Explainable AI and Block chain for Cyber Resilient Online Retail: A Framework for Enhanced Security and Trust

S Syed Abuthahir, G Jagan Naik, K. Damodhar Rao, Janjhyam Venkata Naga Ramesh, Pradeep Jangir, Kuchipudi Prasanth Kumar

***Abstract*—Online retail platforms frequently encounter challenges such as cyberattacks, data breaches, device malfunctions, and operational disruptions. These issues have intensified in recent years, highlighting the urgent need for businesses to prioritize resilience. Traditional cybersecurity systems are increasingly ineffective against sophisticated cyber threats. In response, we propose a novel resilience framework that combines Explainable Deep Learning with a Blockchain-based consensus mechanism. This approach enhances cyber incident response by enabling faster problem detection, transparent identification of exploited features and vulnerabilities, and more informed decision-making. By integrating these technologies, our solution offers significant improvements in resilience. To validate our method, we trained and preprocessed data using National Accounting Bureau datasets and tested the framework on real-world online retail platforms. The results demonstrate enhanced business continuity, stronger cyber resilience, and improved decision-making capabilities.**

***Index Terms*— Explainable deep learning, Blockchain technologies, Cyber resilience, Online retailing platforms, Operations continuity.**

I. Introduction

THE Technological advancements in sectors such as the Internet of Things (IoT), Cloud Computing, and Big Data have significantly propelled the growth of the online retail supply chain. This surge has led to more efficient and autonomous production processes, enabling consumers not only to purchase but also to resell products that may be otherwise unavailable [1]. As a result, online retailers have become pivotal players in the global economy, offering enhanced purchasing transparency, reduced costs, and unprecedented convenience [2]. Despite this progress, the industry continues to face notable challenges, including vague product descriptions, price inflation due to intermediaries, and critical concerns related to cybersecurity and consumer trust [3]. In response to the escalating threat landscape, particularly cybersecurity incidents, online merchants are increasingly investing in strategies to enhance cyber resilience (CR) [4]. Effective incident management requires strategies capable of detecting, containing, mitigating, and recovering from disruptions rapidly to maintain operational performance and productivity. To achieve this, strategies must emphasize agility, scalability, and robust cybersecurity, which are essential for optimizing operational efficiency and sustaining competitive advantage [5]. Consequently, online retailers are now prioritizing the fortification of their systems against cyber threats while simultaneously enhancing their decision-making frameworks in the face of cyber disruptions [6]. Key CR capabilities include redundancy, anomaly detection, inter-organizational collaboration, and structured recovery processes.

However, a critical gap remains in the literature regarding online retail, even amidst research into cutting-edge technologies such as cloud computing and artificial intelligence (AI) in customer relationship management. While secure data storage and real-time anomaly detection are vital for ensuring transaction authenticity and transparency, these elements are often underrepresented in existing studies, which tend to focus primarily on post-disruption recovery strategies [7]. Additionally, the sophisticated challenges posed by advanced persistent threats (APTs) remain insufficiently addressed in the current body of research. The emergence of Blockchain Technology (BT) has catalyzed a transformation across multiple industries by offering unmatched levels of security, transparency, and operational efficiency. Its integration into e-commerce is especially promising, providing a robust infrastructure for secure transactions and streamlined supply chain management. Despite its growing adoption, further research is warranted into Blockchain-based Retail Platforms (BRP), particularly in relation to CR. The unique advantages and implementation challenges of Blockchain for enhancing corporate accountability in e-commerce form the core motivation behind this study [8].

This research addresses the existing knowledge gap by

Manuscript received November 7, 2024; revised August 19, 2025.

S Syed Abuthahir is an Assistant Professor of Computational Intelligence Department, School of Computing, SRMIST, KTR, Chennai 603203, Tamilnadu, India (e-mail: drsyedabuthahir@rediffmail.com).

G Jagan Naik is a Professor of Computer Science and Engineering (Data Science) Department, CMR Institute of Technology, Hyderabad, Telangana, India (e-mail: gjnaik1106@gmail.com).

K. Damodhar Rao is a Professor of Computer Science and Engineering Department, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India (e-mail: damodhar.k@sreenidhi.edu.in).

Janjhyam Venkata Naga Ramesh is an Adjunct Professor of Computer Science and Engineering Department, Graphic Era Hill University, Dehradun, India (e-mail: jvnramesh@gmail.com).

Pradeep Jangir is an Assistant Professor of Biosciences Department, Saveetha School of Engineering. Saveetha Institute of Medical and Technical Sciences, Chennai, India (e-mail: pkjmtech@gmail.com).

Kuchipudi Prasanth Kumar is an Assistant Professor of Computer Science and Engineering Department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India (e-mail: kprashanth510@gmail.com).

proposing a comprehensive Cyber Resilience Strategy (CRS) tailored specifically for BRPs. Our approach combines the robust security of a Private Blockchain Consensus Protocol (BCP) with the predictive strength and transparency of Explainable Deep Learning (XDL). This integrated framework aims to minimize the ripple effects of cyber disruptions, accelerate recovery, and reduce interruption-related costs. Representing a pioneering fusion of XDL and Blockchain within the realm of CR for online retail platforms, this study offers meaningful contributions to academic discourse and practical guidance for industry professionals. By providing actionable insights, the study supports improved decision-making and the realization of Sustainable and Secure Cyber Practices (SSCP). Furthermore, an empirical investigation involving several online retail enterprises across North Africa will validate the proposed framework. This dual contribution not only highlights the limitations of traditional CR methods but also presents a forward-looking model that integrates advanced technologies to enhance resilience in online retail [9].

II. Literature review

A. Cyber resilience for online retailers

Online merchants offer a comprehensive software-based solution that enables users to remotely browse, select products, and complete transactions. However, ensuring secure and uninterrupted product delivery requires resilient and well-protected supply chain networks. Online retail platforms are increasingly vulnerable to a wide range of cyber threats, including injection attacks, Distributed Denial of Service (DDoS) attacks, and Advanced Persistent Threats (APTs), all of which can compromise system availability, data confidentiality, and integrity. Injection attacks, in particular, pose a substantial risk. In 2021, they accounted for approximately 40% of all web application attacks, making them one of the most widespread threats to online businesses [9]. These attacks involve embedding malicious code into web applications, often enabling unauthorized access or manipulation of sensitive data. Due to their stealthy nature, injection attacks are difficult to detect and mitigate, leaving online retailers especially exposed.

DDoS attacks also present serious concerns, as they can render online platforms inaccessible to legitimate users, severely damaging both the financial performance and reputation of a business. According to Mittal et al. [10], the growing complexity and sophistication of DDoS attacks have made their detection and prevention increasingly difficult. Among all threats, Advanced Persistent Threats (APTs) represent the most severe and enduring risk. These attacks utilize highly sophisticated techniques and often exploit zero-day vulnerabilities to infiltrate systems and target specific individuals or organizations. APTs can cause extensive damage by compromising sensitive customer information, depleting financial resources, and significantly harming brand reputation. Research by the European Union Agency for Cybersecurity (EUAC) [11] has shown that conventional security measures are insufficient to defend against APTs, particularly in the retail and supply chain sectors. Despite the growing awareness of these risks, many proposed cybersecurity solutions remain theoretical or based on simulations that lack validation through real-world experimentation. Consequently, their applicability to actual online retail environments remains questionable. Moreover, existing studies often focus broadly on supply chain security rather than addressing the specific requirements of online retail systems, particularly those built on Blockchain infrastructure.

Currently, many online retailers lack a clear and actionable strategy for responding to cyberattacks, despite the availability of various detection and prevention methods [12]. A strategic, well-defined response plan is essential not only to minimize damage during an attack but also to restore customer trust in its aftermath. A more holistic and practical approach to Cyber Resilience (CR) is required—one that extends beyond mitigation and encompasses proactive readiness and rapid recovery. Azadeh et al. [13] emphasize the need for innovative CR strategies within e-commerce supply chains, while Annarelli et al. [14] stress the importance of CR in enhancing risk awareness and reducing the likelihood of supply chain incidents. Nonetheless, CR continues to be a significant challenge for online businesses. In a constantly evolving threat landscape, it is imperative for online retailers to adapt and strengthen their crisis response mechanisms to maintain operational continuity and competitive advantage.

B. Cyber resilience for Blockchain-based online retailers

Blockchain Technologies (BTs) are driving a substantial transformation in the field of online trading by enhancing trust, transparency, and security. Unlike traditional centralized systems, BT operates on a decentralized and tamper-resistant framework, ensuring the authenticity of transactions and peer-to-peer communications without the need for third-party validation [15], [16]. This inherent design addresses critical privacy and security concerns within supply chains while promoting transparent and auditable interactions [17], [18]. The integration of robust security features significantly reduces the risk of fraud across the entire supply chain, safeguarding data confidentiality and integrity [19], [20]. Emerging research highlights the vital role of Blockchain in advancing Cyber Resilience (CR). Studies have demonstrated BT's potential to strengthen defenses against cyberattacks. For instance, Lohmer et al. [21] examined resilience metrics in blockchain-coordinated supply chains, comparing two models—one incorporating Blockchain coordination and one without. The results indicated a notable improvement in CR in the Blockchain-enhanced model. Similarly, Shukla and Shyam [22] introduced a Blockchain-based architecture designed to improve consumer responsiveness in e-commerce systems. Their framework leveraged a decentralized and tamper-proof infrastructure to ensure secure data storage and reliable transaction processing.

