SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V13I5P102

Volume 13 Issue 5, 9-20, May 2026

Original Article

Cyber Resilient Cloud and Edge Digital Platforms for Data Intensive and Digital Twin Enabled Information Systems

Abdinasir Ismael Hashi[1], Osman Abdullahi Jama[2]

[1,2]*Computer Science, Somali National University, Mogadishu, Somalia.*

[1]*Corresponding Author : nasirhaji@snu.edu.so*

Received: 21 March 2026 Revised: 28 April 2026 Accepted: 13 May 2026 Published: 29 May 2026

Abstract - *The high rate of oil and gas digitalization has brought about a lot of complications in the processes of handling occupational health and safety in distributed infrastructures. The conventional safety measures are usually reactive in nature and therefore opening systems to break down in terms of the operations, and also due to human error. That is why it is urgent to preventively combat the risks by combining HFE with the latest digital technologies. It is against this backdrop that this paper proposes a cyber-resilient, cloud-edge platform-based digital twin technology in developing better OHS through real-time monitoring and predictive analytics. The approach is a design-science approach, which includes the integration of a zero-trust approach to access, an adaptive security approach, and an automated self-healing approach to make sure that the System undergoes constant synchronization. A high-fidelity simulated validation shows the high-detection rate of 99.95% of the operational anomalies present in the System and shows that the platform recovered all nodes with a 100% node recovery rate, since it enabled automated failure and recovered system throughput to 85.85%, even after experiencing simulated disruptions. The evidence based on these findings shows that the application of the concept of HFE into the framework of resilient digital systems is highly likely to positively contribute to the process of proactive risk management in high-stakes energy contexts.*

Keywords - *Human Factors and Ergonomics (HFE), Occupational Health and Safety (OHS), Oil and Gas Sector, Proactive Risk Management, Digital Twin Technology.*

1. Introduction

With the drastic digitalization occurring within the industries as well as the society as a whole, there is unparalleled growth in the area of data creation, processing, and transfer that occurs over the distributed computing infrastructures. Contemporary organizations appear to be becoming ever more dependent upon complex information systems, which establish the formulation of cloud computing, edge computing, and the concept of digital twins [1]. They are fundamentally changing the design, deployment, and management of systems focused on data-intensive services, offering the capability to achieve real-time monitoring, predictive analytics, and intelligent decision-making in key fields of smart cities, manufacturing, healthcare, energy systems, transportation, and other important infrastructure [2]. As the use of interconnected digital systems continues to increase, so do the vulnerability to cyber threats, failures of operation, and system disruptions. In this regard, cyber-resilient cloud and edge digital platforms have surfaced as a major facilitator towards ensuring the safety, availability, and sustainability of information systems with high levels of data and those that can be equipped with digital twins [3]. Figure 1 shows the Cloud-Edge-Digital Twin Architecture, which incorporates a Cyber Resilience Layer to enable three functions. The System delivers real-time data synchronization while detecting threats and maintaining operational capabilities during faults.

Cloud computing provides capacity and scalability of resources in terms of both storage and processing of large amounts of data produced by sensors, "Internet of Things (IoT)" devices, and cyber-physical systems with scalability and affordability [5]. Edge computing is the complement to the cloud paradigms as it proposes to relocate the computation to the point of data generation, which would dramatically decrease the Latency, network congestion, and reliance on centralized infrastructures [6].

Cloud and edge convergence bring about the opportunity of hybrid and distributed architectures with the ability to handle the high-performance demands of real-time and mission-critical applications [7]. Digital twins: Digital representation of physical assets, processes, or systems. Digital twins use this convergence to constantly synchronize with real data to be able to simulate behaviour, optimize performance, and anticipate events of failure [8]. These integrations require platforms that safely handle fast and heterogeneous streams of data, are operational, and preserve data integrity in dynamic and possibly adversarial environments [9].

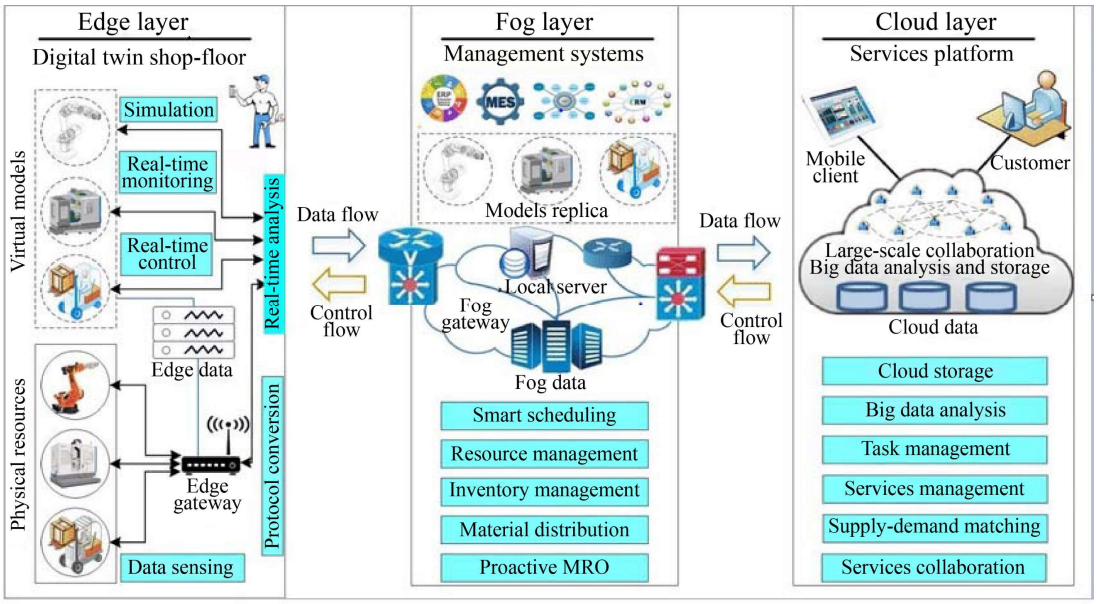

Fig. 1 Architecture of a cyber-resilient cloud and edge platform for data-intensive and digital twin-enabled systems [4]

However, even though cloud-edge-digital twin ecosystems have the potential to transform healthcare, the ecosystems have significant issues with cybersecurity, fault tolerance, patient data privacy, and data system stability [10]. Some of the threats committed by cyber criminals, such as "Distributed Denial-of-Service (DDoS)", ransomware, data poisoning, and manipulation of predictive models, are significant risks to physical and digital assets [11]. Also, interruptions in digital twins due to network disruption, hardware failures, software migrations, or misconfigurations may impede the synchronization of a digital twin and undermine the realm of accuracy in decision-making. Conventional security measures are not usually adequate to combat the complexity and dynamism of such threats, especially with their major emphasis on prevention. As a result, the concept of cyber resilience, which refers to the ability of a system to predict, tolerate, recover, and change in response to a cyber-event, has emerged as a key feature in the development of the next generation of digital platforms[12]. Cyber-resilient cloud-edge-digital twin ecosystem in Figure 2 needs data synchronization and fault tolerance, and security mechanisms to ensure system integrity.

