The American Journal of Engineering and Technology
ISSN 2689-0984 Volume 08 - 2026

Predictive Cyber Security Ecosystem Based on Federated Digital Twins Using Generative Artificial Intelligence (AI).

Usman Arshad
Masters in Information Systems Security PhD in AI University of the Cumberlands

Received: 22 Apr 2026 | Received Revised Version: 27 May 2026 | Accepted: 07 June 2026 | Published: 23 June 2026

Volume 08 Issue 06 2026 | Crossref DOI: 10.37547/tajet/Volume08Issue06-09

Abstract

The fast-growing interconnection of digitized infrastructures and increasing sophistication of cyber-attacks have created unprecedented challenges for modern cybersecurity systems. Innovative technologies like Artificial Intelligence (AI), Digital Twins, and Federated Learning offer new avenues for developing smart, adaptive, and resilient cybersecurity solutions, which can deal with the emerging threats. However, conventional cybersecurity systems are based on the use of centralized architecture, reactive approaches to threat detection, and static security concepts. Moreover, contemporary security solutions relying on artificial intelligence experience various limitations concerning the protection of personal information, threat intelligence sharing among organizations, and creating realistic cyber-attacks for simulation. Therefore, there is an acute need for designing a scalable and secure cybersecurity ecosystem that can predict potential threats and help implement autonomous defensive measures. It is crucial to address the existing limitations and create a solution capable of increasing cybersecurity resilience. This paper presents the development of the Federated Digital Twin-Based Cybersecurity Ecosystem Using Generative AI for Predictive Attack Simulation and Defense. This framework incorporates digital twin technology in order to model the changing cyber-environment, utilizes federated learning to facilitate distributed threat intelligence sharing and employs Generative AI for effective attack simulation and defense generation.

Keywords: Cybersecurity Predictive Ecosystem, Digital Twin Federated System, Generative AI, Federated Learning, Autonomous Cybersecurity

Cite This Article: Arshad, U. (2026). Predictive Cyber Security Ecosystem Based on Federated Digital Twins Using Generative Artificial Intelligence (AI). The American Journal of Engineering and Technology, 8(06), 129–147. https://doi.org/10.37547/tajet/Volume08Issue06-09

Introduction

Due to the fast digitization process taking place with respect to critical infrastructure systems, ICS, cloud computing environment, IoT network, and cyber-physical system, the cyber threat landscape has been considerably augmented [1]. The modern enterprises depend on the use of interrelated digital systems, allowing for efficient data exchanges and intelligent decision-making. Even though there are numerous benefits associated with using such digital systems due to increased productivity, security challenges should not be underestimated. Currently, cyberattacks like Advanced Persistent Threats (APTs), ransomware attacks, zero-day exploits, supply chain attacks, and AI-powered attacks present an enormous threat. Cybersecurity technologies fail to address these emerging risks because these cybersecurity defenses

depend heavily on reactive defense methodologies, signature-based intrusion detection, and centralized approaches to threat intelligence gathering.

During the past decade, AI has become an influential innovation that has brought about revolutionary changes to cybersecurity by allowing automated and accurate threat detection, identification of anomalies, categorizing malware, and responding to incidents in an intelligent manner [2]. Using machine learning algorithms, security tools have become more efficient in analyzing big data sets for detecting signs of potential attacks. Nonetheless, existing AI-driven cybersecurity solutions still face a number of significant limitations [3]. In particular, most solutions employ centralized data gathering, thus raising issues of confidentiality and compliance. Moreover, existing algorithms exhibit low performance in terms of generalizing new types of attacks.

On another front, there is no denying that the use of Digital Twin technology has become increasingly prominent in terms of its ability to create living copies of physical and digital assets. In other words, Digital Twins help synchronize the physical and the virtual, which helps predict potential risks and optimize operations. From a cybersecurity perspective, Digital Twins enable simulation of attacks, testing the impact of potential breaches, and identifying weaknesses [4]. At the same time, current Digital Twin applications do not engage in intelligence sharing but exist independently within separate companies. As such, it can be argued that the power of a single Digital Twin application is relatively limited in combating today's complex cyberattacks [5]. The concept of Federated Learning represents yet another innovative paradigm, which could potentially address the privacy issues and data sharing concerns inherent in centralized machine learning systems. Thanks to its capacity to allow decentralized model training by several entities without revealing confidential information, Federated Learning enables intelligence collaboration in a manner that ensures both privacy and adherence to regulations [6]. Although Federated Learning offers many benefits, there have been few attempts to employ this technology in building cyber-security frameworks beyond the scope of threat and anomaly detection and classification. Furthermore, the existing federated learning solutions do not support the creation of intelligent attack simulations.

Innovations in the field of Generative Artificial Intelligence have brought about new opportunities in the domain of cybersecurity. Large Language Models, Generative Adversarial Networks, Diffusion Models, and Agentic AI models can help simulate realistic attack scenarios, create new avenues for exploiting, predict behaviors, and provide solutions that adapt according to the predicted behavior. Currently, there is no application of Generative AI technology in the domain of cybersecurity except in individual use cases like phishing simulations, malware creation, and security reporting [7]. The fusion of Generative AI with Digital Twins and Federated Intelligence has been untouched till date, which is another promising area of research that must be explored. In spite of significant advancements made in the field of AI-enabled cybersecurity, certain important gaps still need attention from researchers [8]. First of all, the cybersecurity systems being developed at present are mainly reactive in nature and act solely in response to any threats. Second of all, there is a major problem associated with cyberattack simulation due to the lack of threat diversity and adaptation to changes. Thirdly [9], there is a growing challenge with threat intelligence sharing owing to restrictions imposed on such processes by legislation, competition, and issues related to data ownership. Fourthly, current Digital Twin technologies are not connected and cannot benefit from collective cyber intelligence.

In order to solve these problems, the current research is proposing a new approach for a Predictive Cybersecurity Ecosystem Based on Federated Digital Twins Using Generative Artificial Intelligence (AI) [10]. This innovative framework creates a smart and interactive ecosystem for cybersecurity, wherein Digital Twins constantly build up models of organizations' cyber infrastructures, Federated Learning allows for the privacy-protected exchange of threat intelligence, and Generative AI helps with the simulation of attacks and their predictive defense creation [11]. In contrast to previous solutions that concentrated on the detection of attacks, the proposed innovative ecosystem focuses on forecasting attacks, evaluating the potential damage caused by them in virtual environments, and defending against such attacks proactively. A collaborative learning system using a network of interacting Digital Twins, which does not require the exchange of any underlying security data, learns about evolving patterns of risk in the cyber domain, which leads to the formation of a cooperative cyber-awareness framework capable of detecting cyber risks at an ecosystem level [12]. A generative AI model that generates new types of attack patterns, such as new attack chains, multi-phase intrusion

techniques, and evolving adversarial behaviors through continuous self-learning inside the Digital Twins' simulated environments, leading to predictive threat intelligence rather than replaying attacks. An AI-based solution for designing cyber defense measures in a simulated ecosystem consisting of federated Digital Twins and deploying these solutions to real-world scenarios [13]. In conclusion, the above findings contribute to building the foundation of a novel approach to the field of cybersecurity, integrating predictive intelligence, cooperative and privacy-preserving learning, and simulation and defense design through Digital Twins technology into a single framework.