Further exploration by Singh et al. [23] emphasized Blockchain's contribution to supply chain CR through the integration of data encryption, smart contracts, and consensus mechanisms, thereby establishing a secure and transparent platform for supply chain operations. However, despite these advances, integrating communication technologies with supply chain management continues to present chal-

lenges—especially in the online retail sector. High transaction volumes and the demand for real-time processing create scalability, security, and performance constraints for Blockchain networks within e-commerce environments. Moreover, BT is not entirely impervious to cyber threats. Despite its well-regarded security properties, Blockchain networks remain vulnerable to sophisticated attacks that may disrupt communications and compromise system reliability. To address such vulnerabilities, researchers have begun exploring the integration of BT with Artificial Intelligence (AI) as a pathway to enhance CR. One notable effort in this direction is the framework proposed by Navaneethan and Janakiraman [24], which combines Blockchain with machine learning algorithms to detect and prevent attacks on e-commerce systems. While this integration holds great promise, its practical application within supply chain management systems still faces considerable challenges. A critical concern lies in the explainability of AI systems—particularly those utilizing deep learning or complex machine learning models. In high-stakes scenarios, such as threat detection and incident response, the opaque nature of AI decision-making can hinder user trust, regulatory compliance, and ethical accountability.

Therefore, it is imperative to develop innovative solutions that combine the strengths of Blockchain and AI while also prioritizing explainability and transparency. Enhancing interpretability within AI-driven systems is essential to building user confidence, ensuring compliance, and supporting ethical deployment. By achieving this balance, the integration of BT and AI can significantly improve Cyber Resilience Management (CRM) in the fast-growing e-commerce landscape.

C. Explainable Deep Learning Applications for Anomaly Detection in Supply Chains

Explainable Deep Learning (XDL), a specialized subset of Explainable Artificial Intelligence (XAI), aims to make the decision-making processes of deep learning models transparent and interpretable to human users [25]. XAI focuses on enabling AI systems to provide understandable justifications for their outputs, which is essential for fostering trust, enhancing accountability, reducing bias, and promoting ethical use of AI technologies [26]. Particularly in high-stakes domains such as supply chain management, the integration of XAI is crucial for ensuring that AI systems remain trustworthy, transparent, and equitable. XDL encompasses a range of techniques that allow users to understand how deep learning models generate specific outcomes. This interpretability is especially valuable in supply chain operations, where opaque recommendations from traditional algorithms often hinder trust and adoption. For example, product recommendation engines often use complex models that provide little insight into the rationale behind their suggestions. By contrast, XDL enables these systems to offer clear and interpretable recommendations, thereby improving user trust and decision accuracy [27].

Several case studies underscore the practical benefits of XDL in supply chain contexts. Chuning and Yongji [28] utilized a Long Short-Term Memory (LSTM) based deep learning approach to enhance demand forecasting accuracy, demonstrating XDL's value in inventory management. In another application, Su et al. [29] introduced the ACTION framework in humanitarian logistics, leveraging XAI to prioritize strategic decisions with increased transparency and effectiveness. From a cybersecurity perspective, XDL is particularly useful in anomaly detection. It can help explain why a particular anomaly was flagged, offering insights into both the detection process and the nature of potential threats. This transparency not only strengthens the system's reliability but also enables more informed and rapid incident response. Consequently, XDL has attracted growing attention for its potential in real-time threat identification within supply chains.

Despite these promising developments, the application of XDL in supply chain management—especially in Blockchain-based Retail Platforms (BRPs)—remains underexplored. Existing studies largely focus on controlled or hypothetical environments, which may not accurately reflect the complexities of real-world e-commerce ecosystems. Key operational challenges such as varying customer preferences, dynamic product inventories, multifaceted vendor relationships, and fierce market competition are often overlooked. Moreover, there is a noticeable lack of comprehensive cyber resilience strategies that incorporate XDL specifically for BRPs. To address these gaps, further research is needed to develop and evaluate robust XDL-based frameworks tailored to the dynamic and heterogeneous nature of online retail platforms. Such efforts could significantly enhance anomaly detection, strategic planning, and overall resilience in modern supply chain systems.

D. Research Scope

As the e-commerce industry continues its rapid expansion, online retailers face an escalating array of cyber threats, including data breaches, ransomware attacks, and denial-of-service incidents. These threats not only compromise the security and confidentiality of customer data but also significantly affect the operational integrity and economic stability of digital retail platforms. In this evolving landscape, advanced technologies such as Explainable Deep Learning (XDL) and Blockchain-based Business Continuity Planning (BCP) are becoming critical for ensuring customer retention and overall cyber resilience (CR). XDL models offer strong capabilities in detecting anomalies within large-scale, complex datasets, positioning them as effective early warning systems for cyber threats in the e-commerce domain.

Concurrently, BCP—leveraging Blockchain's secure and transparent architecture—can automate responsive actions based on insights derived from deep learning models. Despite their promise, existing research integrating deep learning (DL) and Blockchain technology (BT) for CR has notable limitations. While DL excels at pattern recognition for threat detection, it often lacks interpretability, making it difficult to understand or justify the model's decisions. In domains where decision accountability is paramount—such as e-commerce—this opacity can undermine consumer trust and regulatory compliance. Blockchain has been studied for its potential to enhance traceability and reliability in cyber defense strategies. However, challenges remain in integrat-

ing BT with real-time anomaly detection systems, particularly around scalability and timely response. In high-volume environments like online retail, even minor delays in addressing cyber threats can result in substantial financial and reputational losses. Existing BT solutions often fail to meet the rigorous demands of this sector.

To address these gaps, this study proposes a novel framework that synergizes the predictive power of XDL with the automation and security strengths of Blockchain-enabled BCP. Within the online retail context, the proposed system is designed to: 1. Detect anomalies in real time, 2. Provide interpretable explanations for each anomaly, and 3. Trigger automated responses based on a predefined BCP strategy.

The deep learning model will incorporate a variety of techniques, including Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), Autoencoders (AEs), and Generative Adversarial Networks (GANs). Each method serves a specific function: GANs simulate sophisticated cyberattack patterns to strengthen detection robustness, AEs reduce dimensionality and extract nuanced features indicative of threats, RNNs are employed for detecting temporal anomalies within sequential data, and CNNs analyze image-like or time-series interaction data with spatial structures.

The model will be trained using the Numenta Anomaly Benchmark (NAB) dataset to identify key features contributing to anomalous behavior. To enhance transparency, the Local Interpretable Model-Agnostic Explanations (LIME) technique will be used to clarify the reasoning behind each detection. These insights will then inform the design of an automated BCP strategy, enabling smart contracts on a decentralized ledger to respond to detected anomalies in a secure and transparent manner. Depending on the severity and nature of the irregularity, these smart contracts can initiate actions ranging from alerting relevant personnel to executing defensive mechanisms.

To evaluate the efficacy of the proposed framework, an experimental study was conducted with various online retailers in North Africa. The study simulated multiple cyberattack scenarios to assess how the framework responds to system outages. A set of resilience metrics was used to measure system performance, including:

Time to Detection (TTD): the interval between the onset of a cyberattack and its identification, Time to Incident (TTI): the latency in recognizing the impact of an anomaly, Time to Failure (TTF): the duration before system operations are impaired, and Time to Recovery (TTR): the period required to restore normal operations post-incident. TTD is particularly critical, as a shorter detection time indicates a more proactive and responsive system. Similarly, minimizing TTR is essential to reduce downtime and ensure business continuity.

III. Methodology

Employing advanced techniques is essential in CR for effectively pinpointing and addressing risks and anomalies, especially within the e-commerce industry. We aim to integrate diverse and distinctive concepts into our research methodology. This methodology outlines a systematic approach that begins with the collection and preparation of data, progresses to advanced anomaly detection utilizing deep learning techniques, and ultimately culminates in the execution of a business continuity strategy aimed at improving incident response. A meticulous strategy for addressing cyber risks is guaranteed by the careful design of each stage to enhance the preceding one. The complete study technique is illustrated in Figure 1.