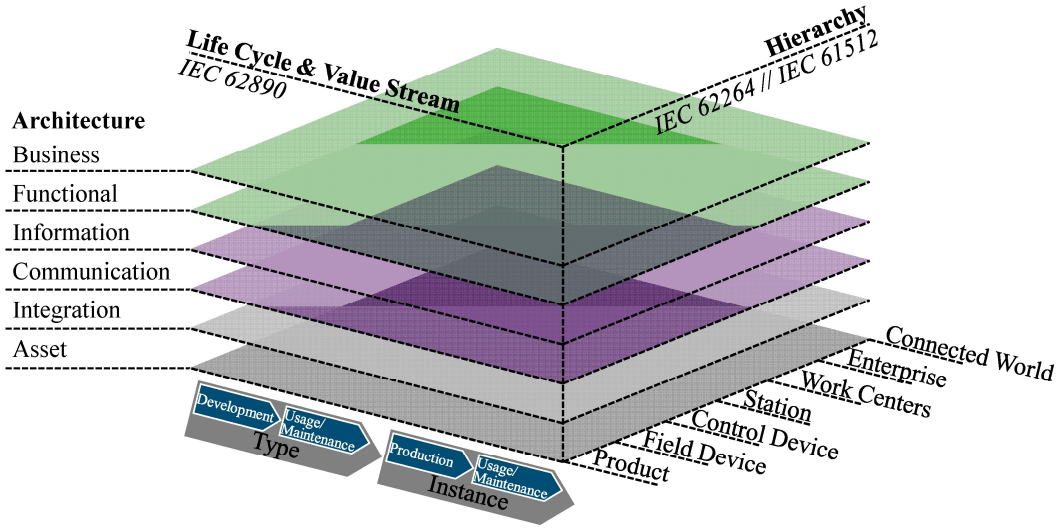

Fig. 2 Cyber-Resilient Cloud–Edge–Digital Twin Ecosystems [13]

Cyber-resilient cloud and edge environments are frameworks that combine the concepts of security-by-design, real-time defensive functions, redundancy, and self-healing capabilities to maintain the sustained functionality in unfavourable circumstances [12]. Zero-trust architectures, secure virtualization, container isolation, trusted execution environments, and distributed identity management are some of the techniques that strengthen defenses against attacks on the System. Furthermore, resilience is effectively improved by the association of

clever workload coordination, dynamic allocation of resources, fault detection, and automated recovery of cloud as well as edge nodes. In the case of digital twin-enabled systems, resilience also means maintaining the fidelity and consistency of virtual models even in the face of disruption, faulty, or corrupted inputs, and changing Latency [13]. In this situation, it is necessary to maintain search and physical systems in order to properly analyse the integrity of analytics and predictions, and make a decision [14].

The fact that present-day information systems are data-intensive supports the necessity of resilience. Modern systems are based on massive, heterogeneous datasets and contain structured, semi-structured, and unstructured data from various sources [15]. Deploying integrity, provenance, and availability of data to distributed platforms is important in ensuring reliable analytics and precise behaviour of digital twins. Edge analytics and federated learning are some of the approaches that have become popular to handle sensitive data on the edges and decrease exposure, as well as to reduce communication overhead. Nevertheless, they also add more attack surfaces and coordination burden, and so, it is necessary to have more cyber-resilient architectures, which are inherently centrally or decentrally coordinated components [16].

The major objective of this Study is to come up with resilient cloud-edge architectures that combine security, fault tolerance, and flexibility to support the incessant and precise operation of data-intensive and digital twins-enabled platforms, as follows:

- To investigate and characterize resilient architecture of mutual cloud and edge platforms in aid of data-intensive and digital twin-enabled information systems.
- To investigate the security and protection practices, such as adaptive defense, availability, and self-healing approaches, to guarantee system seamlessness at the time of cyber-attacks and system failure.
- To explore data management, integrity, and synchronization issues in the distributed cloud edge to achieve digital twin fidelity and reliability.
- To examine how artificial intelligence and machine learning can contribute to the level of cyber resilience, cyber threat detection, and recovery within cloud and edge infrastructures.

The Study helps to design more advanced cloud-edge platforms that can handle complex applications with high stakes and guarantee sturdier and uninterrupted operations, as well as protection of the data against foreseen and new cyber threats. Organizations that require the utilization of digital twin technologies and distributed computing paradigms to enable the realization of sustainable, intelligent, and reliable operations in an industrial and societal environment that is becoming more interconnected need such platforms [17, 18].

This Study creates a complete conceptual framework through its initial section, which details current advancements in cloud and edge computing, cyber resilience, and digital twin-based information systems. At the same time, it points out the current strategy's limitations while highlighting some of the important components that are needed but are currently missing, which are needed to ensure an overall robust and resilient system within an organization can be developed. In this paper, there is an overall cyber-resilient platform architecture design that includes three main components, namely, security operations and data management, as well as various methods for security functionalities that are needed to ensure trustworthiness for conducting security operations across distributed systems of an organization reliably and securely. In this Study, there is an overall analysis of different methods for adaptation that are needed to ensure the reliability and overall integrity of an organization's System with the ability to ensure continuous operations despite different cyber and overall challenges.

At the same time, this Study presents some of the main conclusions and overall knowledge that was noted while highlighting some of the further research that should be conducted to ensure better cyber-resilient digital platforms can be developed within an organization that can support different data-intensive applications as well as digital twin capabilities.

2. Literature Review

The literature reviewed enables the representation of the current state of DT research characterized by rapid maturation, and, at the same time, it also indicates the existence of structural, security, and management gaps in the new technology spheres. Initial and seminal literature underlines that holistic frameworks and architectures are necessary in order to help go beyond isolated prototypes that increase the adoption of DT. Particularly, Villegas et al. (2026) [19] explicitly stated that the lack of an end-to-end lifecycle management is one of the key obstacles, and a truly integrated DT lifecycle framework that is in turn aligned with ISO 23247 is proposed to bridge the technical and managerial aspects. Simultaneously, Qian et al. (2024) [20] presented a specific layer of integrating CPS-DT, with abstraction and interoperability being identified as requirements in the context of scalable DT ecosystems. Likewise, as the discussion continues it has been further expanded with indexing surveys of Advanced Data Science Platforms (ADSPs) systematically mapping data ingestion, analytics, optimization, and continual learning processes of DTs, CPS, and robotics (Kabir et al., 2025) [21]. Collectively, these papers turn out to be converging on the belief that DT efficacy should not just be reliant on fidelity of simulations but uniform structures, governance of lifecycle, and tight data pipelines that are capable of sustaining long-term development besides cross-domain integration.

With architecture as a background, the literature base on resilience, reliability, and security is large as DTs are integrated to critical systems, and distributed systems, and systems. Areghan et al. (2025) [22] synthesized the cyber-resilience issues of smart manufacturing DT settings, and

promoted AI-guided graph-based ETL, and cloud-based resilience approaches to highlighting the extended attack surface owing to cyber-physical interdependence. Coexisting, Sahu et al. (2025) [23] also dealt with operational resilience at the edge; they provide an adaptive fault-tolerance system via a Hybrid Genetic-PSO algorithm that has a high availability and energy-competitive DT migration during node failures. At the infrastructure level, Coppolino et al. (2023) [24] and Epiphaniou et al. (2023) [25] emphasized the use of DTs to monitor and model the cybersecurity of critical national infrastructure, which makes the DT-based simulation and monitoring answer the requirements of the regulations like the NIS2. Simultaneously, Suganya et al. (2024) [26] applied cyber protection to the 6G Edge-of-Things network, demonstrating that DT-powered attack detection and online learning can be used to improve proactive protection. Together, these studies formally prove the use of DTs as active cyber resilience instruments and transform them into passive just imitations but self-healing security-conscious operational resources.

