Effective Online Teaching Learning during COVID-19 Pandemic

Purna Chandra Sethi¹,³, Prafulla Kumar Behera²

¹ Department of Computer Science, Rama Devi Women’s University, Bhubaneswar, Odisha, India, 751022
² Department of Computer Science and Applications, Utkal University, Bhubaneswar, Odisha, India, 751004
³ pursa.sethi@gmail.com

Abstract. The COVID-19 pandemic has resulted in a dramatic change in our day to day life. It affected not only the normal working of many organizations but also the traditional classroom teaching and learning methodologies. Since everyone has to maintain social distancing to follow COVID-19 guidelines, work from home is being preferred as the best alternative as a preventive measure from spreading the pandemic. In its severe impact, schools, colleges, and universities were shut down, pushing nearly 1.2 billion students out of the classroom. As a result, the education system has to suddenly adapt to a distinctive online-based e-learning approach over digital platforms. Research tells that online learning motivated more towards the retention of online resources with less cost in terms of money and time. But, it has also brought many challenges along the way. In this research work, we focus on some of the major challenges such as information security and network bandwidth problem during online teaching. The related security measures being adopted in our research work to secure personal information during any online teaching and learning process. We also focus on some basic learning models for provisioning effective online-based teaching and learning.

Keyword: E-learning, Information Security, Elgamal Cryptography Algorithm, Elgamal Digital Signature, Network failure, Auto-Resolution Adaptation (ARA).

1. Introduction

COVID-19 pandemic is a respiratory based infectious disease caused by SARS-CoV-2 (Severe Acute Respiratory Syndrome Coronavirus-2) virus, first found on 17 November 2019 in Wuhan, Hubei, China, and spread across 188 countries over the globe. The official name was given as COVID-19 (previously named as “2019 novel corona virus”) due to the virus which is responsible for the disease [1]. According to CSSE (Centre for Systems Science and Engineering), Johns Hopkins University live report dated 5th September 2020, 26.66 million COVID positive cases are recorded across the globe out of which 17.95 million recovered and 8.76 lakh are deceased and in India out of total 40.24 lakh positive cases, 21.81 lakh are recovered and 69561 are deceased [2].

COVID-19 severely affected all most all sectors starting from the financial market to education. Due to lockdown and shutdown, the financial crisis arises not only in private sectors but also in public sectors. The financial market is primarily controlled in terms of Institutional investments, Banking and Capital Markets, Geo-economics, International Security, Oil and Gas, Media, Entertainment, Culture and Private Investments, Global Governance, Global health, Public finance and social protection,
Future of economic progress, Education, etc. The COVID-19’s workforce impact is visible in the field of Corporate Governance, Agile Governance, Inclusive design, Workforce and employment, Public finance and social protection, Future of economic progress, Education and skills, Future of health and healthcare, Defining racism, Retail, Consumer, Goods and Lifestyle, Advanced manufacturing and production, Aviation, Travel and tourism, Supply chain and transport, etc. In this paper, we will primarily focus on the impact of COVID-19 in the field of education. We also focus on the motivation from the traditional classroom teaching to online methods along with the problem associated with the online teaching methodologies. We have presented our research work to overcome some major problem that occurs during online teachings such as security of information and network bandwidth management in terms of a compromised approach to provide better end-to-end service.

The remaining part of the research paper is organized as follows: Section 2 deals with the literature overview, Section 3 focuses on motivation, and Section 4 shows our proposed method for achieving end-to-end information security during teaching over online mode. It also presents our proposed method for network traffic management using Auto-Resolution Adaptation (ARA) by compromising with the reduced video quality. Section 5 will provide the performance of the proposed model Section 6 shows the conclusion and future work.

