Project-Based Learning Approach in Undergraduate Engineering Course of Cryptography and Security in Computer Science

Bhagyashri Panapt, Charusheela Pandit

Computer Engineering Department, ViMEET, Kumbhivali, Raigad, Maharashtra.
Computer Engineering Department, ViMEET, Kumbhivali,Raigad, Maharashtra.
bhagyashrishreya@gmail.com
cmpandit@vishwaniketan.edu.in

Abstract

The core idea of project-based learning (PBL) is to focus on the real-world problems that capture students' interest and develop critical thinking and problem-solving skills in students. We present in this paper how project-based learning help students to learn factors in project design and how technology can support students when they work on the projects. It presents the difference between traditional learning and project-based learning and also presents the execution of a project-based approach used in the work of the course conducted for sixth-semester students of the University of Mumbai that is Cryptography and System Security. Cryptography is a technique to convert the data from plain text to encrypted text and Vice a Versa. Security provides protection to any information from theft or damage from hardware or software. In our institute, Cryptography and System Security course are chosen for designing the PBL approach from Couse Level Project-Based Learning (CLPBL) because of its difficulty is higher level and importance in Industry. In the CLPBL process the teacher gives the key concept of projects to students and students will find out an appropriate solution for a given problem by using different security techniques, algorithms and authentication methods, etc. After completion of projects, students submit implementation, as well as documentation and the teacher, will evaluate them by using different assessment tools. Resulting from this is the students built enough confidence to implement not only what they learned in the class but also practically they can implement these concepts.

Keywords
Project-base learning, CLPBL, Security, Cryptography

Introduction

In traditional teaching, we begin by conveying the information, usually in descriptive class, and then presenting the problem to be solved, assuming that the contents previously conveyed will allow the students to understand and solve the problem.
In PBL the order changes. It begins by presenting the problem and the students try to obtain the information necessary to understand and solve the problem. The teacher changes their role, no longer delivering the information, but does help the student to get it and understand it. Project-based learning (**PBL**) is a practical approach in which small groups of students engage in tasks and learn as they attempt to solve relevant problems. Students ask and rewrite the questions, debate ideas, generate predictions, experiments, collect data, draw conclusions, communicate and detecting ideas, clarify the approaches, and create products.

Vishwaniketan Institute of Management Entrepreneurship and Engineering Technology (**ViMEET**) affiliated to University of Mumbai, is following the traditional as well as a project-based learning system. In ViMEET, the Course Level Project Based Learning (**CLPBL**) is being conducted for second and third-year students.
In this paper, we present a learning system that is built upon project-based learning. This learning system is capable of generating different issues from Cryptography and Security domain, that developing appropriate solutions, evaluating students' solutions and referring them to acceptable learning materials.
Course level project-based learning(CLPBL) is for higher education, the student attainment goes beyond content knowledge, to prepare and challenge the student to direct their own learning, solve problems of academic significance and to move beyond controlled information containment. Project-Based Learning in the Classroom ideas must be explored, developed, integrated, and resolved within the context of a particular assignment as knowledge construction at advanced levels take on new meaning. Rather than being the source of content expertise, teachers are challenged to be the coordinator of knowledge and motivators of action learning. Unlike assignments of traditional learning, the PBL approach recognizes and values unpredictable outcomes. Higher-level thinking and an extended thought process are to be expected from the students for real-world problems and life-skill expertise. PBL can be a leading factor in making

students successful and capable. At this level, students experience responsibility for academics that guide them into the essentials of lifelong learning and are validated through their decisions and actions. For this responsible instructional outcome, classes with large enrollments become easier to manage because learning is student-centered.

Computer Science and Engineering department of ViMEET is chosen Cryptography and System Security course of sixth-semester for the Course level project-based learning approach because of importance in Industry and difficulty in higher level. In this CLPBL process the teacher who has been assigned for the CLPBL course, he/she designs the problem statement of projects, but only project ideas or concepts are given to students. Students have to do a lot of brainstorming to identify the correct solutions. After completion of the projects students submit their report of projects to the teacher. Teachers are evaluating the projects throughout the semester by observing student activities.