Last but not least, the recent literature demonstrates the spread of DT paradigms to collaborative, urban, and human-oriented applications and highlights its role in decision-making and policy formulation. Hossain et al. (27) achieved this through demonstrating how urban-scale DTs can facilitate proactive, heat-risk management through real-time sensing, geospatial, and socio-economic indicators, so that urban resilience planning is not Reactive but Preventative. Alourani et al. (2025) [28] also enhanced this vision now by involving a specially developed AI-IoT-DT architecture of smart cities that are confirmed using the traffic and pipeline management applications, and ensure significant reductions in response time and maintenance costs without the use of privacy invasion through federated learning. Simultaneously, Alcaraz et al. (2025) [29] presented the notion of DT communities, which concern inter-organizational cooperation, which is achieved based on hybrid RBAC-OrBAC access control so that it does not jeopardize confidentiality and allows sharing knowledge without any risk. Jameil et al. (2024) [30] depicted the application of DTs in the healthcare sector in collaboration with edge computing and efficient cryptographic techniques to enhance secure and personalized remote healthcare. Combined, the series of studies methodically demonstrates the transition to DT ecosystems that are collaborative, policy-conscious, and people-centred, and upholds the necessity of providing integrated management of lifecycle, strong security, and standardized underpinnings to succeed in real-world deployment.

The reviewed literature shows that Digital Twin research has made important progress, yet there are still essential research gaps that need to be addressed. Existing studies often focus on isolated aspects such as architecture, resilience, or application domains, lacking a holistic approach that integrates lifecycle management, cybersecurity, interoperability, and cross-domain collaboration. The deployment of scalable systems, real-time synchronization, fault tolerance, and secure data sharing for urban industrial and healthcare applications remains difficult. This situation prevents organizations from using Digital Twin ecosystems in their actual data-intensive operational environments.

3. Methodology

The suggested methodology in Figure 3 is based on a design-science and an experimental research methodology to design and test a cyber-resilient cloud-edge digital platform to build data-intensive and digital twin-enabled information systems. The paper starts with a requirement analysis based on current weaknesses in integrating clouds and edges, cybersecurity, and synchronizing digital twins. Hybrid cloud edge architecture is then developed and built in resilience schemes/mechanisms like adaptive security, fault tolerance, and self-control. Its methodology combines empirical data of cybersecurity in the real world with digital twin modeling to assess the behavior of a system in both normal and adversarial situations. The evaluation of resilience, performance, and digital twin fidelity is done by experimental validation in simulated cloud-edge environments. The results are compared with regard to the suitability of the offered architecture concerning the assurance of safe, resilient, and uninterrupted functionality of a system.

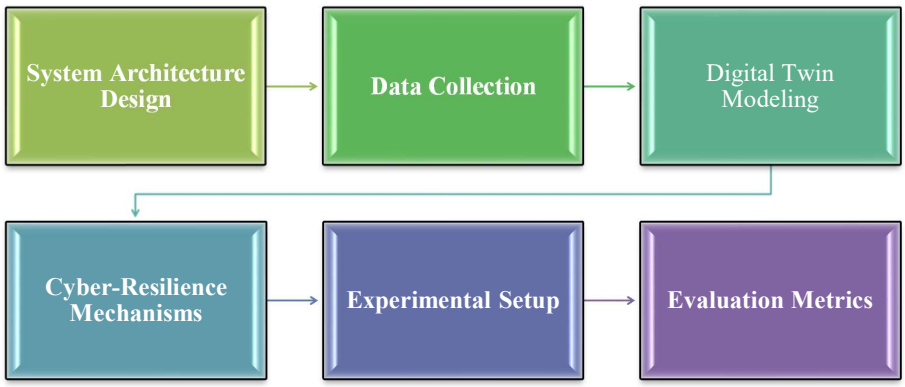

Fig. 3 Framework of research methodology

3.1. System Architecture Design

The hybrid cloud–edge system architecture provides cyber-resilient support for data-intensive systems that utilize digital twin technology. The system architecture connects IoT devices and sensors to data generation systems while using edge nodes for low-latency processing and local analytics, and cloud platforms for large-scale data storage and advanced analytics, and extended digital twin modeling. Digital twin components maintain continuous data synchronization with physical assets through their connection to cloud and edge systems. The architecture achieves cyber resilience through its implementation of fault tolerance systems and redundancy measures, adaptive security controls, and self-healing capabilities, which operate throughout all system components. The System maintains its operational capacity during cyber-attacks or system failures through zero-trust access and secure virtualization, workload replication, and automated failover techniques. The architecture enables real-time data ingestion and edge analytics and predictive modeling and resilient digital twin synchronization to deliver dependable system performance and data protection and effective decision-making in changing and threatening situations.

3.2. Data Collection

The Edge-IIoTset Cyber Security Dataset serves as an authentic dataset that researchers use to study cybersecurity protections in cloud, edge, and Industrial IoT environments [31]. The System creates data through a testing environment that models actual Internet of Things devices and edge computing and cloud computing systems. The dataset contains normal network traffic together with various types of cyber-attacks, which include DDoS attacks, DoS attacks, malware, injection attacks, and man-in-the-middle attacks. The System provides various network and System features that researchers can use to create machine learning systems that detect intrusions and study cyber resilience in data-intensive systems and digital twin-enabled systems.

3.3. Digital Twin Modeling

Digital twins build their own virtual images of assets and processes through the application of a combination of actual real-time information received through sensors and historical operational information gathered from their cloud and edge systems. The digital twin system uses data-driven models to continuously update its own systems in order to have an exact replica of the actual physical systems. This constant alignment between physical entities and their images or replicas, whether applied in an edge or cloud environment, is done through the application of the digital twin's secure synchronizations and data fusion techniques. The digital twin accuracy assessment basically compares the actual physical systems with the predicted System in order to determine the exact deviation between the two:

$$F_{DT} = 1 - \frac{||X_P(t) - X_{dt}(t)||}{||X_p(t)||} \quad (1)$$

Where $X_p(t)$ denotes the physical system state and $X_{dt}(t)$ represents the digital twin state at time t. The intentional introduction of cyber disruptions, which include data loss, data poisoning, and delayed updates, allows researchers to assess their impact on synchronization precision, model dependability, and decision-making effectiveness.

3.4. Cyber-Resilience Mechanisms

To ensure the safe and reliable functionality of their data-heavy and digital twin platforms, the System employs cyber-resiliency of its cloud and edge infrastructure across the whole cloud and edge infrastructure. The System needs zero-trust access control that would validate all the users' devices and service requests and then give them access. The organization implements secure virtualization along with container isolation and trusted execution environments to prevent the movement of attacks and isolate the compromised parts of the System. The machine learning in the System is used to develop anomaly and intrusion detection models that are deployed on both edge and cloud levels to identify threats based on recent and previous data use patterns. To measure the intrusion detection accuracy, this Study uses such metrics as: Detection Rate (DR):

$$DR = \frac{TP}{TP+FN} \quad (2)$$

where TP represents true positives, and FN denotes false negatives. The System has automated fault detection systems that coordinate with failover systems and self-healing systems to identify the occurrence of faults and implement workload redistribution as the System is automatically trying to restore its services. The System relies on the current mechanisms to enhance the system uptime, maintain the integrity of the digital twins data, and build a more resilient defense against emerging cyber threats.