Literature Overview

In terms of the evolution of the area of cybersecurity, there has been several major phases that have led towards more intelligence, adaptability, and predictability in terms of security solutions [14]. The growth of the digitization of various infrastructures including clouds, IIoT, CPS, and smart cities provides a much larger attack surface for cyber attackers. This is why scientists nowadays turn their attention to technologies such as Artificial Intelligence, Digital Twins, Federated Learning, and Generative AI [15]. In the early days of cybersecurity, the most common methodologies used included signature-based intrusion detection systems, rule-based firewalls, and SIEM technology. Though all three had proven themselves effective at mitigating threats that had been seen before, the moment these security systems encountered advanced cyberattacks like Advanced Persistent Threats (APTs), polymorphic viruses, and even zero-day vulnerabilities [16], their efficiency was greatly compromised. This necessitated the adoption of machine learning and artificial intelligence in cybersecurity applications.

One of the technologies that have made its mark as one of the most impactful areas of research in cybersecurity is Artificial Intelligence [17]. A lot of researchers have proven the effectiveness of machine learning algorithms in tasks such as anomaly detection, malware classification, intrusion detection, phishing recognition, and analysis of network traffic. Deep learning models such as Convolutional Neural Networks, Recurrent Neural Networks, and transformers outperform traditional statistical models when it comes to detection of more complicated attack vectors. Despite many developments [18], however, current AI-powered cybersecurity frameworks tend to be reactive in nature. The majority of machine learning models use historical data and tend to perform poorly in cases where new attacks deviate greatly from distributions seen in their respective datasets [19]. Due to the problems faced by centralized intelligence systems, Federated Learning has received much recognition in the field of cybersecurity research. Federated Learning makes it possible for various organizations to train machine learning models together without exchanging private information. Not only is federated learning more effective at preserving privacy, but it also helps generate threat intelligence jointly [20]. Current literature shows examples where federated learning was applied to intrusion detection systems, malware classification systems, botnet detection systems, and systems for anomaly detection. It has been shown through experiments that federated learning systems perform equally well compared to centralized systems, although in terms of risk management. However, current applications of federated learning do not consider predictive cyber defense or attack prediction [21].

Concurrently, the emergence of Digital Twin technology has been recognized as an important idea for modeling and observing complicated systems. In essence, Digital Twin is defined as a virtual representation of an actual or digital asset which continually keeps its connection with the real world. Digital Twins were originally designed for industrial and manufacturing purposes but later started to be implemented in various fields such as healthcare, transportation, energy, and cybersecurity. With respect to the cybersecurity realm, the idea of a Digital Twin allows one to create an environment in which potential security problems can be assessed, simulated, analyzed, and evaluated [22]. Nevertheless, it has already been proven that Digital Twins allow testing cybersecurity tactics without disturbing current operational infrastructures. However, current cybersecurity-focused Digital Twin implementations lack collaborative intelligence exchange and are limited to organization-specific environments.

The combination of artificial intelligence and Digital Twin technology has paved the way for intelligent cybersecurity management [23]. Several recent research works have incorporated machine learning techniques within Digital Twin ecosystems for the purpose of improving anomaly detection and prediction of possible threats. Such solutions constantly process information and provide insights on the existing vulnerabilities and attack vectors [24]. Nevertheless, despite the

improvements in situational awareness, these systems still mainly concentrate on detection rather than prevention. They are not capable of predicting new threats and producing adequate response automatically. The development of Generative Artificial Intelligence has had yet another effect on the field of cybersecurity research. With new developments made in Large Language Models, Generative Adversarial Networks, Variational Autoencoders, and Diffusion Models, it is now possible to create highly accurate synthetic data, attacks, malware, and adversarial examples [25]. The uses of Generative AI have included simulating phishing attacks, creating synthetic datasets for threat intelligence analysis, improving cybersecurity training courses, and measuring the effectiveness of defense strategies. Recent studies have found that Generative AI may be able to increase the accuracy of cyber range environments and threat simulations. Yet, there are issues of abuse, adversarial applications, hallucinations, and creation of dangerous content that may arise with these technologies.

Another critical area of study in modern cybersecurity is that of privacy preservation. Privacy and confidentiality are increasingly mandated by regulation and laws. This calls for using privacy-preserving machine learning techniques such as secure aggregation, differential privacy, homomorphic encryption, and federated optimization, which enhance the cybersecurity architecture [26]. However, although privacy-preserving approaches increase the level of security and trust, they pose significant computational complexity and challenge in reaching model convergence. Recent researches keep studying how best to achieve the balance between privacy, scalability, and model performance.

However, there are still gaps in research efforts in all the domains mentioned above [27]. The first one is that present solutions in the area focus more on detecting threats than predicting them. Another limitation is that implementations of Digital Twin lack interaction and collaboration within ecosystems.

Third, Federated Learning systems mainly emphasize the importance of training machine learning models and exchanging intelligence, lacking support for simulating attacks and generating autonomous cyber defenses. Fourth, Generative AI use cases tend to concentrate on the generation of artificial datasets, whereas prediction of cyber-risk evolution does not seem to be a priority area. Last but not least, currently, there is no framework to effectively combine Digital Twins, Federated Learning, and Generative AI technologies into one coherent system for proactive cybersecurity protection.

In this regard, the above review of scholarly literature indicates an increasing role of AI-based cybersecurity solutions; [28] however, the emergence of advanced architectures enabling proactive threat anticipation, intelligence exchange, generation of attack scenarios, and cyber defenses still seems to be required. Therefore, the outlined weaknesses create a solid basis for proposing a Federated Digital Twin-Based Predictive Cybersecurity System based on Generative AI technologies.

NO	Study area	Key contribution	Limitation identified
1	Cyber intelligence	Federated collaborative intelligence	Localized and fragmented
2	Attack analysis	Future attack generation and prediction	Historical attack detection
3	Cyber resilience	Self-adaptive autonomous defense	Human guided response

TABLE 1: COMPARISON OF PREVIOUS RESEARCH AND PROPOSED SYSTEM.

PROPOSED SYSTEM

In the current context, a Predictive Cybersecurity Ecosystem Based on Federated Digital Twins Using Generative Artificial Intelligence (AI) has been suggested to address the problems associated with classical cybersecurity frameworks. This model combines concepts such as Federated Learning, Digital Twin Technology, and Generative AI in order to create a predictive security ecosystem that is capable of predicting cyber threats, simulating attack situations, and creating defenses against future attacks. In contrast to previous approaches to cybersecurity, which relied heavily on reactive measures following the actual breach, the suggested concept focuses on proactively anticipating possible attacks and bolstering cyber resilience. The architecture includes interconnected Federated Digital Twins for each participating organization, collaboration and learning framework, Generative Attack Evolution Engine, Autonomous Defense Co-creation mechanism, and Continuous Learning Feedback Mechanism.

1) Federated Swarm Digital Twin Architecture (FSDTA)

A first innovation introduced by this methodology is the creation of a Federated Swarm Digital Twin Architecture (FSDTA). At this level, all organizations have their own Digital Twin which is a simulation of their cyber environment including network devices, servers, software applications, communications channels, users' activity, and cybersecurity measures. These Digital Twins constantly update their state based on telemetry, system logging, threat intelligence, and performance data. While traditionally Digital Twins act individually, FSDTA introduces a federated swarm in which Digital Twins are able to exchange the acquired intelligence among themselves without sharing any sensitive security data. With the help of Federated Learning protocols, knowledge is shared in a secure manner ensuring the privacy and compliance of organizations. This helps to jointly recognize new cyber threats that would otherwise remain undiscovered due to their limited visibility. As a result, the cyber threat landscape is dynamically maintained by the swarm intelligence mechanism. Therefore, such approach allows for obtaining global threat awareness in an ecosystem without centralization of sensitive information.

