Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 15s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Review Of Intrusion Detection System In Various E-Commerce Platforms

Shabeena Nafees[1*], Anil Kumar Pandey[2], Satya Bhushan Verma[3]

[1*,2,3]Department of Computer Science and Engineering, Shri Ramswaroop memorial University, Barabanki, India, 225003.
Email ID: qds186@gmail.com, Email ID: anipandey@gmail.com, Email ID: satyabverma1@gmail.com

Cite this paper as: Shabeena Nafees, Anil Kumar Pandey, Satya Bhushan Verma, (2025) Review Of Intrusion Detection System In Various E-Commerce Platforms. *Journal of Neonatal Surgery*, 14 (15s), 1620-1632.

ABSTRACT

The twenty-first century has witnessed a rapid growth of technological advancements aiming to lead the world towards a new era of innovations. E-commerce is a phenomenal product of this innovatory stream, and its influence extends far beyond traditional retail. The application circle of e-commerce is widespread in almost every sector of our life, including areas such as healthcare, finance, education, and more, proving its validity and impact on our routine life vividly. E-commerce communications depend on modern devices such as laptops, personal computers, communication sensors, servers, switches, etc. The expanding domain of e-commerce applications is bringing the involvement of more communication devices, which raises a serious question about the security of the whole communication system. Integrating suspicious entities with the mainstream communication network may create malicious activities resulting in severe outcomes. Hence, we need a secure communication framework to ensure attack-efficient and reliable communication streams, especially in critical sectors like healthcare, where data privacy and system integrity are paramount. This paper reviews different efficient and secure electronic payment systems, with an emphasis on their application across various sectors, including healthcare, Supply chain.

Keywords: *Machine learning, e-commerce, malicious activity, threat detection framework, IDS*

1. INTRODUCTION

E-Commerce, also known as electronic commerce or internet commerce, refers to performing products, goods, or service-related transactions over the internet [1].

Since it offers a global and user-friendly set of technologies, the Internet is quickly replacing other networks as the preferred infrastructure for e-commerce and e-business. Numerous industries, including retail, wholesale, and manufacturing, make use of E-many commerce's useful uses [2]. Through the use of the Internet and electronic commerce, information about consumer habits, tastes, and demands may be gathered. As a result, this aids in marketing tasks like setting prices, negotiating, improving products' features, and fostering relationships with customers. Numerous retail and wholesale settings are ideal for implementing e-commerce [3].

E-retailing, sometimes known as "online retailing," is the practice of selling products directly to end users via specially built online stores that mimic traditional brick-and-mortar shops down to the last detail. E-commerce is widely utilized by the financial sector. Through E-banking or online banking, customers can view their savings and loan account balances, make transfers to other accounts, and even pay their bills. Online stock trading is another use for E-commerce [4]. There are a plethora of online resources where investors can gain knowledge about the market, including news, charts, company profiles, and analyst ratings. The logistics of a company's supply chain also benefit from the widespread adoption of electronic commerce. Some businesses band together to create an online marketplace where they can easily buy and sell items, share market data, and manage administrative tasks like stock management. When goods and services move quickly between companies, the economy as a whole benefit. The deployment of business models is hampered by several strategic and competitive concerns. Businesses may be hesitant to take part in widespread electronic exchanges out of concern that their competitors will gain access to proprietary information [5].Using the Internet's interactive features, businesses may get to know their customers better and provide better service all around. Web personalization allows businesses to tailor material to a user's browsing experience based on their preferences, and this includes technology that allows for the delivery of tailored information and advertisements through mobile commerce platforms [6]. Web sites, e-mail, and phone access to customer service professionals all allow businesses to save money while better serving their clientele. Online banking, often known as electronic banking or E-banking, is an electronic payment system that enables customers of a financial institution to perform financial transactions via the firm's website. Internet banking, e-banking, virtual banking, and other names all describe the same concept [7].

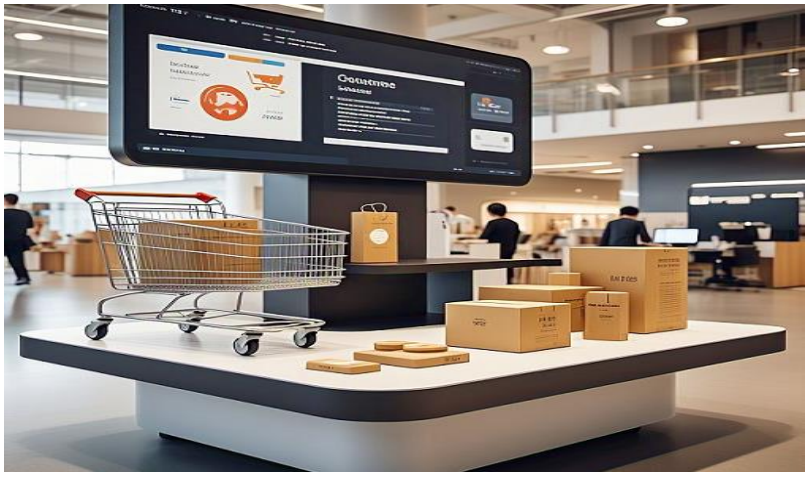

Figure 1: e-Commerce system

2. REVIEW OF APPROACHED USED FOR SECURITY IN E-COMMERCE

Table 1 : Review of Approached

S.No	Year	Publisher	Research Contributions	Strengths	Limitations
1	2022	Hindawi	Researchers have proposed a cloud-based infrastructure to provide efficient and secure transactional communications,	Efficient detection of security attacks	High resource utilization of the proposed system
2	2022	Wiley	A threat analysis framework is designed	End-to-End secure communication	Computation overhead increases
3	2022	Springer	An efficient communication model is presented	Prevention against malicious entities	Communication delay increases
4	2022	Elsevier	An AI-based secure and efficient communication mechanism is proposed	Attack detection and Prevention	Not suitable for resource-constrained environments
5	2021	IEEE	AI empowered threat detection model is designed	DDoS attack detection	It demands high resource consumption
6	2022	IJCSIS	A reliable E-Commerce management system is proposed	Botnet attack detection	Not suitable for large networks
7	2021	Elsevier	Blockchain-based security scheme is presented	Cyber attack prevention	Computational overhead increases
8	2021	IEEE	A privacy-preserving mechanism is designed	Secure communication tunnel	High resource consumption
9	2021	IEEE	A blockchain-based secure framework is formulated	Malicious traffic analysis	Higher latencies experienced