Figure 1 illustrates the methodology employed for the analysis of e-commerce platforms utilizing the NAB dataset. We specifically investigate anomalies in data streams such as website traffic, transaction volumes, and user behavior. Our primary focus is on synthetic time series data, specifically that derived from files such as "artificial_cd_1.csv" and "artificial_cd_2.csv," which contain a significant number of systematic and stochastic outliers. The RapidMiner application is utilized to carry out comprehensive data preprocessing during the initial phase of our methodology. This approach ensures that any unnecessary or absent data will be systematically removed, providing you with confidence in the integrity of your dataset. The next phase involves label encoding, which is the transformation of categorical data into a numerical format. Subsequently, any discrepancies are addressed through the implementation of scaling and normalization techniques. A crucial component of this process is feature extraction, which seeks to pinpoint characteristics that signal advanced persistent threats (APTs) and distributed denial of service (DDoS) attacks. The anomaly detection system employs a hybrid model that integrates CNN and GAN architectures, alongside convolutional neural networks, recurrent neural networks, artificial neural networks, and GANs, to effectively differentiate between standard and atypical behavior. The implementation of binary categorization facilitates this outcome. An extensive assessment of the effectiveness of these models is conducted using metrics such as the correlation coefficient and different error evaluations.

Our methodology inherently emphasizes robustness and practicality. The dataset from the National Statistical Bureau (NASB) was utilized because of its thorough modeling of online purchasing behaviors. This modeling can capture both typical and atypical patterns, akin to outliers. Choosing this option ensures that the data utilized to improve our models will faithfully represent the intricate and often unpredictable dynamics of online retail operations. The selection process for our models included convolutional neural networks (CNNs), recurrent neural networks (RNNs), artificial neural networks (AEs), generalized adversarial networks (GANs), and a hybrid CNN-GAN. These models were selected for their unique capabilities in simultaneously identifying intricate and subtle data patterns. Generative Adversarial Networks (GANs) excel in producing realistic data simulations, while Autoencoders (AEs) effectively reduce data dimensionality. Convolutional Neural Networks (CNNs) are adept at identifying spatial patterns, and Recurrent Neural Networks (RNNs) handle sequential data efficiently. Overall, CNNs stand out as the most effective option. A hybrid CNN-GAN model that leverages the strengths of architectures.

This deliberate choice ensures a comprehensive approach that addresses a diverse range of anomalies, spanning from the most straightforward to the most complex. No matter how straightforward or intricate the anomaly in question may be, this strategy ensures that all key variables are taken into consideration. The transparency of XDL is improved by LIME when it is used to deep learning models. For both the durability of the system and the detection of threats, transparency is absolutely necessary. By making some little modifications to the data that is being supplied, the LIME method is able to produce a new dataset consisting of simulated cases. To determine how accurate, the model's predictions are, simulated data is utilized in the evaluation process. This is followed by the development of a linear model via LIME, which is a reflection of the deep learning model at the particular input data point. Taking this technique makes it easier to have a better understanding of the predictive mechanisms that the model possesses. By adopting LIME, online shops can improve their ability to pinpoint potential hazards related with anomaly detection. This is accomplished by establishing which input data elements have a major impact on the performance of the model in finding abnormalities. These crucial features have the potential to reveal potential dangers, such as ineptitude, fraud, or other abnormalities. Lime's interpretability makes it possible to gain a better understanding of the anomaly detection process. The information in question is essential for incident response since it allows for a speedy determination of the nature and severity of the danger. As part of our project, we developed a business continuity plan (BCP) with the intention of improving the incident response and customer relationship management (CR) capabilities of an e-commerce platform. The protocol is responsible for establishing the fundamental framework for the reception of transactions and blocks, as well as the guidelines that regulate the behavior of nodes. Even in the face of continuing attacks, we make sure that the validation of transactions and the execution of blocks are carried out as part of our collaborative process. This helps to ensure that the network continues to function properly. It is possible to improve the protocol's robustness by assigning authoritative roles to many nodes during the validation process. This strategy improves the performance of the network even while it is operating under difficult conditions. For the purpose of preserving the highest possible level of functioning, the system discovers and removes any blocks from the previous two rounds that have not been validated. In the course of our research, we examined three distinct retail businesses in North Africa that are known for their implementation of Blockchain technology. For your convenience, they are offered in a wide variety of sizes, ranging from very little to very large. The simulation of cyberattacks on these companies is the first phase of this three-part empirical inquiry. The purpose of this simulation is to evaluate the features of such occurrences as well as the level of severity they possess. Second, in order to guarantee the accuracy of our anomaly detection system, we put it through a series of tests that make use of a variety of deep learning models. In conclusion, in order to strengthen the resilience of our incident response activities, we implement specific approaches that are derived from the business continuity plan.

IV. Cyber resilience framework for online retailing platforms

Cyber resilience (CR) is vital for e-commerce platforms due to the growing range of cyber threats, including phishing, spyware, and ransomware. These vulnerabilities can compromise customer trust, disrupt services, and result in financial losses. To address this, integrating Extreme Deep Learning (XDL) and Blockchain-based Protocols (BCP) offers a powerful strategy for enhancing CR. XDL enables rapid analysis of large datasets to detect anomalies, uncover hidden patterns, and predict cyber threats such as injection attacks, distributed denial of service (DDoS) attacks, and advanced persistent threats (APTs). BCP complements this by serving as a secure validation layer, authenticating transactions and automating incident responses. Depending on the type and severity of the anomaly detected, BCP can initiate defensive actions or escalate alerts to relevant stakeholders for coordinated intervention. This hybrid XDL-BCP framework provides a comprehensive defense mechanism, improving the reliability and security of e-commerce operations. To better illustrate this concept, Figure 2 presents a detailed depiction of the proposed model, helping to deepen understanding of its structure and benefits in bolstering cyber resilience.

A. Explainable Deep Learning-Based Model for Real-Time Anomaly Detection

This study leverages the Numenta Anomaly Benchmark (NAB) dataset, a widely acknowledged standard in anomaly detection research. The NAB dataset covers a diverse range of domains such as data centers, manufacturing systems, and environmental sensors, making it an ideal benchmark for assessing the effectiveness of anomaly detection models across multiple sectors. Our primary objective is to detect anomalies specific to e-commerce systems by using relevant files from the NAB dataset. To align with the dynamic nature of online shopping—characterized by fluctuations in traffic, transaction patterns, and user behavior—we selected synthetic time-series files like "artificial_cd_1.csv" and "artificial_cd_2.csv." These files were chosen because they simulate the kind of temporal variations and anomalies (e.g., sudden spikes, drops, and gradual drifts) often observed in e-commerce environments. Such patterns are indicative of potential fraud, system failures, or shifts in user activity. The selected files offer both complexity and variability, providing a realistic approximation of e-commerce data while enabling controlled testing. Their synthetic nature allows the model to be trained on a range of anomaly types, improving adaptability and robustness. Since anomalies in time series data typically develop gradually, the model is trained to identify irregular behavior over time, a critical requirement for real-time anomaly detection systems. Furthermore, the dataset's format and structure support scalability, making the results applicable to large-scale e-commerce systems.

B. Data Preprocessing, Encoding, and Transformation

Data preprocessing plays a vital role in preparing time-series data for anomaly detection in e-commerce platforms.