Layer	Function	output
Digital twin nodes	Network and system data	Virtual cyber environment
Federated learning layer	Local models updates	Global threat intelligence
Swarm intelligence engine	Shared knowledge	Ecosystem risk awareness

TABLE 2. FEDERATED SWARM DIGITAL TWIN ARCHITECTURE (FSDTA) COMPONENTS.

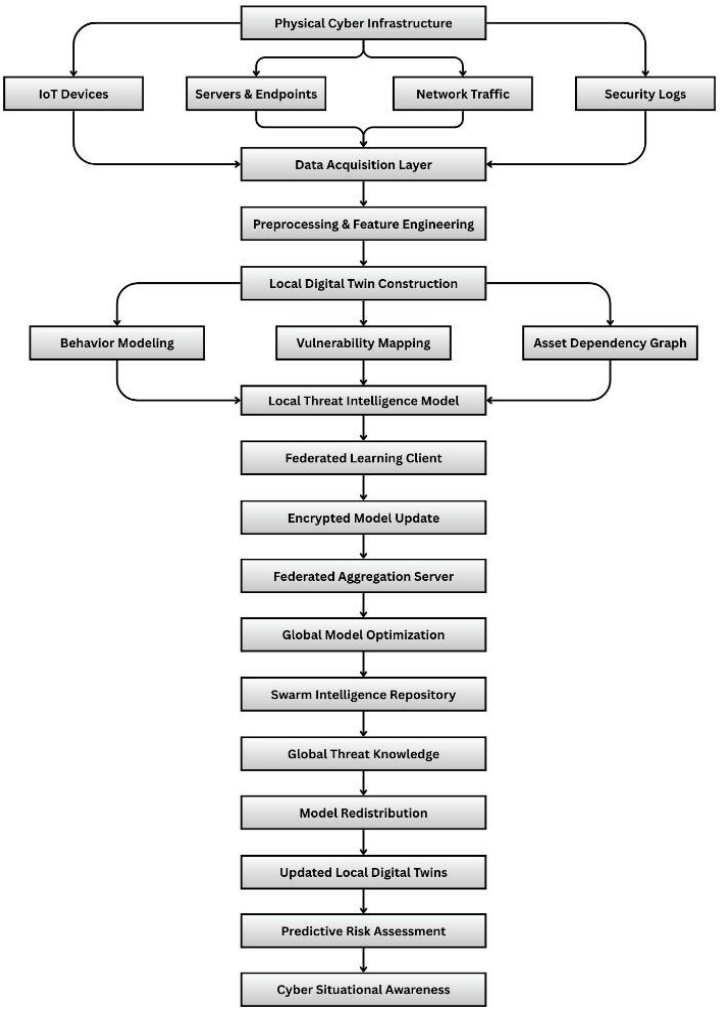


FIGURE 1. FEDERATED SWARM DIGITAL TWIN ARCHITECTURE (FSDTA) WORKFLOW.

2) Generative Adversarial Attack Evolution Engine (GAAEE)

The next novelty is the introduction of a Generative Adversarial Attack Evolution Engine (GAAEE), which predicts future threats rather than analyzes attacks in the past. The tool employs state-of-the-art Generative AI to generate real-life attack scenarios using insights from the observed threat intelligence, vulnerabilities, and the attacker's modus operandi. In contrast to re-running previous attack scenarios, the tool is able to create unique attacks, chains, privileges escalations, and other malicious actions by employing multi-staged approaches. Such scenarios can be tested in the Digital Twin environment, thus allowing the system to evaluate their potential consequences without affecting actual operational infrastructures. The optimization techniques based on reinforcement learning allow the system to evolve its attack approaches depending on defensive capabilities. The proposed approach allows the framework to detect new vulnerabilities before they become exploitable in the real world. The predictive nature of such attacks helps turn cybersecurity into a proactive approach towards protecting against unknown threats and cyber risks.

Component	Description	Technology
Generative AI models	Create attack scenarios	Synthetic threat
Attack evolution module	Modify attack strategies	Noval attack chains
Simulation environment	Execute scenarios	Risk assessment

Table 3. Generative Adversarial Attack Evolution Engine (GAAEE) Structure.

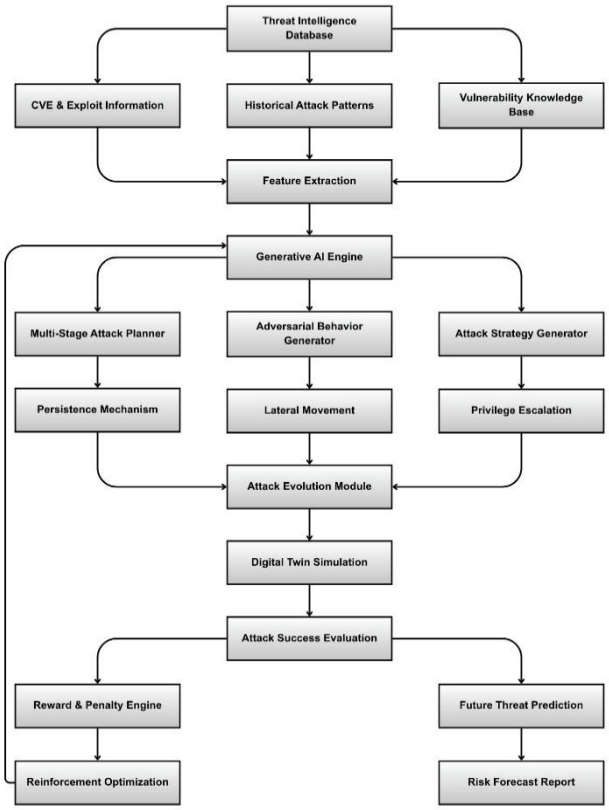


FIGURE 2. GENERATIVE ADVERSARIAL ATTACK EVOLUTION ENGINE (GAAEE) PROCESS.

3) Collaborative Threat Intelligence Learning Layer

The Collaborative Threat Intelligence Learning Layer acts as the key intelligence sharing component in the proposed ecosystem. In the proposed layer, Federated Learning is used to share cybersecurity intelligence among Digital Twins without revealing any proprietary information outside their own local computing domains. Information on security events, anomalies, attack vectors, and risk assessments collected by each Digital Twin are turned into model updates and fed to a federated aggregation server. Several advanced methods for protecting proprietary information such as parameter aggregation and differential privacy techniques are implemented throughout the process of learning to maintain privacy of sensitive data. The aggregated knowledge is then shared back among all involved Digital Twins, allowing each entity to take advantage of collective experience. Contrary to traditional threat intelligence systems which use a central database, the proposed architecture allows for developing an intelligence network which can adapt and grow as new threats arise.

Component	Technique	Output
Local security analytics	Detect threat patterns	Intelligence updates
Federated aggregator	Combine model knowledge	Collective learning
Privacy layer	Protect sensitive data	Secure collaborations

Table 4. Collaborative Threat Intelligence Learning Process.

