilities are used by lecturers because, in this facility, the lecturers will upload materials. For student facilities, they will be able to view and download materials that have been uploaded to the LMS.

2. Form Login

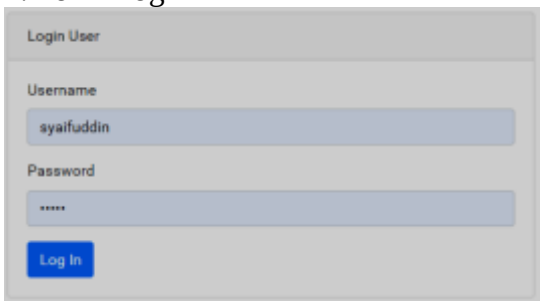

Figure 2. Forum Login

Lecturers use this form to enter the LMS. This form is useful to facilitate one lecturer's work with other lecturers in providing material through the LMS. The username and password used when logging in must be the same as those entered during registration.

3. Material Upload Form

Figure 3 Result Material Upload

In this facility, lecturers can upload project materials that students will work on. In addition to uploading lecturers, they can also delete material if the project material contains errors or wants to be corrected.

4. Student Form

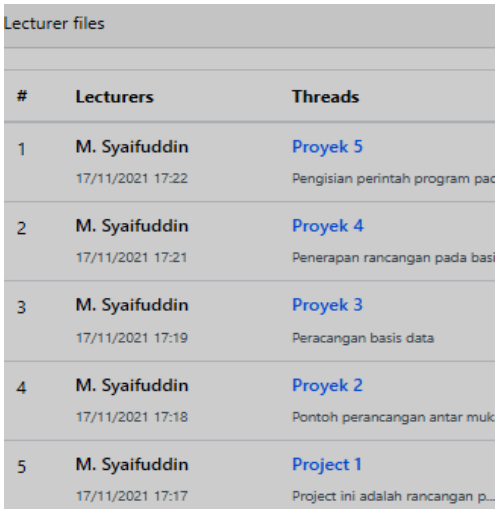

Figure 4 Student Facilities

This form is used to see the project given by the lecturer to work on. The lecturer at the LMS will upload the

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VIII No 2, April 2022, hlm. 147 - 152 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v8i2.1381
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

project given at each meeting.

5. Result Project

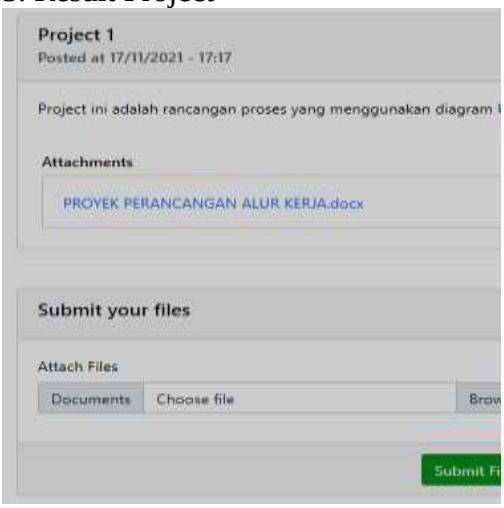

Figure 5 Result Project

In this facility, students can see more details about a given project. In this facility, students will be able to view and download the given project. In addition to downloading, students will upload completed projects in this facility.

CONCLUSION

This study succeeded in developing a learning device in the form of an LMS (Learning Management System) using the R & D research method. Based on the application of the product in the field, namely the 7-semester students of the STMIK TRIGUNA DHARMA Information System program, this product can increase motivation and learning outcomes. This is because it is easy to get information/teaching materials, and there is clearer project supervision and the availability of teaching materials at LMS. As a result, this product greatly helps students and lecturers to achieve and improve their cryptography learning.

ACKNOWLEGMENTS

We thank the Kementrian Pendidikan and Kebudayaan (KEMENDIKBUD) for supporting and funding this research.