### 2. Literature Overview

Education and skills are considered the building block of a growing society. According to the world economic forum, new education and skills depend on different parameters such as Innovation in teaching, digital knowledge and relevant education, the state-of-the-art in curricula design, basic and quality education, motivation for learning and research, etc. Educational innovation starts with social innovation to entrepreneurship and the industrial revolution. It is also affected by virtual and augmented reality, development of finance, behavioral science, aging, and the future of computing. Virtual and augmented reality leads to a conceptual and simulated environment for a real understanding of facts in education. Due to social innovations and the fourth industrial revolution, education innovations are reached a greater extent.

Due to the Covid-19 pandemic, the offline mode of classroom teaching is completely affected. Hence, everyone is forced to adopt the online mode of teaching and learning platform. This online mode of teaching leads to many challenges because of the technical aspects as well as the physical aspects. In [4] the authors provided a case study about students’ attitudes regarding online learning. The researcher considered 126 samples of undergraduate students (84 female and 42 male) for the survey and collected various information that deals with different economic, technical, and physical aspects. Out of the 126 students, 65 (51.6%) students agreed that the signal strength problem interrupts the teaching during online classes. In [5], the authors had considered five distinct questions whose analysis is the basis of the whole research paper. The paper primarily focused on the adoption of student-centric online courses using effective ICT tools. The paper finally raised various problems that arise during the online teaching at both students as well as teachers’ ends. In [6], the author has performed the SWOC (Strengths, Weaknesses, Opportunities, and Challenges) analysis of e-learning mode given student, faculty as well as institutional aspects. In [7], the authors stated that the Covid-19 pandemic has opened a new face and trend in education. In a survey of 200 persons within the age range between 18 and 26, 74% likes the online mode of teaching due to the flexibility in timing and minimum wastage of transition time from one place to the other.

During the online mode of teaching, network traffic and information security play a vital role in the effectiveness of the whole process. To deal with the network traffic management, in [8, 9] the authors proposed a webpage rank based network traffic management scheme for dynamic bandwidth assignment within a network. To deal with the information security aspects, in [10, 11] the authors proposed a modified algorithm so that without prior knowledge, identifying the actual message will be nearly impossible. Here, we have proposed a hybrid model using a mathematical model that will not only provide the security to information but also manage the online mode of teaching with a compromise in terms of degradation in the quality of the video.
3. Motivation
In the current scenario, who has more information is considered to be more powerful and rich. Many companies providing a free platform to attract more user accessibility so that they can acquire personal information and can make a business out of the collected information. Apart from the issues generated from IPR, their many other related issues arise such as information security, network bandwidth, etc. During online platform access such as mobile apps, we are bound to accept all the terms and conditions without which they won’t provide the platform access. This forced agreement to the terms and conditions of access to personal information also lead to the violation of Intellectual Property Rights (IPR). To control the security issues, we focused on three major aspects such as data confidentiality in terms of cryptography algorithm implementation, data integrity in terms of digital signature, and availability of information to authorized users to achieve information security. The network traffic management will be done using an intelligent system that will adjust the resolution of the video to the available bandwidth.

4. The Proposed Model
The proposed model for effective online teaching in a secured manner is depicted in figure-1.

![Proposed Model for Effective Online Teaching](attachment:image)

Information Security deals with the implementation of security techniques at the application layer of the TCP/IP model [3]. Information security stands on three fundamental pillars such as Confidentiality, Integrity, and Availability. Confidentiality deals with the protection of resources from unauthorized access. Integrity deals with the protection of data from unauthorized change to ensure the reliability and correctness of the information. Availability represents that only authorized users have access to the resources to achieve information security. Confidentiality is achieved using an access control mechanism. We have achieved this in terms of CHAP (Challenge Handshake Authentication Protocol). Integrity is achieved by restricting the unauthorized alteration of information in terms of cryptography algorithm implementation. We have used the Elgamal Cryptosystem for achieving the integrity among the users during communication. Finally, the availability property is achieved in terms of Elgamal digital signature algorithm implementation to verify the authentication of the sender. We have applied the end-to-end encryption technique so that the information attack can be minimized and even if an attacker gets the ciphertext, it can’t easily decrypt the data to get the actual information. The digital signature algorithm implementation will provide confidentiality that the information is sent by an authentic sender only.
4.1. Confidentiality
Confidentiality is the first pillar of information security that deals with protecting the information from unauthorized user access. This is defined in terms of CHAP [12]. The CHAP is a 3-way handshaking point-to-point protocol that performs a periodic verification. It is used for authentication between the sender and the receiver. The 3-way handshaking is achieved in three steps such as challenge, response, and accept/reject. The whole process of CHAP can be represented as given in figure-3.