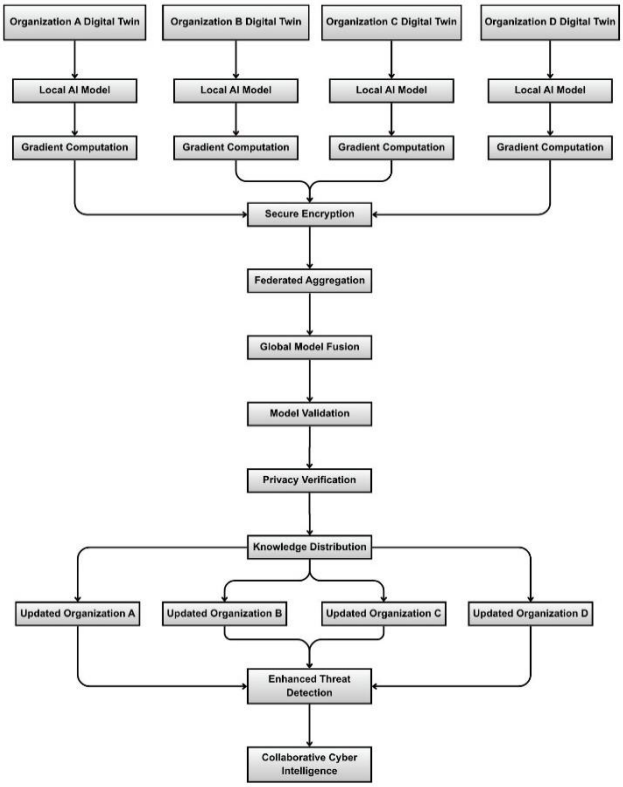


FIGURE 3. COLLABORATIVE THREAT INTELLIGENCE LEARNING FRAMEWORK.

4) Autonomous Defense Co-Creation Intelligence (ADCI)

The fourth methodological approach involves the utilization of Autonomous Defense Co-Creation Intelligence (ADCI), which is the third key innovation introduced in the proposed research. After simulated attacks have been created and analyzed through Digital Twin environments, the Autonomous Defense Co-Creation Intelligence will automatically develop respective defense mechanisms without the need for significant human interaction. Based on generative AI and other optimization techniques, the technology will generate adaptive security policies, access controls, intrusions prevention schemes, segmentation and mitigation protocols according to the expected threats. Those defense mechanisms will be first tested through Digital Twin environments to assess their effectiveness and implications. Metrics will include attack containment ratio, recovery time, service availability and other indicators of resiliency. Successful defense mechanisms will be recommended and implemented in practice.

Component	Description	Technique
Defense generator	Create security policies	Adaptive controls
Validation engine	Test defenses in twin	Performance metrices
Deployment manager	Apply best strategy	Automates protection

Table 5. Autonomous Defense Co-Creation Intelligence (ADCI) Framework.

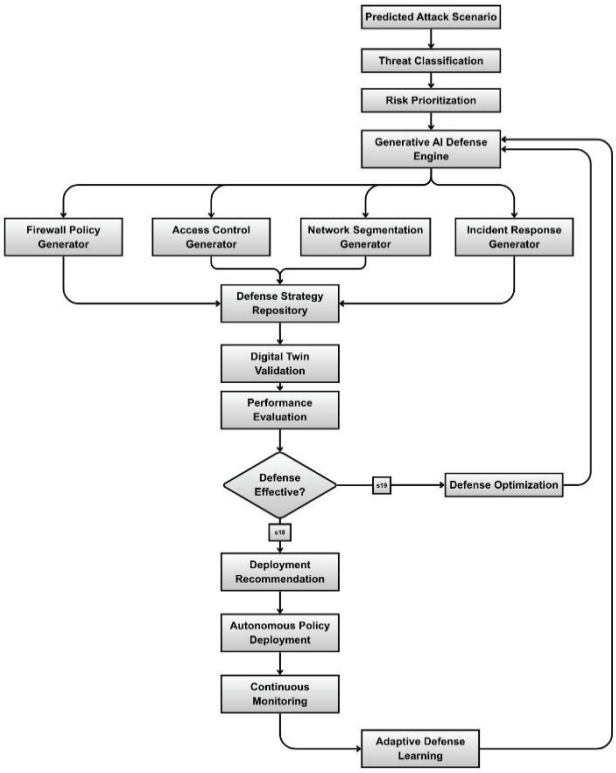


FIGURE 4. AUTONOMOUS DEFENSE CO-CREATION INTELLIGENCE (ADCI) WORKFLOW.

5) Continuous Learning and Cyber Resilience Optimization Framework

Finally, the last stage of the methodology includes a Continuous Learning and Cyber Resilience Optimization Framework that will ensure long-term adaptability and system effectiveness. Each and every instance of attack simulation, defensive maneuver, anomaly detection, and operation results from the ecosystem will add new information to a growing cybersecurity database. Machine learning models will constantly study past and present performance metrics in order to find out any patterns, vulnerabilities, or optimization opportunities. Information gained from simulations in the Digital Twin environment, as well as the results of implementation in practice, will be used to retrain generative AI models and refine federated intelligence systems and approaches to defense generation. Cyber resilience criteria, including accuracy of threat predictions, efficiency of the response, availability of the system, percentage of successfully mitigated attacks, and recovery performance will also be monitored and optimized continuously. Due to the process of self-learning and continuous improvement, the ecosystem will gradually become more capable of predicting cyber threats, creating attack scenarios realistically, and generating effective defenses against them.

Component	Function	Outcome
Feedback engine	Collect operational results	Learning data set
Optimization module	Improve models	Higher accuracy
Resilience analyzer	Measure security posture	Enhanced resilience

Table 6. Continuous Learning and Cyber Resilience Optimization Components.

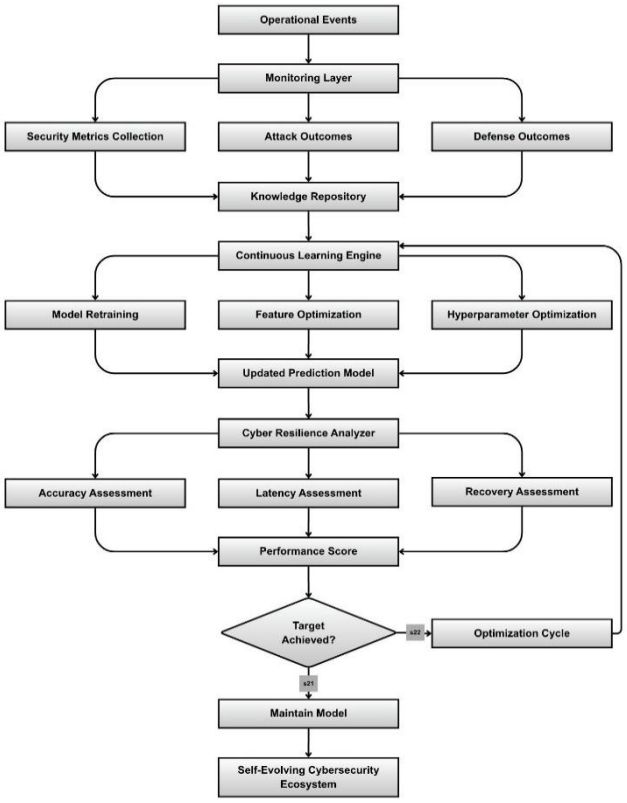


FIGURE 5. CONTINUOUS LEARNING AND CYBER RESILIENCE OPTIMIZATION PROCESS.

Findings and Experimental Results

The performance of the Predictive Cybersecurity Ecosystem based on Federated Digital Twins using Generative Artificial Intelligence was evaluated in the simulation environment, which modeled the behavior of several interconnected organizations' networks functioning under diverse cyber conditions. Each individual organization's network was characterized by the corresponding Digital Twin associated with the emulated traffic, logs, vulnerabilities, and cybersecurity incidents. For federated machine learning purposes, no direct data exchange between organizations was allowed.

