[1]Basil Hanafi
[2]Mohammad Ubaidullah Bokhari
[3] Md Ashraf Siddiqui

Cruciality of securing user data due to increasing Digital Learner traffic over the Internet using Adversarial Neural Cryptography

Journal of Electrical Systems

Abstract: - In recent years, the whole globe has been afflicted with a devastating viral virus known as COVID-19 that has interrupted the operations of every organization. COVID-19 has significantly impacted education, causing it to struggle to function as smoothly as before. However, it has also ushered in a new era of e-learning, necessitating the provision of suitable facilities for users and learners. The growing number of users has led to an increase in digital threats to vulnerable systems on the widespread web of devices. The need for more diverse, versatile, and robust techniques is rising day by day, and Adversarial Neural Cryptography has the potential to be in the Line. The notions of Machine Learning and Digital Securities are being implemented in numerous manners for which ANC can perform the role of new technology to secure communication lines of a Digital learner from several learning platforms over the Cloud. This paper explores the possible threats, reasons, and potential steps taken to secure the user of the Digital Learning Platforms by various organizations. In extension to this, the concept of Adversarial Neural Cryptography is also introduced in the light of E-Learning Platforms with a conceptual model to secure communication.

Keywords: E-learning, E-commerce, Cryptography, Adversarial Neural Cryptography.

I. INTRODUCTION

Due to the pandemic that afflicted the whole world, online learning platforms have surged in popularity in recent years, allowing people to continue their everyday professional and academic lives from the comfort of their own homes. Another important cause for this phenomenon is the capacity of digital learning portals to give a platform for users to acquire various skills and academic domains in order to become well-versed in their specific expertise with well-known specialists from all over the world. The information exchanged on these platforms and websites spread extremely quickly making it appealing to attackers. The secrecy and security of these platforms must be questioned from numerous perspectives. Any Individual accessing and utilizing the Internet needs to be concerned regarding privacy and security essentially when upload or download of a file is required. These files can be Documents, Videos, and Images. Also, one must be very careful and concerned especially when crucial Information is shared over the web. This information can be gathered by the attacker through various sources around the Internet and can be used for its own evil requirements. It is easy to gather such sensitive Information over weakly secured platforms in comparison to well-established digital portals on the Internet. The Internet serves users of almost every age in today's world, but children in the initial phases are more prone to such threats and can become easy targets through several learning and recreational online platforms. The idea of this study primarily revolves around numerous privacy concerns along with their respective security threats which can enable an attacker to gather crucial Information about the user and use it according to the need, especially through E-learning Digital Platforms. With the help of this, a user can protect themself and avoid being attacked by any harmful entity on the Internet [1].

Initially, when the Internet started to become popular and fashionable to use in the nought era, it felt like a wonder to share Information and knowledge around the globe irrespective of the user's geographic location. It was a never-felt experience for Humans. During that time the users were limited in numbers and the concept of attacking the users in the network was also too primitive to be implemented. However, the development of the Internet led to an increase in the number of users and proportionally the number of attacking entities on the Internet. No Strict user guidelines were available and required at that time for the user to exchange information [2]. With the beginning of the new century in the 2000s, Social networking sites started revolutionizing the concept of personal

[1] *Corresponding author: Basil Hanafi, Aligarh Muslim University, Aligarh

[2] Mohammad Ubaidullah Bokhari, Aligarh Muslim University, Aligarh

[3] Md Ashraf Siddiqui, Aligarh Muslim University, Aligarh

ideas and information sharing online with anyone you wish around the globe. This served as the foundation of the e-learning concept in the beginning phases [3]. Online learning platforms can be believed as the Intersection of Social Networking and e-commerce Web Applications as the idea is to share the Information for educational purposes and sometimes it can lead to a business model through charging for such developed online courses for the sake of e-learning. The widespread pandemic all over the world has given some new dimensions in this domain as an expert were able to share their respective skills, knowledge, and expertise via the Internet with other Internet users for educational purposes to several quarantined students and professionals with the help of a centralized application known as Online learning platform [4]. In the International market, many such applications are available for learning and educational purposes through Internet sites, web portals, and mobile applications. Coursera, EDX Learning, Udemy, and many others are there to serve the purpose. There are several challenges that can be faced by a user in the process of Online Learning through various digital learning Platforms. Some of them are listed below:

(1)Data privacy and Protection of the User,

(2)Cybersecurity and hacking risks,

(3)Ensuring secure payment methods,

(4)Protecting against malicious software and viruses,

(5)Authentication and access control,

(6)Confidentiality of student information,

(7)Compliance with regulations such as GDPR,

(8)Securing online exams and assessments,

(9)Ensuring the privacy of communication between learners and Instructors,

(10) Regular security updates and monitoring.

Understanding the patterns and functioning of attacks on Learning Platforms can help overcome challenges in interacting with users from various fields, such as Engineering, Science, Commerce, and Arts. As online learning sites become more popular, people often overlook the need to safeguard their information on social networking sites, viewing it as a personal communication tool. As information is published in various formats, it can lead to unparalleled access to personal and corporate information. The amount of information saved on social networks is appealing to attackers who can exploit this information to cause devastating effects on someone's life globally. Therefore, it is crucial to protect users' information and ensure their safety on these platforms [5]. The Internet for educational purposes can have devastating effects on mental, social, physical, economic, and personal health. India has made efforts to encourage online learning for students, such as NPTEL and Swayam, to promote education and business. E-learning platforms can be a subset of social media applications, and if security concerns are not taken into account, users can be exposed to a range of attacks that can breach sensitive data, putting them in a risk zone [6]. In addition, social networks may be divided into a variety of categories based on their functions. Social networks can be for any usage like social connections, multimedia sharing, professional, discussion forums, and educational portals. The need for a robust and versatile method to secure the network connecting the user with the E-learning Cloud is increasing day by day. Various attempts are being made to develop some highly efficient ways to secure the channel using Machine learning. One such technique is Adversarial Neural Cryptography which is being explored and researched for successful applications in the Modern World as it possesses huge potential to replace various previous techniques to encrypt data passing within the network. This study revolves around the following Research Objectives:

(1) To Understand the Impact of the COVID-19 Pandemic on the Adoption of E-learning Platforms: Analyze how the global health crisis has accelerated the shift towards digital learning and the consequent rise in digital

learner traffic over the internet. This includes evaluating the operational challenges and opportunities presented by this sudden shift.

(2) To Identify and Assess the Security Threats to E-learning Platforms: Investigate the variety of cyber threats that have emerged or intensified with the increasing reliance on digital learning platforms. This involves cataloging common cyberattacks and understanding their potential impact on users' privacy and data security.