3.5. Experimental Setup

The researchers develop an experimental system that allows them to test their cyber-resilient digital platform on cloud and edge computing systems. The researchers built a simulated cloud-edge environment that utilizes the technologies of virtualization and containerization to run cloud servers that both offer centralized analytics and digital twin services, and edge nodes process the data on the IoT devices that demand immediate processing. The paper evaluates common system behavior and three attack scenarios comprising Distributed Denial-Of-Service (DDoS) attacks, data injection attacks, and node failure events. The performance measurement of the System applies the Latency (L), Availability (A), Recovery Time (RT), Data Integrity (DI), and data Detection Accuracy (DA) as the important key performance indicators. Availability is computed as:

$$A = \frac{T_{uptime}}{T_{uptime} + T_{downtime}} \quad (3)$$

Detection accuracy is evaluated as:

$$DA = \frac{TP+TN}{TP+TN+FP+F} \quad (4)$$

Such experiments measure the efficacy of cyber-resilience systems in continuing the systems, improving protection, and retaining their digital counterparts.

3.6. Evaluation Metrics

The test with the proposed cyber-resilient cloud and edge digital platform evaluates its efficiency by performing a system of measurements, which is capable of evaluating the capacity of the platform to resist attacks, its defenses, its functionality, and its accuracy in the simulation of the digital twin. Mean Time To Recovery (MTTR) indicates the average time to recover the services once they have failed:

$$MTTR = \frac{\sum T_{recovery}}{N_{failures}} \quad (5)$$

Fault Tolerance Rate (FTR) reflects the System's ability to continue functioning despite faults. Security Metrics evaluate protection effectiveness. The False Positive Rate (FPR) is:

$$FPR = \frac{FP}{FP+TN} \quad (6)$$

While Response Time (RT) measures the delay between threat detection and mitigation. The System Performance Metrics are used to measure the operational efficiency using three measurements that include: Latency (L), Throughput (Th), and resource Utilization (RU) during normal conditions and during an attack. Digital Twin Metrics determines the reliability of the model. Synchronization Delay (SD) is the delay between physical and virtual systems in updating the data, and Model Accuracy (MA) is used to measure the accuracy of prediction when a disruptive event occurs. The metrics define the capacity of information-intensive cloud-edge systems that utilize the digital twin technology to ensure security and operational performance.

4. Result and Analysis

The experimental data verify that this platform is capable of ensuring that there is proper synchronization between physical assets and digital twins under stressful situations. When initially examined, the experimental data revealed that this System offers a nearly flawless intrusion detection rate of 99.95%, coupled with a complete node recovery capacity of 100%, as enabled by automatic failover. In spite of reducing system throughput to 64.8%, these self-healing mechanisms managed to elevate system throughput to a desirable level of 85.85%. These parameters verify that zero trust and adaptive security mechanisms are effectively ensuring system availability and integrity.

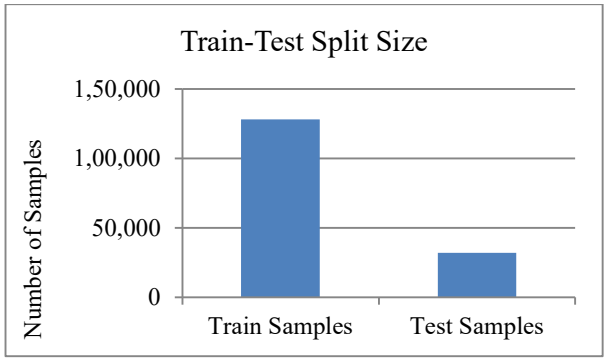

Fig. 4 Numeric Distribution of Training and Testing Samples for Cyber Resilient Cloud–Edge Digital Twin Enabled Information Systems

Figure 4 provides an approximate segregation of the train–test data used to model the Cyber Resilient Cloud and Edge Digital Platforms supporting data-intensive and Digital Twin–enabled information systems. About 127,000 samples are given for training (≈80%), while about 32,000 samples are left for the test set (≈20%). This allows the learning algorithms to be trained on a sufficient scale and diversity of data that captures operational behaviors and, in turn, cyber threat patterns of cloud–edge environments. The size of the test set is numerically retained as adequate to give a statistically reliable and unbiased performance evaluation. This distribution supports the robust generalization of models, correct detection of cyber anomalies, and trustworthy Digital Twin synchronization within large-scale cyber-physical systems.

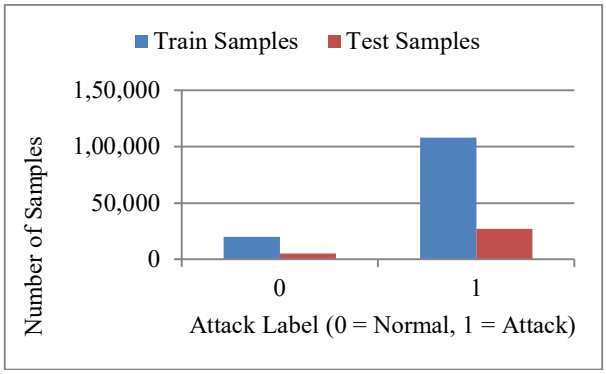

Fig. 5 Numeric Class Label Distribution in Training and Testing Sets for Cyber Resilient Cloud–Edge Digital Twin Enabled Information Systems

Figure 5 is a numerical distribution of the classes of the training and testing data used to design Cyber Resilient Cloud and Edge Digital Platforms to support data-intensive and data-driven Digital Twin-based information systems. Speaking of the percentage of the data, 4,500 training and 1,000 testing samples of the normal data are apparent, denoted by 0. Otherwise, the percentage of the data samples in the attack class, which is labeled 1, is considerably larger than the normal class. More specifically, the training data sample has around 107,000 samples and 27,000 testing data samples of the attack category. Numerically, the ratio of the data samples is over 95, which allows the learning structure to fit the different patterns of cyber threats and still achieve appropriate generalization.

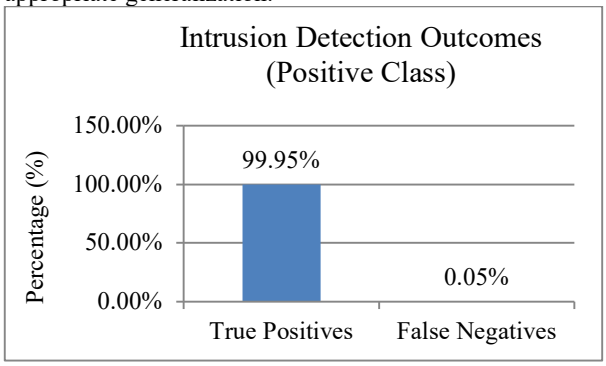

Fig. 6 Numeric Intrusion Detection Outcomes for the Positive (Attack) Class in Cyber Resilient Cloud–Edge Digital Twin Enabled Information Systems

The numeric values of intrusion detection of the positive class are presented in Figure 6, which indicates the attack class of the Cyber Resilient Cloud and Edge Digital Platform of data-intensive and Digital Twin Information Systems. The True Positive Rate is revealed as about 99.95%, as the results indicate that practically all the cases of the attack type are correctly recognized by the suggested approach to intrusion detection.

That is, the False Negative Rate is approximately 0.05, also known as 5 in every 10,000 occurrences of the attack type are not detectable. This low False Negative value also indicates that the proposed method is very sensitive and strong enough to identify intrusion and provide cyber situational awareness in combination with receiving correct information on the Digital Twin.

