STM JOURNALS

Journal Title
ISSN

www.stmjournals.com

E-learning on Cloud using Advanced Encryption Standard

Vaibhavi Pawar[1], Dr K. S. Thakre[2], Abhishek Pujari[3], Pranali Wagh[4], Yash Pawar[5]
[1]Student, Information Technology, SCOE, Pune
[3]Student, Information Technology, SCOE, Pune
[4]Student, Information Technology, SCOE, Pune
[5]Student, Information Technology, SCOE, Pune
[2]Professor, Information Technology, SCOE, Pune

Abstract

Various benefits of Information Technology have created different tools that help learning at any place and anytime. As the technology is changing, education system also needs to be changed for faster, comfortable and easy learning. E-learning plays an important role in establishing a good learning environment and also provides learners with different background, preferences, and locations to optimize the quality of learning through the delivery of learning material. Cloud providers have platforms for users to design, deploy and run applications located in the cloud. Using this facility, we propose an E-learning web-based system using cloud, which is specifically targeted towards engineering students and teachers, who can upload the studying material of respective course which can be of any form such as text files, videos, audios. The students can access it from any location. We also provide test assessments for students who want to get through the mock and final examinations of their curriculum. The planned e-learning system includes the fringe platform on a web server for teachers and students. The proposed system provides additional concern of security for teachers as well as students. When teacher uploads data on cloud Advanced Encryption Standard (AES) algorithm runs at the backend. Similarly, when student downloads course material, security check is done using Elliptical Curve Cryptography (ECC) algorithm.

Keywords: *E-learning, Cloud, Advanced Encryption Standard, Elliptical Curve Cryptography, K-Nearest Neighbour.*

INTRODUCTION

Information technology has made it possible to work and study from distance learning in user comfortable spaces other than traditional classrooms. The most important feature is the direct interaction between teachers and students which should be powered by information technology to make the learning process more efficient. Cloud provides built-in data processing resources, data storage, relevant internet software for remote access. Cloud services, large network access, resource pooling, rapid elasticity and calculated service are fundamental features cloud computing. E-learning is the future of education which can provide courses and various opportunities to students in traditional form of education. E-learning has an important impact on university education. It is an ever expanding and endless information field. In existing system, the method in which students learn from an instructor in a classroom is often seen, but information technology is now used to learn without actually having a

teacher directly in front of students. Different types of study material will be uploaded by teachers for students, for example, video, text document, image will help students through the curriculum. Distance learning affects higher education greatly. It is a regularly increasing the infinite and never-ending universe of knowledge. A cloud-based e-learning platform is portable and can dramatically improve investment productivity and management capacity. The data owner may want to protect his / her privacy from providers of cloud services to prevent cloud servers from damaging data privacy.

LITERATURE SURVEY

In [1] Mohsen Maroui, OnsNasfi have proposed system that offers an innovative approach for the delivery of media services that can be accessed from smart devices to share different educational materials, including text, images, and videos. Writer further discusses Pedagogical Indexing. Pedagogical indexing is done in a documentary language which allows the user to search for artifacts used in education. Author aims to suggest a model for indexing pedagogical texts to teach Arabic. The author creates a database which allows for the following applications: Adding text to the database, searching text based on problematic questions and the specifics of the Arabic language and support to select text. An application for the Arabic Language cloud-based e-learning system is also explained by the author. In [2] Haibo Yi et. al. has developed an effective Cloud Computing based learning administration system, which enables student learning and system interaction to be advanced. The learning mainframe system consisted of three platforms, that is to say IaaS, SaaS, PaaS learning platform. Software as a service, learning platform: SaaS is a licensing and distribution model for software where it is centrally managed and licensed on the basis of a subscription. Platform as a Service learning platform :PaaS supply customers the framework to create, operate and manage apps without the need to build and maintain the infrastructure related to the app's production and launch. Infrastructure as a service, learning platform: IaaS corresponds to services available online that exclude users from infrastructure information, such as physical computing, location, data partitioning, scaling, protection, etc. The, author further explains that SaaS learning software services provide a computer learning guide framework, lesson system and programme. VS 2015 Group, C-Free, Eclipse, SQL Server, Apache for computer learning offers the PaaS software framework. The IaaS learning platform offers network basis, computer infrastructure, programming learning storage infrastructure. In [3] Seppo J. Sirkemaa has done survey on E-learning and Modern learning environments. The e-learning and mlearning debate illustrates the skills needed on the new labor market and underlines the value of technology for modern society. The author describes the e-learning ability. Generally speaking, e-learning is education's future. Elearning makes possible to study regardless of space and time because "traditional" education is linked to classrooms. It can also create new groups of students who do not have other kinds of education available. Author explains Mobility of Education. When our lifestyle is mobile and widely utilizes information technology, solutions that require distance study are inevitable. Ideally, learning at the individual student's own rate could be possible whenever the student is sufficient. Mobility usually refers to a user who carries a mobile terminal device that is wireless to the network. Mobility is divided into three principal classes. Mobility of terminals: terminal mobility refers to technologies and devices that allow mobile access from everywhere. Personal mobility: personal mobility applies to users having to connect during their journeys-they should be able to access telecommunications from anywhere. Personal mobility also means that mobile users must be able to contact wherever they may be. Mobility of service: mobility of service refers to services accessed via a mobile terminal. The Author also explains the difficulties faced with elearning. When students do not know the technology, the atmosphere can be controlled overwhelmingly. There are many settings, for example, that have to be configured to connect to a network from a mobile terminal. Teachers must also master technology and understand the network limitations. The role of students and teachers in modern learning environments is therefore evolving. In [4] Lillian-Yee-Kiaw Wang et al The author has done a study to forecast how cloud e-learning applications will proceed. In an ever-changing digital era, conventional e-learning methods have become inadequate, particularly in higher education,