PBL in Cryptography and Security

Cryptography is a widely known process of encrypting and decrypting messages. It can use anything from numbers to letters. We can pass messages without knowing others what the message is with the use of protocols, algorithms, and strategies. Cryptography is based on the sender and recipient having keys. When the sender wants to send a message, the sender encrypts the technology, and then sends the message. If the message is hacked the hacker will not understand the message. After the message reaches the recipient the message can be decrypted and read by the recipient.
Security needs against attackers and hackers. Security provides confidentiality, integrity, and availability from data hardware, software, and firmware of a computer system. Security protects the information from unauthorized access and loss.

The Cryptography and Security approach in project-based learning will show how cryptography and Security work in a real-world problem. Humans love to be secure. If anyone proved that something is secure and useful, humans will accept it. This will allow humans to feel safe enough to try to change old inefficient aspects of life with the new method given to them. In this approach, we are providing the method which uses cryptography for better securing information and data. It will allow using smarter and more secure methods. During these small transitions can observe many changes. Changing to a cryptography system is beneficial in the end as well as during the process. Society will be insecure due to some attackers. It will make small changes first. It will also have to be an attractive change. Using safe security of cryptography must attract the person by attractiveness as well as efficiency. The change will be slow in cryptography taking over other aspects of life that are not online, but certainly can be done. This change will have a major impact while and after it is being introduced into the everyday life of humans. The major impact can come from studying and learning science while this change is taking place. It will also reduce the vulnerability of paper documents. Translating languages isn't hard, but translating cryptography without a key is very difficult. Due to this, the work in this approach will be beneficial for society.

The principle behind this to prove that Cryptography can be effective and useful anytime and anywhere if used properly. Currently, cryptography is being used all over the globe, even by unsuspecting people. It is being used online. Everything that is secured or even slightly protected online is using cryptography. This little-known star of our lives protects and safeguards are valuable online information. Seeing that cryptography work is well, other forms of data storage and information safekeeping may be updated to use cryptography. For safety reasons, even written documents can be made into cryptography.

When we used cryptography and security concepts in our day-today life then every student needs to know how these concepts used in our life. So with the traditional system, it's not possible too much because in the traditional learning system theoretical part of the concepts expressed widely not actual implementation. So students cannot implement any concept that much effective in real-life. Due to this reason student needs to know what are the real-world problems and how to solve those problems with the help of those concepts learn previously, how to implement all these concepts and in day-to-day life by using project-based approach.

To enhance these concepts, In our institute, Cryptography and System Security course are chosen for designing the PBL approach from Couse Level Project-Based Learning (CLPBL) because of its difficulty is higher level and importance in Industry.

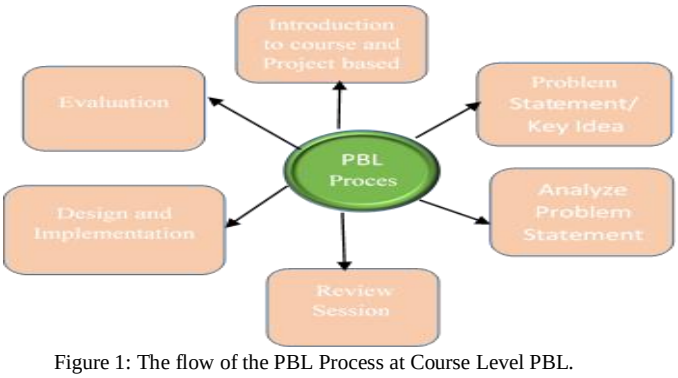

Figure 1: The flow of the PBL Process at Course Level PBL.