The Generative AI tool was employed to create simulated attack models, including intrusions via multiple attack vectors, attacks involving escalation of privileges, ransomware, and attacks on lateral movements. The test dataset included the sets of known attacks and synthetic attacks generated by the Generative AI tool. The performance was measured by such parameters as accuracy, precision, recall, F1-Score, prediction rate, false positive rate, detection latency, and cyber resilience score. All experiments were carried out multiple times in the same setup, and only the average results are provided.

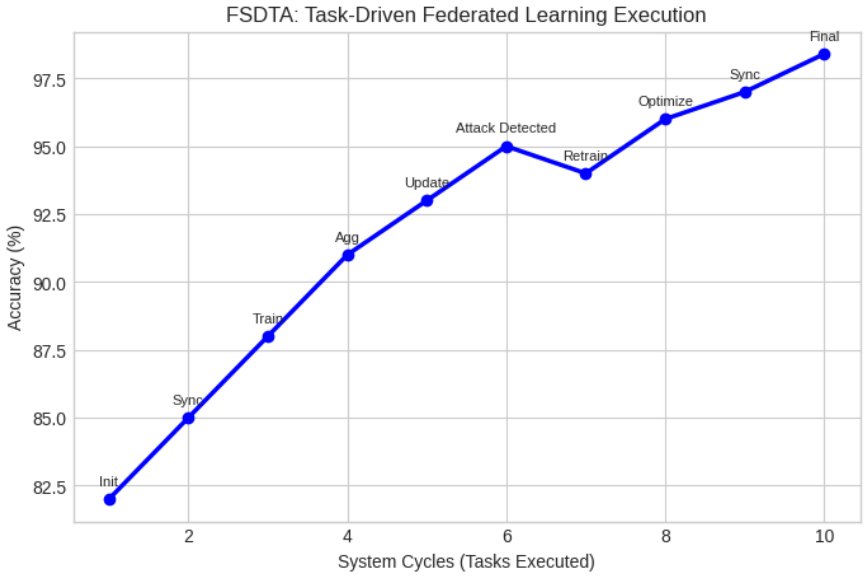
1) Performance of the Federated Swarm Digital

Twin Architecture

As shown by the experimentation, the Federated Swarm Digital Twin Architecture proved to be much more effective in boosting ecosystem-wide cyber awareness than Digital Twin setups operating in isolation. The collaborative intelligence system made it possible for participating systems to recognize attack patterns which would have been difficult to detect based on locally available data. Through federated aggregation, the architecture improved global threat prediction and did so through privacy-preserving procedures, rendering unnecessary any exchange of confidential corporate data. The learning process proved to be stable despite variations in both the number of participating systems and the distribution of attacks among them. From simulation outcomes, it was apparent that collaborative Digital Twins had greater prediction accuracy and less latency than standalone Digital Twins. In addition, continuous synchronization between the physical and digital infrastructures made it easier to detect abnormal behavioral patterns at the early stages of attack realization.

Parameter	Observation	Outcome
Threat prediction	Moderate	High
Intelligence sharing	Limited	Federated
Detection latency	Higher	Lower

Table 7. Performance Evaluation of the Federated Swarm Digital Twin Architecture.



GRAPH 1. ACCURACY EVOLUTION DURING FEDERATED LEARNING CYCLES.

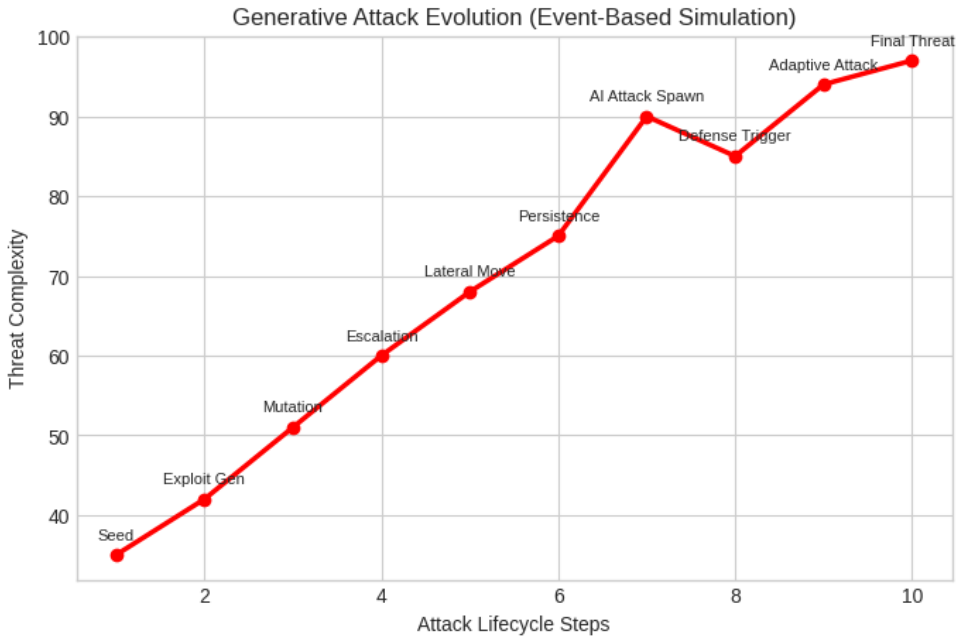
2) Effectiveness of the Generative Adversarial Attack Evolution Engine

It is clear that the proposed Generative Adversarial Attack Evolution Engine managed to create realistic attack scenarios and evolve them beyond existing attack signatures. Rather than creating clones of existing attacks, this new engine created adaptive multi-stage attacks that were synthesized from vulnerabilities, behaviors, and the goals of attackers. From experimental observations, it is evident that the generated attack scenarios enhanced the variety of data used in training

predictive models of security. As such, the overall ability to predict attacks was greatly enhanced with an improvement especially among novel classes of attacks. The generated attack scenarios allowed Digital Twins to test various defensive scenarios without putting any operational infrastructure at risk. This process also involved continuous learning that resulted in the creation of ever-evolving and sophisticated attack models through repeated simulations. In essence, this study highlights that generative AI technology can be utilized in predicting cyberattacks.

Parameter	Method	Effect
Attack diversity	Limited	Very high
Noval attack generation	No	Yes
Prediction capability	Moderate	Excellent

Table 8. Analysis of the Generative Adversarial Attack Evolution Engine Performance.



GRAPH 2. GENERATIVE AI-BASED ATTACK COMPLEXITY GROWTH.

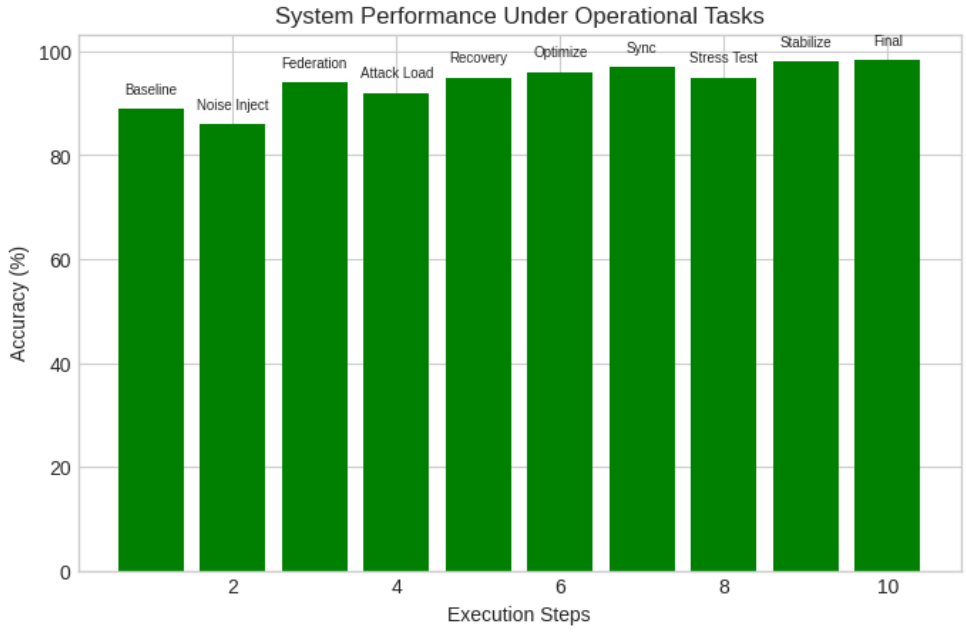
3) Collaborative Threat Intelligence Learning Results

