PROJECT OVERVIEW

Learning is based on information or knowledge and communication technologies. The E-learning is the latest technology of learning which is getting much more popular in academicians. E-learning technology has multiple data formats which make fluent and flexible learning to learner. Today's word there is no end for learning either it may for academicians or professionals at this situation e-learning may play effective role for just in time learning.

This E-learning platform comes up with huge data as student records, learning courses record, course materials. Course material are having in the form of textual data like books etc and in the form of visualizations like mp4 videos. To make more convenient to e learning platform provides virtual classroom to each individual learner at his own place, on his own convenient time. E-learning can able to reduce learning costs, motivate students, improve flexibility of course delivery, it expands the capabilities of the business, it make learning available anytime, anywhere.

INTRODUCTION

E-Learning exploits interactive technologies and communication systems to improve the learning experience. It has the potential to transform the way we teach and learn across the board. It can raise standards, and widen participation in lifelong learning. It cannot replace teachers and lecturers, but alongside existing methods it can enhance the quality and reach of their teaching, and reduce the time spent on administration. It can enable every learner to achieve his or her potential, and help to build an educational workforce empowered to change. It makes possible a truly ambitious education system for a future learning society

2.1 Advantages of e- learning

1. Online Learning Accommodates Everyone's Needs

The online method of learning is best suited for everyone. This digital revolution has led to remarkable changes in how the content is accessed, consumed, discussed, and shared. Online educational courses can be taken up by office goers and housewives too, at the time that suits them. Depending on their availability and comfort, many people choose to learn at weekends or evenings.

2. Lectures Can Be Taken Any Number Of Times

Unlike classroom teaching, with online learning you can access the content an unlimited number of times. This is especially required at the time of revision when preparing for an exam. In traditional form of learning, if you cannot attend the lecture, then you have to prepare for that topic on your own; in eLearning, you can attend the lectures whenever you want with ease.

3. Offers Access to Updated Content

A prime benefit of learning online is that it makes sure that you are in synchronization with modern learners. This enables the learner to access updated content whenever they want it.

4. Quick Delivery of Lessons

eLearning is a way to provide quick delivery of lessons. As compared to traditional classroom teaching method, this mode has relatively quick delivery cycles. This indicates that the time required to learn is reduced to 25%-60% of what is required in traditional learning. There are some of the reasons why the learning time is reduced by eLearning:

- Lessons starts quickly and also wrapped up in a single learning session. This enables training programs to easily roll out within a few weeks, or sometime even days.
- Learners can define their own speed of learning instead of following the speed of the whole group.
- Saves time as a student does not need to travel to the training venue. You can learn at the comfort of your own place.
- Students can choose to study specific and relevant areas of the learning material without focusing on each and every area. For example, they can skip certain areas they do not want to learn.

5. Scalability

E-Learning helps in creating and communicating new training, policies, concepts, and ideas. Whether it is for formal education or entertainment, eLearning is very quick way of learning!

6. Consistency

E-Learning enables educators to get a higher degree of coverage to communicate the message in a consistent way for their target audience. This ensures that all learners receive the same type of training with this learning mode.

7. Reduced Costs

E-Learning is cost effective as compared to traditional forms of learning. The reason for this price reduction is because learning through this mode happens quickly and easily. A lot of training time is reduced with respect to trainers, travel, course materials, and accommodation.

This cost effectiveness also helps in enhancing the profitability of an organization. Also, when you are studying at your own place, you are relieved from paying for travel expenses (e.g. accommodation) when training happens in another city/state and/or external learning materials.

8. Effectiveness

E-Learning has a positive influence on an organization’s profitability. It makes it easy to grasp the content and digest it:

- It results in improved scores on certifications, tests, or other types of evaluation.
- Higher number of students who achieve ‘pass’ or mastery’ level.
- Enhanced ability to learn and implement the new processes or knowledge at the workplace.
- Help in retaining information for a longer time.

9. Less Impact on Environment

As eLearning is a paperless way of learning, it protects the environment to a lot of extent. As per a study done on eLearning courses, it has been found that distance-based learning programs consumed around 90% less power and generated 85% less amount of CO2 emissions as compared to traditional campus-based educational courses. With eLearning, there is no need to cut trees for obtaining paper. Thus, eLearning is a highly eco-friendly way of learning.