to meet the requirements of upgraded learning. E-learning can be turned into a flexible, shared, content reusable and scalable learning methodology by cloud computing. While literature-wide Cloud e-learning architecture has been suggested, limited research to investigate usability factors that predict consistency in the use of cloud e-learning applications has been performed. For factor analysis, five usability factors have been identified, namely Computer Self Efficiency, Enjoyment PEU and UP. Author explains e-learning data collection. This research validated the proposed theoretical model to predict how information and computer science students in a private university in Malaysia will continue using the cloud e-learning program. In [5] Teodor B. Iliev et al have proposed an efficient, scalable, sustainable e-learning platform that reduces overall ownership costs. The components suggested are the front portal for web-host teachers and students, and the load balancing and open-source relation data support portal service. Different resources are provided by affordable hardware and open source software like KVM, Docker and Puppet. This system is designed to provide infrastructure based on modern methods and instruments. During our operating system Linux and Basics of Programming education, writers must find pragmatic solutions for a growing number of students due to the numerous infrastructural challenges that face. The paper focuses on two main architecture sub-sets–front and back. Two portals teacher and student are the front-end of the network. Each platform will be dedicated to the specific tasks and needs of predefined groups of people. Teacher Portal's main objective is to provide the teachers and their assistants with easy-to-use and administrative functions. Some features include tests and course work, a number of tasks and lock / unlock courses functionality. The main objective of the Student Portal is to allow students to review grades, scores from assignments and launch workshops. High Availability Proxy i.e. HA Proxy was used for Load Balancing and Failover. It can balance private cloud with your own public cloud provider. The main / master data base Back-end designs rely on the HA Proxy software, the open source load balancing and proxy solution for Linux or Unix operating systems. The software is open source. It is commonly used to enhance the performance and reliability of a service through the sharing of work load over several servers. My SQL or MariaDB's popular drop-in substitute. Two independent virtual machines will have the Master DB installed on minimum 2 CPUs and 4 GB RAM. Master DB shall contain information concerning student ID, first and last name, the present term, courses assigned by students in their curriculum, as well as the score points of their exercises and the appropriate course grade. In [6] Qasim Alajmi et al have conducted a survey on the effectiveness of the classic E-Learning Model in the cloud. Actor proposes that cloud computing be adopted as a means of saving / saving costs and enhancing student-educator interactions. Cloud-based training has become increasingly popular with experts arguing that the conventional e-learning model is being replaced / improved. The study uses a quantitative technique in which two institutions were involved. The respondents answered and submitted an assessment questionnaire’s. Based on the results of the report, it was clear that the cloud-based e-learning model would solve conventional e-learning problems effectively. In the e-learning platforms, it is necessary to improve the protection of the content. Authors have had to formulate research questions so that This paper's main objective, namely the cloud-based electrical learning model, can be accomplished via the conventional E-learning model. A comparison of the traditional e-learning model and the cloud-based model was made by the author based on factors such as content safety, information-sharing, and upgrade.

