engineering proceedings

Proceeding Paper

Design and Simulation of AI-Enabled Digital Twin Model for Smart Industry 4.0 †

Md. Humayun Kabir *, Jaber Ahmed Chowdhury, Istiak Mohammad Fahim, Mohammad Nadib Hasan, Arif Hasnat and Ahmed Jaser Mahdi

Department of Computer and Communication Engineering, International Islamic University Chittagong, Kumira Chattogram 4318, Bangladesh; jaberahmediiuc@gmail.com (J.A.C.); istiakfahim94@gmail.com (I.M.F.); nadibhasan.gtu.in@gmail.com (M.N.H.), arifhasnat83@gmail.com (A.H.); jasermahdi@gmail.com (A.J.M.)

* Correspondence: mdhkrrabby@gmail.com; Tel.: +880-151-528-6984

† Presented at the 10th International Electronic Conference on Sensors and Applications (ECSA-10), 15–30 November 2023; Available online: https://ecsa-10.sciforum.net/.

Abstract: One of the core ideas of Industry 4.0 has been the use of Digital Twin Networks (DTN). DTN facilitates the co-evolution of real and virtual things through the use of DT modelling, interactions, computation, and information analysis systems. The DT simulates product lifecycles to forecast and optimizes manufacturing systems and component behavior. Industry and Academia have been developing Digital Twin (DT) technology for real-time remote monitoring and control, transport risk assessment, and intelligent scheduling in the smart industry. This study aims to design and simulate a comprehensive digital twin model connecting three factories to a single server. It incorporates remote network control, IoT integration, advanced networking protocols, and security measures. The model utilizes the Open Shortest Path First (OSPF) routing protocol for seamless network connectivity within the interconnected factories. Access Control List (ACL) and Authentication, authorization, and accounting (AAA) mechanisms ensure secure access and prevent unauthorized entry. The Digital Twin Model is simulated using Cisco Packet Tracer, validating its functionality in network connectivity, security, remote control, and motor efficiency monitoring. The results demonstrate the successful integration and operation of the model in smart industries. The networked factories exhibit improved operational efficiency, enhanced security, and proactive maintenance.

Keywords: Industry 4.0; Digital Twin; Internet of Things; artificial intelligence; network requirements

Citation: Kabir, M.H.; Chowdhury, J.A.; Fahim, I.M; Hasan, M.N.; Hasnat, A.; Mahdi, A.J. Design and Simulation of AI-Enabled Digital Twin Model for Smart Industry 4.0. *Eng. Proc.* **2023**, *56*, x. https://doi.org/10.3390/xxxxx

Published: 15 November 2023

1. Introduction

A digital twin network is a computer simulation model of the communication network, including the environment in which it operates and the application traffic it carries. It uses the Internet of Things (IoT) to enhance decision-making in complicated systems by facilitating learning and reasoning. According to a study, adopting DT and IoT technologies is projected to generate economic benefits ranging from USD 5.5 trillion to USD 12.6 trillion worldwide by 2030. The smart manufacturing industry is predicted to expand from $214.7 billion in 2020 to $384.8 billion in 2025, with a CAGR of 12.4% [1]. Despite smart manufacturing's many advantages, including integrated components and digitization, maintenance remains a significant obstacle. Maintenance is a pivotal determinant that exerts a significant economic impact on the sector, garnering notable emphasis in the era of digitalization. The entire manufacturing cost is projected to include maintenance expenses ranging from around 15% to 40% [2]. Based on the U.S. Department of Energy findings, it has been shown that predictive maintenance offers cost savings of around 8-12% compared to preventive maintenance and can yield savings of up to 40% compared to reactive maintenance [3]. The adoption rate of predictive maintenance experienced a modest increase from 47% to 51% from 2017 to 2018. This implementation of predictive maintenance strategies reduced equipment failure rates from 61% to 57% [4]. Hence, the maintenance process exerts a direct impact on the economic aspects of the industry. Furthermore, in the contemporary era of Industry 4.0, the utilization of intelligent maintenance techniques incorporating digital twin (DT) technology has the potential to yield substantial advantages compared to existing maintenance methodologies [5].

Therefore, it is imperative to comprehend the concept of a digital twin and the potential of digital twin technology in facilitating an organization's digital transformation. A digital twin refers to a computer-generated model replicating a tangible object's characteristics and behavior or a procedural operation. Digital twins undergo dynamic transformations throughout the life cycles of entities and processes, facilitated by utilizing real-time IoT data. Novel network applications have emerged as a result of society and industry being digitally transformed [6]. Complex requirements for these applications make it difficult for them to be managed by conventional network management techniques like network over provisioning or admission control. For instance, cutting-edge communication technologies like holographic telepresence and augmented reality/virtual reality demand extremely low deterministic latency, yet modern industrial advancements like vehicular networks demand real-time network topology adaptation. The behavior of current networks is very dynamic and heterogeneous due to the rapid increase in linked devices. Modern communication networks have gotten so sophisticated and expensive to manage as a result. The DT paradigm has lately been adopted by other industrial sectors to describe complex and dynamic systems [7]. A DT's primary strength is in its ability to accurately replicate a complex system eliminating the need for costly, time-consuming human interaction. DT enables smart production, as shown in Figure 1 Industry 4.0, enhancing the performance and design of complicated engineering items, or simulating physical interactions [8].

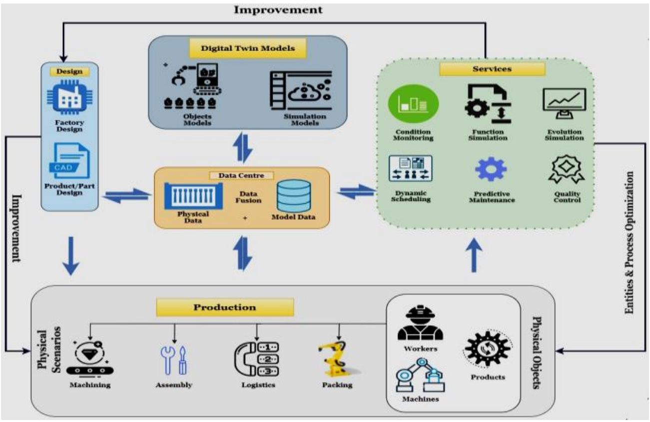


Figure 1. Digital Twin General Network Architecture [2].

To examine various situations and forecast decision outcomes, computer simulations are accomplished. Digital twins vary and are updated frequently to mirror changes in their physical counterparts for timely engagement [9]. Artificial intelligence algorithms and network setups, which are at the heart of modern technologies, are made possible by necessary techniques trained on large volumes of data obtained from numerous connected sensors on physical objects [10]. In addition to raising significant issues for their organizations and procedures, this drives up the expenses for manufacturing businesses. Because of this, it is expected that AI-driven DT technology would be able to successfully assist decision-making in multi-objective issues by adapting traditional model-based methodologies to shifting boundary circumstances and providing a demand-oriented, real-time assessment foundation. Many studies have previously provided descriptions and definitions of DT from the standpoint of broad ideas and technological frameworks. [11] Not only that, but product design, simulation, and modeling would not be able to take use of their own unique enabler, artificial intelligence diagnostics and prognostics for faults [12]. The industrial technology revolution has brought attention to manufacturing concepts like personalized and distributed manufacturing. These new manufacturing paradigms and Industrial Internet of Things (IIoT) make connected micro smart factories in factory-as-a-service systems inefficient in cost and production [13]. A digital twin, which employs a digital version of a process with identical manufacturing elements, synchronized information, and functional units, was created to tackle these issues. The digital twin leverages up-to-date information from the Internet to collect data from IIoT devices and operates in many applications. It also generates the components of a detailed digital twin application design and defines procedures. This study could help managers organize the benefits of digital twin utilization through a hierarchy by providing real-time monitoring, tracking information, and operational decision-making support [14]. The proposed application also effectively mitigates cost and production inefficiencies, leading to the optimal functioning of a manufacturing system. We explore the problem into several phases:

Technical Complexity: From functional requirement selection and architecture planning to integration and verification of the final (digital) models.

Data Incompatibility: We address as well how physical components exchange real-time information with DTs, as well as experimental platforms to build DTs (including protocols and standards).

Security Risks: Interoperability between different systems and devices can increase the risk of security breaches, as it creates more opportunities for hackers to exploit vulnerabilities.

In this paper, we aim to Design a Digital Twin Model for Smart industries that are AI-enabled. The paper's primary contributions include.

1. We focus on the construction of DTs network model.
2. More specifically, we focus on determining (methodologically) how to design, create and connect physical objects with their virtual counterpart. Which will improve interoperability, resilience, and security in smart manufacturing systems.
3. To implemented an Access Control List (ACL), and Authentication, Authorization, and Accounting (AAA) system to judiciously manage access to computer resources, enforce rules, audit usage, and deliver the data required to charge for services.
4. The proposed digital twin network model incorporates remote access capabilities.

The remainder of the article is organized as follows: Section 2 introduces the Digital Twin Frameworks for Development. Section 3 discusses the simulation result. Finally, Section 4 summarizes the main findings of this work.

2. Digital Twin Frameworks for Development

Digital transformation encompasses a convergence of various cutting-edge technologies, including Big Data, cloud computing, Internet of Things, Industrial Internet of Things, sensors, artificial intelligence (AI), machine learning, and numerous more. These technologies are undergoing continuous evolution. Therefore, it is postulated that digital transformation (DT) constantly evolves alongside these technologies. The technological advancement of digital twin applications in industrial processes has experienced substantial progress over forty years. The adoption of digital twins for real-time monitoring and improvement of processes has been made possible by the recent technological developments in sensing, monitoring, and decision-making tools within the context of Industry 4.0. A design for digital twins ensures that devices with virtual copies work well together in the cyber-physical domain and that data and information can flow easily between digital twins, physical twins, and the outside world. The architectural framework encompasses diverse tangible devices, sensors, and data-gathering systems inside the physical realm. These components facilitate data transfer, processing, collecting, calculating, and sharing within the virtual environment.

This research aims to design and simulate a digital twin model for smart industries that unites three separate factories in a single server. The study aims to examine the viability, effectiveness, and practical effects of creating a digital twin model that uses the OSPF routing protocol, ACL, AAA, connected IoT materials, remote network control, and motor efficiency monitoring made possible by artificial intelligence. Cisco Packet Tracer is used as a simulation tool to investigate these components' integration further. In Figure 2, with Cisco Packet Tracer, a network simulation tool, construct a digital twin model and set up the virtual network environment, including routers, switches, IoT devices, and network security features. Implement OSPF routing protocol, ACL rules, and AAA procedures within the network topology.

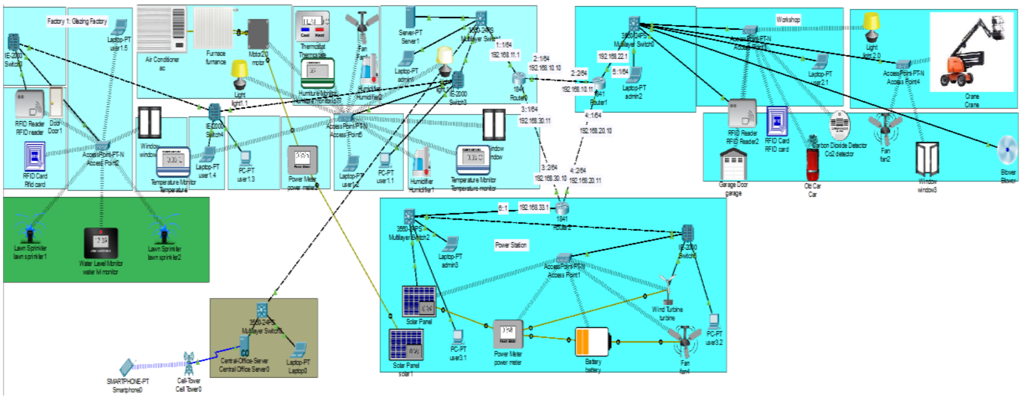
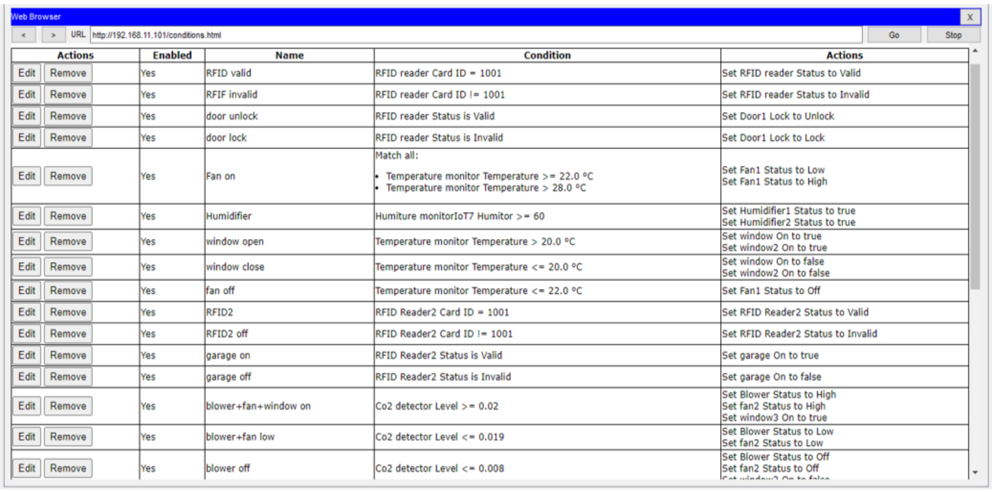


Figure 2. Proposed simulation of Digital Twin Model for Smart Industries.

Figure 3 shows the working conditions of IoT devices that integrate with the proposed smart factory network topology. The working conditions will be automated and updated based on real-time sensor data.



Web Browser

URL http://192.168.11.101/conditions.html

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	RFID valid	RFID reader Card ID = 1001	Set RFID reader Status to Valid
Edit Remove	Yes	RFIF invalid	RFID reader Card ID != 1001	Set RFID reader Status to Invalid
Edit Remove	Yes	door unlock	RFID reader Status is Valid	Set Door1 Lock to Unlock
Edit Remove	Yes	door lock	RFID reader Status is Invalid	Set Door1 Lock to Lock
Edit Remove	Yes	Fan on	Match all: • Temperature monitor Temperature >= 22.0 °C • Temperature monitor Temperature > 28.0 °C	Set Fan1 Status to Low Set Fan1 Status to High
Edit Remove	Yes	Humidifier	Humiture monitorIoT7 Humitor >= 60	Set Humidifier1 Status to true Set Humidifier2 Status to true
Edit Remove	Yes	window open	Temperature monitor Temperature > 20.0 °C	Set window On to true Set window2 On to true
Edit Remove	Yes	window close	Temperature monitor Temperature <= 20.0 °C	Set window On to false Set window2 On to false
Edit Remove	Yes	fan off	Temperature monitor Temperature <= 22.0 °C	Set Fan1 Status to Off
Edit Remove	Yes	RFID2	RFID Reader2 Card ID = 1001	Set RFID Reader2 Status to Valid
Edit Remove	Yes	RFID2 off	RFID Reader2 Card ID != 1001	Set RFID Reader2 Status to Invalid
Edit Remove	Yes	garage on	RFID Reader2 Status is Valid	Set garage On to true
Edit Remove	Yes	garage off	RFID Reader2 Status is Invalid	Set garage On to false
Edit Remove	Yes	blower+fan+window on	Co2 detector Level >= 0.02	Set Blower Status to High Set fan2 Status to High Set window3 On to true
Edit Remove	Yes	blower+fan low	Co2 detector Level <= 0.019	Set Blower Status to Low Set fan2 Status to Low
Edit Remove	Yes	blower off	Co2 detector Level <= 0.008	Set Blower Status to Off Set fan2 Status to Off

Figure 3. AI Condition of IoT Device used Smart Industries.

Figure 4 shows the multi-area OSPF configuration in the proposed network. The OSPF protocol actively receives and processes link-state data from neighboring routers, utilizing this information to construct a comprehensive topology map encompassing all routers inside the network. ACLs can control network access, prevent attacks, and maximize bandwidth. It is done by carefully identifying network message flow and working with other technologies. ACLs are essential for network security and service quality. All networks require user management for security. Configuration ACLs in the proposed network shown in Figure 5. The AAA framework provides security to provide particular users access to designated resources and document their operational activity. The technology is popular because it scales well and centralizes user data. Most practical AAA implementations use the Remote Authentication Dial-in User Service (RADIUS). Configuration AAA in the proposed network shown in Figure 6.

```
router ospf 1
 router-id 1.1.1.1
 passive-interface GigabitEthernet0/0
 network 192.168.72.1 0.0.0.0 area 0
 network 192.168.95.1 0.0.0.0 area 0
 network 192.168.127.1 0.0.0.0 area 1
 auto-cost reference-bandwidth 10000
```

```
router ospf 1
 router-id 2.2.2.2
 passive-interface GigabitEthernet0/0
 network 192.168.80.1 0.0.0.0 area 0
 network 192.168.95.2 0.0.0.0 area 0
 auto-cost reference-bandwidth 10000
```

```
router ospf 1
 router-id 3.3.3.3
 passive-interface GigabitEthernet0/0
 network 192.168.104.1 0.0.0.0 area 1
 network 192.168.127.2 0.0.0.0 area 1
 auto-cost reference-bandwidth 10000
```

Figure 4. OSPF Configuration in Multi Area Factory Router.

```
Admin-1: Router-0:
Router(config)#access-list 100 deny ip 192.168.11.11 0.0.0.0 192.168.22.12 0.0.0.0
Router(config)#access-list 100 deny ip 192.168.11.11 0.0.0.0 192.168.33.5 0.0.0.0
Router(config)#access-list 100 deny ip 192.168.11.11 0.0.0.0 192.168.33.3 0.0.0.0
Router(config)#access-list 100 permit ip any any
Router(config)#int eth0/1/0
Router(config-if)#ip access-group 100 in
Router(config-if) #exit
Router(config)#exit
Router#wr
```

```
Admin-2: Router-1:
Router(config)#access-list 101 deny ip 192.168.22.11 0.0.0.0 192.168.11.13 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.11 0.0.0.0 192.168.11.3 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.11 0.0.0.0 192.168.11.14 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.11 0.0.0.0 192.168.11.32 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.11 0.0.0.0 192.168.11.4 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.11 0.0.0.0 192.168.33.5 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.11 0.0.0.0 192.168.33.3 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.12 0.0.0.0 192.168.33.3 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.12 0.0.0.0 192.168.33.5 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.12 0.0.0.0 192.168.11.13 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.12 0.0.0.0 192.168.11.3 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.12 0.0.0.0 192.168.11.14 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.12 0.0.0.0 192.168.11.32 0.0.0.0
Router(config)#access-list 101 deny ip 192.168.22.12 0.0.0.0 192.168.11.4 0.0.0.0
Router(config)#access-list 101 permit ip any any
Router(config)#int eth0/1/0
Router(config-if) #ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
```

```
Admin-3 Router-2:
Router(config)#access-list 102 deny ip 192.168.33.11 0.0.0.0 192.168.11.13 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.11 0.0.0.0 192.168.11.3 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.11 0.0.0.0 192.168.11.14 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.11 0.0.0.0 192.168.11.32 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.11 0.0.0.0 192.168.11.4 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.11 0.0.0.0 192.168.22.12 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.5 0.0.0.0 192.168.22.12 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.5 0.0.0.0 192.168.11.13 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.5 0.0.0.0 192.168.11.3 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.5 0.0.0.0 192.168.11.14 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.5 0.0.0.0 192.168.11.32 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.5 0.0.0.0 192.168.11.4 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.3 0.0.0.0 192.168.11.13 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.3 0.0.0.0 192.168.11.3 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.3 0.0.0.0 192.168.11.14 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.3 0.0.0.0 192.168.11.32 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.3 0.0.0.0 192.168.11.4 0.0.0.0
Router(config)#access-list 102 deny ip 192.168.33.3 0.0.0.0 192.168.22.12 0.0.0.0
Router(config)#access-list 102 permit ip any any
Router(config)#int eth0/1/0
Router(config-if)#ip access-group 102 in
Router(config-if)#exit
Router(config)#exit
```

Figure 5. ACL Configuration in Network.

```
Router(config)#username admin0 secret admin0jf35
Router(config)#hostname Router0
Router0(config)#radius-server host 192.168.11.101
Router0(config)#radius-server key radiusjf35
Router0(config)#aaa new-model
Router0(config)#aaa authentication login default group radius local
Router0(config)#line console 0
Router0(config-line)#login authentication default
Router0(config-line)#end
Router0#
```

```
Router1(config)#username admin1 secret admin1jf35
Router1(config)#aaa new-model
Router1(config)#aaa authentication login default local
Router1(config)#line console 0
Router1(config-line)#login authentication default
Router1(config-line)#end
Router1(config)#ip domain-name ccnasecurity.com
Router1(config)#crypto key generate rsa
Router1(config)#aaa authentication login SSH-LOGIN local
Router1(config)#line vty 0 4
Router1(config-line)#transport input ssh
Router1(config-line)#login authentication SSH-LOGIN
```

```
Router(config)#username admin3 secret admin3jf35
Router(config)#aaa authentication login default local
Router(config)#line console 0
Router(config-line)#login authentication default
Router(config)#ip domain-name ccnasecurity.com
Router(config)#crypto key generate rsa
Router2(config)#aaa authentication login SSH-LOGIN local
Router2(config)#line vty 0 4
Router2(config-line)#transport input ssh
Router2(config-line)#login authentication SSH-LOGIN
```

Figure 6. AAA Configuration in Network.

3. Results and Discussion

The entrance door opens automatically when a valid RFID card is presented to the RFID reader. A lawn sprinkler will automatically explode when the garden water level drops. The fan rotates slowly if room temperature is >22.0 °C and quickly if it is >28.0 °C. A light turns on when motor efficiency decreases by less than 35%. However, if motor efficiency drops below 20%, light will blink and be seen in a workplace by blinking another light. The motor runs on solar electricity. The humidifier releases water vapor or steam to boost air moisture if the hygrometer exceeds 60% humidity. The device continually monitors water levels using smart sensors. The system activates lawn sprinklers when the water level dips, optimizing watering and conserving water. An automatic humidity management system uses a hygrometer and humidifier to maintain appropriate air moisture levels. The humidifier produces water vapor or steam when the hygrometer detects humidity above 60%, increasing surrounding moisture. The device controls fan speed by ambient temperature. The fan slows at 22.0 °C or above. If the temperature exceeds 28.0 °C, the fan speed rises, aiding temperature regulation shown in Figure 7a.

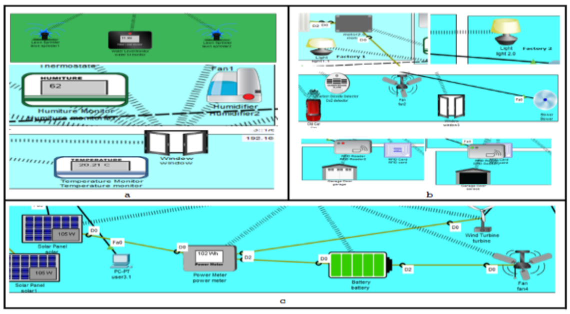


Figure 7. (**a**) Sensor Output of Factory 1, (**b**) Sensor Output of Factory 2 & (**c**) Sensor Output of Factory 3.

The garage door opens automatically when a valid RFID card is scanned in front of the RFID reader. The blower fan will spin swiftly and open the window if the vehicle smokes (carbon dioxide level rises −0.02%). Blinking lights alert the workshop when factory −1's motor efficiency drops. Raw materials will then be delivered from the workshop to factory 1. The system evaluates motor efficiency and activates lights at specified levels. A light turns on when motor efficiency drops below 35%. The light blinks, and a similar light in the workplace (Factory-2) blinks to inform personnel if efficiency drops below 20%. The gadget detects vehicle smoke using CO2 levels. Smoke extraction and ventilation are improved by activating a high-speed blower fan and opening the car window when CO2 levels climb 0.02%. Every authorized person receives an RFID card. A microprocessor on these cards/tags' stores identifying numbers and access credentials. Presenting a valid RFID card to the RFID reader opens the door show in Figure 7b. Power meters display and quantify power absorption. Solar and wind turbines will power stations. The battery provides backup power in case of emergencies. A power meter monitors absorbed power, a power station gathers energy from solar panels and wind turbines, and a battery backup ensures power delivery in unexpected circumstances show in Figure 7c.

4. Conclusions

Digital twins (DTs) offer novel opportunities for the optimization, monitoring, simulation, prediction, diagnosis, and control of physical processes. These resources provide valuable insights for developing novel business models and decision support systems, as well as enhancing operational efficiency. This paper comprehensively analyzed the most current scholarly works, concentrating on the DT factory. As documented in contemporary scientific literature, the methodological techniques utilized for constructing decision trees have been thoroughly examined and briefly explained. Based on the abovementioned findings, a comprehensive examination has been conducted to ascertain the requisite procedures for systematically constructing a DT. This process encompasses many stages, including design, modeling, and execution. It has been determined that the expansion of digital technologies (DTs) will rely on the integration of complementary technologies, including artificial intelligence (AI), the Internet of Things (IoT), and big data analysis. The significance of network connectivity is elevated as it facilitates the transmission of data from the tangible entity to be analyzed by its digital equivalent. In this study, we examine the development of secure DTs intending to enhance the safeguarding of sensed data. Our objective is to establish dependable systems well-suited for essential operations by examining viable methods of fortifying data protection.

Author Contributions: Conceptualization, M.H.K.; methodology, M.H.K.; J.A.C.; and I.M.F.; software, J.A.C.; and I.M.F.; formal analysis, M.H.K.; J.A.C.; and I.M.F.; writing—original draft preparation, J.A.C.; and I.M.F.; writing—review and editing, M.H.K.; supervision, M.H.K. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Javaid, M.; Haleem, A. Digital Twin applications toward Industry 4.0: A Review. *Cogn. Robot.* **2023**, *3*, 71–92.
2. Warke, V.; Kumar, S.; Bongale, A.; Kotecha, K. Sustainable Development of Smart Manufacturing Driven by the Digital Twin Framework: A Statistical Analysis. *Sustainability* **2021**, *13*, 10139. https://doi.org/10.3390/su131810139.
3. Benotsmane, R.; Kovács, G.; Dudás, L. Economic, social impacts and operation of smart factories in Industry 4.0 focusing on simulation and artificial intelligence of collaborating robots. *Soc. Sci.* **2019**, *8*, 143.
4. Segovia, M.; Garcia-Alfaro, J. Design, Modeling and Implementation of Digital Twins. *Sensors* **2022**, *22*, 5396. https://doi.org/10.3390/s22145396.
5. Wu, Y.; Zhang, K.; Zhang, Y. Digital twin networks: A survey. *IEEE Internet Things J.* **2021**, *8*, 13789–13804.
6. Tsaramirsis, G.; Kantaros, A.; Aldarraji, I.; Piromalis, D.; Apostolopoulos, C.; Pavlopoulou, A.; Alrammal, M.; Ismail, Z.; Buhari, S.; Stojmenovic, M.; et al. A Modern Approach towards an Industry 4.0 Model: From Driving Technologies to Management. *J. Sens.* **2022**, *2022*, 5023011.
7. Fuller, A.; Fan, Z.; Day, C.; Barlow, C. Digital twin: Enabling technologies, challenges and open research. *IEEE Access* **2020**, *8*, 108952–108971.
8. Mozo, A.; Karamchandani, A.; Gómez-Canaval, S.; Sanz, M.; Moreno, J.I.; Pastor, A. B5GEMINI: AI-Driven Network Digital Twin. *Sensors* **2022**, *22*, 4106. https://doi.org/10.3390/s22114106.
9. Zhou, C.; Yang, H.; Duan, X.; Lopez, D.; Pastor, A.; Wu, Q.; Boucadair, M.; Jacquenet, C. *Digital Twin Network: Concepts and Reference Architecture*; Internet Engineering Task Force: Fremont, CA, USA, 2021.
10. Rathore, M.M.; Shah, S.A.; Shukla, D.; Bentafat, E.; Bakiras, S. The role of ai, machine learning, and big data in digital twinning: A systematic literature review, challenges, and opportunities. *IEEE Access* **2021**, *9*, 32030–32052.
11. Kabir, M.H.; Kabir, M.A.; Islam, M.S.; Mortuza, M.G.; Mohiuddin, M. Performance Analysis of Mesh Based Enterprise Network Using RIP, EIGRP and OSPF Routing Protocols. *Eng. Proc.* **2021**, *10*, 47. https://doi.org/10.3390/ecsa-8-11285.
12. Biller, B.; Biller, S. Implementing Digital Twins That Learn: AI and Simulation Are at the Core. *Machines* **2023**, *11*, 425. https://doi.org/10.3390/machines11040425.
13. Thelen, A.; Zhang, X.; Fink, O.; Lu, Y.; Ghosh, S.; Youn, B.D.; Todd, M.D.; Mahadevan, S.; Hu, C.; Hu, Z. A comprehensive review of digital twin—Part 1: Modeling and twinning enabling technologies. *Struct. Multidiscip. Optim.* **2022**, *65*, 354.
14. Park, K.T.; Nam, Y.W.; Lee, H.S.; Im, S.J.; Noh, S.D.; Son, J.Y.; Kim, H. Design and implementation of a digital twin application for a connected micro smart factory. *Int. J. Comput. Integr. Manuf.* **2019**, *32*, 596–614.