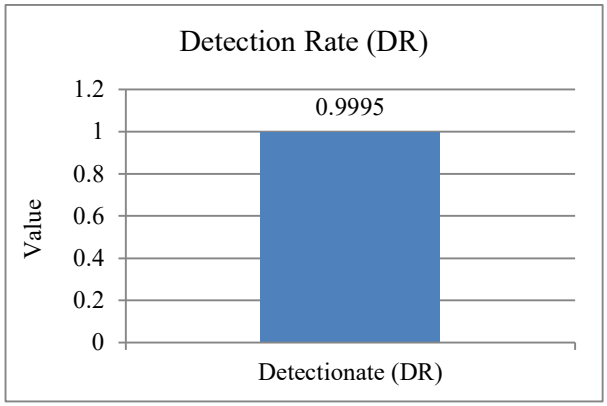

Fig. 7 High Detection Rate Achieved by the Proposed Cyber Resilient Cloud–Edge Intrusion Detection Framework

Figure 7 shows the Detection Rate (DR) of a system within a "Cyber Resilient Cloud and Edge" regime. The DR has a near-perfect score of 0.9995—or 99.95%—according to the data label found atop the bar chart. To emphasize the perfect score that the Detection Rate is closer to, the y-axis is severely truncated in order to display the values that lie in 0.95 to 1.00. It means that out of 10,000 cases of computer security breaches or data discrepancies handled in the Digital Twin processing model, 5 cases go undetected. Obviously, a high DR value like the presented one is necessary in a computer system with high demands for data, as well as one dependent on the seamless edge-to-cloud connections with the capacity to withstand advanced cyber threats that may interfere with the digital twin synchronizations.

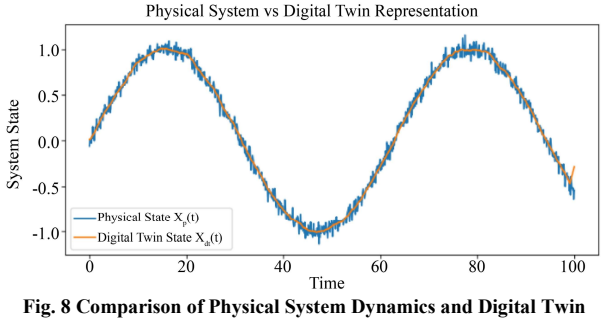

Fig. 8 Comparison of Physical System Dynamics and Digital Twin Representation in a Cyber Resilient Cloud–Edge Environment

In Figure 8, the real-time monitoring of a physical asset and its virtual counterpart in a cyber-resilient infrastructure is displayed. The blue line represents the physical state Xp (t)and swings around a high frequency 1.1 to -1.1 on the System State axis across 100 units of time; it is simply noisy raw data that is characteristic of edge-level sensors in data-intensive applications.

In the meantime, our orange line that is circa Digital Twin stateX_dt (t), furnishes us with some smooth filtered form that follows very nearly with much fidelity whatever main sinuoidal trend that the physical System adopts. This form of alignment would play a critical role in any platform outlined as cyber-resilient, as in this case, it is the priority that the Digital Twin can distinguish between operational noise and malicious data injection.

In maintaining such steady-state tracking, it may ensure that data employed in higher-level decision-making remains correct and in step, even though there is a natural volatility caused by edge-to-cloud data streams.

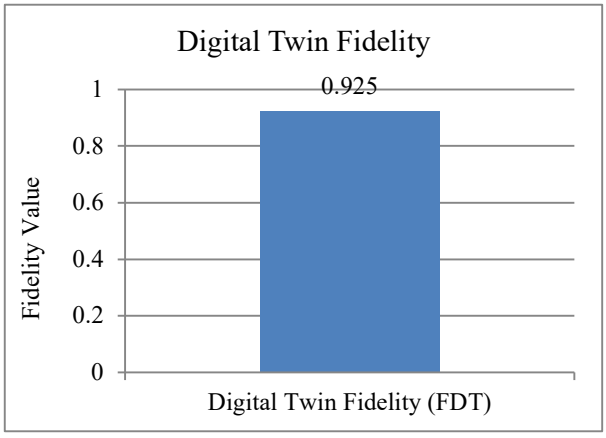

Fig. 9 Measured Digital Twin Fidelity Demonstrating High Accuracy in Cyber Resilient Cloud–Edge Information Systems

Figure 9 provides context for this paper's discussion on Cyber Resilient Cloud and Edge Digital Platforms. The above bar chart illustrates the quantified Digital Twin Fidelity or (F_{DT})An essential figure that must always be guaranteed in a Digital Twin to ensure an exact replication of its physical counterpart.

The figure, as shown in the bar chart, measures a high Digital Twin fidelity level at 0.925, implying an exact correlation between the state of the physical System under consideration and that of its virtual version. This state of accuracy in the digital representation of any data-driven information system is essential in detecting anomalies.

This quantified Digital Twin fidelity figure implies that the platform ensures the elimination of any possible edge-level sensor noises while retaining the main signal. High Digital Twin fidelity implies that the cyber-resilient System can make an accurate distinction between any legitimate system variation and any attempt at varied cyber manipulation.

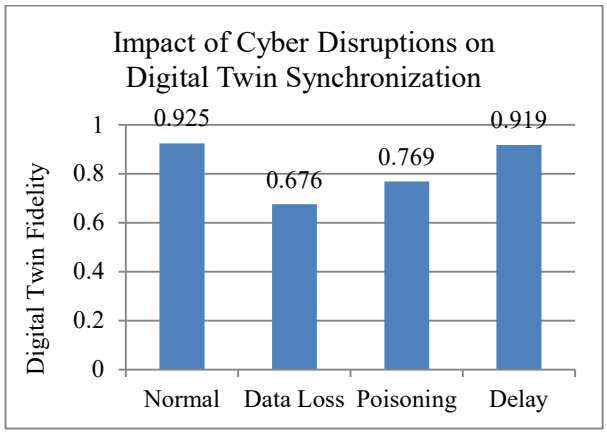

Fig. 10 Impact of Cyber Disruptions on Digital Twin Fidelity across Edge-to-Cloud Platforms

Figure 10 provides the particular case of Cyber Resilient Cloud and Edge Digital Platforms, this bar chart is used to assess quantitatively the impact of different antagonistic factors on the integrity of a Digital Twin. For example, under normal operations, there is an appreciable synchronization between the real world and its Digital Twin, with a high fidelity score of 0.925. However, there are certain cyber factors that substantially downgrade this synchronization. "Data Loss" is identified as the most critical factor that could downgrade the score to 0.676. "Poisoning" cyber-attacks, in turn, reduce the fidelity score to 0.769. "Delays" are identified as the least critical factor in disrupting synchronization, with a high fidelity score of 0.919.

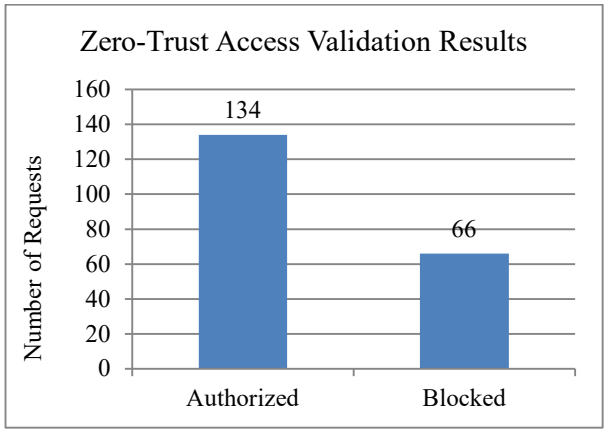

Fig. 11 Zero-Trust Validation: Authorized vs. Blocked Access Requests in a Resilient Information System

Figure 11 presents a visual of the effectiveness of the Zero Trust Access Validation. Within the data-intensive cyber-resilient cloud and edge digital platform, the effectiveness of the Zero Trust Access Validation was evident by the 200 access requests processed by the System and the categorization of access requests based on security protocols. Evidently, the Zero Trust Access Validation mechanism was effective because approximately 134 access requests were successfully authorized, implying that most access requests are legitimate with the enabled digital twin of the digital System. Additionally, the chart portrays the 66 access requests that were blocked by the mechanism of Zero Trust access validation, implying that the Zero Trust architecture was effective in successfully blocking potential malicious attempts to access critical data-intensive digital resources.