SYSTEM ARCHITECTURE

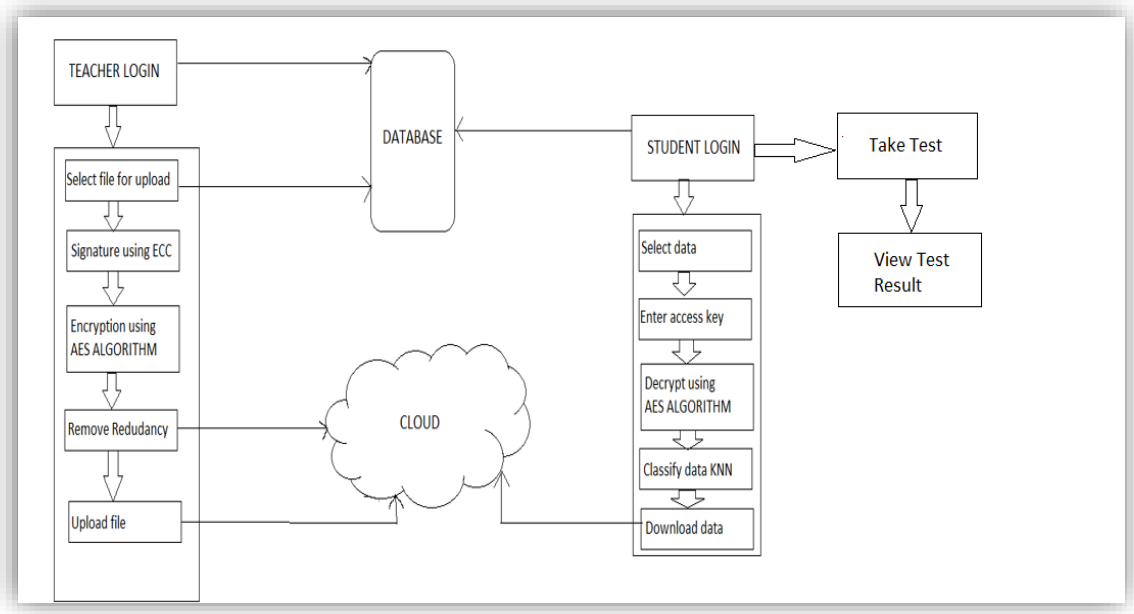

Fig 1: System Architecture

As shown in Fig 1, the system consists of two entities who are going to interact with system first is the teacher and second is the student. Each teacher and student will have to first register to the system. Once registration is done the teacher as well as the student will enter the system by giving valid credentials. The teacher can upload the chosen material, every material which is to be uploaded on the cloud will be assigned a unique key so as to avoid redundant material on cloud, this unique key will be generated by using the Elliptic Curve Cryptography (ECC) Algorithm. The next step will be securing the data i.e. Data was encrypted by using the Advanced Encryption Standard (AES) algorithm and then uploaded further to the cloud. Simultaneously, the student can login into the system once registered successfully. Student can either access the uploaded data or might the take test assessment. Student can select their respective branch and the can choose the data or material they want to access. If the student wants to download the material, firstly he/she has to enter the unique key which has been sent to their respective mails. Upon entering the valid key they can download the material. The data is decrypted using the same algorithm which is used for encryption. We are also implementing the classification algorithm K-Nearest Neighbour (KNN), for classification of data. The proposed system is implemented using three algorithms:

1.AES Algorithm (Advanced Encryption Standard): The AES is a 128-bit block-length cipher. AES makes different lengths of key: 128,192,256 bits. We have AES with a 128-bit block length. The encryption key is composed of ten rounds of 128bit keys encoding. The 4x4 byte matrix made of the 128-bit input block is called the state array.
Pseudo Code for Advanced Encryption Standard following are the steps involved:

1. Add Round Key(S,&w[0])
2. for j=1 step 1 to 9
3. sub Bytes(S)
4. shift Rows(S)
5. mix Columns (S, &w[i*4])
6. end for
7. sub Bytes(S)
8. shift Rows(S)
9. Add Round Key(S, &w[40])

2.ECC Algorithm (Elliptical Curve Cryptography): ECC is used to establish a key (digital signature) to encrypt a file to the cloud. Further bandwidth and additional process power are required for a longer key. The ECC algorithm enables small key size, while providing a higher safety level.

Pseudo Code for Elliptical Curve Cryptography the following steps are taken to sign a message m by the sender:

1. Step 1. It calculates a hash function for cryptography.
2. Step 2. A random integer of [1,n-1] is then chosen by sender
3. Step 3. Pair (r,s) computation.
4. Step 4. r= x1 (mod n) where (x1, y1) =k*G.
5. Step 5. s= k-1(e+ dA*r).
6. Step 6. This pair determines the signature (r, s).
7. Step 7. This signature is forwarded to the receiver.
8. Conditions: K = key(fixed),(r, s)= key pair signature, x1=fixed, y1=Fixed).