Figure 1 describes the flow of the PBL process when it considered at the Course Level. It describes after selection of course for CLPBL, the teacher who has been assigned for CLPBL, he/she designs the problem statement, but only project ideas or concepts are given to students. The teacher becomes a guide to this learning

process, and every student is the leading player of this learning. In this approach, the job of a teacher is to guide the student to find the best solution to the problem. Students also assume a new role and move from a generally static attitude, in which they expect to receive the knowledge, to be active subjects of their own learning. It is difficult for them to make this change but the teacher must get them involved, instead of listening; that they speak and communicate, instead of receiving explanations; analyze, obtain information, make decisions and do, rather than waiting for knowledge. Students have to do a lot of brainstorming to identify correct cryptographic techniques, cryptographic components, algebraic structures, hashing algorithms, and authentication techniques. For this process, students refer to some books and they also discuss with their teachers and friends and find out effective encryption algorithms, hashing techniques, etc. for the real-world problems given as projects. It develops a student's ability to work with other students, building teamwork and group skills. The teacher represents the learning outcomes of the course as well as he/she clears the explanation of basic concepts used in the course by giving some examples. He/ she has highlighted the concepts covered in the lecture and students are mapped these concepts with the learning outcomes as well as the concepts of projects covered. Simultaneously teacher designs the stepwise activities that involve in each project. Then he/she find out which topics are covered by each and every project from the syllabus. After this he/she designed the factors considered in project design such as student capabilities, Finance required for any project, College infrastructure, Is it challenging for students?, Can it be completed in time, Can course content be learned to fulfill? Etc.

Considering these factors he/she gives the rating to project design like high, medium and low. On the other side, a teacher takes a follow-up of students' progress by scheduling review sessions and gives any suggestions or changes to students. According to that, the students give their reviews on the project and also they report the completion of the project. Students are engaged with their activity to involve in a project means they are trying to finding out the solution for the project in various ways, by different-different concepts used in cryptography and security. Teachers find out the program outcomes that students will learn when the project is completed. Suggestions and changes will be checked in the next review and give remarks to them. After completion of the project students submits survey reports of projects and teachers evaluate them.

In the evaluation scheme, he/she defines some criterion that is the rubrics. A rubric is a grading tool that represents the performance, expectations for project work. A rubric provides clear descriptions of the characteristics of the work-related to each component, at every level. Rubrics give grades by finding patterns in student achievement or student error, it also provides analyzed information about student strengths and weaknesses of technical knowledge. It gives the score for individual parts of the product or performance of the student. It helps a student how to improve their performance regarding what is expected for each criterion. We use different parameters to evaluate the projects with the help of rubrics like security objectives, mechanisms, choosing appropriate algorithms from the cryptography and security concepts.

We sum up the PBL process with the help of one case study which is implemented by our students. When we start this process at that time we state the learning outcomes of the PBL process like:

CLO1. Apply the knowledge of symmetric cryptography to implement simple ciphers.
CLO2. Able to analyze and implement public key algorithms like RSA and El Gamal, hashing algorithms.
CLO3. To explore the different network tools to gather information about networks like sniffers, port scanners and other related tools for analyzing packets in a network.
CLO4. Able to set up firewalls and intrusion detection systems using open source technologies and to explore email security, web security and attacks on it.

After stating the course learning outcome we gave the key idea of a project to a student that is how to overcome the issue of manual bus pass checking system and some students travel without paying fees. Then our students started their brainstorming task such as finding the actual problem it is mean that they analyzed the problem and search for an appropriate solution with the help of a security concept. After this, they represented their analyzed work in the form poster at the time of the review session. At the time of the review session, students explained why they select the Triple-DES algorithm and how the project flow is. On another side, the teacher assessed their activities and has given some suggestions for implementing techniques in the project.

For this process, students referred to some books and they also discussed with their teachers and friends and did a lot of brainstorming to identify correct cryptographic techniques, cryptographic components, algebraic structures, hashing algorithms, and authentication techniques to find out the effective solution for the real-world problems given in their project. After finding all these things they gained actual concepts used in the project then they try to implement this. In a described case study, the students used the Triple-DES algorithm for encrypted as well as decrypted information and overcome the real-world problem. The Triple-DES algorithm used the concept of the Data Encryption Standard (DES)/ Data Encryption Algorithm (DEA). In the Triple-DES algorithm, we can use three different configurations of keys. In the first configuration, keys are used three independent keys and this is the most secure. In the second configuration, the first and third keys are

the same and the third configuration uses three identical keys. When identical keys are used, it works the same as DES. When we used the first type of key configuration – the 16 sub-keys are derived from key one with Initial permutation that includes the block is split into left and right halves. The right half is sent through the F function, Expansion permutation, XOR with the sub-key for the round, Substitution, Permutation, XOR the result of the F function with the left side and swap the right side the new left side, and the result is the new right side. Repeat the above steps 14 times. The right half is sent through the F function, Expansion, permutation, XOR with the sub-key for the 16th round, Substitution, Permutation, XOR the result of the F function with the left side and combine the left and right sides of the block together and complete with final permutation.

With all these methods, students have implemented the code for the given problem statement in Figures 3, 4, 5 and 6.

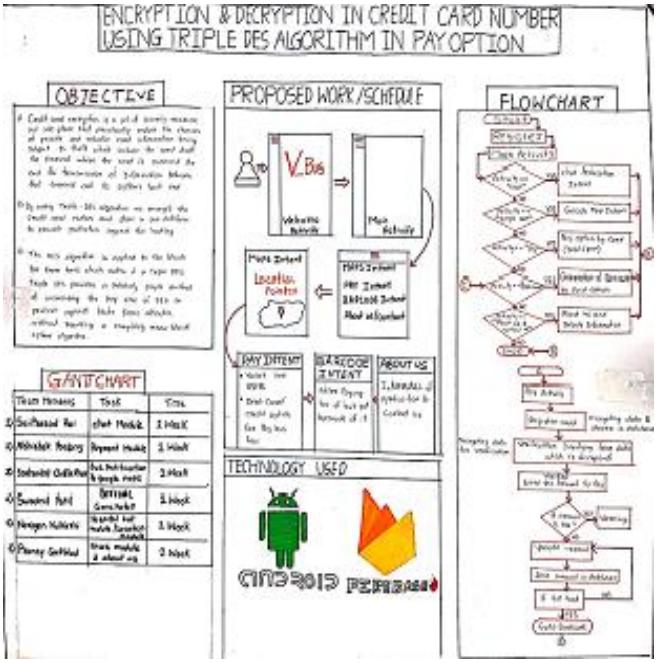

figure 2: Poster presented at the review session

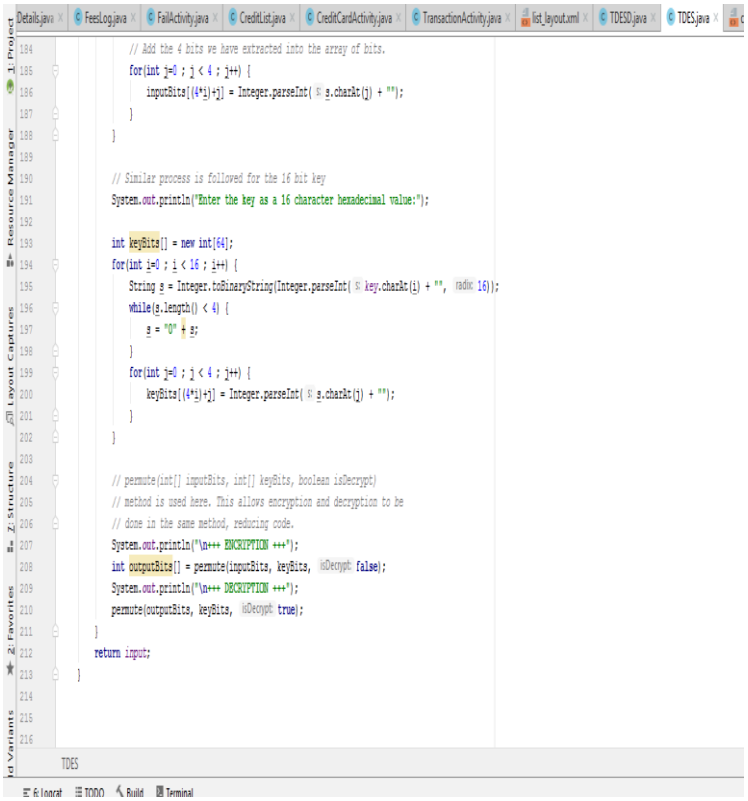

figure 3: Encryption Part

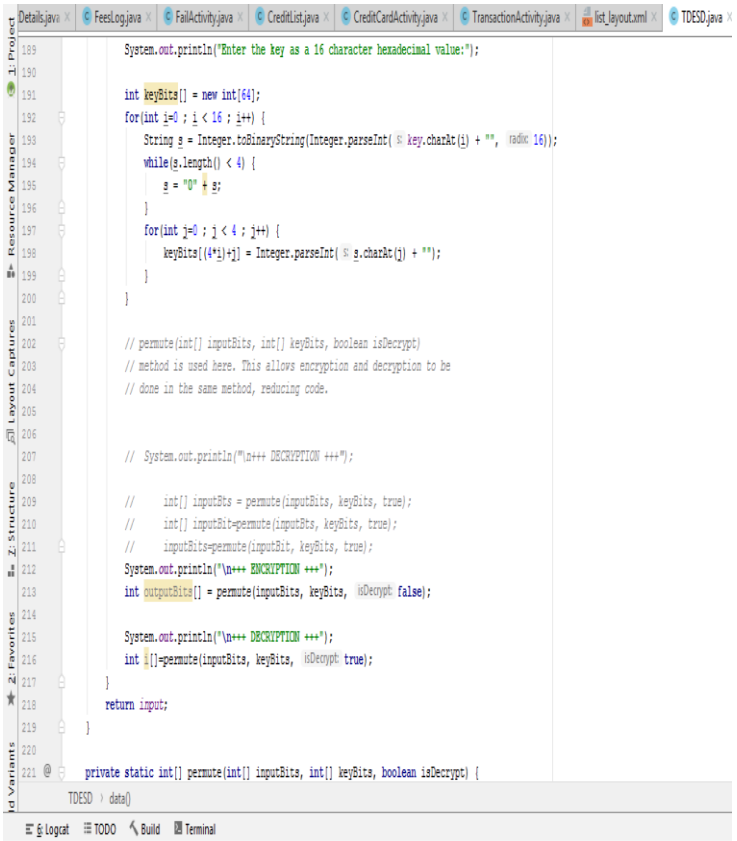

figure 4: Decryption part

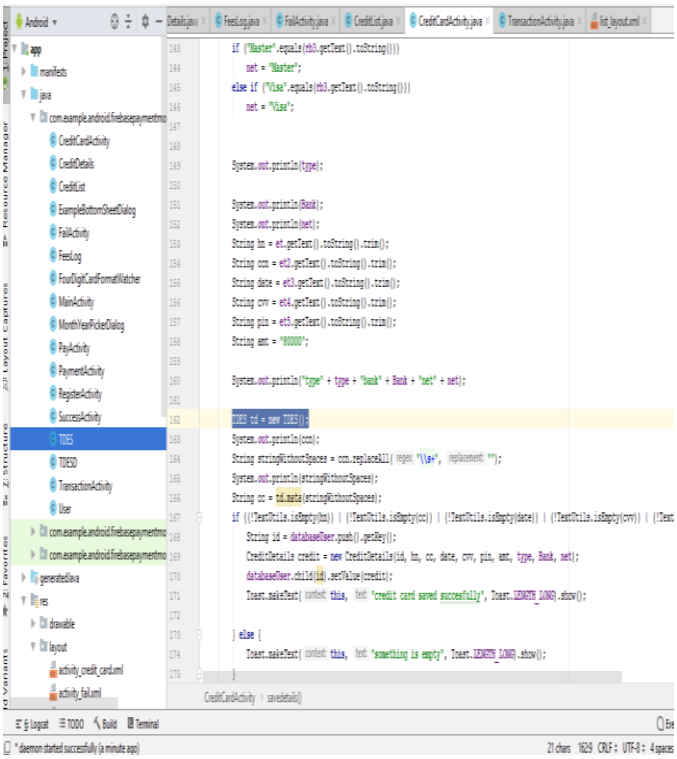

figure 5: Implementation in Activity

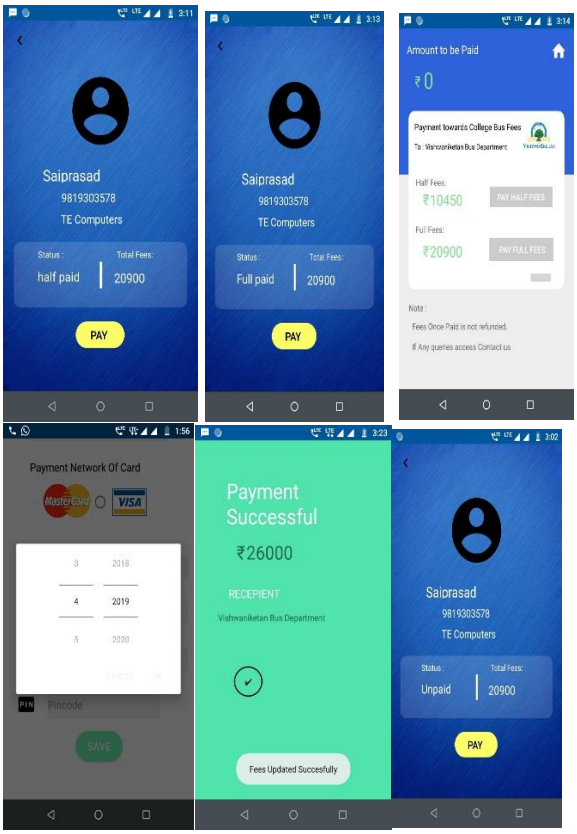

figure 6: GUI Interface

The actual output of the code given in figure 6.

By using this Triple–DES algorithm, students encrypt the credit card no. and store it into a database to provide protection against hacking. The DES algorithm is applied to the block cipher three times which makes it a Triple-DES. Triple-DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks without requiring a completely new block cipher algorithm.

After completion of this implementation of an android application based on security, students presented the outputs with live demo to the teachers and the teacher evaluated them by using rubric parameters considered for the PBL process and the grades are given to them.

The rubric parameters considered for evaluation as shown in figure 7.

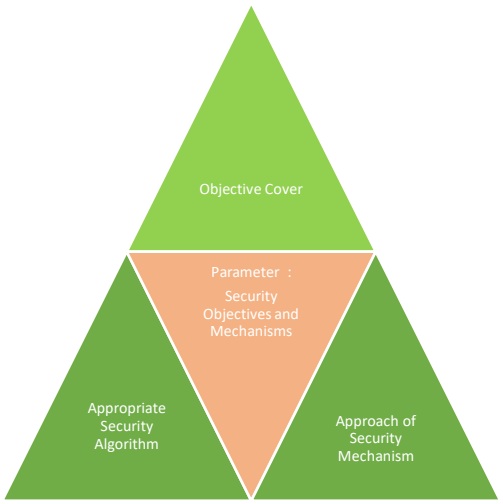

figure 7: Rubrics Design

According to this, the teacher evaluates student's projects and grades have given to them.

Results

An objective of the course is students can be able to analyze the given problem. They have to do a lot of brainstorming to identify correct cryptographic techniques, cryptographic components, algebraic structures, hashing algorithms, and authentication techniques and find out an appropriate solution for the problem. The main goal is to involve the students' in a PBL approach actively engaging students during the learning process, solving problems and different difficulties faced in project activities. To evaluate this goal during the course and after completion of the course, we interacted with students and took the responses about a PBL approach.

The class consists of 70 students, 80% of the students were interested to learn the course by using this approach and they were motivated not only to learn the course in-depth but also learn the effective algorithms from the course. Apart from the course, they have learned a fundamental skill (like reading, writing), mathematical skills along with problem-solving, teamwork, information collecting, time management, and handling high technological tools from a project-based learning approach. When students referred to different books at that time they developed the quality of reading as well as writing. When they wrote the End Semester Exam at that time they showed these skills as well as mathematical skills along with problem-solving, time management very effectively. In the exam, they improved their paper writing quality as compared to the last exam.

Following are students reactions with respect to course level project-based learning:

" We implemented the Triple-DES security algorithm for increasing security while storing the data in firebase. We learned and applied something new that was not in our syllabus. It also increased our knowledge regarding the course Cryptography and System Security. The PBL implementation was on credit card number which was encrypted and stored in firebase and while retrieving would be decrypted and showed in the interface of the app, since the credit card is an information value."

"The project-based learning process is quite unique in its own way. It makes us learn things by ourselves and Project-Based Learning is something in which we learn or understand the concepts taught in class by the means of building projects. So, this semester PBL was on the Cryptography and System Security course in which we implemented the concepts of data encryption, decryption and authentication concepts in our projects. To see their real-time working which proved to be very helpful, in terms of understanding which gave us enough confidence to implement not only what we learned in the class but outside the class also. "

Conclusion

Monotonous concepts of the course do not understand when students learn the course by a traditional learning process. due to this reason, for a greater understanding of that concept, the course will select for the project-based learning process. So it concluding that greater student interests ruling to better performance and deeper learning. In the traditional learning process, those concepts are very tedious, uninteresting, boring, etc. that the PBL process makes it very simple, understandable, interesting as well as challenging also. We concluded that, after the use of the PBL approach, the students improved knowledge of the respective subject which is used for the semester exam.

The project-based learning is not only useful for the students but teachers also. Teachers use the project-based approach at that time they learned multi leading, teamwork, professional development, new multiple technologies from the PBL approach.

We have concluded that the project-based learning process is useful for students as well as teachers also. When students gave presentations in review session they build up the presentation skill as well as teamwork. When teachers use PBL at that time they also learn how to evaluate the real-world problem according to course parameters.

References

1. An intelligent PBL -PBL-based tutoring system for cryptology domain by Aleksandar Jevremovic, Sasa Adamovic, Goran Shimic, Marko Sarac, Mladen Veinovic, Milan Milosavljevic.
2. An Innovative Approach Carried Out in Data Structures and Algorithms Lab by Sujatha C1, Jayalaxmi G. N2, Suvarna G.K3 Department of Computer Science and Engineering, B.V. Bhoomaraddi College of Engineering and Technology, Vidyanagar, HUBLI – 580031 State: Karnataka.
3. Motivating Project-Based Learning: Sustaining the Doing, Supporting the Learning Phyllis C. Blumenfeld, Elliot Soloway, Ronald W. Marx, Joseph S. Krajcik, Mark Guzdial & Annemarie Palincsar in ISSN: 0046-1520 (Print) 1532-6985 (Online) Journal homepage: https://www.tandfonline.com/loi/hedp20
4. Project-Based Learning of Programming Subject: a Case study on Data Structures Shridhar T Doddamani Department of Automation and Robotics, BVBCET, Hubli *Journal of Engineering Education Transformations, Volume 31, No. 3, January 2018, ISSN 2349-2473, eISSN 2394-1707*
5. Project-based Learning Experience on Data Structures Course Carolina Gallardo Pérez, Pilar Martínez García, Jesús Sánchez López Department of Information Structure and Organization Escuela Universitaria de Informática - Universidad Politécnica de Madrid (EUI-UPM)Madrid, Spain{cgallardo, pmartin, jsanchez}@eui.upm.es
6. Using Rubrics to Measure and Enhance Student Performance Sharon Karkehabadi, M.Ed. Student Learning Outcomes Specialist Spring 2013 Faculty Workshop Series Office of Institutional Research, Planning, and Assessment Northern Virginia Community College.

Web References

1. https://nwcommons.nwciowa.edu/education_masters?utm_source=nwcommons.nwciowa.edu%2Feducation_masters%2F12&utm_medium=PDF&utm_campaign=PDFCoverPages