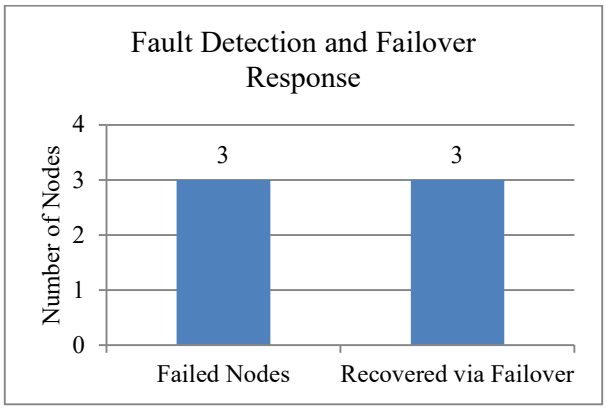

Fig. 12 Fault Tolerance Performance: 100% Node Recovery via Automated Failover Mechanisms

Figure 12 provides the context of Cyber Resilient Cloud and Edge Digital Platforms. The above bar chart represents the evaluation of fault tolerance capability. As is evident from the bar chart, there exists a 1:1 recoverability ratio among the critical infrastructure parts. To be more precise, the System was able to detect 3 Failed Nodes from the network, which was intensive with regard to the data handled. At the very same time, the "Recovered via Failover" metric of the System indicates a 100% efficiency rate with regard to the recovery of 3 Nodes from the network. Such a balance is extremely vital within the context of Digital Twin-enabled systems, where the recovery is instantaneous, thus preventing the loss of data through the failure of the physical components of the edge system.

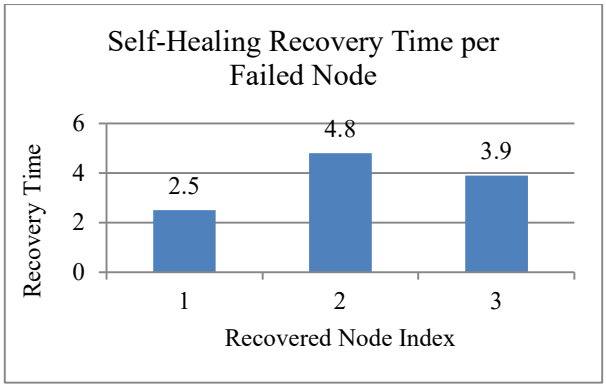

Fig. 13 Self-Healing Performance: Variability in Recovery Time per Individual Failed Node

Figure 13 shows the architecture of Cyber Resilient Cloud and Edge Digital Platforms. The contribution evaluates, through the provided bar chart, the operational efficiency of Self-Healing Recovery Time for failed infrastructure components. The data follows the speed of restoration for three specific recovered nodes. Node 1 is the most efficient with a time of approximately 2.5 units for

recovery, followed by Node 3 at about 3.9 units. In the case of Node 2, it required the longest time, approximately 4.8 units. In data-intensive and digital twin-enabled systems, these are intervals that must be minimized to avoid divergence in the states of the physical and virtual assets. This could give an overview of how variable the recovery times are, providing evidence that the platform non-trivially adapts to heterogeneous faults to ensure high-availability, continuous synchronization from the information system, considering localized failures of its nodes.

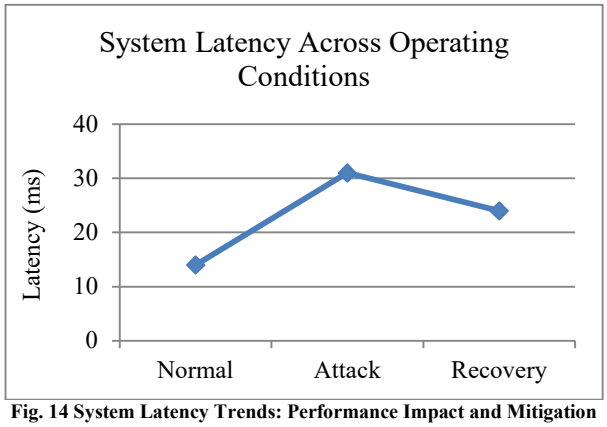

Fig. 14 System Latency Trends: Performance Impact and Mitigation during Cyber Attack and Recovery Cycles

Figure 14 evaluates how the system latency varies at the various stages of operation of a cyber-resilient cloud and edge digital platform. Baseline latency in the System is relatively low, i.e., 13.7 ms in the so-called Normal regime, and this implies that the System can support operations that are data-intensive and fluid-intensive. At one stage of the attack, the curve of Latency reaches the peak of approximately 31.2 ms, and this reflects the time required for the computations of security protocols or interference in digital twin synchronization with adversaries. Once the process of resilience has been initiated, the resilience phase latency reduces considerably to approximately 24.4 ms. This trend gives quantification of the shock absorption capability of the platform, plus it partially recovers performance, but the current Latency signals the security cost that requires payment to ensure system integrity in the post-attack stabilization of the System in a digital twin setup.

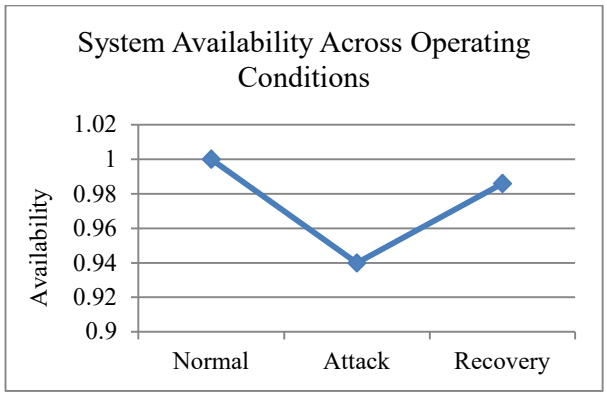

Fig. 15 System Availability Trends: Resilience and Recovery Performance under Adversarial Conditions

The figure on the Cyber Resilient Cloud and Edge Digital Platforms concept illustrates a line graph, where System Availability- the main measure of availability in data-intensive information systems- plots against each other as plotted in Figure 15. When running under Normal conditions, the availability level of our platform stands at 1.00. On the contrary, at the simulated Attack stage of our platform operation, the availability of our System is hit by a sharp decline to about 0.938. The reduction in number is indicative of the ease with which real-time data synchronization in our digital twin concept is susceptible to attacks. The Recovery stage of the data confirms our platform in the provision of cyber resilience by restoring our System to reach a level of 0.986 with regard to availability. Our System can self-heal and recover successfully in case of an attack operation, but still, there is some extent of effect that is observed to necessitate the use of failover techniques.