2.2 Existing approach

In this E-learning platform comes up with huge data as student records, learning courses record, course materials, and in the form of visualizations like mp4 videos. To make more convenient to E-learning platform provides virtual classroom to each individual learner at his own place, on his own convenient time. E-learning can able to reduce learning costs, motivate students, improve flexibility of course delivery, it expands the capabilities of the business, and it makes learning available anytime, anywhere. So these data is required security for privacy maintaining purpose so that we use two approaches

- SHA Algorithm
- Data mining methods

2.2.1 SHA Algorithm

In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

Since 2005 SHA-1 has not been considered secure against well-funded opponents, and since 2010 many organizations have recommended its replacement by SHA-2 or SHA-3. Microsoft, Google, Apple and Mozilla have all announced that their respective browsers will stop accepting SHA-1 SSL certificates by 2017. In 2017 CWI Amsterdam and Google announced they had performed a collision attack against SHA-1, publishing two dissimilar PDF files which produced the same SHA-1 hash.

SHA-1 produces a message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD2, MD4 and MD5 message digest algorithms, but generates a larger hash value (160 bits vs. 128 bits). SHA-1 was developed as part of the U.S. Government's Capstone project. The original specification of the algorithm was published in 1993 under the title Secure Hash Standard, FIPS PUB 180, by U.S. government standards agency NIST (National Institute of Standards and Technology).This version is now often named SHA-0. It was withdrawn by the NSA shortly after publication and was superseded by the revised version, published in 1995 in FIPS PUB 180-1 and commonly designated SHA-1. SHA-1 differs from SHA-0 only by a single bitwise rotation in the message schedule of its compression function. According to the NSA, this was done to correct a flaw in the original algorithm which reduced its cryptographic security, but they did not provide any further explanation.[citation needed] Publicly available techniques did indeed demonstrate a compromise of SHA-0, in 2004, before SHA-1 in 2017.

Applications

- **Cryptography**

Further information: Cryptographic hash function and Applications
SHA-1 forms part of several widely used security applications and protocols, including TLS and SSL, PGP, SSH, S/MIME, and IPsec. Those applications can also use MD5; both MD5 and SHA-1 are descended from MD4.

SHA-1 and SHA-2 are the hash algorithms required by law for use in certain U.S. government applications, including use within other cryptographic algorithms and protocols, for the protection of sensitive unclassified information. FIPS PUB 180-1 also encouraged adoption and use of SHA-1 by private and commercial organizations. SHA-1 is being retired from most government uses; the U.S. National Institute of Standards and Technology said, "Federal agencies should stop using SHA-1 for...applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010" (emphasis in original), though that was later relaxed to allow SHA-1 to be used for verifying old digital signatures and time stamps.

A prime motivation for the publication of the Secure Hash Algorithm was the Digital Signature Standard, in which it is incorporated. The SHA hash functions have been used for the basis of the SHACAL block ciphers.

- **Data integrity**

Revision control systems such as Git, Mercurial, and Monotone use SHA-1 not for security but to identify revisions and to ensure that the data has not changed due to accidental corruption. Linus Torvalds said about Git:

If you have disk corruption, if you have DRAM corruption, if you have any kind of problems at all, Git will notice them. It's not a question of if, it's a guarantee. You can have people who try to be malicious. They won't succeed. ... Nobody has been able to break SHA-1, but the point is the SHA-1, as far as Git is concerned, isn't even a security feature. It's purely a consistency check. The security parts are elsewhere, so a lot of people assume that since Git uses SHA-1 and SHA-1 is used for cryptographically secure stuff, they think that, Okay, it's a huge security feature. It has nothing at all to do with security; it's just the best hash you can get.
I guarantee you, if you put your data in Git, you can trust the fact that five years later, after it was converted from your hard disk to DVD to whatever new technology and you copied it along, five years later you can verify that the data you get back out is the exact same data you put in.
One of the reasons I care is for the kernel, we had a break in on one of the Bit Keeper sites where people tried to corrupt the kernel source code repositories. However Git does not require the second pre image resistance of SHA-1 as a security feature, since it will always prefer to keep the earliest version of an object in case of collision, preventing an attacker from surreptitiously overwriting files.

2.2.2 Data mining approach

For data mining methods we briefly discuss in chapter no 4.