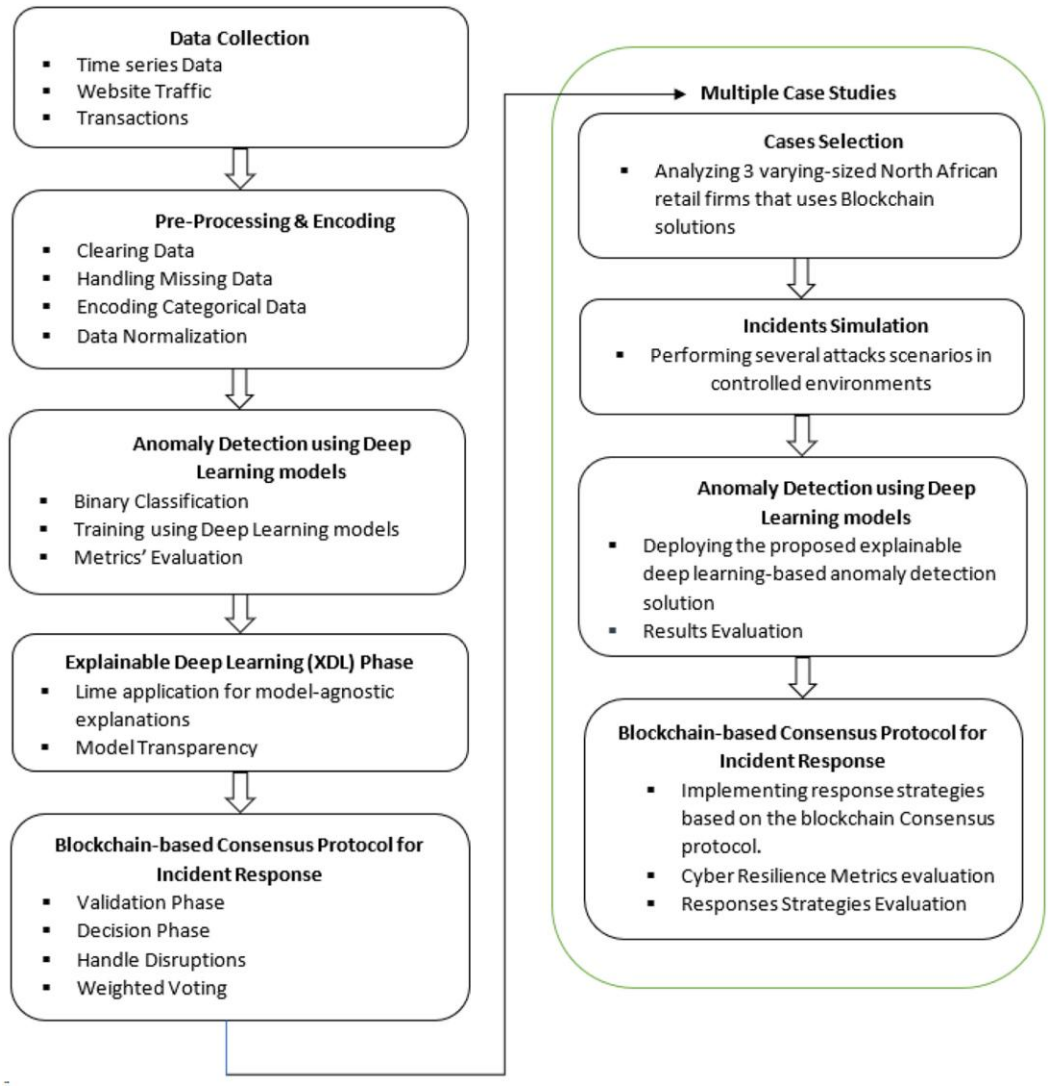

Fig. 1. Scenario of research methodology

The quality and compatibility of input data significantly influence the performance of deep learning models. This phase involves several key steps, including preprocessing, encoding, and transformation. Preprocessing includes the removal of irrelevant or duplicate data, handling missing values, and correcting for inconsistencies such as time gaps or seasonal effects. These steps ensure the integrity and reliability of the dataset, which is essential for accurate modeling. The next stage is encoding, where categorical and time-based data are converted into numerical formats using techniques like label encoding. This process enables deep learning algorithms—particularly CNNs and GANs—to effectively utilize both temporal and categorical features of the dataset. Following encoding, the transformation phase involves scaling and normalization to ensure uniformity in feature magnitudes. Feature extraction then focuses on identifying the most informative variables while eliminating redundant ones, thus streamlining the learning process. Features are categorized into numerical and nominal types, with correlation analysis used to remove superfluous attributes. These transformations optimize the dataset for detecting both common and previously unseen anomalies.

C. Deep Learning-Based Anomaly Detection

Deep learning has revolutionized cybersecurity, especially in the area of anomaly detection. In this study, the focus shifts from forecasting to classification, where the goal is to categorize data as either "normal" or "anomalous." This classification approach enhances the system's ability to detect potential security threats quickly and accurately. To this end, we employ a combination of advanced deep learning architectures, including Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), Autoencoders (AEs), and Generative Adversarial Networks (GANs). RNNs are particularly suited for processing sequential data, making them effective for time-series analysis. CNNs are employed to extract spatial features, particularly from structured user interaction data.

GANs and AEs play complementary roles: GANs are utilized to simulate complex anomalies by generating data that mimics real-world threats, while AEs focus on dimensionality reduction and uncovering hidden patterns in the data. The hybrid uses of CNNs and GANs has proven especially effective for identifying subtle and complex anomalies that might be overlooked by conventional models. The performance of

these models is evaluated using metrics such as forecast time, Mean Absolute Error (MAE), Root Mean Square Error (RMSE), Mean Squared Error (MSE), and the correlation coefficient (R). A high R-value indicates strong alignment between predicted and actual data, confirming the model's reliability.

D. Explainable Deep Learning (XDL) Phase

Explainable Deep Learning (XDL) enhances the cyber resilience of Business Operations and Recovery (BOR) systems by making model decision-making transparent and interpretable. In this study, we apply Local Interpretable Model-Agnostic Explanations (LIME), a widely used technique capable of interpreting any DL model regardless of architecture. LIME explains a model's predictions by generating synthetic samples similar to a target input and analyzing how the model responds to these variations. A local linear model is then fitted to approximate the DL model's behavior around the instance in question. This localized approximation provides human-understandable insights into the factors influencing the model's predictions. We use LIME to determine which features DL models rely on to detect different types of cyberattacks. By selecting representative examples from the test set, LIME provides class probability estimates that we compare against actual labels. We then cross-reference LIME's key features with established cybersecurity literature to validate their relevance. Finally, we assess how model performance varies with the inclusion or exclusion of these features, analyzing the impact on detection accuracy, false positives/negatives, and overall system effectiveness. This process ensures that the model's decisions are not only accurate but also justifiable and aligned with real-world cybersecurity knowledge.

E. Blockchain-Based Consensus Protocol for Incident Response

Blockchain technology (BT) has proven its value in enhancing the security, transparency, and efficiency of distributed systems such as supply chains. In this research, we extend its utility by integrating explainable DL outputs into a Blockchain-based consensus protocol (CP) designed for automated incident response in cybersecurity. The core idea is to embed XDL results into the Blockchain architecture, ensuring that anomaly detections are both verifiable and actionable. The interpretable outputs from XDL models help security teams understand the rationale behind anomaly alerts, enabling timely and informed responses. The proposed CP consists of two primary stages: validation and decision-making. During the validation stage, authority is rotated among nodes to prevent single points of failure. Each node retrieves unvalidated blocks from the last two rounds before a timeout occurs, ensuring resilience against cyber disruptions.

A weighted voting mechanism is employed in the decision stage, where votes are adjusted based on the type of threat and the historical performance of nodes. This adaptive approach ensures robustness by customizing response actions according to the context of the detected anomaly. By integrating DL, interpretability, and blockchain consensus mechanisms, the proposed protocol delivers a decentralized, transparent, and automated framework for managing cyber incidents in real time.

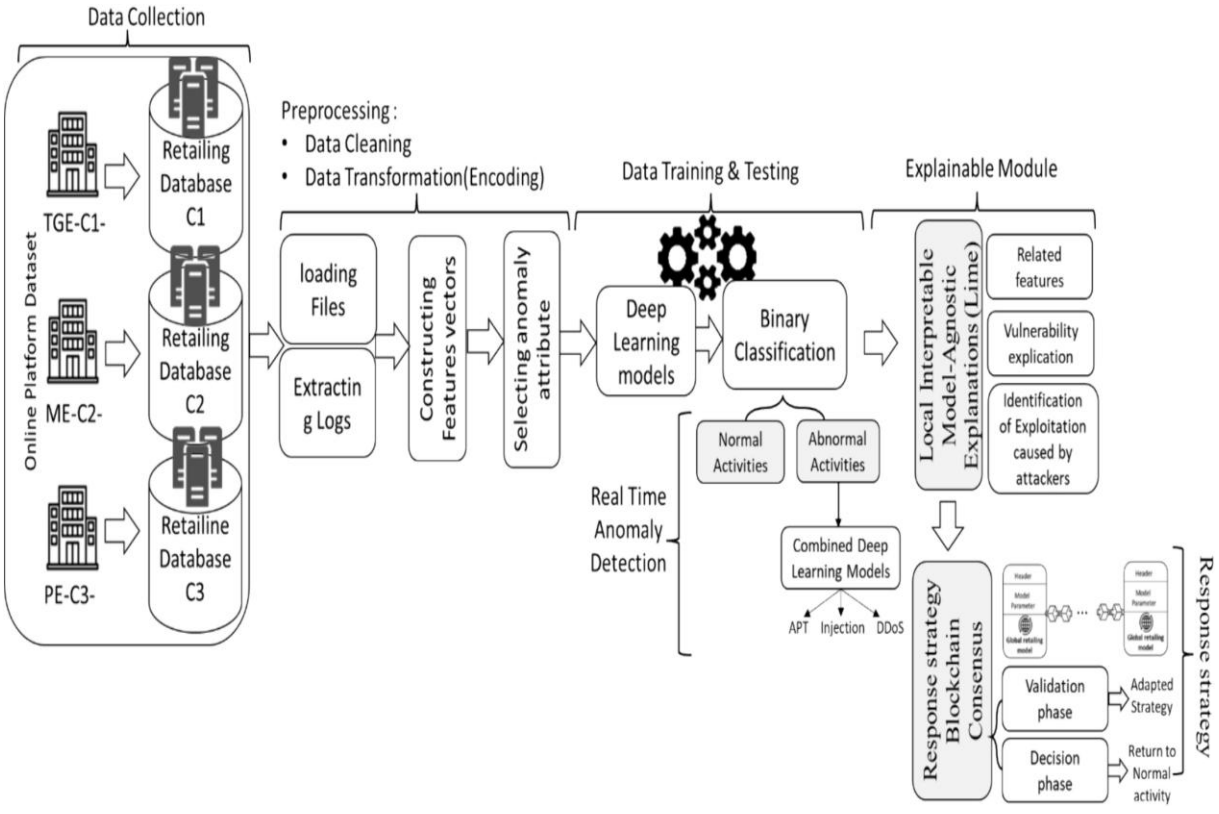

Fig. 2. Cyber Resilience framework architecture for Online Retailing Platforms

To ensure fast and efficient consensus even under slow network conditions, greater weight is assigned to nodes with higher voting scores—typically those with a history of completing more blocks or experiencing fewer and less severe attacks. After validation, a block must be approved and certified by the majority of the network to achieve finality during the decision phase. Each type of attack has a corresponding voting score threshold, calculated based on the node's completed block history and the severity of the attack. A node's vote strength is primarily influenced by the number of blocks it has successfully completed and the seriousness of the attack it has faced. Nodes earn higher voting scores when they have completed more blocks and endured fewer or less intense attacks. To address concerns about the integrity of the block recall mechanism, our protocol employs cryptographic hashing and digital signatures for authentication. These mechanisms prevent tampering and ensure the validity and integrity of block contents. Furthermore, the recall process is secured using a threshold-based validation: a recalled block can only be reinstated into the blockchain with consensus from a sufficient number of trusted nodes.