The steps of CHAP can be represented as:
1. Challenge: The system sends the user a challenge packet containing a challenge value, usually consisting of a few bytes of data.
2. The user applies a predefined function that takes the challenge value and the user’s password and creates a result. The user sends the result in the response packet to the system.
3. The server does the same in the reverse direction and finally accepts or rejects the activities.

This 3-way handshaking protocol provided confidentiality among users during communication.

4.2. Integrity
Integrity is achieved using the Elgamal Cryptography algorithm [13]. Elgamal Cryptography algorithm is not only a public key cryptography algorithm but also a digital signature algorithm for verifying the user’s authenticity. It is based on the difficulty of computing the discrete logarithm in the finite filed. The algorithm consists of three steps such as:
- Key generation
- Encryption
- Decryption

The whole process of the Elgamal cryptography algorithm is depicted in figure-4.
4.2.1. Key Generation

The Key generation involves the following steps:

Step 1: Select a large prime number \( p \).

Step 2: Select \( d \) as the private key to be a member of the group \( G = \langle \mathbb{Z}_p^*, x \rangle \) where \( 1 \leq d \leq p - 2 \).

Step 3: Select \( e_1 \) to be a primitive root in the group in the group \( G = \langle \mathbb{Z}_p^*, x \rangle \).

Step 4: Find \( e_2 = e_1^d \mod p \).

Step 5: Set the public key of Bob as \( (e_1, e_2, p) \) and send it to Alice.

4.2.2. Encryption

Anyone can send a message \( (P) \) to Bob using his public key. If the fast exponential algorithm is used, encryption in the Elgamal cryptography algorithm can be done in polynomial time complexity. The encryption algorithm involves the following steps:

Step 1: Select a random number \( r \) in the group \( G = \langle \mathbb{Z}_p^*, x \rangle \).

Step 2: Calculate \( C_1 \leftarrow e_1^r \mod p \)

\( C_2 \leftarrow (e_2^r \times P) \mod p \)

Step 3: Send \( (C_1, C_2) \) as the resultant cipher text to Bob.

4.2.3. Decryption

Bob will use the decryption algorithm to get the message from the cipher text \( (C_1, C_2) \). The decryption algorithm involves the following steps:

Step 1: Find the value for the plain text \( (P) \) from the received cipher text \( (C_1, C_2) \) as:

\[
P \leftarrow (C_2 (C_1^d)^{-1}) \mod p
\]

Step 2: Return \( P \)

- **Proof of Elagamal Cryptography Algorithm**

This can be done using the decryption function. The Elgaml decryption expression \( "C_2 (C_1^d)^{-1}" \) can be verified to get the plain text \( (P) \). This can be done as:

\[
(C_2 (C_1^d)^{-1}) \mod p = ((e_2^r \times P) \times (e_1^{-d} \times e_1^{-d} \mod p)
\]

\[
= ((e_1^{-d} \times P) \times (e_1^{-d} \times e_1^{-d}) \mod p)
\]

\[
= P
\]

4.3. Availability

Availability denotes that the available information can only be accessible by the intended recipient. This is done in terms of Elgaml digital signature [13]. The block diagram of Elgaml digital signature is depicted in figure-5.
Fig-5: Elgamal Digital Signature

The digital signature has two phases such as signing and verification. The digital signature also uses the public and private keys generated at the key generation phase of the Elgamal cryptography algorithm. Later, the signing operation is performed at the sender end and the verifying operation is performed at the receiver end for the authentication of the sender.

4.3.1. The Signing Phase
The signing process by Alice involves the following steps:
- Step 1: Choose a Secret random number \( r \) (which needs to be different for each message)
- Step 2: Calculate the first signature \( S_1 = e^1 r \mod p \)
- Step 3: Calculate the second signature \( S_2 = (M - d \times S_1) \times r^{-1} \mod (p - 1) \)
  Where, \( r^{-1} \) is the multiplicative inverse of \( r \mod p \).
- Step 4: Alice sends \( M, S_1 \) and \( S_2 \) to Bob.

4.3.2. The Verifying Phase
The verifying process by Bob involves the following steps:
- Step 1: If \( 0 < S_1 < p \) and \( 0 < S_2 < p - 1 \) Then
   Calculate \( V_1 \leftarrow e^1 M \mod p \)
   \( V_2 \leftarrow e^2 S_1 \times S_2 \mod p \)
- Step 2: If \( V_1 = V_2 \) Then
  The message \( M \) is accepted
Else
  The message \( M \) is rejected

4.3. Network traffic management using Auto-Resolution Adaptation (ARA) technique
In the current Covid-19 scenario, physical classroom teaching is far from reach. As a result, online teaching in the form of video conferencing is becoming the only alternative. The video conferencing is done over the mobile or system. Video conferencing incurs a lot of network bandwidth. The network bandwidth depends on many parameters such as network technology such as 3G or 4G, ISP (Internet Service Provider) and the number of Mobile towers, wireless communication technology such as VoLTE (Voice over Long Term Evolution) or LTE (Long Term Evolution), type of deicing depends on the size of RAM and available free space on the device, etc. Due to the large adaptation of online services for all most all activities, the bandwidth fluctuation is becoming the major problem in the current scenario.

Video conferencing is normally made among a group of people out of which the person who sets-up the meeting is called as the host. The broadcasting of video signal is made following different resolutions such as SD (Standard Definition), HQ (High Quality), HD (High Definition), QHD (Quarter High Definition), Full HD, WQHD (Wide Quad High Definition), Ultra HD, etc. Each type of video will incur different bandwidth. Hence if a host broadcasts the signal in high resolution and at the client end the signal strength is weak, then streaming and voice breaking will occur frequently, and
the client will be disconnected. So we have proposed an auto adaptation of video technique depending on the available bandwidth at the client end so that irrespective of the host broadcasting signal it will be converted to appropriate resolution and accordingly bandwidth utilization will be minimum. In general, the bandwidth requirement depends on the application used for the online (virtual) meeting. Normally, 1.5 to 2.5 Mbps bandwidth is required for the hassle-free online (virtual) meeting. But in many places, the bandwidth frequently fluctuates and even in 0.5 Mbps bandwidth, the user is not disconnected. If the bandwidth falls below that then, the user may be disconnected from the virtual meeting. So, depending on the available bandwidth, if the system updates the video into that form then, the users would continue participating in the virtual meeting at a cost of compromising with the quality of the video. A comparison of different types of video considering different parameters is presented in table-1 given below.

| Type of Video | Resolution | Pixel Count (in pixel per inch) | Server bandwidth required (in Kbps) | Client bandwidth required (in Kbps) |
|--------------|------------|---------------------------------|-------------------------------------|-------------------------------------|
|              |            |                                 | Inbound | Outbound | Inbound | Outbound |
| SD           | 640×480    | 480P                            | 256     | 256      | 128     | 128      |
| ED           | 854×480    | 480P                            | 512     | 512      | 256     | 256      |
| HQ           | 1024×768   | 768P                            | 1024    | 1024     | 512     | 512      |
| HD           | 1440×1080  | 1080P                           | 2048    | 2048     | 1024    | 1024     |
| Full HD      | 1920×1080  | 1080P                           | 4096    | 4096     | 2048    | 2048     |
| WQHD         | 2560×1440  | 4×720P                          | 8192    | 8192     | 4096    | 4096     |
| Ultra HD     | 3840×2160  | 4×1080P                         | 16384   | 16384    | 8192    | 8192     |

Table-1: Comparison of different types of Video

The comparison bar chart containing the bandwidth required for different types of video is depicted in figure-6.

Fig-6: Bandwidth Required Comparison Bar Chart

5. Performance
The performance of the proposed model depends on the algorithm. Due to CHAP, only the authentic users can participate in the process. The Elgamal Cryptography algorithm provided the whole process end-to-end security and the Elgamal digital signature provided the authentication of the whole process. Finally, the proposed Auto-Resolution Adaptation technique provided a solution to network traffic management for a compromised service.
6. Conclusion

Based on the above implementation and review of the performance the following conclusions can be made:

- Information encrypted using the Elagamal cryptography algorithm is very difficult to crack. Without the knowledge of the public key and private key pair, the decryption can be made. Due to the discrete logarithm feature used in the Elgamal algorithm, the security of the proposed method increased significantly.
- Higher the key size, the higher will be the information security.
- End-to-end encryption technique using the Elgamal cryptography algorithm provided advancement in information security instead of direct data transmission.
- The proposed Auto-Resolution Adaptation (ARA) technique provided a solution to network traffic management for a compromised service.

7. Future Work

ECC algorithm uses a reduced key for encryption to provide equivalent security. So instead of the Elagamal Cryptography algorithm, ECC may be used for the end-to-end security of information. Faster cryptography algorithms such as the quantum cryptography technique might be used to crack the information in the manageable period. The proposed Auto-Resolution Adaptation technique provided a compromised service. So, reorientation in this field may be done to improve the quality of the video using some mechanism.

Reference

[1] https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it
[2] COVID-19 Dashboard, Center for Systems Science and Engineering (CSSE) at Johns Hopkins University. (https://coronavirus.jhu.edu/map.html)
[3] Purna Ch. Sethi, Prafulla Ku. Behera, “Methods of Network Security and Improving the Quality of Service – A Survey”, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 5, Issue 7, July 2015, P1098-1106
[4] Muhammad Adnan, Kainat Anwar, “Online learning amid the COVID-19 pandemic: Students’ perspectives”, Journal of Pedagogical Research · June 2020, P45-51.
[5] Chrysi Rapanta, Luca Botturi, Peter Goodyear, Lourdes Guàrdia, Marguerite Koole, “Online University Teaching During and After the Covid-19 Crisis: Refocusing Teacher Presence and Learning Activity”, Postdigital Science and Education, https://doi.org/10.1007/s42438-020-00155-y.
[6] Shivangi Dhawan, “Online Learning: A Panacea in the Time of COVID-19 Crisis”, Journal of Educational Technology Systems, 2020, Vol. 49 (1) 5–22.
[7] Shatakshi Lal, Nardev Singh, “CoVid-19: Unmasking the new face of Education”, https://doi.org/10.26452/ijrps.v11iSPL1.2122
[8] Purna Ch. Sethi, Prafulla Ku. Behera, “Internet Traffic Classification for Faster and Secured Network Service”, International Journal of Computer Applications (IJCA), Volume 131 – No.4, December 2015, P15–20
[9] Purna Ch. Sethi, Prafulla Ku. Behera, “Secure Packet Inspection using Hierarchical Pattern matching implemented Using Incremental Clustering Algorithm”, December-22-24, ICHPCA-2014 (IEEE International Conference)
[10] Purna Ch. Sethi, Prafulla Ku. Behera, “Network Traffic Management using Dynamic Bandwidth on Demand”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 6, June 2017, P369-375
[11] Purna Ch. Sethi, Prafulla Ku. Behera, “Secure and Faster Data Transmission using Dynamic Network Traffic Management”, CSI2020 - “Digital Democracy - IT for Change” Springer International Conference, Dt-16/01/2020- 18/01/2020. (Accepted for publication)
[12] Behrouz A. Forouzan, “Data Communication and Networking”, 4th Edition, P352-353
[13] Bernard Menezes, “Network Security and Cryptography”, 3rd Edition, P110-112