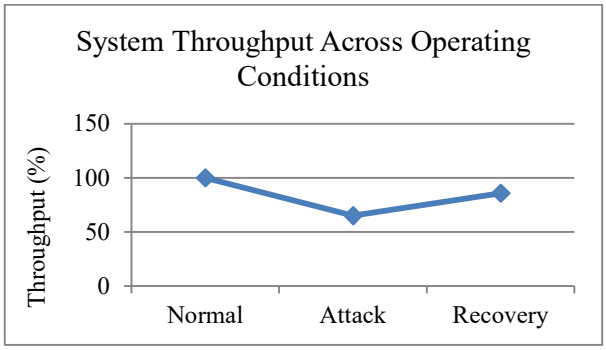

Fig. 16 Throughput Dynamics: Performance Degradation and Partial Restoration during Cyber Attack and Recovery

Figure 16 shows the context of the Cyber Resilient Cloud and Edge Digital Platforms, and the graph represents the evolution of the data efficiency rate, i.e., the System Throughput (%) in the context of the Digital Platforms. It can be typically seen that, within the context of the Normal operation mode, the System Throughput (%) is near-optimal, reaching the high rate of nearly 99.5%, which is acceptable due to the high requirement of data processing that is typically required by various information systems. However, the rate drops dramatically to near 64.8% in the context of the Attack operation mode, showing the high overhead that typically describes the data processing required by the digital systems. During the Recovery operation mode, the rate increases substantially to near 85.9%.

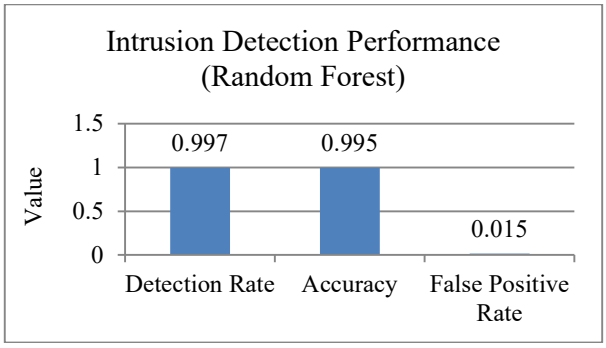

Fig. 17 Intrusion Detection Performance: High-Accuracy Threat Classification using Random Forest Models

Figure 17 provides the architecture of Cyber Resilient Cloud and Edge Digital Platforms. This bar chart measures the performance of a Random Forest-based Intrusion Detection System (IDS). The performance of the System can thus be described as exceptional, given the high classification metrics achieved by the IDS. For example, the Detection Rate is considered high, recording 0.997, while the Accuracy of the System is also high, recording 0.995. The presence of such high accuracy is crucial in any data-driven information systems, given its role in ensuring that all malicious activities are detected by the digital twin information system. At the same time, it ensures that there are no disruptions to the legitimate information flows facilitated by the digital twin-enabled edge-to-cloud information system through the use of a low False Positive Rate, which records only 0.015.

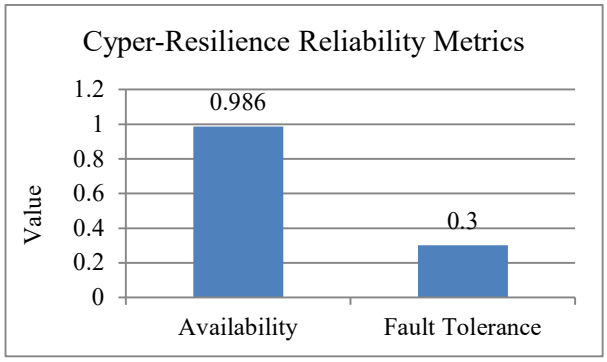

Fig. 18 Resilience Benchmarking: Final Availability and Fault Tolerance Ratings for the Integrated Digital Twin Platform

Figure 18: Framework of Cyber Resilient Cloud and Edge Digital PlatformsAs can be seen in the above bar chart, a definite evaluation of the above metrics related to Cyber Resilience Reliability can be acquired, while the above cyber resilient digital platform reflected a high score of 0.986 in terms of the Availability metric, which comprised a high percentage of 98.6% of the time that this data-intensive information system manages to function even in the presence of adversarial conditions, thereby offering a critical recovery criterion in consideration of the fluctuations that were observed during the past cycles of operation. Moreover, the System also reflects a number that measures the Fault Tolerance metric at 0.300, comprising the inherent capability of the information system to function while some of the edge components and cloud nodes fail.

Figure 19 represents the final operational state of a data-intensive information system while in its recovery phase, in the context of Cyber Resilient Cloud and Edge Digital Platforms. The Latency stabilizes at 24.36 ms, higher than the baseline but successfully mitigated from the peak of 31.2 ms during active adversarial conditions. System Throughput has been recovered to 85.85%, which represents a resilient recovery from the 64.8% drop caused by cyber disruptions. Besides, Resource Utilization remains at 63.12%, whereby the synchronization of the Digital Twin does not over-leverage the edge to cloud infrastructure. Finally, Response Improvement by 6.87 units quantifies efficiency gains by self-healing protocols that ensure long-term reliability in digital twin-enabled frameworks.

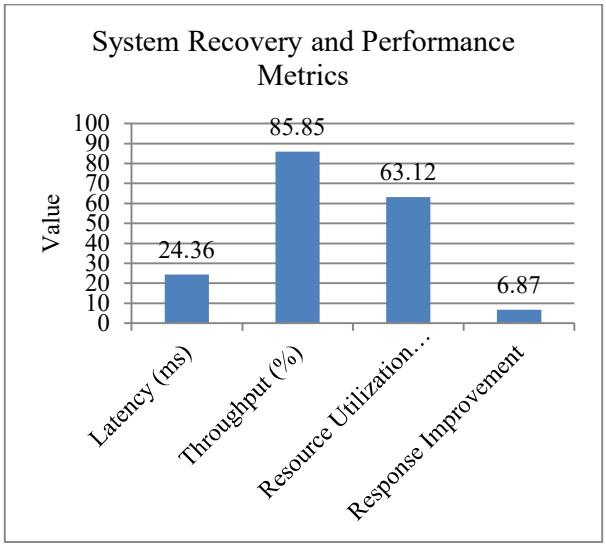

Fig. 19 Post-Attack Stabilization: System Performance and Resource Efficiency Metrics during the Recovery Phase

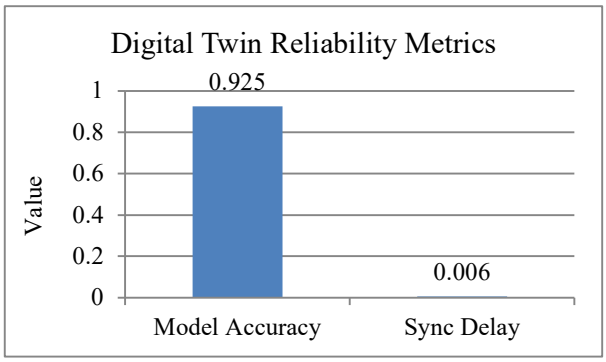

Fig. 20 Digital Twin Reliability: High Model Accuracy paired with Minimal Synchronization Delay

Figure 20 shows the context of a Cyber Resilient Cloud and Edge Digital Platforms. This bar chart analyses the Digital Twin Reliability Metrics that are considered essential in a data-intensive information system. The digital platform provides an increased Model Accuracy of 0.925. This is because the digital twin achieves almost perfect correlation with the actual counterpart existing in the real world at 92.5%. In order to enhance the accuracy of the digital twin application with such high values, the Sync Delay is similarly minimized to an extremely low value of 0.006. Such low values of time delays are very critical during the synchronization of an information system, particularly in an environment where an extremely high demand is recorded during the processing of digital information.