V. Experimental results

A. Case Background

This empirical study on customer retention (CR) focuses specifically on the North African retail sector. Three retail businesses—designated as C1, C2, and C3—were selected to represent a mix of large multinational corporations and small to medium-sized enterprises (SMEs). These organizations were purposefully chosen to capture a broad spectrum of characteristics, ensuring the applicability and generalizability of the study's findings across diverse business environments. The North African region was selected due to its rapid economic development and its emerging status as a strategic market for global businesses. To construct our model, we extracted relevant operational parameters from the databases of the participating companies. For example, the daily interest in a single product ranged between 200 and 500 units. Delivery times—an essential aspect of e-commerce logistics—varied from one day to a full week, depending on order volume and customer location. Furthermore, the profit margin associated with holding costs and production services was estimated at 15–25% of the product's annual value.

These operational metrics play a crucial role in formulating an effective response strategy and business continuity plan (BCP). Our experimental investigation is structured into three comprehensive phases. First, we simulate various cyber-attack scenarios in a controlled setting within each company to analyze their existing security measures. Next, we deploy a cutting-edge anomaly detection system built on XDL architecture to detect attack vectors and pinpoint vulnerabilities. Finally, we implement a set of response strategies aligned with the proposed BCP. The primary objective is to enhance system robustness and facilitate faster incident response. Key CR metrics—such as disruption propagation, recovery time, and associated costs—are measured to assess the effectiveness of the proposed strategy. The findings will highlight both strengths and weaknesses in current cybersecurity practices, providing actionable recommendations for improving customer retention.

B. Modeling Injection, Flooding, and APT Attacks

Given the increasing reliance of retail businesses on cloud infrastructure and mobile platforms, they have become prime targets for cybercriminals. Threats such as phishing, ransomware, and advanced persistent threats (APTs) exploit these vulnerabilities. In our study, we simulate a variety of cyber-attacks—including injection, flooding (DDoS), and APTs—to illustrate the diverse challenges facing online retailers. We specifically selected these three types of attacks due to their frequency and potential impact. Injection attacks, such as SQL injection and cross-site scripting (XSS), target system vulnerabilities to access or alter sensitive data, compromising both data integrity and customer trust. Flooding attacks aim to overwhelm systems with excessive traffic, disrupting service availability, particularly during peak sales periods. APTs, which involve prolonged and targeted infiltration by well-resourced attackers, pose a significant threat to high-value digital assets and require advanced mitigation strategies.

To emulate these attacks, we employed a range of penetration testing tools. SQLMap was used to probe database vulnerabilities via simulated SQL queries, while LOIC and Hping3 generated traffic surges to test resilience against flooding attacks. For APT scenarios, we simulated intrusions through phishing and social engineering techniques, mimicking how adversaries might implant malware or exfiltrate critical data. These simulations provide valuable insights into the vulnerabilities of each company's systems and underscore the need for layered, resilient cybersecurity frameworks.

C. Anomaly Detection Using the XDL Model

Detecting injection, flooding, and APT attacks is a complex task, owing to large data volumes, evolving user behavior, and dynamic threat vectors. Our anomaly detection framework leverages an Extended Deep Learning (XDL) architecture to address these challenges. The framework incorporates multiple advanced models, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders (AEs), Generative Adversarial Networks (GANs), and a hybrid CNN-GAN model to maximize detection accuracy. We trained and evaluated these models using datasets containing different types of cyberattacks—brute-force attempts, injection payloads, malware behavior, and APT traces. Figures 3, 4, and 5 (referenced in the original work) present the detection outcomes for each model under flooding, injection, and APT conditions.

Results indicate that the hybrid CNN-GAN model consistently outperforms others in identifying anomalies across all three attack types. While CNNs and RNNs demonstrate reliable performance in favorable data conditions, they fall short compared to the hybrid model. APT attacks, due to their complexity and multi-stage nature, significantly degrade model accuracy compared to injection.

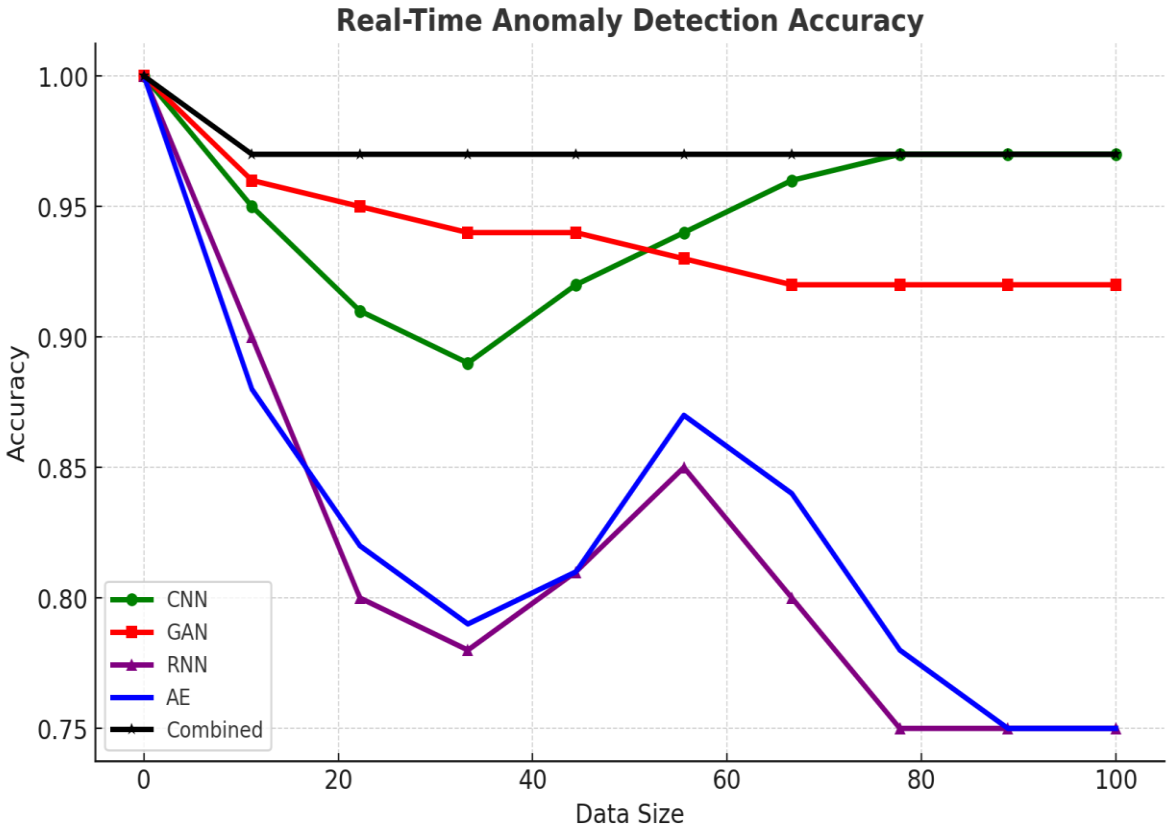

Fig. 3. Real-time anomaly detection under false data injection attack

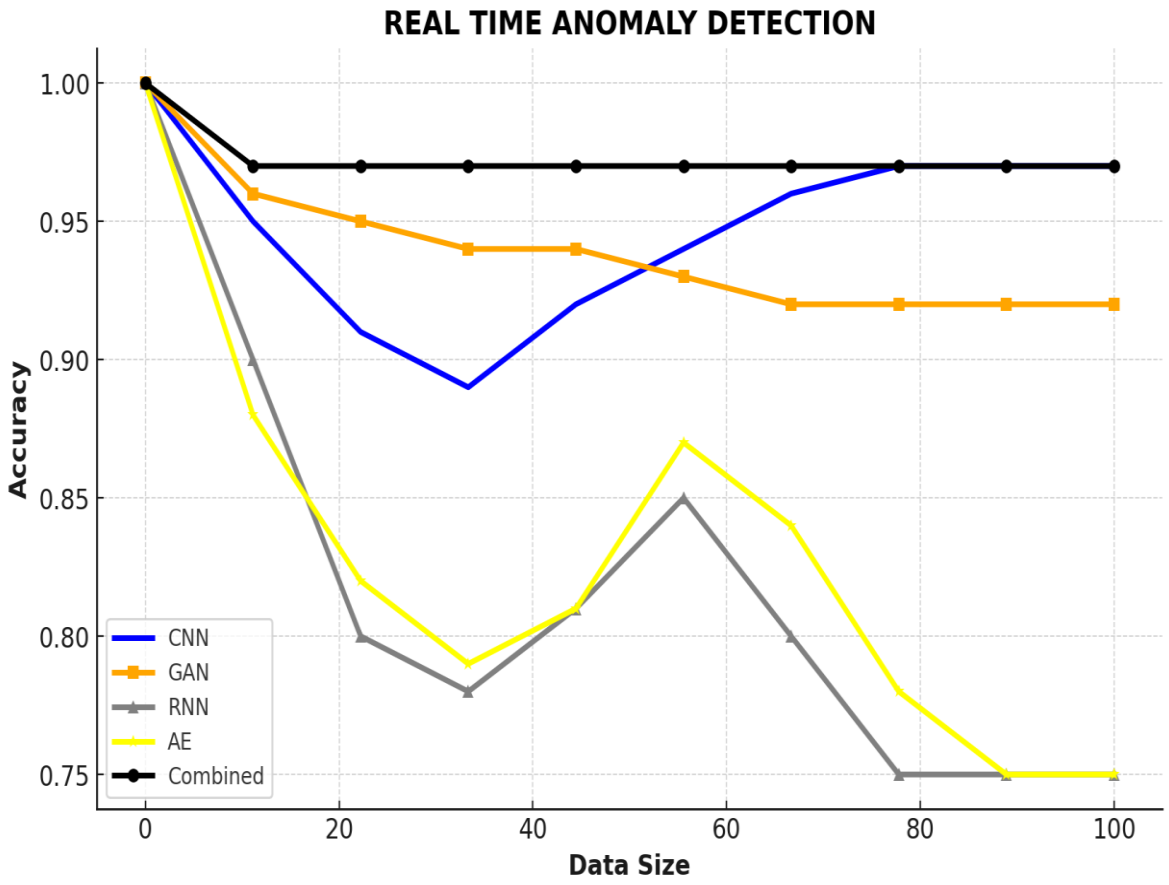

Fig. 4. Real-time anomaly detection under flooding attack conditions on the input variables

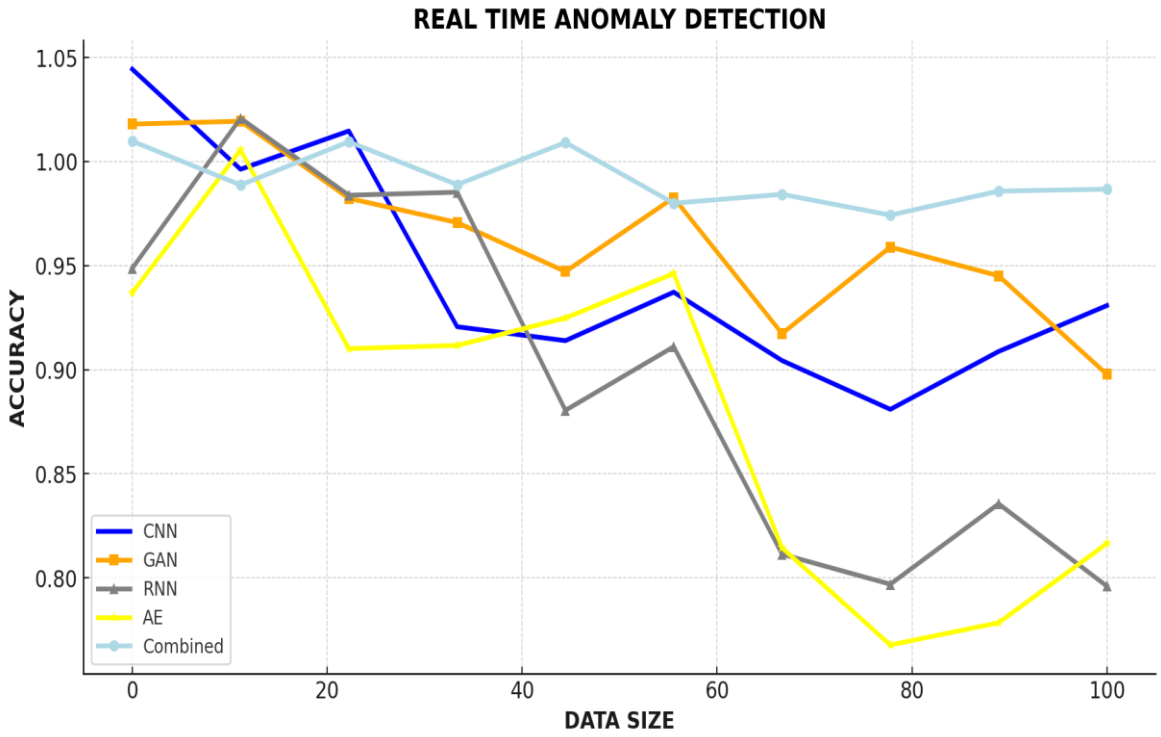

Fig. 5. Real-time anomaly detection under APT attack conditions on the input variables

To improve resilience, we prioritized optimizing model recall and precision, minimizing false positives and false negatives. By thoroughly analyzing performance metrics, we fine-tuned each model to reliably distinguish legitimate activity from actual threats, substantially reducing the likelihood of missed or incorrect alerts. Furthermore, we integrated LIME (Local Interpretable Model-Agnostic Explanations) to enhance model transparency. LIME helps elucidate the decision-making process of the XDL models, offering critical interpretability—particularly valuable for diagnosing false alarms and improving trust in automated cybersecurity responses.

D. Blockchain-Based Consensus Protocol for Incident Response

As part of our incident response strategy, we propose a blockchain-enabled consensus protocol tailored to the needs of online retailers. Designed within the framework of a business continuity plan, this protocol provides a dynamic response mechanism that adapts based on the identified threat type. The XDL model plays a crucial role by analyzing the nature and severity of each cyber-attack and transmitting this information to the consensus protocol. For instance, if an APT is detected, the protocol can isolate compromised systems and prioritize an immediate response by the security team.

This blockchain-based approach enhances the integrity and traceability of the response process. It ensures that all participating nodes—particularly those with strong security track records—contribute to decision-making, improving resilience and ensuring timely, coordinated incident handling. By integrating deep learning insights with decentralized trust mechanisms, the protocol establishes a robust framework for defending digital retail infrastructures against evolving cyber threats.

To enhance the resilience of online retail platforms against cyber-attacks, we propose a robust incident response framework grounded in a Blockchain-based Consensus Protocol (CP), aligned with a broader Business Continuity Plan (BCP). This protocol is designed to dynamically adapt to the nature and severity of detected attacks, enabling timely and appropriate responses. The CP utilizes output from the XDL-based anomaly detection model to guide actions—such as isolating compromised nodes or escalating alerts to security personnel—especially in the case of advanced persistent threats (APTs). The CP outlines clearly defined responsibilities and roles for all stakeholders involved, ensuring coordinated response efforts. For each type of attack, a tailored response strategy is devised, considering the operational context and specific security requirements of the e-commerce environment.

E. Cyber Resilience Evaluation

To evaluate the robustness of our system post-BCP implementation, we conducted a comparative analysis focusing on variations in system performance—particularly waiting time, operational cost, and incident propagation—before and after the deployment of our Blockchain-based strategy. Our methodology combined theoretical modeling with practical data analytics. We utilized Python (with libraries such as Pandas, NumPy, SciPy, and Matplotlib) and R for data processing, statistical analysis, and visualization. These tools allowed us to quantify performance metrics under different attack scenarios and visually illustrate the impact of our mitigation strategies.

Particularly, disruption cost served as the central metric, given its significance in online retail supply chains. We investigated how the presence of a BCP—and specifically the integration of Blockchain technology—affected the scale and duration of disruptions.

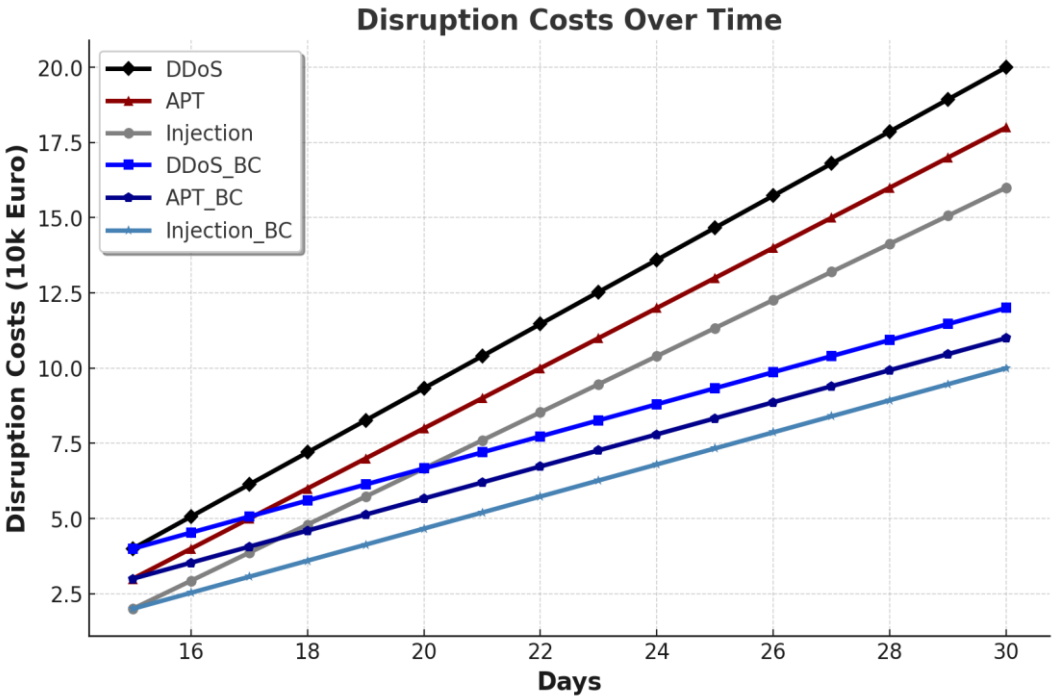

Fig. 6. Disruption Costs per Day

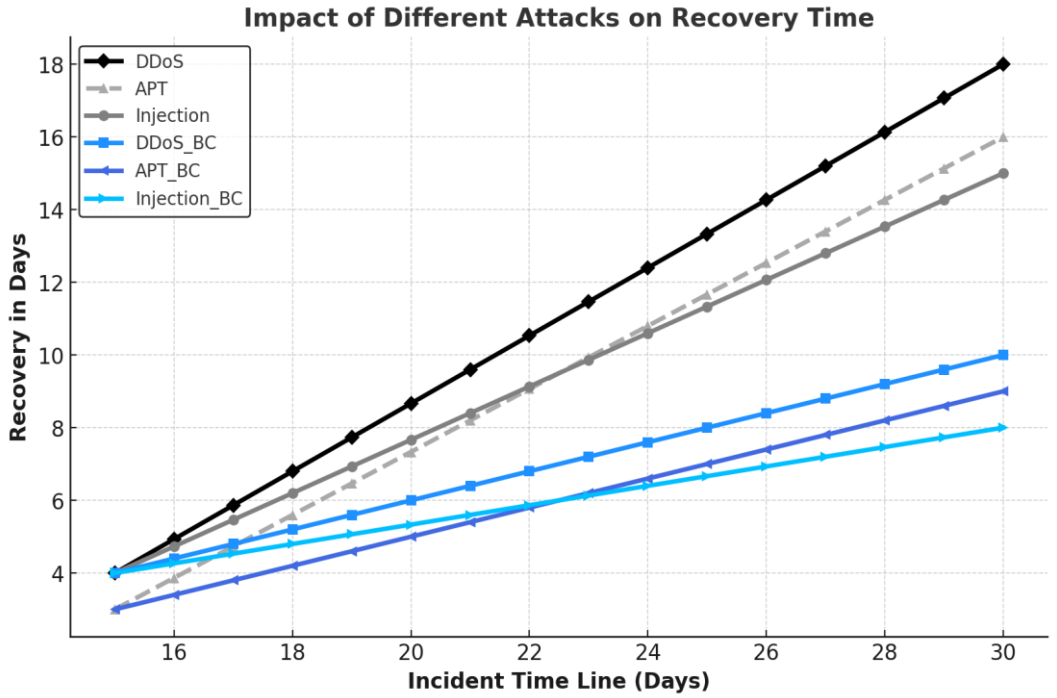

Fig. 7. Recovery time per day

As illustrated in Figure 6, our findings reveal that the Blockchain-enhanced strategy considerably reduces disruption-related costs compared to traditional methods. The protocol's ability to provide rapid response and secure validation directly contributes to minimizing downtime and loss, highlighting its effectiveness in bolstering cyber resilience.

Performance Analysis and Broader Implications of the Blockchain-Based Cyber Resilience Framework: Our results demonstrate that the Blockchain-based strategy is particularly effective in scenarios involving prolonged and high-intensity cyberattacks. Specifically, the cost-saving benefits of the proposed model increase with the severity and duration of the attack.

This finding underscores the growing robustness and adaptability of Blockchain-driven approaches in enhancing cyber resilience within the e-commerce sector. Attacks such as flooding, injection, and advanced persistent threats (APTs) typically require several hours to recover from. In our study, recovery time was measured by calculating the total downtime over a given period, divided by the number of disruptive incidents. As depicted in **Figure 7**, the implementation of our Business Continuity Plan (BCP) significantly reduced the recovery time across all three attack types.

The analysis also revealed nuanced performance differences between the baseline and Blockchain-based models

under various attack conditions. While the baseline model showed slightly better performance under injection attacks, the Blockchain-based solution outperformed it in handling APTs and DDoS attacks. This suggests that the Blockchain model is more adept at containing complex, multi-vector threats, thereby limiting their spread and minimizing overall damage. Our research introduces a novel approach to enhancing cyber resilience (CR) in online retail supply chains by integrating an Explainable Deep Learning (XDL) model with a Blockchain-based BCP. This dual-layered framework not only detects and mitigates cyber threats but also ensures transparent, informed decision-making through explainable AI outputs. A key advantage of the model is its interpretability, which helps stakeholders better understand the rationale behind threat detection and response actions.

The consensus protocol (CP) embedded within the framework enables secure and transparent communication among stakeholders during incident response. By facilitating shared access to reliable data and collective decision-making, the protocol helps avoid confusion, delays, and conflicts. This is further reinforced through a weighted voting mechanism for block validation, which expedites consensus even under network latency, enhancing the protocol's resilience in real-world conditions. Empirical results affirm that the combined use of XDL and Blockchain significantly improves critical resilience metrics, including reduced disruption cost, faster recovery times, and limited attack propagation. While the primary focus of our study is the North African e-commerce market, the findings carry broader implications. The proposed framework offers a scalable and adaptable blueprint for global application, with relevance to diverse socio-economic and technological landscapes.

The societal benefits of improved CR in online retail are far-reaching. In an era of escalating concerns about cybersecurity and data privacy, providing a secure online shopping experience enhances customer trust and loyalty. By safeguarding digital transactions, our framework plays a pivotal role in boosting consumer confidence in e-commerce platforms. Economically, robust CR measures reduce losses from cyber incidents such as data breaches and service outages. This financial protection encourages innovation and investment, as businesses are more willing to pursue digital transformation in a secure environment. By fostering a climate of trust, our framework contributes to both economic stability and technological advancement.

While our results are promising for the e-commerce sector, it is important to consider how the framework might be applied across other industries such as healthcare, finance, and manufacturing. These sectors share similar digital vulnerabilities but operate under distinct regulatory, operational, and privacy constraints. Therefore, future research should explore the adaptability and scalability of the XDL-BCP framework across different domains. Such exploration would validate the robustness of the approach and support the development of comprehensive CR solutions suitable for diverse digital ecosystems.

Theoretically, our work contributes to the ongoing discourse on the effectiveness of XDL algorithms in enhancing supply chain resilience. It also brings attention to the underexplored role of Blockchain technology in CR, opening new avenues for academic inquiry and innovation. Practically, our study offers actionable insights for e-commerce platform managers. By adopting explainable DL algorithms and Blockchain protocols, organizations can proactively detect and respond to cyber threats. This not only ensures the security and reliability of their platforms but also protects the integrity of the supply chain.

Despite its promising results, the study acknowledges several limitations. Our simulation environment, while detailed, may not fully capture the complexity and diversity of real-world cyber threats. Moreover, implementing a Blockchain-based architecture requires substantial technical expertise and resources, which could pose challenges for smaller firms. Focusing exclusively on XDL and BCP may also overlook other emerging technologies that could contribute to CR. Additionally, network scalability—particularly determining the optimal number of nodes—remains a delicate task. Striking the right balance is crucial to maintaining both performance and security. While the framework has proven effective against medium to high-impact threats, its performance in low-impact or highly dynamic threat environments warrants further investigation.

VI. CONCLUSION

Organizations, especially BORP, have prioritized corporate responsibility, data security, transparency, and trust above all else. The paper begins by outlining a strategy for identifying anomalies through XDL techniques and provides a thorough explanation of the results. Despite the differences in parameter complexity, data size, and node count, the findings indicate that a CNN/GAN hybrid model attains remarkable accuracy, reflected in a correlation coefficient (R) of 99.01. Secondly, we suggest utilizing LIME for accurate interpretation of results, as well as for elucidating features and vulnerabilities related to disruptions. A BCP has been developed to respond dynamically to cyber incidents utilizing the XDL model data, thereby enhancing CR. To evaluate the feasibility of our approach, we conducted an experimental study on three e-commerce platforms in North Africa. This study examines various potential applications of XDL and Blockchain technology to assist online merchants in enhancing decision-making and developing more effective CRS. The findings emphasize the substantial impact of our proposed BCP implementation on essential resilience metrics, including disruption cost, recovery time, and incident propagation. Our framework offers several advantages compared to existing CR approaches that are currently in use. The core of our platform lies in the transparency and security offered by BT, enabling us to focus on proactive anomaly detection and real-time responses rather than relying on traditional methods that often emphasize post-incident recovery strategies. Our approach distinguishes itself by utilizing XDL, which simplifies the anomaly detection process, making it more accessible for evaluation and comprehension.

Investigation into the application of Explainable Deep Learning (XDL) and Blockchain in small and medium-sized enterprises offers a hopeful pathway for the future. It would

be advantageous if these intricate technologies could be streamlined and rendered more accessible, allowing a greater number of individuals to reap their benefits. This project aims to identify methods for enhancing the usability and cost-effectiveness of our system while maintaining its effectiveness. This will enable small and medium-sized enterprises (SMEs) to enhance their Cyber Resilience (CR). It is essential to examine the scalability and flexibility of our proposed architecture in various industries beyond e-commerce. This study will involve assessing the effectiveness of the framework across different supply chain environments, including those present in healthcare, finance, and industrial sectors, among others.

REFERENCES

[1] Rejeb, A., Simske, S., Rejeb, K., Treiblmaier, H., & Zailani, S. (2020). Internet of Things research in supply chain management and logistics: A bibliometric analysis. Internet of Things, 12, 100318. https://doi.org/10.1016/j.iot.2020.100318

[2] Zkik, K., Belhadi, A., Kamble, S., Venkatesh, M., Oudani, M., & Sebbar, A. (2024). Cyber resilience framework for online retail using explainable deep learning approaches and blockchain-based consensus protocol. Decision Support Systems, 182, 114253. https://doi.org/10.1016/j.dss.2024.114253

[3] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2022). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors, 23(8), 4117. https://doi.org/10.3390/s23084117

[4] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance. Issues and Practice, 47(3), 698. https://doi.org/10.1057/s41288-022-00266-6

[5] Amajuoyi, Chinazor & Nwobodo, Luther & Adegbola, Mayokun. (2024). Transforming business scalability and operational flexibility with advanced cloud computing technologies. Computer Science & IT Research Journal. 5. 1469-1487. 10.51594/csitrj. v5i6.1248.

[6] Achaal, B., Adda, M., Berger, M., Ibrahim, H., & Awde, A. (2024). Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. Cybersecurity, 7(1), 1-30. https://doi.org/10.1186/s42400-023-00200-w

[7] Ahi, A. A., Sinkovics, N., Shildibekov, Y., Sinkovics, R. R., & Mehandjiev, N. (2022). Advanced technologies and international business: A multidisciplinary analysis of the literature. International Business Review, 31(4), 101967. https://doi.org/10.1016/j.ibusrev.2021.101967

[8] Noor, A. (2021). Adoption of Blockchain Technology Facilitates a Competitive Edge for Logistic Service Providers. Sustainability, 14(23), 15543. https://doi.org/10.3390/su142315543

[9] Tan, W. C., & Sidhu, M. S. (2021). Review of RFID and IoT integration in supply chain management. Operations Research Perspectives, 9, 100229. https://doi.org/10.1016/j.orp.2022.100229

[10] Mittal, M., Kumar, K. & Behal, S. Deep learning approaches for detecting DDoS attacks: a systematic review. Soft Comput 27, 13039–13075 (2023). https://doi.org/10.1007/s00500-021-06608-1

[11] Gan, C., Lin, J., Huang, D., Zhu, Q., & Tian, L. (2022). Advanced Persistent Threats and Their Defense Methods in Industrial Internet of Things: A Survey. Mathematics, 11(14), 3115. https://doi.org/10.3390/math11143115

[12] Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences, 34(10), 8176-8206. https://doi.org/10.1016/j.jksuci.2022.08.003

[13] Azadeh, A., Salehi, V., Salehi, R., & Hassani, S. M. (2017). Performance optimization of an online retailer by a unique online resilience engineering algorithm. Enterprise Information Systems, 12(3), 319–340. https://doi.org/10.1080/17517575.2017.1365173

[14] Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. Computers & Industrial Engineering, 149, 106829. https://doi.org/10.1016/j.cie.2020.106829

[15] Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. Computers & Industrial Engineering, 149, 106829. https://doi.org/10.1016/j.cie.2020.106829

[16] F. A. Sunny et al., "A Systematic Review of Blockchain Applications," in IEEE Access, vol. 10, pp. 59155-59177, 2022, doi: 10.1109/ACCESS.2022.3179690.

[17] Carvalho, A., & Karimi, M. (2021). Aligning the interests of newsvendors and forecasters through blockchain-based smart contracts and proper scoring rules. Decision Support Systems, 151, 113626. https://doi.org/10.1016/j.dss.2021.113626

[18] Baddu Naik Bhukya, V. Venkataiah, S. Mani.Kuchibhatla, S. Koteswari, R V S Lakshmi Kumari, and Yallapragada Ravi Raju, "Integrating the Internet of Things to Protect Electric Vehicle Control Systems from Cyber Attacks," IAENG International Journal of Applied Mathematics, vol. 54, no. 3, pp433-440, 2024.

[19] U. Agarwal et al., "Blockchain Technology for Secure Supply Chain Management: A Comprehensive Review," in IEEE Access, vol. 10, pp. 85493-85517, 2022, doi: 10.1109/ACCESS.2022.3194319.

[20] Swathi Dasi, Swarupa Rani Bondalapati, Mummidi P Subbaraju, Divya Nimma, Pradeep Jangir, R Vijaya Kumar Reddy, and N Zareena, "IoT-Based Intelligent Energy Management for EV Charging Stations," IAENG International Journal of Computer Science, vol. 51, no. 11, pp1853-1861, 2024

[21] Lohmer, J., Bugert, N., & Lasch, R. (2020). Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: An agent-based simulation study. International Journal of Production Economics, 228, 107882. https://doi.org/10.1016/j.ijpe.2020.107882

[22] Shukla, S., & KC, S. (2023). Leveraging Blockchain for sustainability and supply chain resilience in e-commerce channels for additive manufacturing: A cognitive analytics management framework-based assessment. Computers & Industrial Engineering, 176, 108995. https://doi.org/10.1016/j.cie.2023.108995

[23] Kumar Singh, R., Mishra, R., Gupta, S., & Mukherjee, A. A. (2022). Blockchain applications for secured and resilient supply chains: A systematic literature review and future research agenda. Computers & Industrial Engineering, 175, 108854. https://doi.org/10.1016/j.cie.2022.108854

[24] Ganapathy, G., Anand, S. J., Jayaprakash, M., Lakshmi, S., Priya, V. B., & Pandi V, S. (2024). A blockchain based federated deep learning model for secured data transmission in healthcare Iot networks. Measurement: Sensors, 33, 101176. https://doi.org/10.1016/j.measen.2024.101176

[25] Sheu, R., & Pardeshi, M. S. (2021). A Survey on Medical Explainable AI (XAI): Recent Progress, Explainability Approach, Human Interaction and Scoring System. Sensors, 22(20), 8068. https://doi.org/10.3390/s22208068

[26] Tjoa, E., & Guan, C. (2019). A Survey on Explainable Artificial Intelligence (XAI): Towards Medical XAI. ArXiv. https://doi.org/10.1109/TNNLS.2020.3027314

[27] Bai, X., Wang, X., Liu, X., Liu, Q., Song, J., Sebe, N., & Kim, B. (2021). Explainable deep learning for efficient and robust pattern recognition: A survey of recent developments. Pattern Recognition, 120, 108102. https://doi.org/10.1016/j.patcog.2021.108102

[28] Deng, C., & Liu, Y. (2020). A Deep Learning-Based Inventory Management and Demand Prediction Optimization Method for Anomaly Detection. Wireless Communications and Mobile Computing, 2021(1), 9969357. https://doi.org/10.1155/2021/9969357

[29] Nguyen, S., O'Keefe, G., Arisian, S., Trentelman, K., & Alahakoon, D. (2023). Leveraging explainable AI for enhanced decision making in humanitarian logistics: An Adversarial CoevoluTION (ACTION) framework. International Journal of Disaster Risk Reduction, 97, 104004. https://doi.org/10.1016/j.ijdrr.2023.104004