BIBLIOGRAPHY

[1] G. R. Adiarsi, Y. Stellarosa, and M. W. Silaban, "LITERASI MEDIA INTERNET DI KALANGAN MAHASISWA," vol. 6, no. 4, pp. 470–482, 2015.

[2] A. Junaidi, "Internet Of Things, Sejarah, Teknologi Dan Penerapannya : Review," *J. Ilm. Teknol. Inf.*, vol. 1, no. 3, pp. 62–66, 2015.

[3] S. Palinggi and E. C. Limbongan, "Pengaruh Internet Terhadap Industri E-Commerce dan Regulasi Perlindungan Data Pribadi Pelanggan di Indonesia," *Semin. Nas. Ris. dan Teknol.*, vol. 4, no. 1, pp. 225–232, 2020, doi: 10.30998/semnasristek.v4i1.2543.

[4] M. Syaifuddin, "E-Learning Dalam Pengembangan Pembelajaran Kriptografi," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. VII, no. 2, pp. 117–126, 2021.

[5] T. Hidayat, "ENCRYPTION SECURITY SHARING DATA CLOUD COMPUTING BY USING AES ALGORITHM : A SYSTEMATIC REVIEW," vol. 2, no. 2, 2019.

[6] J. Rahmadoni, "Perancangan Simulasi Pembelajaran Kriptografi Klasik Menggunakan Metode Web Based Learning," *INTECOMS J. Inf. Technol. Comput. Sci.*, vol. 1, no. 1, pp. 34–43, Mar. 2018, doi: 10.31539/intecoms.v1i1.160.

[7] M. Y. Maulana *et al.*, "PERANCANGAN APLIKASI MEDIA PEMBELARAN," pp. 357–367.

[8] A. Hallim, I. Uzzin Nadhori, M. Jurusan Teknologi Informasi, and D. Pembimbing, "PEMBUATAN PERANGKAT LUNAK MEDIA PEMBELAJARAN KRIPTOGRAFI KLASIK," 2010.

[9] T. Arianti and B. Nadeak, "Perancangan Aplikasi Pembelajaran Kriptografi Algoritma GOST dengan Menggunakan Metode Computer Based Instruction," vol. 1, pp. 40–46, 2019.

[10] A. Adil, "APLIKASI MEDIA BANTU PEMBELAJARAN KRIPTOGRAFI DENGAN MENGGUNAKAN ALGORITMA MESSAGE DIGEST 5 (MD5)," vol. 5, pp. 45–51, 1858.

[11] B. Silaban and T. Limbong, "Aplikasi Pembelajaran Pengenalan Kriptografi Algoritma Affine Cipher Dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction," vol. 2, no. 2, pp. 93–99, 2017.

[12] A. R. Rojabi, "Blended Learning via Schoology as a Learning Management System in Reading Class: Benefits and Challenges," *J. Linguist. Trap.*, vol. 9, no. 2, p. 36, 2019, doi: 10.33795/jlt.v9i2.92.

[13] M. N. Multazam, C. A. Korompot, and M. Munir, "Benefits and Difficulties in Using Learning Management System (LMS) in Paragraph Writing Class : A Study of a Lecturer ' s and Her Students ' Perception," vol. 1, no. 1, 2022.

[14] Y. Zheng, J. Wang, W. Doll, X. Deng, and M. Williams, "The impact of organisational support, technical support, and self-efficacy on faculty perceived benefits of using learning management system," *Behav. Inf. Technol.*, vol. 37, no. 4, pp. 311–319, 2018, doi: 10.1080/0144929X.2018.1436590.

[15] R. Nahdliyati □, M. Taufiq, and I. Artikel, "Unnes Science Education Journal EFEKTIVITAS PENDEKATAN SAINTIFIK MODEL PROJECT BASED LEARNING TEMA EKOSISTEM UNTUK MENUMBUHKAN KEMANDIRIAN BELAJAR SISWA SMP," 2016.

[16] Sri Haryati, "(R & D) Sebagai Salah Satu Model Penelitian Dalam Pendidikan," *Academia*, vol. 37, no. 1, p. 13, 2012.