3.KNN Algorithm (K- Nearest Neighbor): The KNN algorithm is a guided algorithm for machine learning that solves problems in classification and regression. KNN algorithm assumes that similar things are nearby. KNN is used in the classification of student test results.

Pseudo Code for K-Nearest Neighbour Algorithm: Following steps are involved:

1. Calculate "d(x, xi)" i=1, 2,.., n; where d indicates the Euclidean point distance.
2. Distance= value(x2−x1)2+(y2-y1)2
3. Euclidean Dispose in non-decreasing order of the calculated n Euclidean distances.
4. Let k be a +ve integer, from this sorted list, take the first k distance.
5. Consider those k-points that suit these k-distances.
6. Let ki denote the number of points in the k class, i.e. k= 0 7. K When you put ki > kj > I > j then you put x to I.

Terms: n=training sample, $x_{i=}$ training data point, k=user defined (K value we can make boundaries of each class).

UML DESIGN

Class diagram: Class chart offers a class static view. It describes the type and relationships of objects that participate in the system.

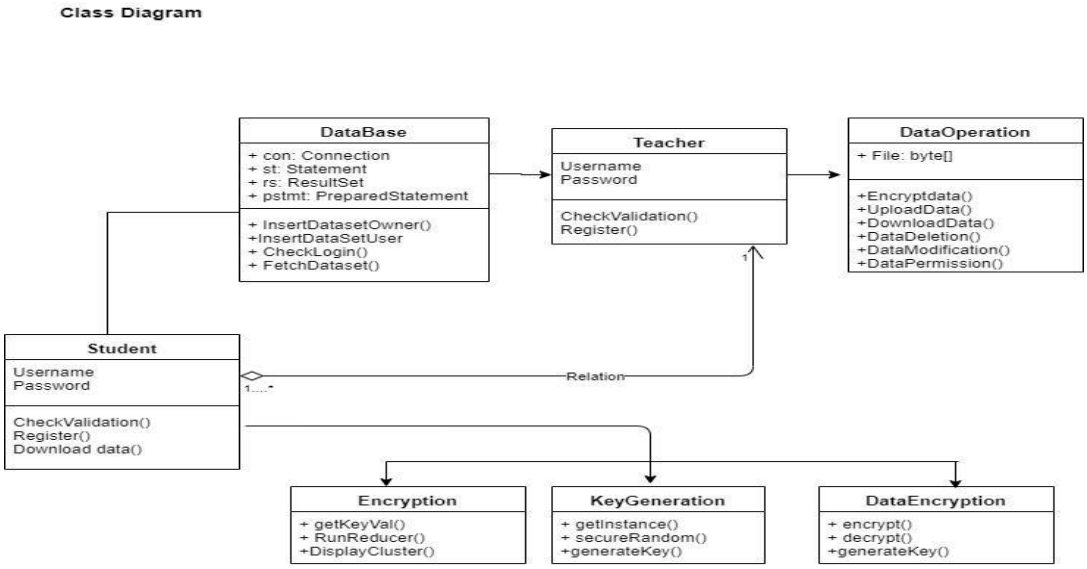

Fig 2: Class Diagram

Use case Diagram: Behavioural UML is a case diagram for use. Use a case diagram model to use actors and cases for a system functionality.