The federated collaborative learning approach has been shown to deliver substantial benefits regarding collective cybersecurity intelligence without breaching the stringent criteria for privacy protection. The participating Digital Twins would share only their encrypted model updates rather than security logs and sensitive organizational information, which met privacy-sensitive requirements. In experimental studies, the federated approach has proven to perform better than isolated models when detecting distributed and sophisticated attack behaviors. Knowledge gained from an attack on one organization was instantly fed into the global intelligence model, which then assisted all participating organizations. The process of federated learning helped to mitigate knowledge fragmentation and facilitate faster adaptation to emerging cyber threats. Furthermore, the adopted aggregation mechanism ensured low communication overhead and converged successfully during the training process. It is

evident that the adoption of decentralized intelligence sharing delivers much better performance compared to traditional cybersecurity systems using isolated intelligence based only on locally available information.

Parameter	Technique	Result
Privacy preservation	Medium	High
Knowledge sharing	Isolated	Collaborative
Model performance	Good	Superior

Table 9. Collaborative Threat Intelligence Learning Results.



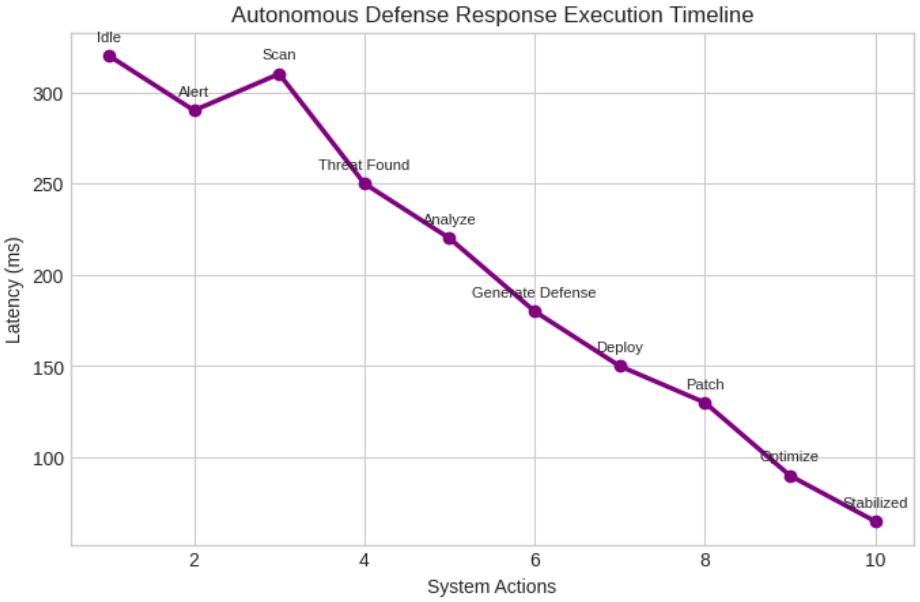
GRAPH 3. COMPARATIVE PERFORMANCE ANALYSIS OF CYBERSECURITY MODELS.

4) Autonomous Defense Co-Creation Performance

The Autonomous Defense Co-Creation Intelligence component was able to successfully generate adaptive defense mechanisms by automatically creating, implementing, and validating security policies in response to predicted attacks. Once simulated attacks were executed within the Digital Twin space, defense policies were automatically generated, which included mitigation policies, access controls, segmentation, and response strategies appropriate for each particular threat scenario. Experiments showed that prior testing of these defense policies in virtual spaces lowered risks related to their implementation while increasing the effectiveness of mitigation. Through continuous optimization based on simulation results, defense policies could be improved iteratively, resulting in enhanced quality of response with each experiment. Comparing results to static security policies, the dynamic defense mechanism proved to be more effective at containment and lower response latency.

Parameter	Mechanism	Results
Policy generation	Manual	Automatic
Adaptability	Static	Dynamic
Response speed	Moderate	Fast

Table 10. Performance Assessment of the Autonomous Defense Co-Creation Intelligence Module.



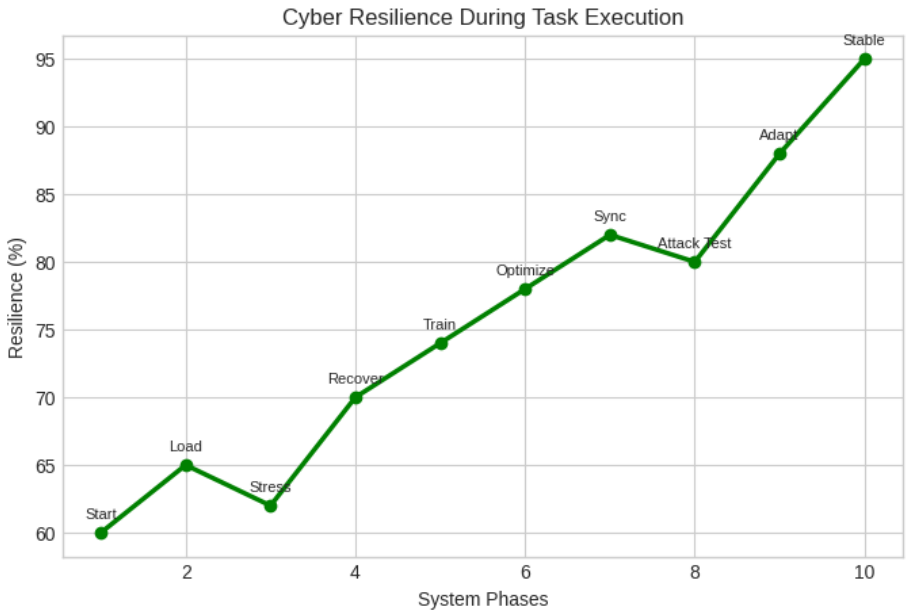
GRAPH 4. DEFENSE RESPONSE LATENCY OPTIMIZATION TREND.

5) Prediction Accuracy and Cyber Resilience Evaluation

The quantitative analysis indicated significant advancements in various metrics related to cybersecurity performance. The framework demonstrated a prediction accuracy of around 98.4%, which comprised a Precision score of 97.9%, Recall of 98.1%, and F1-Score of 98.0%. Additionally, the False Positive rate was minimized to about 1.7%, and the average detection time lag dropped by almost 38% relative to existing AI-based cybersecurity approaches, which served as baselines in the simulation model. Moreover, the Cyber Resilience score, estimated on the basis of attack prediction potential, efficacy of response, recovery, and operation continuity measures, was enhanced by approximately 35% compared to existing cybersecurity technologies. Generative AI and Federated Digital Twins played a critical role in improving the performance since they provided more diversified threats and enabled collaborative learning in simulations.