5. Conclusion

The Study has managed to demonstrate the vitality of incorporating cyber-resistant features like zero-trust access, self-healing systems, and automated failover into the system design and architecture, besides the integrity of data-

intensive digital twin environments. The experimental analysis of the System has determined that despite the reputable impact of cyberattacks on the performance of the System, the effectiveness of the proposed architecture was rather high in ensuring system integrity against cyberattacks. As an example, a near-perfect intrusion detection rate of 99.95 was registered in the System, with a 100% rate of node recovery. In addition, the System has maintained a high availability rating of 0.986 under cyber-attack conditions, as well as maintained a throughput of 85.85% at the recovery stage. This type of research also highlights the importance of the fidelity of Digital Twin Technology, which was configured to 0.925 to ensure that virtual representations are faithful to physical assets since they might be susceptible to operational noises or assistive malicious attacks. This Study represents a comprehensive organizational framework that enables organizations to have reliable, coordinated, and safe systems of information. Considering the ability to detect and the efficiency of self-healing operations, the research guarantees that organizations will experience continuous functioning and remain loyal in decision-making in an increasingly interconnected and threatening digital environment.

References

[1] Maryam Farsi et al., "A Standardised Digital Twin Design Framework for Transport System Decarbonisation," *SSRN*, pp. 1-46, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[2] Wajih Abdallah, and Mansoor Alghamdi, "Digital Twin-enabled AI for Sustainable Traffic Management: Real-time Urban Mobility Optimization in Smart Cities," *PeerJ Computer Science*, vol. 12, pp. 1-28, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[3] Abhishek Baer, "A Cloud-Edge Digital Twin Architecture for Adaptive Battery Health Management in Sustainable Transport Systems," *Electrical and Electronic Engineering*, pp. 1-11, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[4] Manolya Kavakli-Thorne, "Digital Twin Building Blocks for Designing a Generic City-Wide Data Exchange Platform," *Data Structures, Algorithms and Complexity*, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[5] Diagram. [Online]. Available: https://www.researchgate.net/publication/333888971/figure/fig5/AS:771676560166922@1560993437827/Digital-twin-shop-floor-based-on-edge-computing-fog-computing-and-cloud-computing.ppm

[6] Image. [Online]. Available: https://www.mdpi.com/electronics/electronics-13-01373/article_deploy/html/images/electronics-13-01373-g003.png

[7] Konstantinos Evangelos Kampourakis, Vasileios Gkioulos, and Sokratis Katsikas, "Cybersecurity Digital Twins for Industrial Systems: From Literature Synthesis to Framework Design," *Information*, vol. 17, no. 3, pp. 1-38, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[8] Rong Zhou et al., "Digital Twin AI: Opportunities and Challenges from Large Language Models to World Models," *arXiv preprint*, pp. 1-132, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[9] Hideki Nishizawa et al., "Leveraging Digital Twin Technologies: All-Photonics Networks-as-a-Service for Data Center Xchange in the Era of AI [Invited Tutorial]," *arXiv preprint*, pp. 1-22, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[10] Gizealew Dagnaw, Roberta Capuano, and Henry Muccini, "Digital Twins for Cultural Heritage: A Systematic Analysis of the State of the Art," *ACM Computing Surveys*, vol. 58, no. 9, pp. 1-35, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[11] Philipp Mandl et al., "Cloud-Based Digital Twins for Vehicle Dynamics Control with Application to Lateral Stability Enhancement," *IEEE Access*, vol. 14, pp. 1799-1811, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[12] Yurii Litvinov et al., "Theoretical Foundations for Developing a Digital Soil Twin for Southern Russia," *Eurasian Journal of Soil Science*, vol. 15, no. 1, pp. 141-148, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[13] Christos L. Stergiou, and Kostas E. Psannis, "Digital Twin Intelligent System for Industrial Internet of Things-based Big Data Management and Analysis in Cloud Environments," *Virtual Reality & Intelligent Hardware*, vol. 4, no. 4, pp. 279-291, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Krishnashree Achuthan, Brij B. Gupta, and Raghu Raman, "Bridging Cybersecurity with Digital Twin Technology: A Thematic Analysis," *International Journal of Information Security*, vol. 24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[15] Shohin Aheleroff et al., "Digital Twin as a Service (DTaaS) in Industry 4.0: An Architecture Reference Model," *Advanced Engineering Informatics*, vol. 47, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Zhiyuan Li et al., "A Reference Framework for the Digital Twin Smart Factory based on Cloud-fog-edge Computing Collaboration," *Journal of Intelligent Manufacturing*, vol. 36, pp. 3625-3645, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Andrea Salvi, Paolo Spagnoletti, and Nadia Saad Noori, "Cyber-resilience of Critical Cyber Infrastructures: Integrating Digital Twins in the Electric Power Ecosystem," *Computers & Security*, vol. 112, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Jiaxuan Han et al., "Cloud-edge Hosted Digital Twins for Coordinated Control of Distributed Energy Resources," *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 1242-1256, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Sagheer Khan, Tughrul Arslan, and Tharmalingam Ratnarajah, "Digital Twin Perspective of Fourth Industrial and Healthcare Revolution," *IEEE Access*, vol. 10, pp. 25732-25754, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Erik Schultes et al., "Fair Digital Twins for Data-intensive Research," *Frontiers in Big Data*, vol. 5, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Luis Felipe Villegas et al., "Towards a Digital Twin Lifecycle Management Framework," *Enterprise Information Systems*, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[22] Cheng Qian et al., "A New Layer Structure of Cyber-physical Systems Under the Era of Digital Twin," *ACM Transactions on Internet Technology*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Raihan Kabir et al., "A Comprehensive Survey on Advanced Data Science Platforms for Cyber-Physical Systems, Digital Twins, and Robotics," *IEEE Access*, vol. 19, pp. 177269-177304, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[24] Edoise Areghan, "Cyber Resilience in Digital Twin and Smart Manufacturing Environments: Challenges, Strategies, and Future Direction," *Journal of Computational Analysis and Applications*, vol. 34, no. 8, pp. 573-593, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[25] Dinesh Sahu et al., "Adaptive Fault Tolerance Mechanisms for Ensuring High Availability of Digital Twins in Distributed Edge Computing Systems," *Scientific Reports*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Luigi Coppolino et al., "Building Cyber-resilient Smart Grids with Digital Twins and Data Spaces," *Applied Sciences*, vol. 13, no. 24, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Gregory Epiphaniou et al., "Digital Twins in Cyber Effects Modelling of IoT/CPS Points of Low Resilience," *Simulation Modelling Practice and Theory*, vol. 125, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] R. Suganya et al., "An Integration of Digital Twin and 6G Edge Computing Approach to Secure Cyber Physical Systems," *Wireless Personal Communications*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[29] Mohammad Ismail Hossain et al., "Linking Digital Twin Paradigm for Urban Heat Monitoring and Policy Integration to Building Smart City Climate Resilience," *Discover Cities*, vol. 3, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[30] Abdullah Alourani et al., "Hybrid AI-IoT Framework with Digital Twin Integration for Predictive Urban Infrastructure Management in Smart Cities," *Computers Materials & Continua*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[31] Cristina Alcaraz, Iman Hasnaouia Meskini, and Javier Lopez, "Digital Twin Communities: An Approach for Secure DT Data Sharing," *International Journal of Information Security*, vol. 24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[32] Ahmed K. Jameil, and Hamed Al-Raweshidy, "Enhancing Offloading with Cybersecurity in Edge Computing for Digital Twin-driven Patient Monitoring," *IET Wireless Sensor Systems*, vol. 14, no. 6, pp. 363-380, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[33] Kaggle, Edge-IIoTset Cyber Security Dataset of IoT & IIoT. [Online]. Available: https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot