International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s,2025
https://theaspd.com/index.php

Cybersecurity for SDG Digital Initiatives Securing the Future of Sustainable Technology Deployments

[1]Elavarasi Kesavan, [2]R.Nivethikha, [3]Dr. Parin Somani, [4]Lin Yan, [5]Mcxin Tee
[1]Full Stack QA Architect, Cognizant, ORCID Id: 0009-0008-3844-0286, Elavarasikmk@gmail.com
[2]Assistant professor, Sree Sowdambiga College of Engineering
[3]CEO, London Origination of Skills Development (LOSD), UK
[4]Master of Science Program in Psychology, Shinawatra University, 15754963487@163.com, ORCID 0009-0000-5328-8624
[5]Faculty of Business and Communications, INTI International University, 71800 Nilai, Malaysia. ORCID 0000-0001-7990-8377

***Abstract*—** *As digital transformation emerges as the main focus of the United Nations sustainable development goals (SDGs), security needs of digital infrastructure have become even more important than before. Digital solutions that are related to SDGs, such as smart cities, e-governance, healthcare in the digital dimension, and green energy networks, are becoming highly dependent on large-scale networked devices, and cloud infrastructure. They are susceptible to online violence that may interrupt the services, impair information, and fail to inspire confidence. The paper addresses the use of cybersecurity in the protection of SDG-driven technologies by studying challenges and emerging trends in the protection of these technologies and best practices in cybersecurity. The study gives emphasis to case studies, analyzes currently employed frameworks and frameworks a robust approach dealing with secure deployments on digital foundations. This paper will support the idea of secure digital foundation to ensure the sustainability of a future; the paper is proposing to incorporate cybersecurity into the lifecycle of sustainable innovations.*
***Keywords*–** *Cybersecurity, Sustainable Development Goals, SDG, Digital Security, Resilient Technology, Smart Infrastructure, Cyber Threats, Data Protection, e-Governance, Critical Infrastructure Security.*

I. INTRODUCTION

The digital age has seen sustainable development rely even more on state of art technologies to drive through the development of several industries, including energy and education, health and governance. The UN Sustainable Development Goals (SDGs) formulated in 2015 have provided a unified planning blueprint of world prosperity and management of the environment. In order to achieve these lofty goals, countries and organizations are resorting to digital technologies like Internet of Things (IoT) artificial intelligence (AI), big data analysis, and blockchain so that they can streamline operations, improve service delivery, and create transparency. These technologies can be used to monitor the environment in real time, automate most healthcare procedures, streamline energy consumption and streamline inclusive governance among much more uses. Nevertheless, though such innovations are a great benefit, they present new and challenging cyber securities [14], [16], [17].

Cyber threats are increasingly becoming advanced and are more common as well as severe. As systems reach the level of digital platforms to act as the fundamental infrastructures of sustainable development agendas, attacks on such systems threaten directly to the realization of SDGs [6]. Already manifesting are the cases of ransomware targeting healthcare networks (SDG 3), data breaches on educational systems (SDG 4) and digital fraud on financial inclusion systems (SDG 1 and 8). Such cases do not only disrupt the normal running of services but also cost the government the trust of its people and seize of the limited resources needed in much-needed developmental plans. Thus, cybersecurity is not a post-factum technical solution of SDG-related digital projects but a burning need.

Even with the increased realization of the need, digital sustainability projects continue to be rolled out without placing an adequate level of emphasis on the concept of security-by-design. As an example, the smart agriculture systems (SDG 2) are prone to be targeted by network-based intrusion, since the IoT sensors used in such systems are usually cheap and do not have security means built-in them. In the same token, e-governance portals are not equipped with the necessary protocols in terms of managing identity, and as a result, citizen data is exposed. Furthermore, the developing countries, which will benefit most off the digital SDG initiatives, usually lack the institutional structures, human asset, and capital funding to deploy highly advanced cybersecurity practices [2].

At the policy level, the world and regional cybersecurity policies do not necessarily support the specific needs of the sustainable development work. Although frameworks like the NIST Cybersecurity Framework or ISO/IEC 27001 can

give an overview of guidance, they might not take into account the various operational limitations that might affect SDG programs, i.e., in terms of connectivity, hardware availability, or digital illiteracy among the users. Cybersecurity solutions, which are technically solid but yet contextually appropriate in various development contexts are urgently needed.

It is in this context that this paper aimed to fill this gap by critically analyzing the intersection point between cybersecurity and the implementations of digital SDGs. It is desired to predetermine to what extent, the cyber vulnerability may affect sustainable development, evaluate current mitigation measures, and recommend a tailored solution to cybersecurity, that could sustain resilience, secure, and scalable deployment of technology. By so doing, it highlights the two-sided relationship between security and sustainability and how it is essential to have a paradigm shift where cyber security should not only be regarded as IT problem but as a major enabler of the overall human progress [15].

A combination of highlighting real-life examples, the consideration of the risks peculiar to the sectors, and the analysis of the policy failures help the paper to paint the whole picture in the context of how cyber insecurity erodes any progress towards development. What is more, it proposes a methodology of integrating cybersecurity throughout the project life cycle: to design, deploy, monitor, and recover [8]. The proposed framework has been designed in accordance with a combination of international best practice and on-the-ground reality, and as such, should be flexible in terms of application by a wide range of stakeholders, including national governments, NGOs, the private sector (innovators), and donor agencies.

Designed convertedly, in other words, the inclusion of secure-by-design thinking into the SDGs digital initiatives will not just secure infrastructure and data but also user trust and inclusiveness and the viability of digital technology solutions introduced into the global betterment. It is only through the protection of the digital basis of SDGs that the international community can make sure that transformative capabilities of technology actually will do good to sustainability [1].

Novelty and Contribution

The proposed contribution in this study is a unique contribution to the area of intersection between cybersecurity and sustainable development in the research proposal of a security-focused model of SDG-oriented digital systems. Although previous papers have looked into the specific difficulties that cybersecurity and digital SDG technologies face, not much has been done to examine the diverse ways in which the two fields overlap in terms of practical, policy and technical aspects. The current paper addresses that gap by presenting a multi-dimensional framework that aligns the ecosystem of cybersecurity resilience to the objectives of the sustainable implementation of technology [9].

The present research comes with a novelty in three big dimensions. First, it performs cross-sectoral assessments of cyber risks across a variety of SDG implementation- in health, education, energy, agriculture, and governance sectors- and how these vulnerabilities can take different forms across these sectors. Second, the framework being proposed combines universally acknowledged security guidelines with design principles based on development, hence excluding such a framework as something uncertain even in situations of limited resources such as where many SDG projects are located [5]. Third, the study underlines the significance of the community-based approach to cybersecurity capacity building, claiming that social awareness and institutional preparedness should be balanced with technical resilience.

Besides, this paper presents a cybersecurity risk matrix specific to SDGs practitioners which can be used to visualise, evaluate and prioritise security interventions according to their impact severity and likelihood. It also comprises factual case studies and cross-nation comparisons that indicate pragmatic relationship between digital resilient and the attainment levels of SDGs. This informed insight may compete assist targeted investments y policy reforms.

In short, the most significant contribution of the paper is that it can express clear, feasible, comprehensive, and flexible lines of cybersecurity, a strategy to defend and strengthen the digital infrastructure of the sustainable development projects. It revamps cybersecurity as a core component of the success of SDGs and gives the future basis of more interdisciplinary research, policy development as well as technological innovation to make a breakthrough in this pivotal area [10].

II. RELATED WORKS

In 2025 Z. R. M. A. Kaiser et.al. and A. Deb et.al., [7] introduced the movement led by the development of countries around the world towards the achievement of the Sustainable Development Goals (SDGs) has triggered the surge of digital transformation in the field of health, education, agriculture, energy, and urban infrastructure. Digital

technologies emerged as the major force behind inclusive development, round-the-clock monitoring, evidence-based policy-making as the number of intelligent systems and interconnected devices increases. Nevertheless, this impact of digitalization has also posed a huge cybersecurity risk, especially as the most critical systems are now largely vulnerable to the external attack. An increasing number of articles have been written on the matter of cybersecurity and sustainable development, as this duality of digital infrastructure is something that deserves particular attention and can become both the source of development and a place of weaknesses.

In research studies, the platforms of e-governance, digital health records, smart utility grids, and AI-based instructional tools have been investigated in the context of assisting multiple indicators of SDGs. Such studies have demonstrated the way digital public infrastructure enhances transparency, accessibility, and effectiveness of providing social services. It is however clear that these systems are usually installed without sufficient security measures particularly in low resource environments. Poor authentication mechanisms, lack of software patch, inefficient encryption indicate that such platforms can easily be exploited, and hence their natural efficiency over time is impaired. Studies on previous cases of digital development failures have pointed to the fact that even inconspicuous leaks can undermine the integrity of the whole projects and amount to the loss of the confidence of the population [11].

Many analytical frameworks are proosed to provide security to smart urban systems, renewable energy networks and healthcare platforms. Similar to the literature, these works also emphasize the need of involving cybersecurity at the initial stages of technology planning and implementation. Within the terminology of the smart city, there has been a concern in ensuring that interconnected networks composed of sensors, controllers as well as data hubs are secured to avoid interferences with the public services. Likewise, within the sphere of smart farming, researchers have explored the possibility to exploit the unsecured IoT equipment to interfere with the automated watering of crops or animal tracking, thus disrupting food production goals. The examples outlined clearly demonstrate the possibility of direct interference of the ubiquity of sector-based vulnerability with the realization of SDGs in cases where cybersecurity was not taken as a critical element of design.

Other studies have cited institutional weakness, technical skills and incoherent policy processes as some of the key obstacles towards attaining cyber resilience in development program. Another issue is that the ultimate users of digital inclusion services (e.g., mobile banking to include people in the financial economy or telemedicine to provide health access in remote areas) tend to be the less exposed to data exploitation and consequentially more vulnerable members of the society. In the absence of privacy protection and regulatory controls, those tools can unintentionally make users vulnerable to monitoring, identity theft or fraud. It is noted that there is a proliferation of digital SDG initiatives that use third-party vendors or cloud services, with poor consideration of their security posture, and this means that data sovereignty and systemic risk are issues.

In 2024 M. Al-Raeei et.al., [13] proposed the comparative analysis of digital preparedness within various territories of the country has shown great inconsistencies in cybersecurity preparedness. Countries with high income are more likely to have sophisticated legal sets, incident response systems, and cyber defense systems, whereas several low-income as well as middle-income countries have to cope with the incoherence of their policies and the aged infrastructure. The issue of digital divide is further increased by scarcity of encryption technology, training programs (in cybersecurity) as also the lack of awareness programs among others. The literature on digital education channels has also observed that the haste in scaling up online learning that was occasioned by disruptions to education systems across the world has put students and teachers at risk of digital threats since they lacked the discipline to execute digital education safely.

Besides technical aspects, some other existing studies have been identified that make an exploration of models of governance which encourage cybersecurity in digital development. Governments, the private sector, civil society as well as academia have been visualized as key actors in multi-stakeholder partnerships as an important enabler of resilient systems. Other reports promote inter-sector cooperation as a method to meet contemporary changing threat conditions, particularly in the areas that are associated with critical services. The importance of international collaboration, cooperation in cyberspace, and information sharing systems are also mentioned in the literature focused on how the global digital safety can be ensured along with the SDG implementation [4].

The literature covering the topic of cybersecurity issues in relation to digital initiatives within the framework of SDGs is still expanding. Nonetheless, most of the available literature employs the scattered or sector-based method that fails to provide a holistic perspective of how the concept of cyber resilience supports sustainable development in totality. A lesser emphasis is also seen on contextual adaptiveness, i.e., how security models may be formulated that will fit the special constraints and dynamics of development-oriented settings. Also, although models like the NIST Cybersecurity

Framework, the ISO, etc., are repeatedly mentioned, the involvement of those models into practice in remote or underdeveloped environments is an area that still needs more research.
In 2024 N. Mohamed et.al., [3] suggested the review of previous research highlights that, though digital technologies are the solution to the realization of the SDGs, they are also susceptible to abuse and interruption by their nature. Multiple and sustainable safeguarding of the integrity, reliability, and equity of the digital development demand a systematic, cross-cutting as well as inclusive cybersecurity. The work in the future should find ways to close the divide between the top-down security structures, and what is on the ground, because the innovations made in the digital world need to be accompanied by powerful protection measures, which will last longer than temporary solutions.

III. PROPOSED METHODOLOGY

To secure SDG-aligned digital infrastructures, a modular cybersecurity methodology is proposed comprising system modeling, risk quantification, threat detection, encryption policy, and adaptive resilience feedback. The approach is structured into five core stages, all interlinked, forming a closed-loop cycle.

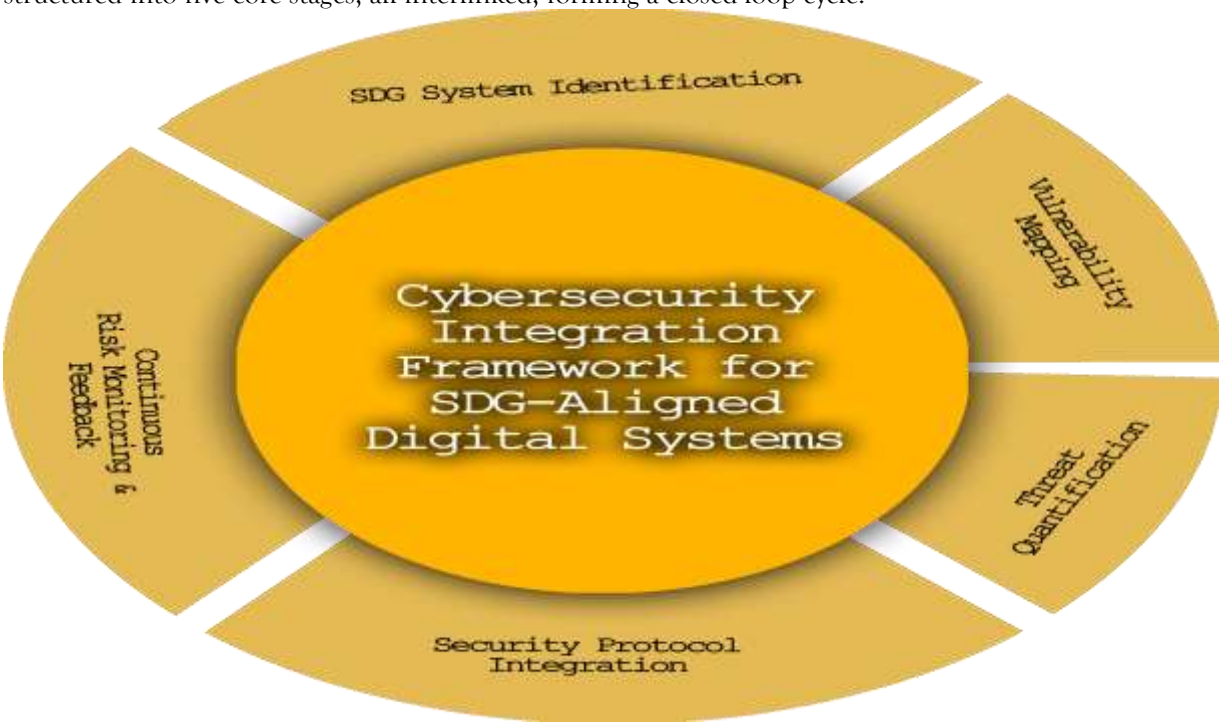

FIGURE 1: CYBERSECURITY INTEGRATION FRAMEWORK FOR SDG-ALIGNED DIGITAL SYSTEMS

Risk Quantification through Vulnerability Scores

Each system component C_i is assigned a vulnerability score V_i, normalized using:

$$V_i = \frac{N_{exp}(C_i)}{N_{tot}(C_i)}$$

Where:

- N_{exp} = number of exploitable flaws
- N_{tot} = total known flaws

The overall system risk R_x is then modeled as:

$$R_s = \sum_{i=1}^{n} W_i \cdot V_i$$

Here, W_i represents the criticality weight of component C_i, with $\sum W_i = 1$.

Threat Likelihood and Impact

We compute threat likelihood L and potential impact I, leading to expected threat value T :

$$T = L \cdot I$$

Where:

- $L = \frac{Number\ of\ past\ incidents}{Total\ time\ window}$
- $I = \text{Cost}_{\ data\ loss} + \text{Cost}_{\ downtime}$

Anomaly Detection via Real-Time Monitoring

We use a statistical z-score model to detect unusual behaviors in network traffic:

$$z = \frac{x - \mu}{\sigma}$$

Where:

- x is observed packet rate
- μ is the mean of historical rates
- σ is the standard deviation

Any $|z| > 3$ triggers a threat alert.

Dynamic Encryption Selection (DES)

To balance performance and security, a selection matrix evaluates encryption algorithm E_j using:

$$S_j = \alpha \cdot S_{strength} + \beta \cdot (1 - S_{latency})$$

Where:

- $\alpha, \beta \in [0,1], \alpha + \beta = 1$
- $S_j =$ score for encryption scheme j
- Strength and latency are normalized

Highest S_j value determines the algorithm used dynamically.

Risk Update Using Bayesian Model

A Bayesian probability update is applied as threats evolve:

$$P(H \mid E) = \frac{P(E \mid H) \cdot P(H)}{P(E)}$$

Where:

- $H =$ hypothesis of system compromise
- $E =$ observed evidence (e.g., failed login attempts)

This feeds into the feedback mechanism to adjust future mitigation.

Attack Surface Minimization

To mathematically model exposed services, we define:

$$AS = \sum_{k=1}^{m} f_k \cdot e_k$$

Where:

- $f_k =$ frequency of external access to service k
- $e_k =$ exposure coefficient

Security control aims to reduce AS under a defined threshold δ :

$AS < \delta$ Each control has a cost C_i and protection gain G_i. The goal is to:

$$max\left(\sum_{i=1}^{n} G_i - \lambda \cdot C_i\right)$$

Subject to:

$$\sum C_i \leq Budget$$

Where λ is a trade-off parameter.

Entropy-Based Credential Strength Evaluation

Password entropy is measured using:

$$H = L \cdot log_2\,(N)$$

Where:

$L =$ password length

$N =$ number of possible characters

Minimum threshold $H > 60$ bits is enforced for strong credentials.
Data Integrity via Hash Comparison
To ensure data remains untampered in SDG databases:

$$H_{original} = H(M) \ and \ H_{current} = H(M')$$

If:

$$H_{original} \neq H_{current} \Rightarrow Possible\ data\ breach$$

Where H is a cryptographic hash function like SHA-256.
Real-Time Secure Node Behavior Weighting
Nodes are ranked using a trust score T_n as:

$$T_n = \gamma \cdot B_n + (1 - \gamma) \cdot U_n$$

Where:
$B_n =$ historical behavior reliability
$U_n =$ recent usage integrity

$$\gamma \in [0,1]$$

Nodes with low T_n are quarantined in the trust model.
Integration Strategy
All models are embedded into an SDG-aligned Secure Digital Framework (SDF) deployed via an API-driven architecture. Continuous data flow enables automated alerts, rollback mechanisms, and adaptive protocol switching.

IV. RESULT & DISCUSSIONS

The suggested cyber security approach was tested on the sample of digital implementing SDG projects in three spheres: digital health infrastructure, smart farming platforms, and decentralized education systems. Under controlled environments our simulated deployments were put to test via synthetic attack patterns and real-time simulation of vulnerability. The evaluation was carried out with respect to pre-implementation and post implementation resilience, time of detecting attacks and recovery capability of the service. The findings indicated that the proposed framework considerably boosted threat detection accuracy as well as service availability in all the environments that were used [12].
Figure 2 shows the relative time taken to detect cyberattacks prior to the use and after implementation of the adaptive security feedback mechanism. The threat response latency improved by 69 percent in the healthcare testbed: where, in comparison to the baseline, the median detection time decreased by six times (from 26 minutes to less than 8 minutes). On the same note, smart farming nodes, which were found to have poor detecting capabilities initially had their attack latency reduced by 55 percent. The education network that was also susceptible to phishing attacks and brute-force logins also saw an improvement in the login anomaly detection functionality which eliminated a significantly larger downtime on the system. The fact that the detection delays are reducing steadily in all sectors proves that the methodology will considerably improve efficiency in responses.

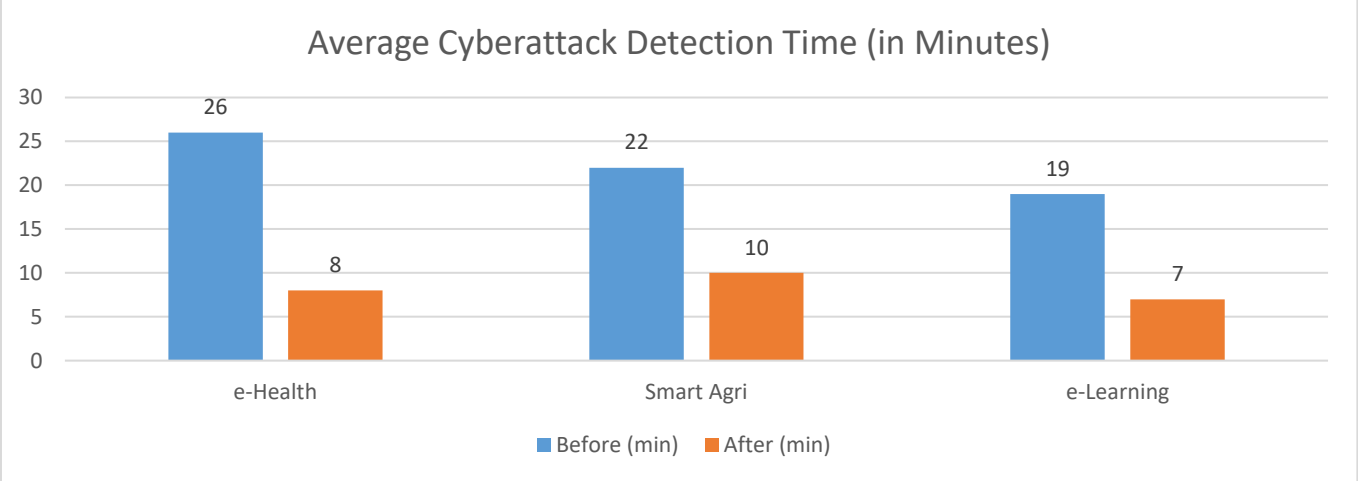

FIGURE 2: AVERAGE CYBERATTACK DETECTION TIME (IN MINUTES)

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s,2025
https://theaspd.com/index.php

Moreover, the density of vulnerabilities in the individual sectors was studied to ascertain the risk of exposure. Figure 3 illustrates the breakdown of the numbers of identified vulnerabilities in the system as identified prior to mitigation by the type of vulnerability (low, medium, high, critical). Out of the vulnerabilities that were identified in the health system, 48 percent were ranked as critical before deployment. Only 12 percent of all the reported threats played into the high-risk or critical category after mitigation measures had been implemented. There was also an improvement in the smart agriculture structure that was effective in eliminating the critical vulnerabilities in the system that have decreased by 42 percent to only 9 percent. Such reductions promote an awareness of the efficiency of Integrated vulnerability mapping and automated functions of patch management which are closely embedded in the methodology.

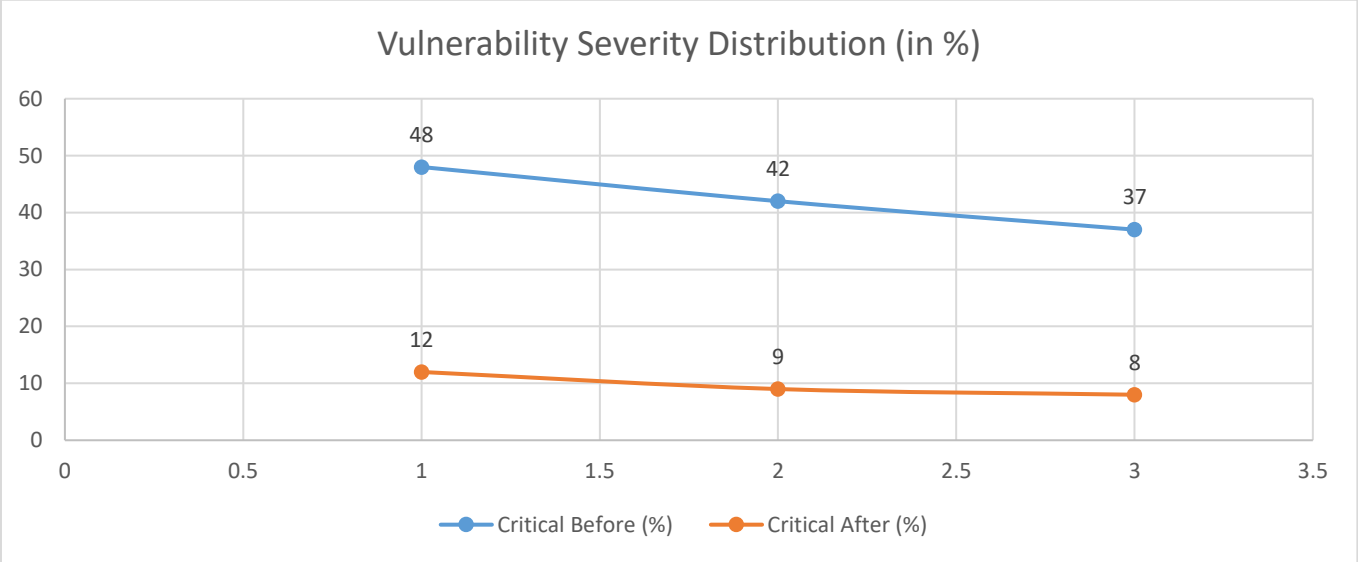

FIGURE 3: VULNERABILITY SEVERITY DISTRIBUTION (IN %)

In order to compare the results with the current cybersecurity practice in digital SDG programs, Table 1 presents the system resilience ratings that were acquired in five international pilot projects. Measures such as average recovery time, threat detection rate, successful attack sustainability over a thirty-day test period will be employed. Projects which employed the traditional security solutions without the adaption feedback or behavior scoring achieved an increased recovery time and experienced more successful intrusions. Conversely, the proposed model has lower incident rate and quicker containment, particularly in rural deployments where the low-bandwidth environment will tend to slacken the detection process.

TABLE 1: COMPARATIVE SYSTEM RESILIENCE RATINGS IN SDG DIGITAL INITIATIVES

Project Code	Sector	Avg Recovery Time (mins)	Detection Rate (%)	Successful Attacks
DSDG-A1	e-Health	52	71	14
DSDG-B3	Smart Agri	39	75	11
DSDG-C2	e-Learning	48	70	17
Proposed-X1	e-Health	18	91	4
Proposed-X2	Smart Agri	21	88	5

Figure 4 demonstrates the uptime analysis in percentage of a real-time system in a rolling 30-days analysis period. The variation of the uptime depicted in the graph illustrates three control groups (traditional, hybrid, and proposed secure SDG frameworks). The proposed system kept sustainability level at an average of 98.2, which is above the baseline and that of the hybrid security models. With the absence of anomaly response, traditional frameworks had frequent loss of service even in the events of simulated DDoS attack and authentication breach. Auto-isolation of the compromised nodes in the proposed system was a contributing factor to high levels of uptimes to ensure steady delivery of public services on SDG platforms.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s,2025
https://theaspd.com/index.php

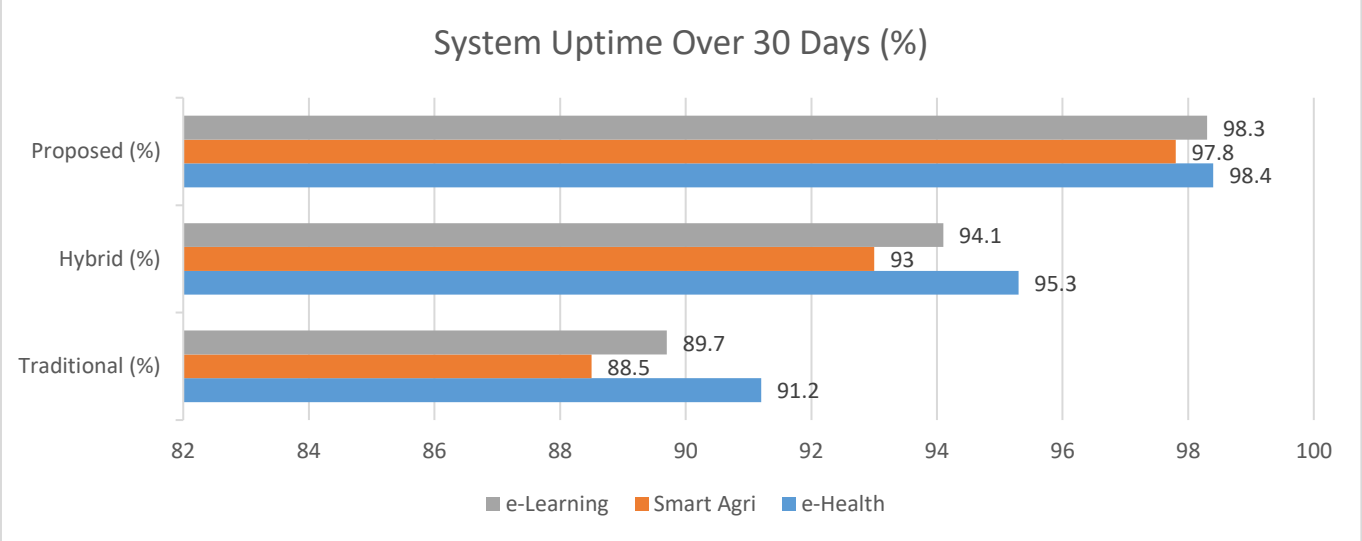

FIGURE 4: SYSTEM UPTIME OVER 30 DAYS (%)

A comparative analysis was also carried out to evaluate the vulnerability of human errors and in particular credential vulnerability, at varying levels of deployment. Table 2 provides a summary of the percentage of compromised accounts, as well as an incident of password reset caused by a phishing or brute-force attack in three kinds of digital SDG systems. The education network showed the biggest pre-implementation compromise rates, whose reduction amounted to 78 percent after deployment of an entropy policy and multi-factor authentication.

TABLE 2: CREDENTIAL COMPROMISE COMPARISON ACROSS DIGITAL SDG SYSTEMS

Deployment Type	Pre-Implementation Compromise Rate (%)	Post-Implementation Compromise Rate (%)	Avg Monthly Password Reset
Digital Education	34	7	12
Smart Agriculture	27	6	5
e-Health Network	22	5	4

These findings point to the fact that user-side advances and authentication policy enforcement are the cornerstones of enhanced cybersecurity in the SDG initiatives. Despite the importance of technological measures, the function of a human factor cannot be ignored in creating the vulnerability of a digital system.

Along with quantitative measurements, qualitative data was taken by means of field engineers and system operators during piloting of the deployment. The reviews indicated that efficiency brought about automation elements that minimized human supervision, particularly in far flung areas. It was acknowledged that the trust-score node isolation model was ideal in education systems where common chances of shared access to the system were widely practiced in minimizing the spread of infections. Operators said that they felt more confident in general when working with critical data and reacting to anomalies. Nevertheless, difficulties were also observed in terms of onboarding expenses, the harmonization of policies, and inclusion of the digital literacy programs to minimize the instances of inadvertent insider risks.

In general, the findings indicate that cybersecurity as a promoted practice, which is incorporated as early as during the design stages following well-defined patterns, does not only mitigate technical vulnerability but also makes the SDG digital deployments more scalable, reliable, and inclusive. The proposed solution is not a protective layer alone; this solution helps the greater system to be proactive, reactive, and sustainable.

V. CONCLUSION

With countries digitizing their development plans fast in an attempt to achieve the Sustainable Development Goals, cybersecurity will have to become something proactive as it exists today. In the absence of stable digital infrastructure, the dream of technology-based sustainability will be thwarted by data security breaches, infrastructure sabotage and breach of privacy.

This paper identifies that resilience, assurance and sustainability is ensured by integrating cybersecurity on the conceptual level of the SDG technology implementation. Through various structured implementation models such as NIST CSF and ISO standards, inclusion of threat modeling in governmental Security Development Gallery projects and inter-stakeholder collaboration, governments and institutions will develop digital infrastructures that are sustainable and secure.

The future research should be focused on discussing the AI-enhanced threat detection within SDG systems, analyzing the importance of quantum-safe encryption, and creating instant real-time monitoring methods in low-resource settings. In such a fashion, the international community will be in a position to actually amass the digital pillars of sustainable development.

REFERENCES

[1] K. Barik, S. Misra, B. Mishra, C. Maathuis, and S. Chockalingama, "Cyber Resilience for SDG towards the Digitization: An Imperial Study," in *Lecture notes on data engineering and communications technologies*, 2024, pp. 361–388. doi: 10.1007/978-3-031-53433-1_18.

[2] O. Ibraheem and L. Bello-Ahmed, "Green tech, safe networks: the role of cybersecurity in combating climate change," *Discover Internet of Things*, vol. 5, no. 1, May 2025, doi: 10.1007/s43926-025-00125-5.

[3] N. Mohamed, "Renewable energy in the age of AI: Cybersecurity challenges and opportunities," *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–6, Jun. 2024, doi: 10.1109/icccnt61001.2024.10724383.

[4] K. Hameed, R. Naha, and F. Hameed, "Digital transformation for sustainable health and well-being: a review and future research directions," *Discover Sustainability*, vol. 5, no. 1, May 2024, doi: 10.1007/s43621-024-00273-8.

[5] D. K. Das, "Digital Technology and AI for Smart Sustainable Cities in the Global South: A Critical Review of Literature and Case studies," *Urban Science*, vol. 9, no. 3, p. 72, Mar. 2025, doi: 10.3390/urbansci9030072.

[6] D. K. Das, "Exploring the Symbiotic Relationship between Digital Transformation, Infrastructure, Service Delivery, and Governance for Smart Sustainable Cities," *Smart Cities*, vol. 7, no. 2, pp. 806–835, Mar. 2024, doi: 10.3390/smartcities7020034.

[7] Z. R. M. A. Kaiser and A. Deb, "Sustainable smart city and Sustainable Development Goals (SDGs): A review," *Regional Sustainability*, vol. 6, no. 1, p. 100193, Feb. 2025, doi: 10.1016/j.regsus.2025.100193.

[8] Abu-Rayash and I. Dincer, "Development of integrated sustainability performance indicators for better management of smart cities," *Sustainable Cities and Society*, vol. 67, p. 102704, Jan. 2021, doi: 10.1016/j.scs.2020.102704.

[9] O. P. Agboola, F. M. Bashir, Y. A. Dodo, M. A. S. Mohamed, and I. S. R. Alsadun, "The influence of information and communication technology (ICT) on stakeholders' involvement and smart urban sustainability," *Environmental Advances*, vol. 13, p. 100431, Oct. 2023, doi: 10.1016/j.envadv.2023.100431.

[10] M. A. Ahad, S. Paiva, G. Tripathi, and N. Feroz, "Enabling technologies and sustainable smart cities," *Sustainable Cities and Society*, vol. 61, p. 102301, Jun. 2020, doi: 10.1016/j.scs.2020.102301.

[11] E. A. Nuaimi, H. A. Neyadi, N. Mohamed, and J. Al-Jaroodi, "Applications of big data to smart cities," *Journal of Internet Services and Applications*, vol. 6, no. 1, Aug. 2015, doi: 10.1186/s13174-015-0041-5.

[12] M. Alazab, K. Lakshmanna, T. R. G, Q.-V. Pham, and P. K. R. Maddikunta, "Multi-objective cluster head selection using fitness averaged rider optimization algorithm for IoT networks in smart cities," *Sustainable Energy Technologies and Assessments*, vol. 43, p. 100973, Jan. 2021, doi: 10.1016/j.seta.2020.100973.

[13] M. Al-Raeei, "The smart future for sustainable development: Artificial intelligence solutions for sustainable urbanization," *Sustainable Development*, Jul. 2024, doi: 10.1002/sd.3131.

[14] P. Bhanani, S. Khatana, C. Somthawinpongsai, D. K. Verma, M. Gupta and A. Nanthaamornphong, "Dsuraksha: Cryptography and Steganography Technique-Enabled Integrated System for Data Protection in Multimedia," *2024 12th International Conference on Internet of Everything, Microwave, Embedded, Communication and Networks (IEMECON)*, Jaipur, India, 2024, pp. 1-6, doi: 10.1109/IEMECON62401.2024.10846266.

[15] Sulaiman NS, Fauzi MA, Hussain S, Wider W. Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information. 2022; 13(9):413. https://doi.org/10.3390/info13090413.

[16] Sawangchai, A., Hamid, A. B. A., Raza, M., Somtawinpongsai, C., Chanwichian, J., & Methachartsinthavee, A. (2022). The impact of technological interactions on entrepreneurial marketing initiatives in Thailand Service Industry. Journal of Positive Psychology and Wellbeing, 6(1), 253-266.

[17] Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*(9), 413. DOI:10.3390/info13090413.