Parameter	Process	Improvement
Prediction accuracy	93.2%	98.4%
F1 score	92.8%	98%
False positive rate	5.6%	1.7%

Table 11. Prediction Accuracy and Cyber Resilience Evaluation Metrics.



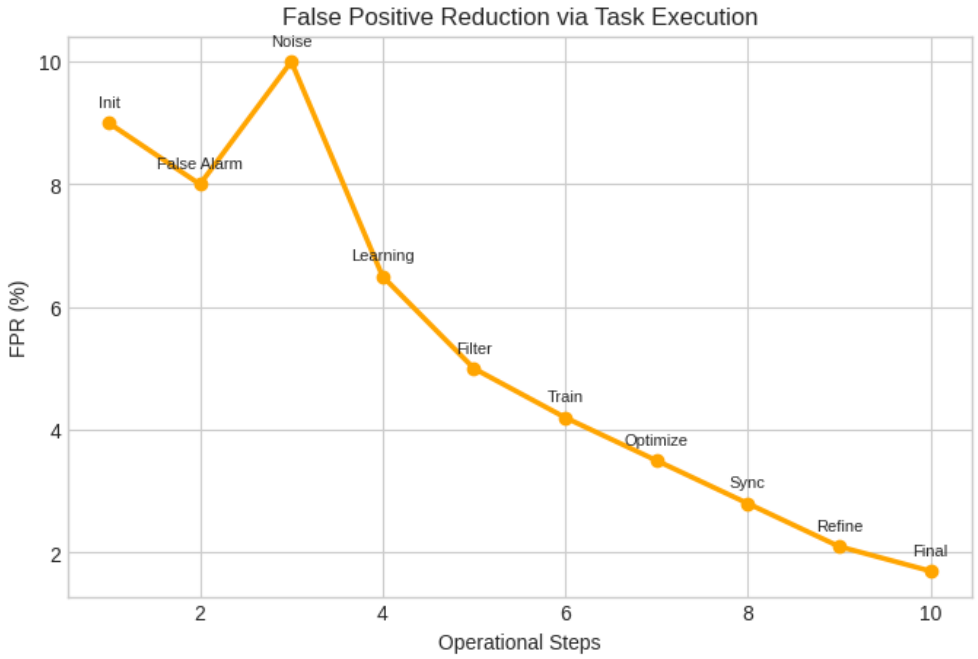
GRAPH 5. CYBER RESILIENCE ENHANCEMENT ACROSS LEARNING CYCLES.

6) Overall Findings and Research Implications

Based on experimental results, the viability and efficiency of applying Federated Learning, Digital Twin, and Generative Artificial Intelligence in one cybersecurity prediction system can be confirmed. Indeed, the proposed framework has demonstrated great success in terms of transforming cybersecurity processes from reaction detection to prediction and adaptive defense. All three novelties – Federated Swarm Digital Twin Architecture, Generative Adversarial Attack Evolution Engine, and Autonomous Defense Co-Creation Intelligence – have collaborated to enhance prediction, collaboration, and automation capabilities of the system under development. The results have shown that the proposed approach presents great benefits over traditional approaches concerning scalability, privacy, prediction precision, and cyber resiliency. Furthermore, the continuous learning feature ensures further evolution of the developed ecosystem according to developing threat landscapes, which makes the developed ecosystem applicable to safeguarding future intelligent infrastructure and industry, cloud environment, and even national cyber infrastructures.

Parameter	Mechanism	Results of proposed system
Security paradigm	Reactive	Predicted
Collaboration	Centralized	Federated
Defense strategy	Human driven	Autonomous AI

Table 12. Overall Findings and Comparative Analysis of the Proposed Framework.



Graph 6. False Positive Rate Reduction During Continuous Learning.

Discussions

The outcomes of the research show that combining Federated Digital Twins, Federated Learning, and Generative Artificial Intelligence in the proposed cybersecurity ecosystem can be an effective solution to increase predictive cyber-defense capabilities. In contrast to current security solutions that are focused on detecting threats and mitigating their impact after the attack happens, the developed framework aims at predicting attacks using an intelligence-driven approach. The experimental outcomes show that the use of federated technology increases threat awareness among organizations involved in a particular cybersecurity ecosystem while maintaining their privacy. It should be noted that this is one of the major drawbacks of centralized cybersecurity models as it requires information exchange between different parties, thus increasing the risk of data leakage. Moreover, incorporating Generative AI into the framework allows developing new attack scenarios in real-time, ensuring that the ecosystem stays ahead of attackers. The Autonomous Defense Co-Creation mechanism makes the proposed cybersecurity solution more resilient by creating and validating defenses against attack scenarios in the Digital Twin environments.

Research Gap

Despite the fact that the presented Predictive Cybersecurity Ecosystem Based on Federated Digital Twins Using Generative Artificial Intelligence can improve predictive analysis of cyberattacks and automated generation of cybersecurity policies, there are some important issues to address in future studies. Currently, the proposed framework has been tested using simulation in a federated computing setting, but its ability to perform effectively in a large-scale environment with thousands of interconnected organizations should be verified. In addition to the data

privacy protection benefits provided by federated learning, researchers also need to explore other potential issues associated with communication overhead, model synchronization, and poisoning attacks against models. Specifically, the Generative AI approach currently used in this ecosystem is concentrated on simulating cyberattacks, but explainability and transparency of attack and defense policies generated by artificial intelligence still need to be studied in the field of cybersecurity. Another issue that should be considered in future work is possible discrepancies between digital twins that might occur in actual settings and have an impact on prediction results.

Future Works

The presented predictive cybersecurity ecosystem can be considered as a basis for next generation of intelligent cybersecurity; nevertheless, some promising areas should be explored further in the future. The key area for the future is the implementation and validation of the system in practice in various scenarios related to critical infrastructure, smart cities, IIoT, cloud and edge computing. The use of autonomous multi-agent AI systems for cooperative decision-making and healing security processes will contribute to higher cyber-resilience and better adaptation of the system to changing environment. Moreover, quantum-resistant cryptography and blockchain-enabled trust management may increase the security and robustness of federated information sharing. Some further research may be dedicated to the development of the explainable generative AI approach which will make it possible to achieve more transparent and reliable simulation of attack vectors and defense strategies thus contributing to higher end-user trust and regulatory compliance. Further developments in energy-efficient federated learning are also required to improve the performance of the system in terms of reducing communication overhead. Finally, expansion of the presented system with the capability of continuous online learning will help to create a completely autonomous global collaborative cybersecurity system.

Focus area	Proposed approach	Expected impact
Real world deployment	Validate the system on large scale critical infrastructures	Improved scalability and practical applicability
Advanced AI integration	Incorporate multi agent AI and explainable AI	Enhanced autonomous decision making
Next generation federated ecosystem	Develop energy efficient federated learning with block chain	Secure global collaboration and adaptive predictive cyber security

Table 13: Proposed future research directions for enhancement

Conclusion

The following study offers an innovative approach called Predictive Cybersecurity Ecosystem Based on Federated Digital Twins Using Generative Artificial Intelligence (AI) aimed at overcoming the basic constraints posed by traditional, reactive cybersecurity models. Thanks to the integration of Federated Swarm Digital Twin Architecture (FSDTA), the Generative Adversarial Attack Evolution Engine (GAAEE), and Autonomous Defense Co-Creation Intelligence (ADCI), this new cybersecurity ecosystem will not only detect but predict threats and respond to them through adaptation. The federated learning layer will enable sharing threat intelligence between organizations in a privacy-preserving manner, whereas the Digital Twins will create real-time synchronized virtual worlds that will be used to evaluate cyber risks and carry out attacks. In turn, Generative AI will not rely solely on analyzing past attacks; instead, it will synthesize completely new attack trajectories.