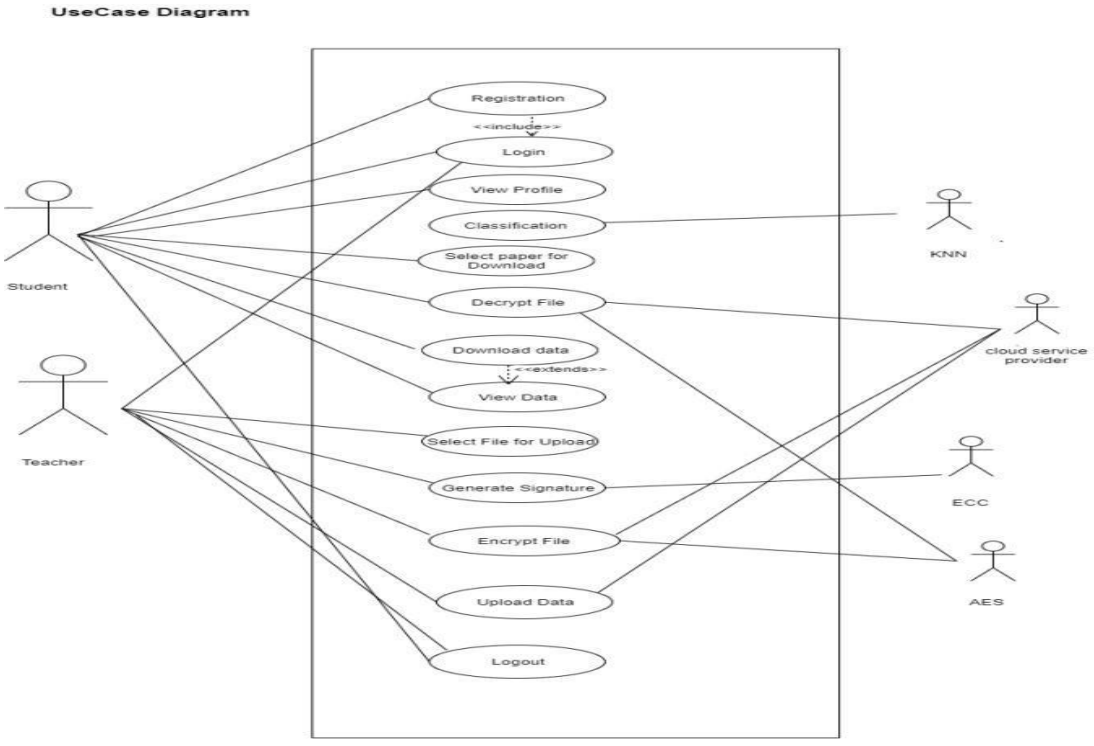

Fig 3: Use case Diagram

RESULT ANALYSIS

This challenge becomes very real in our country and with the implementation of this program for higher education we hope to attract new students who want to develop their skills and increasing their own knowledge. This system is also valuable for appealing rural student to enhance their knowledge, to contribute their own ability to build a nation. In addition to that we wish to give university lecturers and students the opportunity to develop a close relationship with modern technology and new knowledge. This e-learning program is a perfect opportunity for developing countries that are seeking to contribute to the world economy and give everyone an opportunity to learn and adapt. These developing countries may not yet be ready to overcome certain obstacles, but they are currently in progress. We also contribute our efforts towards quality education that helps to produce quality students that they act as powerful weapon to develop our nation.

Dataset Differentiation

Data that is uploaded by respected instructors on cloud is collected from various websites available on internet such as Java point, Tutorial Point, Web3School.

Technologies Used

JSP: JSP technology, like Servlet technology, is used to create a web application. It can be considered as a server extension because it offers more features than servlets such as language of speech, JSTL etc. A jsp page is made up of JSP and HTML tags. The JSP pages are easier to keep than servlet because design and production are different.

Servlet: Server technology (lives on the server side and produces dynamic web pages) is used to create a Web application. Because of the java language, servlet technology is robust and scalable. CGI (Common Gateway Interface) was popular as a server programming language before Servlet.

JAVA: Java is a commonly used class-oriented language designed especially for as few implementation dependencies as possible, as it is a computer programming language. The purpose is to allow app developers to "write once, run anywhere" (WORA), allowing compiled Java code to run in all platforms that support Java without recompiling.

Hardware Software Requirements

Hardware Requirement

1. Processor: Pentium –IV
2. Hard Disk: 20GB
3. RAM: 2GB(Min)

Software Requirement

1. Platform: JAVA
2. Technology: JDK 1.8
3. Database: MySQL
4. IDE: Eclipse
5. Server: Apache Tomcat 7 or 6

Frontend Design

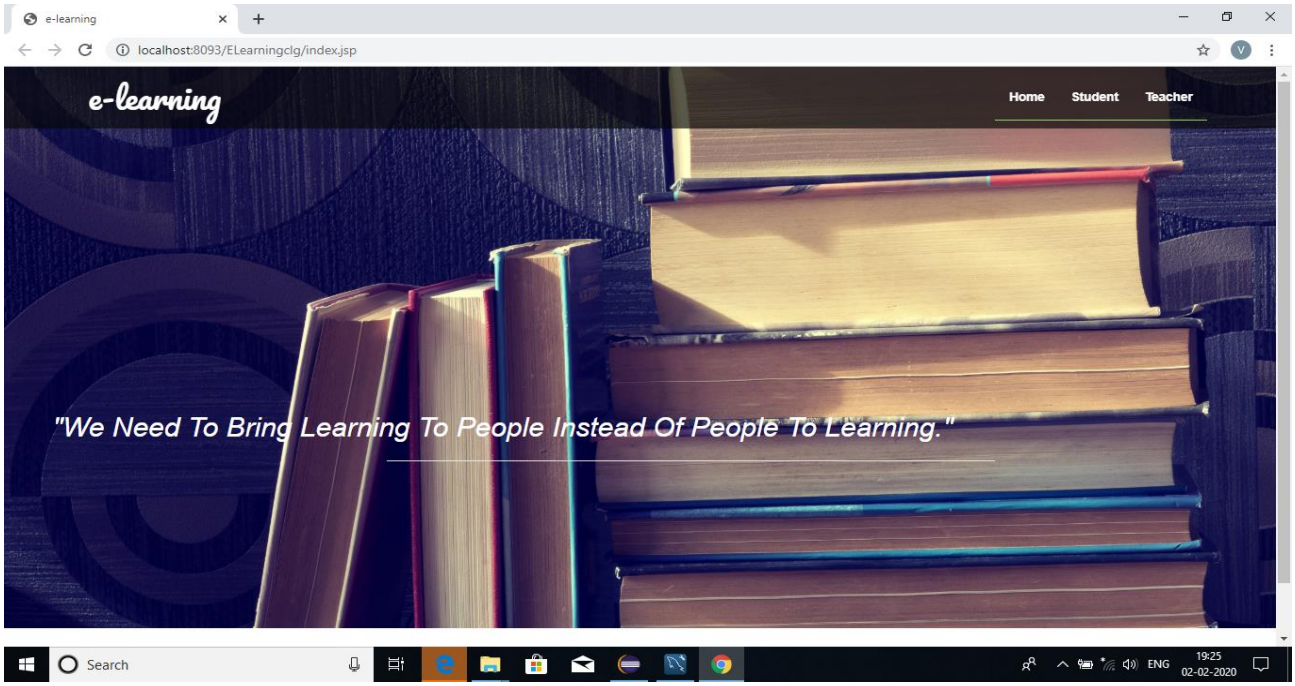

Fig 4: Homepage

The first view of the proposed system is the home page as shown in Fig4, where many tabs have been provided for performing various operations.

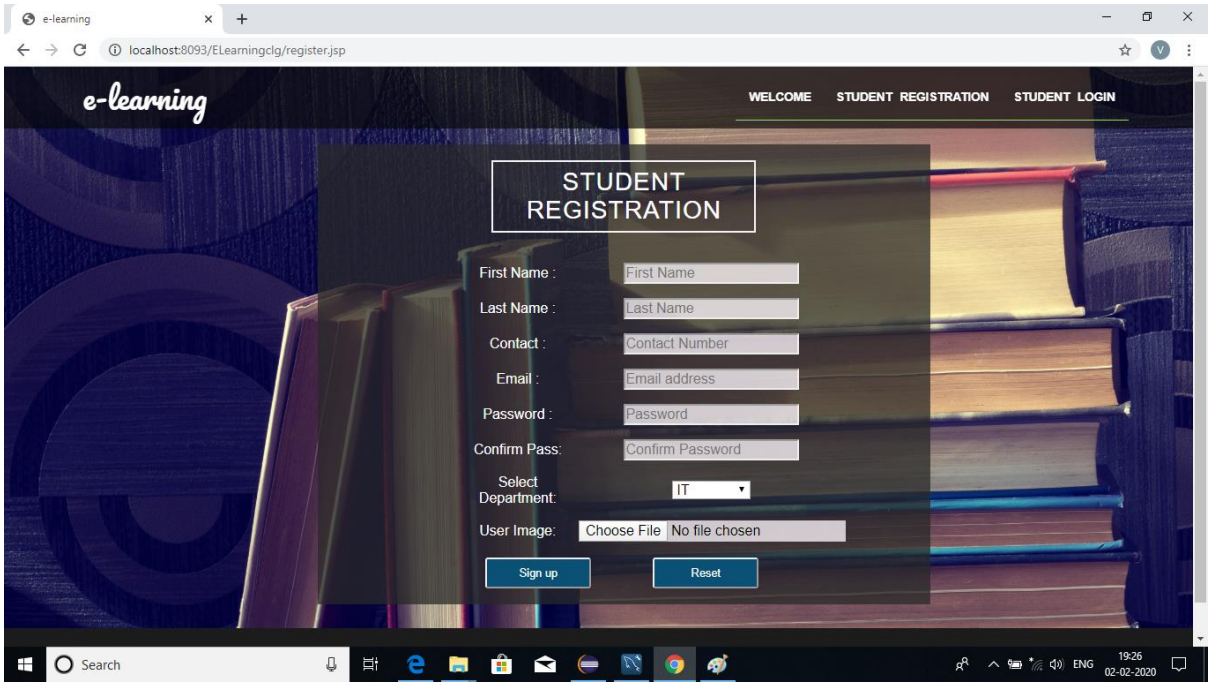

Fig 5: Student Registration Page

As shown in Fig5, on selecting the student tab two tabs are displayed; student registration and student login, if the student has already registered, he/she can directly select the login tab and can log into the system.

.

Fig 6: Student Functionalities

Once the student has logged into the system as shown in Fig 6, student can perform various operations such as create group, view group, select group and logout depending upon his/her requirements.

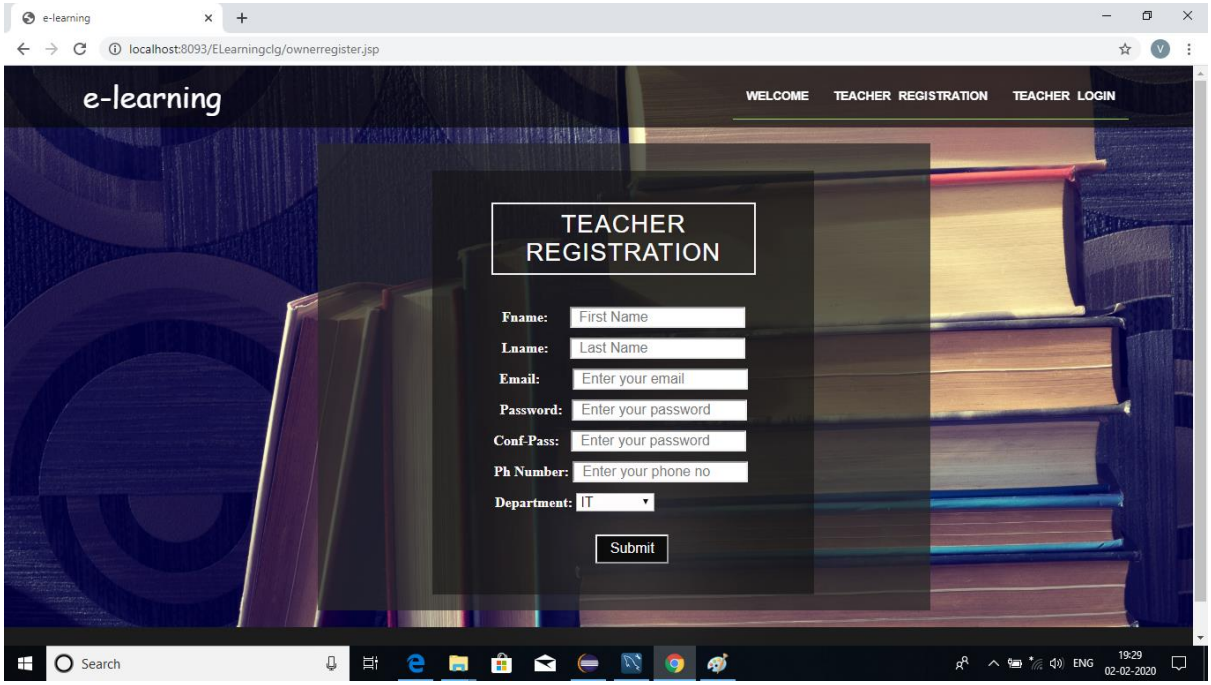

Fig 7: Teacher Registration Page

As shown in Fig 7, on selecting the teacher tab two tabs are displayed; teacher registration and teacher login, if the teacher has already registered, he/she can directly select the login tab and can log into the system.

Fig 8: Teacher Functionalities

Once the teacher has logged into the system as shown in Fig 8, teacher can perform various operations such as view group, upload data, user details and logout depending upon his/her requirements.

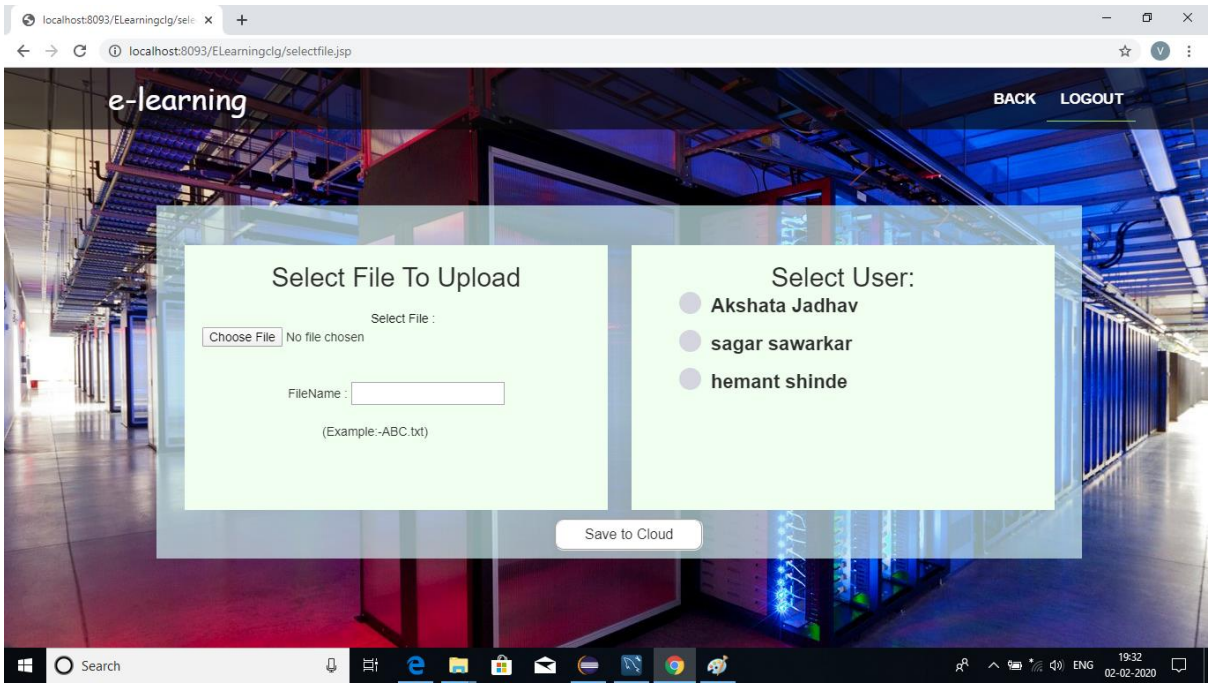

Fig 9: Upload data Functionality

On selecting the upload data functionality, teacher will be redirected to page as shown in Fig 9.Teacher can browse data or files for uploading on the cloud, as well as teacher can also provide an alternate file name .Once the file has been chosen teacher can select number of students to whom the file is to be send**.**

CONCLUSION

We have endeavoured to offer a new and innovative solution. For media services accessible from the cloud based smart devices with a completely integrated service environment that accesses cloud files and makes good use of them. We have proposed the system from security perspective by implementing Advanced Encryption Standard (AES) while uploading the data onto the cloud, Elliptical Curve Cryptography (ECC) while downloading the data from cloud and K- Nearest Neighbour (KNN) for classifying the files having different extensions. Amazon Web Service (Simple Storage Service) S3 cloud is being used to for data storage.

RFERENCES

[1] Mohsen Maraoui, Ons Nasfi **"**Smart Tools for Cloud E-learning System", International Conference on Engineering and Technology, ICET2017.

[2] Haibo Yi, Zhe Nie, "Implementation of Learning Management System Based on Cloud Computing", International Conference on Information Science and Control Engineering, vol. 2, pp. 478-481, 2017.

[3] Seppo J. Sirkemaa, "Analysing e-Learning and Modern Learning Environments", International Journal of Information and Education Technology, Vol. 4, No. 2, April 2014.

[4] Lillian-Yee-Kiaw Wang, Sook-Ling Lew, Siong-Hoe Lau, Meng-Chew Leow "Usability factors predicting continuance of intention to use cloud e-learning application", ScienceDirect2019.

[5] Teodor B. Iliev "Technology E-Learning Environment for the Hybrid Cloud", IEEE2017.

[6] Qasim Alajmi, Ali Sadiq, Adzhar Kamaludin, Mohammed A. Al-Sharafi "E-Learning Models: The Effectiveness of the Cloud-Based E-Learning Model over the Traditional E-Learning Model", 8th International Conference on Information Technology (ICIT)2017.