(3) To Explore the Application of Adversarial Neural Cryptography (ANC) in Enhancing Digital Security: Delve into the principles of ANC and its potential as a novel approach to secure communication between digital learners and e-learning platforms. This includes examining how ANC can be leveraged to protect against cyber threats more effectively than traditional cryptographic methods.

(4) To Develop a Conceptual Model for Securing E-learning Platforms Using ANC: Design and propose a conceptual model that employs ANC to safeguard digital communications within e-learning environments. This model should outline the roles of key components (e.g., Alice, Bob, and Eve in the context of ANC) and detail the process through which security can be enhanced.

(5) To Evaluate the Effectiveness of ANC in Securing E-learning Environments: Through simulation or empirical study, assess the efficacy of the proposed ANC model in mitigating identified cyber threats. This objective includes analyzing the strengths and limitations of ANC in real-world e-learning scenarios and suggesting improvements.

(6) To Offer Recommendations for Implementing ANC in Digital Learning Platforms: Based on the findings, provide actionable recommendations for educational institutions, e-learning platform developers, and cybersecurity professionals on implementing ANC. This should cover both technical and strategic aspects of deployment to enhance the overall security posture of digital learning environments.

To fulfill the Objectives The study revolves around the following Research Questions:

Q1: How has the COVID-19 pandemic impacted the adoption of e-learning platforms and the associated digital security risks?

Q2: What are the primary cybersecurity threats facing e-learning platforms in the current digital landscape?

Q3: How can Adversarial Neural Cryptography (ANC) be applied to enhance the security of digital communications within e-learning platforms?

Q4: What are the challenges and limitations of implementing ANC in e-learning platforms, and how can they be overcome?

Q5: What recommendations can be made for educational institutions and e-learning platform developers to enhance cybersecurity using ANC?

This Paper Will Have Seven Subsections Namely Introduction, Related Work, Post-Covid-19 Security Scenario Based On The Common Attacks On The Users Of The Digital Learning Platforms, Methodology, Atheoretical Framework For Adversarial Neural Cryptography Model To Secure Communication In Elearning Platforms Followed By Conclusion In The End.

II. Related Work

Various methodologies have been implemented since a long time ago (Gudimetla) for securing protocols for M-commerce Secure Mobile Payments and protecting crucial Information of the users [7]. This information can be utilized by the attacking entity in various ways and can affect in an adversarial manner financially and mentally. The concept can protect the user of eLearning portals in several ways. Application-level and Database security for e-commerce applications is very crucial as the attacking entity can bypass and enter the database and hijack the session (Rane) of any eLearning Application [8]. Cryptography can be proved as a very genuine way to protect the user and the application from any kind of attack and threat online (Ritu) for any user of eCommerce or

eLearning Application [9]. It is also very important to secure the financial transactions (Vishvalingam) done for generating businesses and money-related circulation on eLearning Applications [10]. Cryptography can be used in many more ways that can be imagined for securing such e-commerce and eLearning applications (Zaru) as it is much more than just encryption and decryption of intermediate data during transmission [11]. Following that, in this article, we will analyze the encryption mechanisms used in E-Commerce and eLearning which will provide insight for securing eLearning Online Portals in the future.

Research is expanding the understanding of securing Digital Learning Platforms, as data is sent in the IoT realm every second. Encryption and steganography methods can help protect sensitive data. The elliptic Galois encryption technology was introduced for encrypting private data from medical sources. The encrypted data is integrated into a simple image using Matrix XOR encoding steganography. The technique is further optimized using Adaptive Firefly to optimize cover block selection. The encrypted data is then retrieved and decoded, potentially protecting users and students on e-learning platforms [12].

A study aimed to identify security gaps related to IPv6's new features and unaffected ones. IPv6, also known as Iping, is the next generation of the Internet protocol and will eventually replace Ipv4. IPv4 has been successful but has limitations due to limited address space, difficulty in setup, and security issues. The network working group of the Internet Engineering Taskforce (IETF) proposed IPv6, offering new features like quality of services, auto-address configuration, end-to-end connectivity, security, and a simple routing header. This was done to address security concerns and improve the security of digital learners [13].

A study exploring the security implications of IoT devices and their cloud has included a suggested taxonomy of security elements. The term "Internet of Things" refers to the expansion of intelligent sensors into common households, enhancing devices' ability to provide user feedback and awareness. This leads to the development of a "system of systems." The study highlights the importance of addressing the security components of IoT, as the number of digital security risks and attacks is increasing daily. Without addressing these security elements, the concept of IoT would be incomplete [14].

The aim of this section of the study is to spot and cynosure different kinds of vulnerabilities of any Information Subsystem for any e-learning company or organization with which it can be prone to the leakage of user data. Any e-learning technology being utilized through the Internet must be cross-verified for any kind of infiltration when it is released for the user to install or be accessed through the browser in Beta versions or the actual products through security professionals. The crucial Information and assets can be accessed by undesired entities over the Internet and can lead to vulnerabilities by utilizing approaches such as:

- SQL code injection,
- XSS (Cross Side Scripting),
- Remote injection using a virus/trojan file,
- Acquire personalized information about the site, conduct various searches utilizing search engines like username or password,
- Cracking passwords using decryption systems,
- Disclosure of related security features through Web indexing of Scripts or database connection, and
- Session prediction.

E-commerce transactions often involve the transmission of sensitive financial information, such as credit card details. Adversarial neural cryptography can be employed to create cryptographic schemes that are resistant to man-in-the-middle (MitM) attacks, which attempt to intercept and modify credit card transactions to steal money. Additionally, ANC can design secure payment gateways that safeguard credit card information from unauthorized access [15].

E-commerce platforms collect and utilize personal data to enhance user experiences and provide targeted advertising. However, this data must be protected from unauthorized access and potential misuse. Adversarial neural cryptography can enable the development of privacy-preserving protocols for sharing personal data. These protocols allow e-commerce companies to collect and use personal data without revealing it to unauthorized parties.

Fraudulent transactions pose a significant threat to e-commerce businesses, causing financial losses and reputational damage. Adversarial neural cryptography can be applied to develop anomaly detection systems that identify fraudulent transactions in real-time. These systems employ machine learning algorithms to learn the patterns of normal behavior and detect transactions that deviate from these patterns. Unauthorized access to e-commerce accounts can lead to identity theft, financial loss, and data breaches. Adversarial neural cryptography can be employed to design secure authentication systems that prevent unauthorized users from accessing e-commerce accounts. These systems can utilize machine learning techniques to distinguish between legitimate users and potential imposters [16].