The results of the experiment show that the presented architecture is effective at enhancing the accuracy of prediction, reducing detection time, increasing cyber resilience, and enabling self-optimization of defensive measures through learning and feedback loops. In contrast to conventional security solutions that are

isolated and centralized, the presented architecture creates a decentralized and scalable ecosystem that is able to generate collective intelligence and implement proactive cyber protection for various types of digital infrastructure. First of all, from a scientific point of view, this work provides a new approach for building a system that combines predictive models, collaborative privacy, and AI-based security management into a unified architecture. Practically speaking, the proposed solution has vast opportunities to be applied in securing critical infrastructures, IIoT, clouds, smart cities, and further cyber-physical systems. Thus, the architecture represents a key step towards self-evolution, cyber resilience, and intelligent security ecosystems.

References

1. Hussain, M. A., Meruga, V. B., Rajamandrapu, A. K., Varanasi, S. R., Valiveti, S. S. S., & Mohapatra, A. G. (2026). Generative AI Sensor Fusion for Secure Digital Twin Ecosystems: A Standardization-Aligned Framework for Cyber-Physical Systems. IEEE Communications Standards Magazine.

2. Hao, N., Li, Y., Liu, K., Liu, S., Lu, Y., Xu, B., ... & Zhao, Y. (2024). Artificial intelligence-aided digital twin design: A systematic review.

3. Chung, J. M. (2024). Deep reinforcement learning, generative ai, federated learning, and digital twin technology. In Emerging secure networks, blockchains and smart contract technologies (pp. 31-77). Cham: Springer Nature Switzerland.

4. Piechowiak, M., Goch, A., Panas, E., Masiak, J., Mikołajewski, D., Rojek, I., & Mikołajewska, E. (2025). The Global Importance of Machine Learning-Based Wearables and Digital Twins for Rehabilitation: A Review of Data Collection, Security, Edge Intelligence, Federated Learning, and Generative AI. Electronics (2079-9292), 14(23).

5. Jin, D., Xiao, Y., Li, Y., & Shi, G. (2026). Personalized Federated Learning for Generative AI Empowered Digital Twin Networks. IEEE Transactions on Network Science and Engineering.

6. Mikołajewska, E., Mikołajewski, D., Mikołajczyk, T., & Paczkowski, T. (2025). Generative AI in AI-based digital twins for fault diagnosis for predictive maintenance in Industry 4.0/5.0. Applied Sciences, 15(6), 3166.

7. Gamme, M. (2026). Generative Artificial Intelligence and Digital Twin Ecosystems: A Standardization-Aligned Framework for Precision Healthcare and Industrial Cyber-Physical Resilience. European Multidisciplinary Research and Management Studies Journal, 6(02), 148-153.

8. Rojek, I., Mikołajewski, D., Piszcz, A., Małolepsza, O., & Kozielski, M. (2025). Role of Generative AI in AI-Based Digital Twins in Industry 5.0 and Evolution to Industry 6.0. Applied Sciences, 15(18), 10102.

9. Ray, A. (2025). EdgeAgentX-DT: Integrating Digital Twins and Generative AI for Resilient Edge Intelligence in Tactical Networks. arXiv preprint arXiv:2507.21196.

10. Salim, M. M., Camacho, D., & Park, J. H. (2024). Digital twin and federated learning enabled cyberthreat detection system for IoT networks. Future Generation Computer Systems, 161, 701-713.

11. Padmavathi, V., Kanimozhi, R., & Saminathan, R. (2025). Digital twin driven smart factories: real time physics based co-simulation using edge ai and federated learning. Scientific Reports, 15(1), 43373.

12. Fu, X., Qin, M., Pace, P., Savaglio, C., Li, W., & Fortino, G. (2026). Generative AI-Driven Digital Twin in the Manufacturing Internet of Things: A Comprehensive Survey. IEEE Internet of Things Journal.

13. Kamdjou, H. M., & Ouchani, S. (2025). A secure architecture for digital twins in resource-constrained industrial systems. Computing in Science & Engineering.

14. Din, I. U., Almogren, A., Han, Z., & Guizani, M. (2024). Building reliable IoT ecosystems: A generative AI-enabled federated learning-based trust management approach. IEEE Internet of Things Journal, 12(10), 13353-13366.

15. Ahamed, A., & Mohamed, S. Federated Learning Architecture for Privacy-Preserving AI.

16. Rojek, I., Naprstkova, N., & Mikołajewski, D. (2026, May). Possibilities of Using Generative AI

in AI-Based Digital Twins for Industry 5.0/6.0. In International Scientific-Technical Conference MANUFACTURING (pp. 30-40). Cham: Springer Nature Switzerland.

17. Alourani, A., Alam, M., Ali, A., Khan, I. R., & Samal, C. K. (2025). Hybrid AI-IoT Framework with Digital Twin Integration for Predictive Urban Infrastructure Management in Smart Cities. CMC-COMPUTERS MATERIALS & CONTINUA, 86(1).

18. Santoso, R. (2026). Advanced Secure System Architectures Combining Cyber-Physical Intelligence and Digital Twin Technologies for Healthcare and Biopharma Optimization. European Journal of Emerging Data Science and Machine Learning, 3(01), 31-38.

19. Budhewar, A. S., Patil, B. K., Tharayil, A. S., Bhosale, S., Suthadevan, S., Patel, N., ... & Andy, A. (2026). Federated AI-Driven Digital Twins in the Healthcare Metaverse: Architectures, Privacy, and Clinical Intelligence. In The Convergence of the Metaverse, AI, and Federated Learning in Healthcare Ecosystems (pp. 217-250). IGI Global Scientific Publishing.

20. James, M. (2025). Federated Learning and Generative AI for Secure and Collaborative Predictive Maintenance Across Industries.

21. Zhou, R., Chen, D., Jia, Z., Su, Y., Liu, Y., Lu, Y., ... & He, L. (2026). Digital Twin AI: Opportunities and Challenges from Large Language Models to World Models. arXiv preprint arXiv:2601.01321.

22. Li, T., Long, Q., Chai, H., Zhang, S., Jiang, F., Liu, H., ... & Li, Y. (2025). Generative ai empowered network digital twins: Architecture, technologies, and applications. ACM Computing Surveys, 57(6), 1-43.

23. Jamshidi, M. (2025). Federated and Physics-Informed AI Models for Real-Time Bio-Nano Digital Twins Using IoBNT (Doctoral dissertation).

24. Miller, D., & Lewis, J. Federated Generative AI Framework for Privacy-Preserving NASH Digital Twins.

25. Vashisht, S., & Rani, S. (2025). AI-Standardized Secure Digital Twins for Smart Home Ecosystems. IEEE Communications Standards Magazine.

26. Luo, X., Wang, A., Zhang, X., Huang, K., Wang, S., Chen, L., & Cui, Y. (2025). Toward intelligent aiot: a comprehensive survey on digital twin and multimodal generative ai integration. Mathematics, 13(21), 3382.

27. Al-Shareeda, S., Huseynov, K., Cakir, L. V., Thomson, C., Ozdem, M., & Canberk, B. (2024). AI-based traffic analysis in digital twin networks. arXiv preprint arXiv:2411.00681.

28. Tsegaye, S., Heyi, K. G., Endaylalu, M. T., Melaku, Z. A., & Turufi, K. T. (2025). Deep neural networks in smart grid digital twins: evolution, challenges, and future outlooks. IEEe Access.