10	2020	IEEE	Smart communication mechanism for E-Commerce	Malware detection	Computational overhead
11	2020	Elsevier	An attack detection mechanism is presented	DoD, DDoS identification	Not compatible with large networks
12	2021	Elsevier	An efficient attack detection model is proposed	Protection against cyber threats	High resource consumption noticed

Md Arif Hassan et al. Presented E-commerce implies an electronic purchasing and marketing process online by using typical Web browsers. They specified to develop an efficient and secure electronic payment protocol for e-commerce where consumers can immediately connect with the merchant properly. Interestingly, their study does not require the customer to input his/her identity in the merchant's website even though the customer can hide his/her identity and make a temporary identity to perform the service. It has been found that their protocol has much improved security effectiveness in terms of confidentiality, integrity, non-repudiation, anonymity availability, authentication, and authorization.

Amjad Rehman Khan et al. proposes a cloud-based infrastructure to provide efficient and secure transactional communications, It provide an inclusive analysis of intrusion detection based on deep learning techniques followed by different intrusion detection systems. In this review, public network-based datasets of IDS are fully explored and analyzed. Deep learning techniques for IDS have been critically evaluated based on different performance metrics (accuracy, precision, recall, f-1 score, false alarm rate, and detection rate). Furthermore, existing challenges and possible solutions for networks security and privacy have been discussed.

Emad-ul-Haq Qazi et al. developed a non-symmetric deep auto-encoder for network intrusion detection problems and presents its detailed functionality and performance. The authors validate the robustness and effectiveness of the proposed NIDS using a benchmark dataset, i.e., KDD CUP'99. Our DL-based method is implemented in the Tensor Flow library and GPU framework, and it achieves an accuracy of 99.65%. Their stud can be used in network security research domains and DL-based detection and classification systems.

Imtiaz ullah and Qusay h. Mahmoud proposes design and develop a novel anomaly-based intrusion detection model for IoT networks. The proposed convolutional neural network model is validated using the BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23 intrusion detection datasets. Transfer learning is used to implement binary and multiclass classification using a convolutional neural network multiclass pre-trained model. Their study binary and multiclass classification models have achieved high accuracy, precision, recall, and F1 score compared to existing deep learning implementations.

S. Vinoth et al. used the most effective solution instructions to increase cloud security has become important for all cloud operations. This article examines several cloud computing applications in banking and e-commerce, as well as the security issues associated with them. Copyright 2022 Elsevier Ltd. All rights reserved. Selection and peer-review under responsibility of the scientific committee of the International Conference on Advances in Materials Science.

Rafał Kozik et al. Proposes an efficient Post Event Analysis and Incident Response procedure implemented with the use of graph databases and cyber threat intelligence platforms to raise the security capabilities of an organisation by granting the ability to relate current detection to both own past events and incidents reported by other organisations. This approach allows the user to gain a pre-emptive advantage over the malicious actors by learning from the experiences of others.

Idiano D'Adamo et al. Propose that European countries have different sensitivities to the issue of cyber-security, and among them it is possible to identify three groups with different levels of attention to the critical issues of e-commerce. The Netherlands, Sweden and Denmark belong to the group of countries most responsive to e-commerce. This request is part of a broader framework of transition toward sustainable development, i.e., a reliable digital environment where citizens and businesses can exercise their rights and freedoms in complete security.

Harikumar Pallathadka et al. Proposes machine learning and artificial intelligence applications in e-commerce, corporate management, and finance. Sales growth, profit maximization, sales forecast, inventory management, security, fraud detection, and portfolio management are some of the major uses. 2021 Elsevier Ltd. All rights reserved. Selection and peer-review under responsibility of the scientific committee of the International Conference on Nano electronics, Nano photonics, Nanomaterials, Nano bioscience & Nanotechnology.

Farahnaz Behgounia and Bahman Zohuri proposes innovative and dynamic sites utilizing artificial intelligence along with its sub-sets of machine learning drive by deep learning. Such implementation makes the total cost of ownership more revenue driven based upon return on investments for the owners of the site.

Mengyao Zhang et al. proposes the results extracted from the test have been collected to explain the concept and the role

of a data management system in an e-commerce organization using Block chain technologies. The experimental shows that the overall article activities in various parameters are Data Transaction Ratio is 85.46%, Encryption and Decryption time and the size of access ratio as 86.92%, Accuracy ratio as 80.8%, Storage overhead Ratio is 72.81%, and overall performance ratio is 92.30% is better than the previous research work.

3. CRITICAL ISSUES

This section environs multiple research contributions that have been made to ensure the efficiency and security of an e-commerce environment.

i. Network and Communication Security

The network and communication security of e-commerce environments is procuring significant attention these days, and a plethora of research contributions have been made in this regard. Here they discussed some of those research studies that are majorly focusing on the information and communication security of e-commerce networks. In recent years, various Intrusion Detection Systems (IDS) have been developed to address the growing prevalence of security and privacy concerns in most computer networks. Data confidentiality, integrity, and availability are all at risk if IDS protection fails. The goal of this research is to provide a thorough analysis of intrusion detection by comparing the findings acquired from different intrusion detection systems with those obtained using deep learning methods. In this study, researchers analyses and compare all publicly accessible IDS datasets based on networks. The effectiveness of several deep learning approaches for IDS has been thoroughly evaluated (accuracy, precision, recall, f-1 score, false alarm rate, and detection rate). Concerns of privacy and security in networks have also been analysed, along with possible solutions to these problems [8].

Another intrusion detection scheme is presented that is premised on deep learning principles and is specifically influenced by Convolutional Neural Networks (CNN). The authors state their intention to look into the existence of critical security threats in the IoT. To improve the efficiency of the proposed system, CICIDS2017 and UNSWNB15 datasets have been integrated. However, significantly high resource consumption is noticed which disqualifies it from being used in networks with resource constraints networks. In a combination with the BOT-IoT and MQTT-IoT-IDS2020 datasets, CNN is also acquired in an additional anomaly detection mechanism. The primary objective is to analyze network activity to highlight malfunctions in large-scale systems [9].

A combination of Single-Hidden Layer Feed-forward Neural Network (SLFN) and LSTM classifier is regarded as a viable option for clipping healthy features that have a higher likelihood of being used in threat detection. The IoT-ID20 dataset is acquired for training purposes, and the performance is evaluated on systematic performance metrics. The detection capability of the proposed framework is enhanced by employing three different classifiers: Decision Tree (DT), Multilayer Perceptron (MLP), and Long Short-Term Memory (LSTM). User-to-Root (U2R) attacks, Probe attacks, and Remote-to-Local (R2L) attacks are categorized as crucial security threats to the integrity of a communication system. Researchers have attained the Spider Monkey Optimization (SMO) algorithm and the Stacked Deep Polynomial Network (SDPN) algorithm to formulate a detection technique for such security issues. NSL-KDD is integrated for training the system, and on an evaluation scale, the proposed model has demonstrated considerable accuracy of 97% along with 95% precision for attack detection [10].

Researchers have created a threat detection scheme that incorporates Spider Vector Machine (SVM) and Naive Bayes classifiers. The system is trained on the NSL-KDD dataset and evaluated in a scalable virtual simulation environment. The proposed system detects attacks with a remarkable 98% accuracy. To identify potential security risks in IoT environments, researchers have adopted an LSTM technique to reduce the risk of security breaches. The training of the designed model is performed on a large collection of datasets including CIDCC-15, UNSW-NB15, and NSL-KDD. To further lessen the burden on the computer's resources, the proposed system incorporates bio-inspired Firefly Swarm Optimization (FSO) [11].

The authors propose an attack identification framework that conceals the best set of features for spotting threats. When it comes to screen features, Light GBM is used, while PPO2 and ReLU are used to bolster the security system's ability to identify potential dangers. Researchers develop just another intrusion detection technique enabled by reinforcement learning. In conjunction with the BOT-IoT dataset, binary classifiers and multiclass classifiers are used. The designed scheme achieves a respectable 99% accuracy in identifying abnormal traffic. For sequential data extraction, the most effective language models are the GRU classifiers. DoS attacks are accountable for degrading the system's overall performance by accumulating negative effects on its central resources. The NSL-KDD dataset is utilised in conjunction with a multi-CNN-based approach to design another threat detection framework. The simulation results validate the framework's compatibility; however, large-scale networks exhibit a notable degree of complexity [12].

ii. Cloud-based Solutions

One of the most impressive innovations, cloud computing has piqued the interest of computer scientists everywhere. While there are certainly benefits to using cloud computing, there are also significant security concerns that no business can afford to overlook. Successful adoption of Cloud Computing within an organisation requires forethought and an understanding of both existing and anticipated risks, threats, vulnerabilities, and countermeasures. So, all cloud operations must find the best

solution instructions to boost cloud security. Based on a survey of the existing literature, this study seeks to identify and evaluate the most pressing threats to cloud system networks and data security. However, a closer look reveals that virtualization adds extra software to the network system, which may have a negative influence on security. As data center hubs use software to connect their servers, any security breach could have far-reaching consequences. Since users have little say over the cloud's infrastructure, they must rely on pre-established channels of trust. Several banking and e-commerce cloud computing applications are examined along with related security concerns [13].

New ways of thinking about how to apply interconnected technology are now welcome. There has been a meteoric rise in the acceptance of both online shopping and IoT gadgets. The vast attack surface, however, is a cost of this exceptional popularity. The paper suggests implementing a strong procedure for Post Event Analysis and Incident Response. This approach involves linking ongoing threat detection to an organization's historical incidents as well as reported events from other entities. To enhance the organization's security capabilities, this procedure leverages graph databases and cyber threat intelligence platforms. By tapping into insights from various sources, the organization can proactively bolster its defenses against malicious actors.

By drawing on the insights of others, the user can acquire a head start against harmful actors [14].

The pandemic has led to a shift in people's behavior, causing them to change their preferences and avoid direct human interactions. This shift has significantly benefited the e-commerce sector. However, the comprehensive exploration of this phenomenon's intricacies has been lacking in existing literature. The research attempts to fill this knowledge vacuum by looking at how different European countries fare in terms of e-commerce, and also defined the most pressing obstacles to the further growth of this sector. They used a meticulous mashup of a Likert-scale survey and multi-criteria decision analysis (MCDA) to accomplish this goal. The first technique enables us to rank different European nations according to their success in e-commerce, while the second technique looks into the particular difficulties associated with online shopping.

The study's conclusions show that different European countries give the most urgent issues affecting global e-commerce varying levels of attention. The Netherlands, Sweden, and Denmark are among the nations that are most open to the advantages of online trade. This recommendation fits within the broader framework of achieving sustainable development, which includes building a safe online environment where people and organizations can freely exercise their civil liberties. Finally, this study makes a theoretical contribution by establishing a new benchmark for the literature on the state of e-commerce in Europe today in light of the pandemic's effects. Directors may [15].

iii. Artificial Intelligence-based Solutions

The ultimate objectives of using AI in the e-commerce and financial sectors are to establish reliable product quality control standards and discover new approaches to reach and serve customers at low cost. AI has been used to improve customer experience, streamline supply chain management, boost operational efficiency, and reduce team sizes. Deep learning and machine learning are two popular artificial intelligence techniques. Individuals, companies, and government agencies utilize these models to learn from data and anticipate the future. Machine learning models are now being developed for the food industry to handle the complexity and diversity of its data. This article concentrates on the use of machine learning and artificial intelligence in the financial industry, corporate management, and online enterprises, to name just a few. Some of the most common applications include boosting sales, increasing profits, making more accurate sales predictions, handling inventory, preventing theft, and maximising investment returns [16].

Due to the proliferation of mobile devices in recent years, there has been a shift toward conducting virtually all offline activities online. This facilitates our daily lives, but it also introduces various security vulnerabilities because of the Internet's decentralised and anonymous design. Malware can be avoided with the help of firewalls and antivirus software. However, sophisticated cybercriminals prey on customers' lack of security awareness by sending them to fake websites. There are numerous approaches to the difficult challenge of detecting phishing attempts on the market, such as using a blacklist, relying on rules-based detection, looking for anomalies, etc. The literature shows that modern works favour machine learning-based anomaly detection due to its dynamic structure, notably for detecting "zero-day" assaults. In this paper, a machine learning-based phishing detection system is proposed. Eight algorithms are used to assess URLs, and three datasets are used to compare the results to previous research. The results of the studies show that the models that are presented perform remarkably effectively.[17].

The next generation will expect such a shopping portal, given the ongoing transition from analogue to digital technology and the widespread adoption of digital technology in business. To be the most successful and profitable, modern e-commerce sites need to incorporate artificial intelligence and deep learning are added to machine learning. This is because most companies are moving away from static catalogues in favour of more dynamic platforms. These commercial sites now have more business resilience in this fiercely competitive market thanks to the site's approach. In this succinct message, they highlight a number of innovative, constantly evolving websites that utilize AI and the various branches of machine learning powered by deep learning. When implemented, this shifts the focus of the total cost of ownership from expenses to returns on investment made by the site's owners [18].

iv. Blockchain-based Solutions

Over the past two decades, IT has come to be seen as a progressive development with far-reaching effects on society at large. The advancement of technology has greatly improved people's living conditions. Data from various web apps are aggregated and analysed by IT staff. The data gathered is beneficial to management in making decisions. In this study, they take a closer look at the blockchain architecture for managing dynamic data in an online store and reveal its underlying structure (DDMS-BCM). Blockchain's ledger strengthens the system's potential to interact with cutting-edge information systems. A minimal security approach has been suggested to enhance the data handling capabilities of the E-Commerce platform. This study uses the Lightweight Security Scheme for E-commerce Data Management to forecast results from multiple earlier studies. An extensive examination of data management and business process reports is used to identify the analysis parameters. [19].

In the absence of a methodical approach to E-commerce security, it may be impossible to reap the benefits of online shopping. Even online marketplaces like Amazon and Alibaba have started employing these methods to safeguard customer information. The One-Time Password (OTP) is the most often used form of authentication for online purchases. Besides security and compliance, this system also boasts high availability and a high degree of scalability. The significance of various security techniques in the E-Commerce domain is also discussed [20].

Online marketplaces with built-in reputation management let buyers leave feedback on service providers after a transaction has been completed. In the current reputation system, the central server is not protected from arbitrary reputation changes to the provider. In addition, they don't provide inter-service access to your reputation. Since rating actions are correlated with personal information, rates are vulnerable to privacy breaches (e.g., identity and rating). At the same time, malicious raters may launch multiple rating attacks or other types of aberrant rating attacks [21].

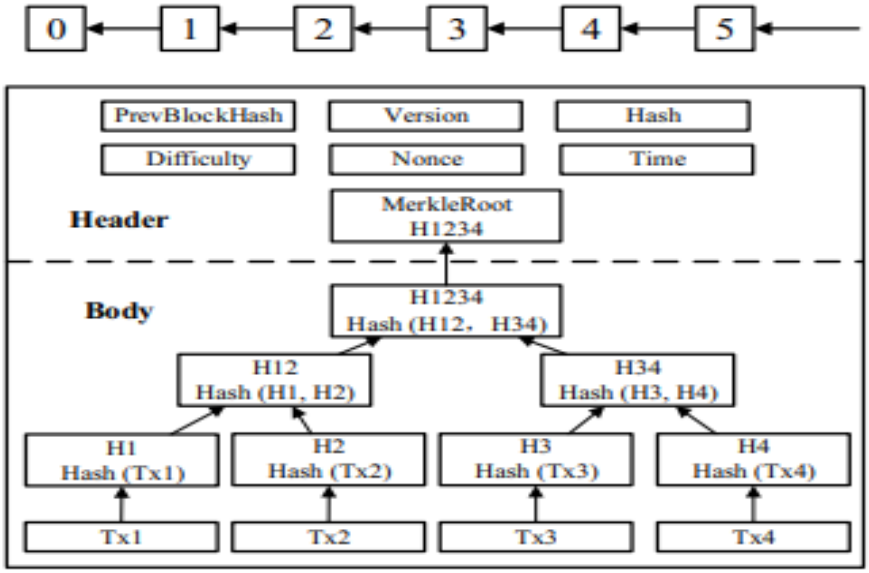

Figure 2 :Block chain Logic Structure

4. SOME OTHER SOLUTIONS

Unfortunately, online transactions are vulnerable to cybercrimes like phishing and cracking, which can result in unhappy customers who report financial losses as a result of their concerns about their personal information's safety. This study aims to ascertain customers' level of worry over the privacy and security of their personal information in relation to online transactions.. This research demonstrates that customer happiness and confidentiality are key components to gaining consumers' trust. However, data privacy and security have a bearing on customer happiness [22].

This study aims to investigate the impact of the 5G Internet of Things on the reliability and safety of agricultural products purchased online. This study focuses on the key technologies of the 5G Internet of Things and how they might be applied to build a circulation information system for agricultural products in order to accomplish real-time positioning, information sharing, and supply chain security. In an experimental study, it was discovered that the e-commerce sector's revenue growth rate was 30%. They study that the 5G Internet of Things is at least largely responsible for the improvement in the quality of e-commerce goods. [23].

In light of the devastating effects of the Pandemic of COVID-19 on commercial activity, this research proposes a methodical methodology for investigating the link between consumers' perceptions of the efficiency of e-commerce platforms (PEEP) and their subsequent behavior concerning the economy. The conceptual model in this investigation was founded on the idea

of uses and pleasure, and a boundary condition of pandemic anxiety was added for clarification. This investigation relies heavily on quantitative survey data and statistical analysis [36]. Using the PLS analytic method on a sample of 617 online customers, this study finds that the correlations between PEEP, economic advantages, and sustainable consumption are moderated by pandemic anxiety. This study contributes by analysing the role of economic gain as a moderator between PEEP and sustainable consumption, a relationship that hinges on one's level of pandemic apprehension. Management and theoretical implications are also examined [24].

The expanding tendencies of e-commerce provide ample chances for the incorporation of new technology. This phenomenon improves engagement with the new anonymous technologies in an indirect manner. Every day, many breaches in computer systems are announced around the globe. While some breaches are relatively minor in terms of the amount of data or funds compromised, many others are catastrophic [37]. Network security is to protect the underlying networking infrastructure from assault, misuse, malfunction, manipulation, destruction, and improper disclosure. If these safeguards are in place, communication devices can perform their important functions without jeopardizing the integrity of the system [25].

When users have access to sensitive information across a shared network in a typical e-commerce setting, network security must always be a top priority. Since there is no such thing as a completely secure network, it is crucial to establish a trustworthy and effective network security solution to safeguard crucial client data. With a dependable network security solution in place, businesses are less susceptible to hacking and other types of data theft. Priority number one is protecting a network from intruders like spyware on your workstations. Additionally, it ensures the confidentiality of any information shared between parties [26].

Network security infrastructure can protect against cyber-attacks and other forms of eavesdropping by encrypting data at many stages of transmission and transmitting it via numerous paths. However, I identified numerous chances to enhance the effectiveness of a resource-constrained e-commerce ecosystem. Various pieces of study have been undertaken over the past few years to propose some relevant security methods to improve the dependability of an e-commerce system. In terms of resource-constrained e-commerce platforms, however, there is still ample room for development. The term resource-constrained describes devices or networks having restricted available resources. The restricted availability of resources requires careful consideration. Consequently, it is difficult to build an adequate security solution to improve the efficiency of a network with limited resources. In this study, they intend to develop a more effective and secure defensive mechanism for such e-commerce communications [27].

5. POSSIBLE SOLUTION

Authors proposed an Intrusion detection framework by incorporating renowned machine learning techniques to ensure the efficiency and robustness of an E-commerce environment. To ensure effective communication that is safe in resource-constrained e-commerce communications, Machine learning-based solutions are seen to be the best option. On a large dataset, a traditional machine learning mechanism-based framework is initially trained [38]. The concerned dataset contains the impressions of all frequently occurring attacks in that particular environment. After finalizing the training the system is placed in real-life communications where it can capture identical impressions. In this way, the identification of any malicious activities becomes easy which tends to make an efficient and resource-constrained E-commerce communication environment.

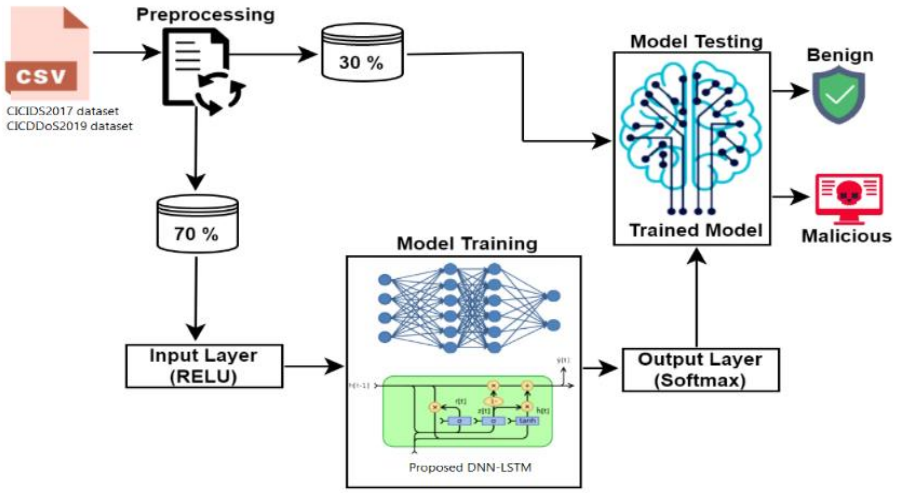

Figure 3: (Proposed Threat Detection Framework)

6. SIMULATIONS SETUP

The empirical performance test of the suggested scheme will be carried out on a computer system of the 8th generation equipped with a 3.33 GHz CPU, 16 GB RAM, and the Windows 10 operating system. The Graphical Processing Unit (GPU) that will used for simulations is a Geforce-1060, and it comes preloaded with the programming language Python as well as the Numpy, Tensorflow, Pandas, and Keras libraries. Scikitlearn is also installed on this GPU. In addition, a rundown of the experimental design can be seen in Table 2:

Table 2: Experimental Setup

Processor	I7, (3.33 GHz)
OS	Windows 10
RAM	16 GB
Language	Python
GPU	Geforce-1060
IDE	Spyder
Generation	8th
Libraries	Numpy, Tensorflow, Pandas, Keras, and Scikitlearn

7. PERFORMANCE PARAMETERS

Table: 3 contains the major performance parameters that we are planning to evaluate the performance of proposed threat detection framework.

Table: 3 Performance Parameters

#	Performance Parameters
1	Threat Detection Accuracy
2	Precision
3	Recall
4	F-Score
5	Cross Validation
6	Confusion Matrix
7	ROC
8	True Positive Rate
9	True Negative Rate
10	False Positive Rate
11	False Negative Rate
12	False Detection Rate
13	Training Time
14	Testing Time

8. RESEARCH GAP

I have studied more than 30 research studies published by various prestigious platforms i.e. IEEE, ELSEVIER, Springer, Hindawi, ACM etc. for the years 2020, 2021 and 2022. All research studies were conducted in the same research domain and various security solutions were proposed to ensure a secure and efficient e-commerce environment. After a critical analysis, we found ample room for improvement as those previously proposed solutions were targeting large-scale stable networks. I decided to design a Machine Learning-based novel and secure Intrusion Detection Framework to improve the efficiency of Resource-Constrained E-commerce Environments. The term resource-constrained refers to describe the devices or a network with limited resources. The limited availability of resources demands significant attention. And hence, designing an appropriate solution to enhance the efficiency of such a resource-constrained network becomes a challenging task. In this research, I aim to improve an efficient and secure defensive mechanism for such E-Commerce communications.

9. SIGNIFICANCE OF RESEARCH

Because cyber attacks can lead organisations to lose money, data, and even their existence, cyber security is crucial for online transactions. Those who would steal from businesses online employ sophisticated methods. When conducting business online, it's important to safeguard not only your information but also that of your clients [28]. The loss of sensitive client data could result from a breach in your cyber security systems. In the end, that could destroy the credibility of your company. Here are some measures one may take to improve the safety of an online shop. E-commerce keeping e-commerce assets safe from tampering, destruction, or disclosure is the goal of security. The three pillars of CIA—information confidentiality, integrity, and availability—should serve as the foundation for any effective e-commerce security strategy [29]. The possibility of white-collar crimes rises in tandem with the popularity of online shopping since more people have access to the means to breach the system's security. The banking industry's provision of Internet Banking as a convenient and adaptable method of online payment for e-commerce is not without its drawbacks, however, just as every coin has two sides. Companies today invest billions of dollars in computer security, with the main concern being the prevention of fraud [30].

10. OVERVIEW OF RESEARCH

When it comes to consumer information, privacy means blocking any efforts that could lead to its disclosure to unrelated parties. The chosen online retailer should be the only one to view a customer's billing details or social security number. Vendors violate confidentiality agreements when they offer outside parties access to sensitive data. Any internet firm must have anti-virus software, a firewall, encryption, and other data security safeguards. [31]. It will be very beneficial in protecting client financial information. Internet store safety also relies on another important principle: integrity. This refers to the practice of preventing unauthorized parties from altering sensitive customer data stored online.

According to this principle, an online store must use consumers' data in its original form, without alterations. Any tampering with the information will cause a customer to lose trust in the reliability of the business. The requirement that both the buyer and the seller be who they say they are is a cornerstone of secure online transactions. In a perfect world, they would be who they claim to be. The business must demonstrate that it is reputable, sells genuine goods, and offers the services it promotes. The buyer must additionally give identity in order for the vendor to feel comfortable with the online purchase [32].

It is possible to ensure authentication and identification. If you are unable to, hiring a professional could be quite helpful. Examples of typical solutions include credit card PINs and client login information. Privacy involves thwarting any actions that would result in the disclosure of customer information to unaffiliated parties. Nobody else ought to [33].

This refers to the practice of preventing unauthorized parties from altering sensitive customer data stored online. According to this principle, an online store must use consumers' data in its original form, without alterations. Any tampering with the information will cause a customer to lose trust in the reliability of the business. The requirement that both the buyer and the seller be who they say they are is a cornerstone of secure online transactions. In a perfect world, they would be who they claim to be. The business must demonstrate that it is reputable, sells genuine goods, and offers the services it promotes. The buyer must also present identification in order for the merchant to feel comfortable with the online transaction. It is possible to ensure authentication and identification.

If you are unable to, hiring a professional could be quite helpful. Examples of typical solutions include credit card PINs and client login information [34]. As a result, the legal doctrine known as the principle of non-repudiation tells parties to a transaction not to retract their actions. Both the company and the buyer must complete their respective parts of the deal. Online shopping might make some people feel unsafe because there is no human presence [35].

11. METHODOLOGY

This study conducts a systematic literature review of the different ML- and DL-based NIDS and investigates the published journal articles between 2020 to 2023.This research work will propose an Intrusion Detection System (IDS) based on Machine Learning. The specific datasets that contain impressions of security threats will be used to train our proposed Intrusion Detection Framework. Once the system will be trained, it will be deployed in a run-time environment where it will

investigate the presence of relevant suspicious entities/security threats in E-commerce communications. The performance of the proposed solution will be tested will some state-of-the-art benchmarked schemes under diversified performance metrics. The study comprised two main objectives. In the first stage I will discovered the current challenges in the e-commerce environment as well as the root cause to create such challenges. There exist a wide space of improvements in this research area, as researchers have proposed various solution for the security of generic e-commerce environments. However, the security of resource-constrained e-commerce environments is still a challenging task that demands significant security solutions.

In the second stage, I present security solution to ensure secure and reliable communication in resource-constrained e-commerce environments which will acquire the basic concepts of deep learning for formulating our proposed intrusion detection model. The proposed system will be formulated using two deep learning algorithms Deep Neural Network and Long Short Term Memory. The proposed system will be initially trained on two comprehensive datasets that contain the impressions of frequently occurring security threats in e-commerce communication. The datasets used in our research are CIC-IDS2017, and CIC-DDoS 2019.

In the third step, I will evaluate the performance of in terms of several performance criteria, the proposed model. The performance of the proposed IDS will then be compared with some benchmarked schemes to get a valid idea about its actual performance. proposed model will be compared from other algorithms. The major approaches used in our research are projected in Figure 4, and a detailed elaboration of these approaches can be seen in Figure 5:

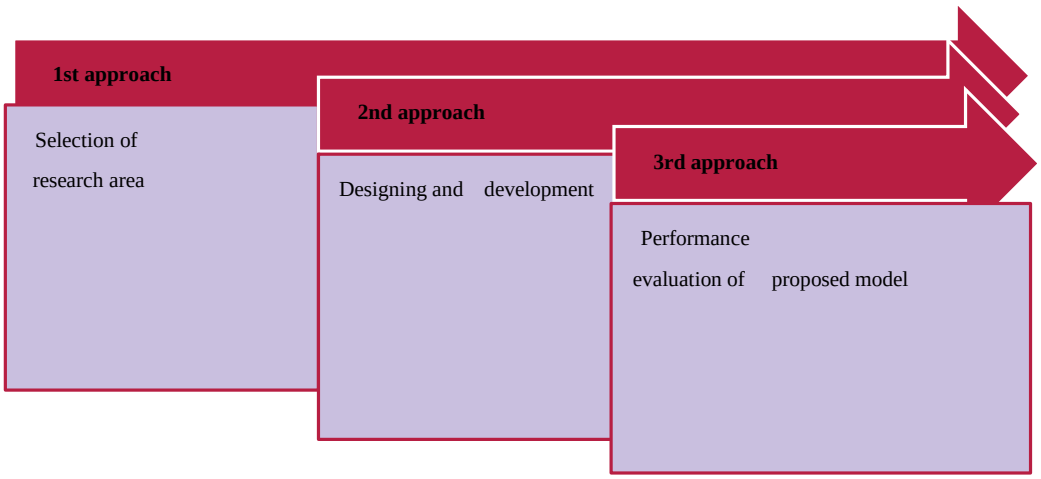

Figure 4 (Major approaches in our Research)

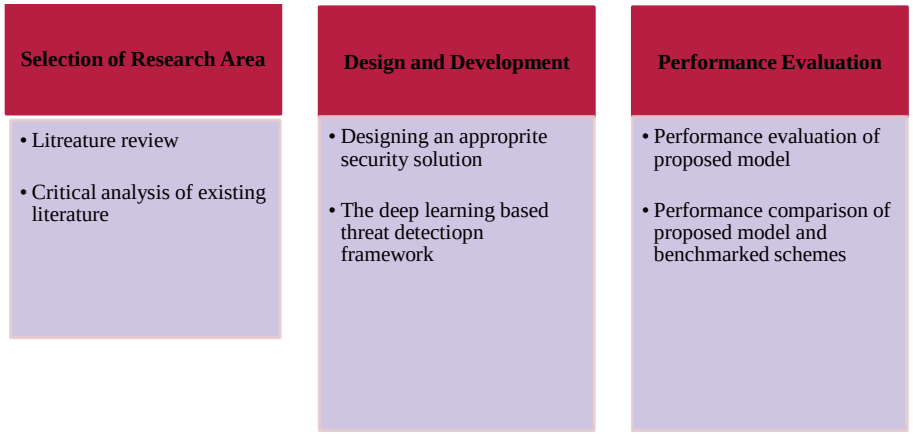

Figure 5 (Details of research and developmental approaches)

S.No	Different methodology	Advantage	Disadvantage/ Limitation
1	Researchers have proposed a cloud-based infrastructure to provide efficient and secure transactional communication.	Efficient detection security attacks	High resource utilization of the proposed system
2	A threat analysis framework is designed	End-to-End secure communication	Computation overhead increases
3	An efficient communication model is presented	Prevention against malicious entities	Communication delay increases
4	An AI-based secure and efficient communication mechanism is proposed	Attack detection and Prevention	Not suitable for resource- constrained environments
5	AI empowered threat detection model is designed	DDoS attack detection	It demands high resource consumption
6	A reliable E-commerce management system is proposed	Botnet attack detection	Not suitable for large network
7	Block chain-based security scheme is presented	Cyber-attack prevention	Computational overhead increases
8	A privacy-preserving mechanism is designed	Secure communication tunnel	High resource consumption
9	A block chain-based Secure framework is formulated	Malicious traffic analysis	Higher latencies experienced
10	Smart communication mechanism for E-Commerce	Malware detection	Computational overhead
11	An attack detection mechanism is presented	DoD,DDoS identification	Not compatible with large networks
12	An efficient attack detection model is proposed	Protection against cyber threats	High resource consumption noticed

This table summarizes 12 research papers/methodologies for secure E-commerce, highlighting their advantages (e.g., attack detection, secure communication) and disadvantages (e.g., high resource utilization, computational overhead).

Conclusion and Future Scope

In this paper, I presented a survey covers the current level of machine learning-based classifiers for threat detection in large-scale e-commerce, with a focus on methods for identifying malicious activities. I selected 12 papers in the literature that proposed specific a good machine algorithm to detect malicious activity with high accuracy and detection rate in a crucial area like malicious activity detection. As future research, researchers may focus on the following issues: detection method, IDS placement strategy, security threat, and validation strategy.

A rising quantity of research will be done in the future on machine learning-based Android virus detection. New frameworks and algorithms that are quick, quick, and powerful enough to detect malicious behavior should be proposed. I intend to assess the performance of the suggested model in terms of attack detection accuracy, precision, recall, and f1-score based on the evaluated publications.

As future research, researchers may plan to propose an Intrusion Detection Framework by incorporating renowned machine learning techniques to ensure the efficiency and robustness of an E-Commerce environment.

REFERENCES

[1] F. Fernández-Bonilla, C. Gijón, and B. J. T. P. De la Vega, “E-commerce in Spain: Determining factors and the importance of the e-trust,” Telecommunications Policy vol. 46, no. 1, pp. 102280, 2022.

[2] I. Zennaro, S. Finco, M. Calzavara et al., “Implementing E-Commerce from Logistic Perspective: Literature Review and Methodological Framework,” Sustainability vol. 14, no. 2, pp. 911, 2022.

[3] A. H. Mohamad, G. F. Hassan, and A. S. J. A. S. E. J. Abd Elrahman, "Impacts of e-commerce on planning and designing commercial activities centres: A developed approach," Ain Shams Engineering Journal, vol. 13, no. 4, pp. 101634, 2022.

[4] Q. Hu, T. Lou, J. Li et al., “New practice of e-commerce platform: Evidence from two trade-in programs,” vol. 17, no. 3, pp. 875-892, 2022.

[5] M. Zeng, R. Liu, M. Gao et al., "Demand forecasting for rural E-commerce logistics: a grey prediction model based on weakening buffer operator," Mobile information systems vol. 2022, 2022.

[6] S. Escursell, P. Llorach-Massana, and M. B. J. J. o. c. p. Roncero, “Sustainability in e-commerce packaging: A review,” Journal of cleaner production, vol. 280, pp. 124314, 2021.

[7] M. Kolotylo-Kulkarni, W. Xia, and G. J. J. o. B. R. Dhillon, “Information disclosure in e-commerce: A systematic review and agenda for future research,” Journal of Business Research vol. 126, pp. 221-238, 2021.

[8] H. Yu, Y. Zhao, Z. Liu et al., “Research on the financing income of supply chains based on an E-commerce platform,” Technological Forecasting and Social Change, vol. 169, pp. 120820, 2021.

[9] T. Tokar, R. Jensen, and B. D. J. B. H. Williams, “A guide to the seen costs and unseen benefits of e-commerce,” A guide to the seen costs and unseen benefits of e-commerce., vol. 64, no. 3, pp. 323-332, 2021.

[10] B. Givan, R. Wirawan, D. Andriawan et al., “Effect of Ease And Trustworthiness To Use E-Commerce for Purchasing Goods Online,” International Journal of Educational Research & Social Sciences, vol. 2, no. 2, pp. 277-282, 2021.

[11] K. Zong, Y. Yuan, C. E. Montenegro-Marin et al., “Or-based intelligent decision support system for e-commerce,” Journal of Theoretical and Applied Electronic Commerce Research, vol. 16, no. 4, pp. 1150-1164, 2021.

[12] S. Elia, M. Giuffrida, M. M. Mariani et al., “Resources and digital export: An RBV perspective on the role of digital technologies and capabilities in cross-border e-commerce,” Journal of Business Research, vol. 132, pp. 158-169, 2021.

[13] R. K. Jamra, B. Anggorojati, D. I. Sensuse et al., "Systematic Review of Issues and Solutions for Security in E-commerce." pp. 1-5.

[14] M. A. Hassan, Z. Shukur, and M. K. J. c. Hasan, “An efficient secure electronic payment system for e-commerce,” computers, vol. 9, no. 3, pp. 66, 2020.

[15] J. Wang, "Research on the Construction of Integrated Management Information System for E-commerce Enterprises Based on Cloud Computing." pp. 1039-1042.

[16] H. Treiblmaier, C. J. E. C. R. Sillaber, and Applications, “The impact of blockchain on e-commerce: a framework for salient research topics,” vol. 48, pp. 101054, 2021.

[17] R.-C. Härting, and C. Reichstein, "Potential Use of Bitcoin in B2C E-commerce." pp. 33-40.

[18] J. Zhang, S. Nazir, A. Huang et al., “Multicriteria decision and machine learning algorithms for component security evaluation: library-based overview,” Security and Communication Networks 2020, vol. 2020, 2020.

[19] S. Vinoth, H. L. Vemula, B. Haralayya et al., “Application of cloud computing in banking and e-commerce and related security threats,” Materials Today: Proceedings, vol. 51, pp. 2172-2175, 2022.

[20] R. Kozik, M. Pawlicki, M. Szczepański et al., "Efficient Post Event Analysis and Cyber Incident Response in IoT and E-commerce Through Innovative Graphs and Cyberthreat Intelligence Employment." pp. 257-266.

[21] I. D’Adamo, R. González-Sánchez, M. S. Medina-Salgado et al., "E-commerce calls for cyber-security and sustainability: How European citizens look for a trusted online environment," Sustainability, vol. 13, no. 12, pp. 6752, 2021.

[22] H. Pallathadka, E. H. Ramirez-Asis, T. P. Loli-Poma et al., “Applications of artificial intelligence in business management, e-commerce and finance,” Materials Today: Proceedings, 2021.

[23] M. Korkmaz, O. K. Sahingoz, and B. Diri, "Detection of phishing websites by using machine learning-based URL analysis." pp. 1-7.

[24] F. Behgounia, B. J. I. J. o. C. S. Zohuri, and I. Security, “Machine Learning Driven An E-Commerce,” International Journal of Computer Science and Information Security (IJCSIS), vol. 18, no. 10, 2020.

[25] M. Zhang, L. Lin, and Z. J. C. C. Chen, “Lightweight security scheme for data management in E-commerce platform using dynamic data management using blockchain model,” Lightweight security scheme for data management in E-commerce platform using dynamic data management using blockchain model." Cluster Computing (2021): 1-15., pp. 1-15, 2021.

[26] N. L. Bhatia, V. K. Shukla, R. Punhani et al., "Growing Aspects of Cyber Security in E-Commerce." pp. 1-6.

[27] M. Li, L. Zhu, Z. Zhang et al., “Anonymous and verifiable reputation system for E-commerce platforms based on blockchain,” IEEE Transactions on Network and Service Management, vol. 18, no. 4, pp. 4434-4449, 2021.

[28] M. J. Girsang, R. Hendayani, and Y. Ganesan, "Can Information Security, Privacy and Satisfaction Influence The E-Commerce Consumer Trust?." pp. 1-7.

[29] Z. Zhu, Y. Bai, W. Dai et al., “Quality of e-commerce agricultural products and the safety of the ecological environment of the origin based on 5G Internet of Things technology,” Environmental Technology & Innovation 22 (2021): 101462., vol. 22, pp. 101462, 2021.

[30] L. T. T. J. J. o. R. Tran, and C. Services, “Managing the effectiveness of e-commerce platforms in a pandemic,” Journal of Retailing and Consumer Services 58 (2021): 102287, vol. 58, pp. 102287, 2021.

[31] Z. Zhu, Y. Bai, W. Dai et al., “Quality of e-commerce agricultural products and the safety of the ecological environment of the origin based on 5G Internet of Things technology,” Environmental Technology & Innovation, 22, 101462., vol. 22, pp. 101462, 2021.

[32] M. H. Gouthier, C. Nennstiel, N. Kern et al., “The more the better? Data disclosure between the conflicting priorities of privacy concerns, information sensitivity and personalization in e-commerce,” Journal of Business Research vol. 148, pp. 174-189, 2022.

[33] O. Saritas, P. Bakhtin, I. Kuzminov et al., "Big data augmented business trend identification: the case of mobile commerce," Scientometrics 126.2 (2021): 1553-1579., vol. 126, no. 2, pp. 1553-1579, 2021.

[34] J.-P. A. Yaacoub, O. Salman, H. N. Noura et al., “Cyber-physical systems security: Limitations, issues and future trends,” Microprocessors and microsystems 77 (2020): 103201., vol. 77, pp. 103201, 2020.

[35] M. Aliyu, M. Umar, N. J. S. J. o. S. Salisu et al., “Assessing User’s Perception on Security Challenges of Selected E-Commerce Websites in Nigeria,” SLU Journal of Science and Technology, 4(1&2), 177-187., vol. 4, no. 1&2, pp. 177-187, 2022.

[36] Verma, S.B., Yadav, A.K. (2021). Hard Exudates Detection: A Review., Emerging Technologies in Data Mining and Information Security. Advances in Intelligent Systems and Computing, vol 1286. Springer, Singapore. https://doi.org/10.1007/978-981-15-9927-9_12

[37] SB Verma, Brijesh P., and BK Gupta, Containerization and its Architectures: A Study, ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, Vol. 11 N. 4 (2022), 395-409, eISSN: 2255-2863, DOI: https://doi.org/10.14201/adcaij.28351

[38] Anamika Agarwal, S. B. V., B. K. Gupta, A Review of Cloud Security Issues and Challenges, ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, Issue, Vol. 12 N. 1 (2023), pp 1-22, eISSN: 2255-2863, 2023, https://doi.org/10.14201/adcaij.31459