III. POST-COVID-19 SECURITY SCENARIO BASED ON COMMON ATTACKS ON THE USERS OF THE DIGITAL LEARNING PLATFORMS

The COVID-19 pandemic initially seemed temporary, lasting until the upcoming year. However, its extended impact has led to new challenges for technical staff and information technology professionals in various organizations and companies, as they face new challenges in their daily tasks and responsibilities [17]. With the passage of such hard times, such professionals are in need to think more about repercussions when they invest, produce, and roll out new prowess.

- What must be undone once the issue has been brought under control?
- Which of the new habits or behaviors will stick around?
- Will IT security professionals have to develop additional safeguards?

There's still a lot of debate about what will happen after the epidemic [18], but there are some things that seem to be certain:

(1) Firms will adopt innovative business models, requiring careful evaluation of cybersecurity and IT rights. Remote workers' monitoring and assistance will become critical. Cybersecurity personnel must ensure systems pass rigorous system and access scrutiny before reconnecting to the network.

(2) Companies must recalibrate surveillance equipment to eliminate outliers and verify for technological holes. They must review data and information availability prerogatives, including remote access to hard graft, to determine if they will be nixed or changed. IT infrastructure must be probed for flaws, unclean passageways, and bogus credentials, as cybercriminals may gain access to typically guarded equipment.

(3) The pandemic has introduced new cyber threats, necessitating security analysts to assess operational processes during downtime and critical distribution networks, including digital supply chain operations, to ensure they can withstand attacks and prevent disruptions during a medical crisis.

(4) Online digital portals' IT security designs should be re-evaluated, including authentication procedures, remote access support, and security authentication based on threat and situation.

(5) Access to the network & bring-your-own-device (BYOD) guidelines must be revised. Information security personal grooming controls should also be included.

(6) Modern technology, including threat intelligence, decentralized finance, big data analytics, artificial intelligence, and machine learning, is crucial for identifying and mitigating undesirable behavior without human involvement. These technologies enable machines to respond to machine agendas without human intervention [19].

Companies should consider contagion insurance for hackers' losses, and security leaders should share their experiences during emergencies. They should analyze adaptability, ease of provision, virtualized reliability, and remote management of security solutions. Partnering with credible partners and regularly practicing exercises can help new enterprises and those during lockdowns thrive [14].

Cybersecurity experts must actively address hazards in the evolving digital environment. Organizations should educate remote employees about online fraud and how to avoid it. E-learning websites and online portals can help train individuals to protect themselves and enhance security in their working infrastructure. Even after the pandemic, employees and cyber security professionals must work together to protect their digital assets and adopt technologies, solutions, and techniques. Switching to cloud-based infrastructure reduces the time needed and helps expand businesses, especially those providing online services like online learning portals. Security can be enhanced and reduced in any dimension over the cloud, depending on the level of threat an organization poses, protecting employees and users.

Cloud service providers play a crucial role in ensuring security in eLearning organizations. They provide data leakage prevention and threat-protection policies to protect users and organizations from harmful entities online. Controlled detection and response services help prolong the security of remote users. Attributes-based and multi-factor authentication-based security services reduce the risk of users accessing study material from any remote location. Online learning and educational portals are susceptible to a wide spectrum of attacks, making it essential for IT professionals to provide security services. Some of the major observable attacks that can be avoided by simply following some required precautions are listed as

A. **Cross Site Scripting Attack (or XSS)**: It is one of the most popular and conventional forms of assault which is done on the application layer through the browser of the target's client-side instead of using the script at the server side as mentioned in Figure 2. This kind of attack is quite convenient for any attacker to gain access and extract sensitive information of the user of any user of eLearning portals. It functions by manipulating and changing the client-side scripts within the web application and executes in favor of the attacking entity on the Internet [20].

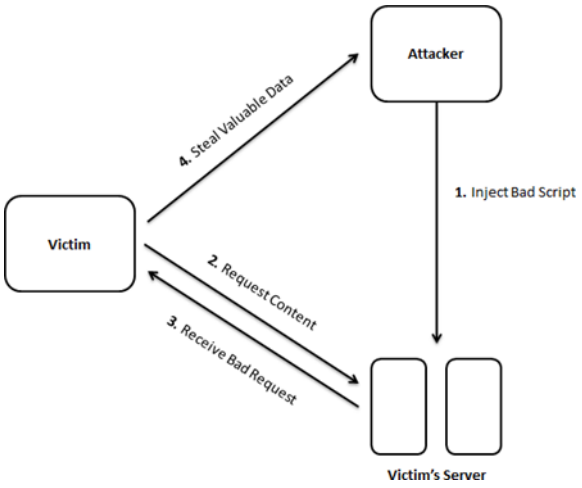

Figure 1. Cross Site Scripting

Figure 2 illustrates the working of the Cross Site Scripting technique which can be used to gain access to the sensitive information of the Application user for malicious purposes. Such attacks are done with the scripts secretly embedded in a web page of an application, which are triggered at any event including the reloading of the page. It is easy to plan this kind of attack due to the implemented security flaws in client-side scripting languages such as HTML and Javascript. There is a wide spectrum of attacks that can lead to the extraction of information of a user with the use of this attack like

- Delicate and personal digital assets and data,
- Identity theft of a user,

- Invading and changing the functioning of the app and browser of the users,
- Disfigurement of the Application for malicious activities,
- DoS and DDoS attacks.

An organization providing services for online learning can safeguard its users by following some simple steps during the development and implementation phase. Some of them are listed below in a confined manner:

- It is needed to be guaranteed that the input from the users is only returned after getting validated and sanitized within the application for the harmful code or part of it,
- Even the websites secured through HTTPS with Safe Socket Layer (SSL) are also prone to this kind of attack, as it assures secure connections, but the program processes the data entered by the user internally. In case the web application is vulnerable to Cross Site Scripting attack, the attacker can inject the malicious code which can run all the time in the background without the knowledge of the user ultimately leading to the incursion,
- Non-alphanumeric characters in the data provided to any such application are needed to be adapted in the form of HTML characters to avoid leakage of sensitive Information returned while searching on the Search Engines,
- The use of good testing methodologies and tools can help a lot get rid of such Cross Side Scripting problems and intended attacks particularly for eLearning Online Applications and online programs before it is released for the users or learners.

B. **SQL Injection Attacks**: This attack can be utilized to offer string input for an eLearning application for the purpose of obtaining an unauthorized access to its database from which various critical information of the users can be extracted [21]. This kind of attack is relatively easy in comparison to others. As illustrated in Figure 3, The attacking entity on the internet can trigger an unexpected event or unnecessary action by injecting a SQL query or a defined set of characters which can ultimately lead to the exploitation of the user of the web Application. Since learning the databases of a single application are centralized whether in terms of mobile or in terms of web applications. Such searches can lead to unwanted data access, authentication bypass, or database shutdown, irrespective of the location of the database web server. The Application can be developed and used in a way that these kinds of attacks can be avoided or surpassed to protect the integrity of the user, some of them are:

- Encrypting the data, which is being stored and retrieved through the database,
- Making sure that the pop-up message or the error message do not disclose anything regarding the user or the architecture of the web application or the database in the development phase,
- Cross check the input from the user for the threatening characters like single quotes which can provide access to the database and internal functioning through SQL injection,
- Application is needed to be developed in a manner that enables the database to take actions accordingly prior to any kind of data provided at the users end and passed with the help of prepared statements.

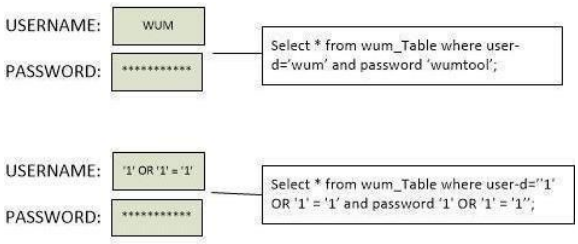

Figure 2. SQL Injection Attacks

As can be visualized in Figure 3 above, the sensitive Information of a Web Application especially the eLearning web Application can also be extracted with the help of URLs using SQL injections. It is a good practice for avoiding such situations, to hide the query string in the URL for any working Web Application by delivering the critical parameters to the URL.

C. **Session Attacks**: It is a way through which the user can be exploited by changing the state and various variables related to that. Conserving the state of a user can help the application to avoid falling off users in such kinds of attacks. It is done with the help of generating and using session IDs which are unique values used for identification of any user at a single time and hard to break through brute forcing or guessing [22].

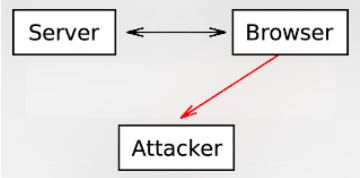

Figure3. Session Hijacking through Browser

They are transmitted from the user's end through the browser utilizing the Query String in the URL or the cookies. Using different techniques and methodologies, session prediction entails predicting a valid session ID (like brute force technique). This attack will be successful if the session ID is visible to the attacker through any means. To hide the session ID sufficient length and well encryption are used.

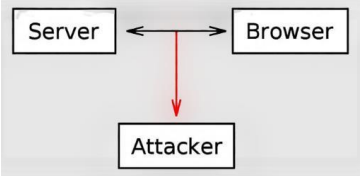

Figure4. Sniffing during a Session

The mentioned scenarios of Session Hijacking and Sniffing within a Session can be visualized with the help of Figure 4 and Figure 5 shown above for which alternative assignment can be used to add security for the user of the web application. Proper expiration of the assigned session ID on the HTTP server is very crucial within the appropriate time frame as it can avoid guessing at the attacker's end using brute forcing and gaining access to the online learning accounts of the users. Session IDs of the users can also be accessed through proxy servers which were stored when the user logged into it. If the Get Requests are sent through the URL, then they are stored in the history, cache, and bookmarks of the History of the browser. It is also easily accessible at that time. The following recommended practices should be followed to avoid concerns with session security:

- The session id should be sufficiently lengthy and unpredictably generated,
- Validate the authentication of the session id,
- Verify the session id for the source of generation through the web application,
- Renew the session id once the user's privilege changes and check for every fixed period,
- Only use cookies to transmit the session id,
- Do not use the "remember me" option,
- Exterminate the session and respective cookies once session ends,
- Expire the session and session id for every fault when occurs in terms of security and after a fixed interval of time in case of inactivity.

IV. METHODOLOGY

The need to strengthen data security and online privacy is urgent due to cyberattacks and data breaches. Encryption is crucial for safeguarding these rights, but governments are constantly threatening encryption. Regulators often cite safety concerns, particularly minors' protection, to justify requests for providers to reduce encryption. They argue that encryption, particularly end-to-end encryption (E2EE), is incompatible with public safety, as it prevents platforms and law enforcement from identifying damaging information, insulating those responsible from accountability [23]

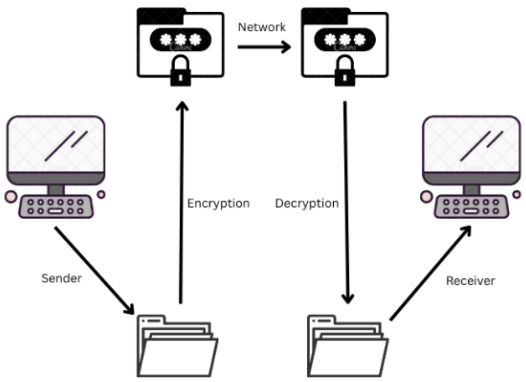

Figure 5. The Concept of Encryption

Figure 1 illustrates the process of encryption for the data that is being sent from one machine which is the sender at one instance to another machine which is the receiver at the same instance. Cryptography is a method of encrypting data before it is sent to a network and decrypted before it is accessed by a machine. Online service providers can identify misuse on their platforms even in encrypted settings, preferring detection methods that don't require access to user files or conversations. Cryptography has been used since Julius Caesar sent instructions to military troops. The technique of converting the plain text of any language into something unreadable or non-understandable format is known as Cryptography as mentioned in Figure Cryptography is a secure method for storing and transmitting information over the internet, ensuring only the intended audience can access and use it. It also aids in user authentication and data protection from theft, eavesdropping, and harmful changes. Despite its complexity, cryptography is a modern mathematical concept with applications in computer science, integrating advanced mathematical concepts with modern practices. Modern Cryptography concerns revolve around four primary objectives:

(1) **Confidentiality:** The intended information will be made available to the intended users only,

(2) **Integrity:** No one will be able to make any kind of change in the Information,

(3) **Non-repudiation:** Once received at the receiver's end sender cannot deny the Information,

(4) **Authentication:** Communication parties can verify each other whenever required during communication over the network. [24]

In today's modern digital world, there is a wide range of applicability for the concept of cryptography from securing digital transactions (financial and e-commerce) to protecting passwords. To summarize, there are three different methodologies to implement cryptographic procedures that can be implemented for securing e-learning online platforms:

(1) Symmetric-key Cryptography:

It is a technique in which the same single key is possessed by the sender as well as the receiver. The intention is to encrypt the text using the key which is needed to be sent by the sender to the receiver. On the other side, sider decrypts and gets the text back in its original form.

(2) Asymmetric-key Cryptography (Public-key Cryptography):

In this technique, two associated keys are utilized for the process of cryptography. The intention is to keep the private key secret and transfer it freely to the public over the network. The public key is used for encryption whereas the private key is used for the purpose of decryption. The development of this technique revolutionized the scenario for transmitting data around the globe over a network.

(3) Hash Functions:

Hash function isn't utilized primarily for transmitting data, as it doesn't require any key in the process. A hash function is a technique to hide data in fixed-sized plain text such as passwords. Hash functions are also used for the purpose of user authentication through Digital signatures and Digital certificates. Nowadays, the technique is also being used for implementing blockchains. [25]

The pandemic has heightened the need for digital infrastructure, causing increased business for cloud service providers and hardware manufacturers. Cybercriminals are targeting organizations' digital assets, leading to growing threats to major corporations, especially in the learning and education sectors, and the causes behind these threats [26]. Digital channels significantly impacted employee knowledge transition and academic learning during the COVID-19 pandemic. They provided entertainment, encouraged lockdown, and protected the future by developing personalities through educational and recreational methods, especially during limited school resources [27].

The shift to online communication for learning and education has increased cyberattack risks, necessitating constant monitoring of physical and application systems by cybersecurity experts. E-commerce and e-learning platform owners must defend their businesses on a large scale, affecting the world, while the information technology department faces significant stress [28]. IT departments are introducing remote working capabilities to new employees, and implementing collaboration technologies from e-learning sites. This increases the risk of data theft, as executives, managers, and staff require access to internal services and applications. Security experts are concerned about granting access without strict restrictions, as many companies don't provide these via the Internet or VPNs. This digital footprint can be exploited by cybercriminals for exploitation or theft. COVID-19 victims are being targeted by phishing emails, downloading malware, disrupting computers, and stealing data and passwords. Attackers create temporary websites or take over weak ones, lure people, install malware, and solicit payments from daily wage employees via email connections [29].

The methodology for researching the effectiveness of Adversarial Neural Cryptography (ANC) in enhancing the security of e-learning platforms due to increased digital learner traffic involves several key steps. This approach integrates theoretical exploration with practical experimentation to assess how ANC can address cybersecurity challenges in digital learning environments. Below is a detailed methodology for this research:

(1) Literature Review

- Objective: To synthesize existing knowledge on cybersecurity threats in e-learning platforms and the role of traditional cryptographic methods in addressing these threats.

- Approach: Conduct a comprehensive review of scholarly articles, conference proceedings, and industry reports on digital learning, cybersecurity threats to these platforms, traditional cryptographic methods, and the emergence of adversarial neural networks in cybersecurity.

(2) Theoretical Exploration of ANC

- Objective: To understand the principles of Adversarial Neural Cryptography and its potential application in securing digital communications.

- Approach: Examine foundational papers and recent studies on ANC, focusing on its mechanisms, the roles of the neural networks involved (Alice, Bob, and Eve), and its theoretical advantages over traditional cryptography in countering modern cyber threats.

(3) Designing the Experimental Framework

- Objective: To create a simulated e-learning environment where ANC can be applied and tested against various cybersecurity threats.

- Approach:

- Simulation Environment Setup: Develop or adapt a simulated digital learning platform environment where communication between users (learners and educators) can be modeled.

- ANC Implementation: Implement the ANC model within this environment, detailing the configuration of the neural networks (Alice, Bob, and Eve), training data, and parameters.

- Threat Simulation: Design scenarios that mimic common cyberattacks against e-learning platforms, such as data breaches, phishing, and more sophisticated threats.

(4) Training and Testing the ANC Model

- Objective: To train the ANC model to secure communications within the simulated e-learning environment and evaluate its effectiveness against simulated cyber threats.

- Approach:

- Training Phase: Train the ANC model using a dataset that represents typical communications in e-learning platforms, adjusting parameters to optimize performance.

- Testing Phase: Test the trained ANC model against simulated cyberattacks, measuring its success rate in preventing data breaches and unauthorized access compared to traditional cryptographic methods.

(5) Practical Implementation Considerations

- Objective: To explore the practicality of implementing ANC in real-world e-learning platforms.

- Approach:

- Feasibility Study: Assess the technical and operational feasibility of integrating ANC into existing e-learning platforms, considering factors like computational resource requirements, scalability, and user experience.

- Implementation Roadmap: Propose a phased roadmap for adopting ANC in e-learning platforms, including pilot testing, user training, and evaluation phases.

(6) Conclusion and Future Directions

- Objective: To summarize findings and suggest areas for further research and development.

- Approach:

- Findings Summary: Present a comprehensive summary of the research findings, emphasizing the potential of ANC in enhancing the security of e-learning platforms.

- Recommendations: Offer recommendations for educators, platform developers, and cybersecurity professionals on adopting ANC.

- Future Research: Identify gaps in the current research and propose future studies to explore ANC's potential further or address its limitations.

This detailed methodology provides a structured approach for investigating the application of Adversarial Neural Cryptography in enhancing the security of e-learning platforms, combining theoretical insights with practical experimentation and analysis.

V. THEORETICAL FRAMEWORK FOR ADVERSARIAL NEURAL CRYPTOGRAPHY MODEL TO SECURE COMMUNICATION IN ELEARNING PLATFORMS

The concept of Generative adversarial neural networks was coined by Ian Goodfellow and then was worked further by M. Abadi to develop the concept of Adversarial Neural cryptography. The Idea of a Generative Adversarial Network was to develop a synchronized Deep learning model in which two Neural Networks namely, Generator and Discriminator, adversarially train each other to get output from a generator that will be real instead of fake out of random noise after training. The main intention of the setup is to increase the probability of the generated data so that it is not discriminable by the discriminator in the setup. This arrangement is considered a zero-sum game between the generator and the Discriminator where the Generator is trying to increase the probability of the Generated (G) Output towards real data and the Discriminator (D) is trying to reduce it [30]. The Loss Function of the Situation is:

$$min_G max_D\, V(D,G) = E_{x\sim p_{data(x)}}[logD(x)] + E_{z\sim p_{(z)}}[log(1 - D(G(z)))] \quad (1)$$

For the Context of Adversarial Neural Cryptography The three neural networks are trained adversarially, namely Alice, Bob, and Eve. Here in the context Alice the Sender and Bob the receiver are trained together in an adversarial manner with Eve as an Evesdropper to the communication. The whole setup is to train the model to attain the following:

1. Alice (Sender or Encoder): The sender neural network takes the plaintext message and encodes it into a ciphertext, which is the encrypted form of the message. The sender's goal is to generate ciphertexts that are difficult to decipher by unauthorized parties.

2. Bob (Receiver or Decoder): The receiver neural network takes the ciphertext and attempts to decode it back into the original plaintext message. The receiver's objective is to correctly reconstruct the plaintext from the ciphertext.

3. Eve (Eavesdropper or Adversary): In ANC setups, there is a third neural network, often referred to as the adversary or eavesdropper. The adversary's task is to intercept and decode the ciphertext to recover the plaintext message. It competes against the sender and receiver in an adversarial manner, hence the name "adversarial" neural cryptography.

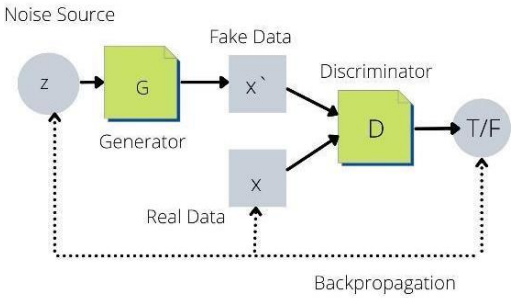

Figure 6. Training process for ANC

The training process involves these neural networks competing with each other:

- The sender aims to generate ciphertexts that are secure, meaning they cannot be easily decoded by the adversary.
- The receiver tries to learn how to decode the ciphertexts accurately.
- The adversary attempts to break the encryption by learning how to decipher the ciphertexts.

This adversarial competition leads to the improvement of the sender and receiver networks, making the encryption and decryption processes more robust over time. The idea is to create cryptographic systems that can withstand attacks, even from sophisticated machine-learning adversaries [31].

Pseudocode for ANC

```
# Pseudo Code for Adversarial Neural Cryptography


# Initialize sender, receiver, and adversary neural networks
initialize_sender_network()
initialize_receiver_network()
initialize_adversary_network()
# Define loss functions for sender, receiver, and adversary
def sender_loss(sender_output, decrypted_output):
    return mean_squared_error(sender_output, decrypted_output)
def receiver_loss(encrypted_message, decrypted_input):
    return mean_squared_error(encrypted_message, decrypted_input)
def adversary_loss(encrypted_message, intercepted_message):
    return mean_squared_error(encrypted_message, intercepted_message)
# Define optimizers for sender, receiver, and adversary
sender_optimizer = initialize_optimizer()
receiver_optimizer = initialize_optimizer()
adversary_optimizer = initialize_optimizer()
# Training loop
for epoch in range(num_epochs):
    # Generate random input data
    input_data = generate_random_input()
        # Sender encrypts input data
    encrypted_message = sender_network(input_data)
        # Receiver tries to decode the encrypted message
    decrypted_output = receiver_network(encrypted_message)
        # Adversary tries to intercept and decode the encrypted message
    intercepted_message = adversary_network(encrypted_message)
        # Calculate sender loss, receiver loss, and adversary loss
    sender_loss_value = sender_loss(input_data, decrypted_output)
    receiver_loss_value = receiver_loss(encrypted_message, decrypted_output)
```

```
    adversary_loss_value = adversary_loss(encrypted_message, intercepted_message)
        # Update sender network
    sender_gradients = compute_gradients(sender_loss_value, sender_network)
    apply_gradients(sender_gradients, sender_optimizer)
        # Update receiver network
    receiver_gradients = compute_gradients(receiver_loss_value, receiver_network)
    apply_gradients(receiver_gradients, receiver_optimizer)
        # Update adversary network
    adversary_gradients = compute_gradients(adversary_loss_value, adversary_network)
    apply_gradients(adversary_gradients, adversary_optimizer)
        # Display progress
    display_progress(epoch, sender_loss_value, receiver_loss_value, adversary_loss_value)
print("Training complete!")
# Testing
test_input = generate_random_input()
test_encrypted = sender_network(test_input)
test_decrypted = receiver_network(test_encrypted)
test_intercepted = adversary_network(test_encrypted)
display_results(test_input, test_decrypted, test_intercepted)
```

Adversarial Neural Cryptography (ANC) is a novel approach that combines elements of adversarial machine learning and cryptography to design secure communication systems. It involves the use of neural networks, which are machine learning models inspired by the structure of the human brain, to create cryptographic protocols that are resistant to various attacks, including those launched by powerful adversaries. This methodology of securing Communications and digital assets can be used for securing the learners and their respective digital assets over eLearning Digital Platforms [32].

Adversarial Neural Cryptography (ANC) can be used to enhance the security of user authentication on eLearning websites in several ways. ANC can help protect user credentials during transmission and storage, making it more difficult for attackers to compromise user accounts. Here's how ANC can be applied for secure user authentication:

1. Secure Communication Channels:

ANC can be used to establish secure communication channels between users and the eLearning website. Neural networks can generate encryption keys for secure data transmission, ensuring that login credentials are protected while in transit. This prevents eavesdropping attacks.

2. Encrypted User Credentials:

When users log in, their credentials (such as usernames and passwords) can be encrypted by the sender (user) using ANC before sending them to the server. The server (receiver) then decrypts and verifies the credentials. This prevents attackers from intercepting and using plaintext credentials.

3. Two-Factor Authentication (2FA):

ANC can work in conjunction with 2FA systems. For example, after a user provides their username and password, a one-time token generated by a 2FA system can also be encrypted using ANC before being sent to the server for authentication. This adds an extra layer of security.

4. Protection Against Brute Force and Dictionary Attacks:

ANC can make it more challenging for attackers to conduct brute force or dictionary attacks against user accounts. Even if attackers gain access to the encrypted credentials, the complexity introduced by the neural network encryption makes it difficult to crack the passwords.

5. Protection Against Man-in-the-Middle Attacks:

ANC can help protect against man-in-the-middle (MITM) attacks, where an attacker intercepts communication between the user and the server. Encryption ensures that even if communication is intercepted, the data remains confidential.

Adversarial Neural Cryptography (ANC) is a method that uses neural networks to encrypt and decrypt messages, while resisting adversarial attempts. It offers numerous advantages, particularly in e-commerce and e-learning applications hosted on cloud platforms. These include enhanced security, scalability, efficiency, customization, adaptability, data privacy, compliance with regulations, and cost-effectiveness. However, challenges include computational resources, specialized expertise, and potential vulnerabilities. Despite these, ANC presents a promising approach to securing e-commerce and e-learning platforms. The theoretical framework for the research on securing user data in e-learning platforms using Adversarial Neural Cryptography (ANC) involves several key concepts and theories that underpin the study. This framework provides the basis for understanding the mechanisms through which ANC can enhance digital security in the context of increased digital learner traffic. The detailed theoretical framework is outlined as follows:

1. Digital Learning and Cybersecurity Challenges

- E-learning Evolution: The shift from traditional classroom settings to online platforms, accelerated by global events such as the COVID-19 pandemic, necessitates a comprehensive understanding of digital learning environments.

- Cybersecurity Threats in E-learning: Identify and describe the various types of cybersecurity threats faced by e-learning platforms, including data breaches, phishing attacks, and more sophisticated threats like Advanced Persistent Threats (APTs).

2. Cryptography and Digital Security

- Basics of Cryptography: Explore the principles of cryptography, including its historical context, and its role in securing digital communications. This includes symmetric-key and asymmetric-key cryptography, and hash functions.

- Limitations of Traditional Cryptography: Discuss the limitations of traditional cryptographic methods when facing modern cyber threats, emphasizing the need for adaptive and dynamic security solutions.

3. Adversarial Machine Learning

- Principles of Adversarial Machine Learning: Introduce the concept of adversarial machine learning, where models are trained to anticipate and counteract adversarial inputs or attacks, enhancing their resilience.

- Applications in Cybersecurity: Discuss the application of adversarial machine learning in cybersecurity, focusing on its potential to improve the detection of and response to cyber threats through continuous learning and adaptation.

4. Adversarial Neural Cryptography (ANC)

- Concept and Origin of ANC: Define ANC, tracing its origins to the work by researchers such as Abadi and Andersen, who explored using neural networks in an adversarial setting to secure communications.

- Mechanisms of ANC: Describe the core mechanism of ANC, which involves training two neural networks (a sender and a receiver) to communicate securely in the presence of an adversary (an eavesdropper). This includes the roles of Alice (sender), Bob (receiver), and Eve (eavesdropper) in the ANC framework.

- Training Process and Objectives: Outline the training objectives for each participant in the ANC model, detailing how adversarial training enhances the security of the communication channel by making it resistant to eavesdropping or decryption by unauthorized parties.

5. Implementing ANC in E-learning Platforms

- Integration Challenges and Considerations: Discuss the practical challenges and considerations involved in integrating ANC into existing e-learning platforms, including computational requirements, scalability, and user impact.

- Potential Benefits and Drawbacks: Evaluate the potential benefits of using ANC to secure e-learning platforms, such as enhanced privacy and data security, against possible drawbacks, such as increased complexity and resource demands.

6. Future Directions and Research Opportunities

- Advancements in ANC and Machine Learning: Project future advancements in ANC and machine learning that could further enhance digital security in e-learning and other domains.

- Research Gaps and Opportunities: Identify gaps in the current understanding and application of ANC in cybersecurity, suggesting areas for future research and exploration.

This theoretical framework sets the stage for investigating how ANC can be effectively applied to secure e-learning platforms, addressing both the technical intricacies of the approach and its practical implications for digital learning environments.

If on a contrary Adversarial Neural Cryptography (ANC) is compared with two traditional cryptographic techniques commonly used in e-commerce and e-learning applications: Symmetric Encryption (e.g., AES) and Asymmetric Encryption (e.g., RSA), then the promising result can be concluded for successful implementation of the above mentioned theoretical Model.

Feature	**Adversarial Neural Cryptography (ANC)**	**Symmetric Encryption (AES)**	**Asymmetric Encryption (RSA)**
Security	High, with dynamic adaptation to threats. Resistant to a wide range of attacks due to constant learning and adaptation.	High, but static. Effective against many traditional attacks but requires strong key management practices.	High, especially for establishing secure channels. However, computational feasibility of breaking it increases with advancements in computing power.
Efficiency	Potentially high with optimized neural networks, but can be resource-intensive during the training phase.	Very high, designed for quick encryption and decryption of large volumes of data.	Lower than symmetric methods due to computational complexity, making it less suitable for encrypting large volumes of data.

Scalability	High, can efficiently process large data volumes and adapt to scaling needs using cloud resources.	High, straightforward to scale up with increasing data loads.	Moderate, scaling is feasible but can be limited by the computational overhead of encryption and decryption processes.
Key Management	Simplified and dynamic, potentially reducing the complexity of key exchanges and renewals.	Complex, requires secure key exchange and management protocols to ensure security.	Complex but facilitated by the public/private key structure. Still requires secure management of private keys.
Adaptability to Threats	Very high, continuously learns and adapts to new threats.	Low, relies on updates and patches to encryption algorithms to address new threats.	Moderate, depends on key length and algorithm updates to stay ahead of computational advancements and threats.
Implementation Complexity	High, requires expertise in machine learning and cryptography. Initial setup and ongoing training can be resource-intensive.	Low, well-documented and widely supported across various platforms and languages.	Moderate, more complex than symmetric encryption due to key generation and management, but well-supported.
Suitability for Data Privacy	High, offers robust encryption that can evolve to protect against emerging decryption techniques.	High, effectively secures data at rest and in transit, assuming proper key management.	High, particularly useful for securing data in transit. Often used for encrypting keys rather than bulk data.
Cost-Effectiveness	Variable, potentially high initial investment but can lead to cost savings through reduced reliance on third-party solutions and mitigation of breaches.	High, minimal operational costs post-implementation. Widely available and does not require ongoing licensing fees.	Moderate, requires more computational resources than symmetric encryption, which can lead to higher operational costs.

This comparison highlights ANC's potential to revolutionize encryption practices, especially for dynamic and scalable cloud-hosted applications in e-commerce and e-learning. It also underscores the importance of weighing implementation complexity and initial investment against the long-term benefits of enhanced security and adaptability. However, its potential to reduce breach-related costs and decrease reliance on third-party solutions could offer long-term savings.

VI. Conclusion

The pandemic led to a shift to online learning and education, significantly impacting society. The hype surrounding virtual classrooms during the pre-COVID period increased the risk of users being trapped by entities and surrendering sensitive information. This led to the development and enhancement of security measures by security professionals and giants. While security and privacy are myths in the digital era, users can avoid threats by following precautions and minor changes in their habits. By avoiding easy access to crucial information on non-trustable web portals, individuals can ensure a secure and efficient learning experience. Although any organization can be compromised it is advisable to access educational and learning portals from trustable service providers like Google, LinkedIn, Coursera, Edx, etc. As these Digital learning platforms recently have grown their businesses in the pandemic era like Unacademy, Byjus, etc., they have proven themselves that they will be decisive entities in the market for economic and financial progressive drift around the globe for their respective Nations

especially. Even Indian government initiatives like SWAYAM, NPTEL, etc. will be helping to grow the economy indirectly the educating the unskilled or uneducated gentry in a particular domain. Whether a Government or private Organization, everyone must always keep track of their security protocols and architecture to safeguard their respective users with the state-of-art techniques of Artificial intelligence and machine learning like Adversarial Neural Cryptography. The development of these digital educational companies will lead to the overall economic, societal, and mental development of any Nation.

Availability of Data and Materials

The data that supports the findings of this study are available from the corresponding author, Basil Hanafi, upon reasonable request. The authors confirm that all relevant data supporting the findings of this research are contained within the article.

Funding

No funding was received for conducting this study.

Acknowledgments

The authors would like to thank the Department of Computer Science at Aligarh Muslim University for providing the resources and environment to carry out this research. Special thanks to the peer reviewers and editors who provided opportunity for reviewing the manuscript.

References

[1] Bhatia, M., & Maitra, J. K. (2018, September). E-learning Platforms Security Issues and Vulnerability Analysis. In 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES) (pp. 276-285). IEEE.

[2] Heikkinen, S., Kinnari, S., & Heikkinen, K. (2009, February). Security and user guidelines for the design of the future networked systems. In 2009 Third International Conference on Digital Society (pp. 13-19). IEEE.

[3] King, D., & Dennis, A. (2012, January). Introduction to Internet and the Digital Economy Track. In 2012 45th Hawaii International Conference on System Sciences (pp. 3039-3039). IEEE Computer Society.

[4] Lee, S., Kim, J., Ko, S., & Kim, H. (2016, August). A security analysis of paid subscription video-on-demand services for online learning. In 2016 International Conference on Software Security and Assurance (ICSSA) (pp. 43-48). IEEE.

[5] Aldheleai, H. F., Bokhari, M. U., & Hamatta, H. S. (2015, April). User Security in e-Learning System. In 2015 Fifth International Conference on Communication Systems and Network Technologies (pp. 767-770). IEEE.

[6] Miguel, J., Caballé, S., Xhafa, F., & Prieto, J. (2014, May). Security in online learning assessment towards an effective trustworthiness approach to support E-learning teams. In 2014 IEEE 28th International Conference on Advanced Information Networking and Applications (pp. 123-130). IEEE.

[7] Gudimetla, S. D. R., Varma, B. S., & Gudimetla, S. R. R. (2016). A Secure Protocol for M- commerce Secure SMS Mobile Payment.

[8] Rane, P. B., & Meshram, B. B. (2012). Application-level and database security for e- commerce application. International Journal of Computer Applications, 41(18).

[9] Ritu, M. (2016). " Cryptography Based E-Commerce Security. Int. J. Adv. Res. Comput. Sci. Softw. Eng., 6(7), 359-362.

[10] Vishvalingam, K., & Sandanayake, T. C. (2017). An Overview of Online Transaction Technologies in E-Commerce. International Journal of Engineer-ing Development and Research, 5(2), 993-998.

[11] Zaru, A., & Khan, M. (2018). General summary of cryptography. Journal of Engineering Research and Application.

[12] Khari, M., Kumar, M., Vij, S., & Pandey, P. (2016, March). Internet of Things: Proposed security aspects for digitizing the world. In 2016 3rd international conference on computing for sustainable global development (INDIACom) (pp. 2165-2170). IEEE.

[13] Wadhwa, M., & Khari, M. (2011). Security holes in contrast to the new features emerging in the next generation protocol. International Journal of Computer Applications, 20(3), 35-39.

[14] Khari, M., Kumar, M., Vij, S., & Pandey, P. (2016, March). Internet of Things: Proposed security aspects for digitizing the world. In 2016 3rd international conference on computing for sustainable global development (INDIACom) (pp. 2165-2170). IEEE.

[15] Shruti, J., Sharma, S., Agarwal, A., & Gupta, S. (2018). A novel hybrid approach of neural network and DNA computing for secure communication. Journal of King Saud University - Computer and Information Sciences, 30(3), 447-454

[16] Rivas, P. (2021). An adversarial neural cryptography approach to integrity checking: Learning to secure data communications. Sensors, 21(18), 5928.

[17] Mehta, S., Saxena, T., & Purohit, N. (2020). The new consumer behaviour paradigm amid COVID-19: permanent or transient?. Journal of health management, 22(2), 291-301.

[18] Abazi, B., & Hajrizi, E. (2022, June). Practical analysis on the algorithm of the Cross-Site Scripting Attacks. In 2022 29th International Conference on Systems, Signals and Image Processing (IWSSIP) (pp. 1-4). IEEE.

[19] Khari, M., Shrivastava, G., Gupta, S., & Gupta, R. (2017). Role of cyber security in today's scenario. In Detecting and mitigating robotic cyber security risks (pp. 177-191). IGI Global.

[20] Patel, H. (2020). E-Commerce Security Threats, Defenses Against Attacks and Improving Security. Defenses Against Attacks and Improving Security (April 1, 2020).

[21] İlker, K. A. R. A., & AYDOS, M. (2019, October). Detection and Analysis of Attacks Against Web Services by the SQL Injection Method. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-4). IEEE.

[22] Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2022, August). Cyber-Security Culture Assessment in Academia: A COVID-19 Study: Applying a Cyber-Security Culture Framework to assess the Academia's resilience and readiness. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-8)

[23] Luminita, D. C. (2011). Information security in E-learning Platforms. Procedia-Social and Behavioral Sciences, 15, 2689-2693.

[24] Ghildiyal, P., & Awasthi, A. (2013). Encryption in E-Commerce. ZENITH International Journal of Multidisciplinary Research, 3(10), 126-136.

[25] Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International journal of information management, 55, 102171.

[26] Le, D. N., Kumar, R., Mishra, B. K., Chatterjee, J. M., & Khari, M. (Eds.). (2019). Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies. John Wiley & Sons.

[27] Pramanik, R., & Prabhu, S. (2022, March). Analysing Cyber Security and Data Privacy Models for Decision Making among Indian Consumers in an e-commerce environment. In 2022 International Conference on Decision Aid Sciences and Applications (DASA) (pp. 735-739). IEEE.

[28] bt Mohd, N. A., & Zaaba, Z. F. (2019). A review of usability and security evaluation model of ecommerce website. Procedia Computer Science, 161, 1199-1205.

[29] Odokuma, E. E., & Musa, M. O. Internet Threats and Mitigation Methods in Electronic Businesses Post Covid-19. International Journal of Computer Applications, 975, 8887.

[30] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2020). Generative adversarial networks. Communications of the ACM, 63(11), 139-144.

[31] Abadi, M., & Andersen, D. G. (2016). Learning to protect communications with adversarial neural cryptography. arXiv preprint arXiv:1610.06918.

[32] Coutinho, M., de Oliveira Albuquerque, R., Borges, F., Garcia Villalba, L. J., & Kim, T. H. (2018). Learning perfectly secure cryptography to protect communications with adversarial neural cryptography. Sensors, 18(5), 1306.