

Preventing Data Tampering in Smart Grids: A Blockchain-Based Digital Twin Framework

Biagio Boi[1(✉)], Christian Esposito[1], and Jung Taek Seo[2]

[1] University of Salerno, Fisciano, Italy
{bboi,esposito}@unisa.it
[2] Gachon University, Seongnam-si, Republic of Korea
seojt@gachon.ac.kr

Abstract. As modern power systems evolve in complexity and dynamism, there arises a pressing need for innovative methodologies to streamline their management and optimization. Decentralization strategies, enabled by edge computing and Digital Twins (DTs), offer promising remedies to these issues by facilitating real-time interaction with physical systems and integrating data for advanced analytics, including predictive forecasting. While Smart Grids have emerged as efficient solutions for enhancing system performance and reducing costs, certain challenges persist. This paper proposes a novel blockchain-based system designed to counter data poisoning within the domain of energy forecasting in smart grids. Our framework not only ensures the integrity of data but also fortifies defenses against attacks aimed at disrupting data-driven applications. Validation in a practical energy forecasting scenario demonstrates the reliability and efficacy of our approach. Results demonstrate the feasibility of the approach while providing positive insights about the detection of attacks.

Keywords: Smart Grid · Digital Twin · Internet of Things

1 Introduction

The advancement in technologies in the last few years enhanced the quality of industrial processes by reducing costs and increasing efficiency. Supervisory Control And Data Acquisition (SCADA) systems are nowadays widely used in industrial applications in order to control wide systems and take actions when necessary or to prevent possible issues related to machines. Federations of devices are typically used in order to sense an environment or take action. These intelligent networks take the name of smart grid; and are usually composed of tons of Internet of Things (IoT) devices exchanging data used in a multitude of applications ranging from smart predictions to disaster prevention. A particular industrial context, where the IoT sensors are saving money and enhancing quality is composed of an electricity network. Traditional approaches in this field are composed of a

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14822, pp. 144–156, 2024.
https://doi.org/10.1007/978-3-031-65318-6_10

central hub that interconnects all the infrastructures. It is common to have different macro-area served by a central hub, and those macro-area cover thousands of users. Such an approach is poorly scalable and currently smart grid faces various challenges related to communication, interoperability and security, usually caused by the underlying technologies [7]. These systems usually leverage old systems and it is difficult to re-use or control data produced in this environment from external access. Decentralization aims to solve these challenges by moving the computation away from centralized systems and by providing a mean for interacting with physical and legacy systems. In particular, through edge computing, it is possible to process produced data in order to minimize data exchanged and make such data more interoperable with external systems. Despite the advantages introduced by decentralization in preventing congestion and improving the reliability of the system, it is hard to control a Cyber-Physical System (CPS) in an efficient and real-time way. To overcome these limitations it is possible to leverage Digital Twins (DTs) technology, which is able to provide a digital copy of physical systems in order to control their behavior and to obtain real-time data. These data are widely used in Machine Learning (ML) applications, to implement prediction or forecasting [8]. Deploying Thin Edge Nodes across various locations within the Smart Grid facilitates bidirectional synchronization between digital twins and physical systems. Moreover, it enables the integration of AI applications for automated decision-making, thereby alleviating operational burdens on grid operators. When combining this technology with energy efficiency context, it is possible to unlock the real potential of these algorithms. Currently, DTs are used in the energy sector to control three different phases: production, storage, and consumption [6], highlighting the importance of data produced, and the need for having a system able to certificate authenticity in the entire data flow. As depicted in Fig. 1, estimation of the energy consumed within a period could be used to buy the right quantity of energy to sell to the customers. Considering the case of wrong data acquisition this can lead to problems related to this estimation, such as overprovisioning or underprovisioning.

These have an automatic impact on the price of the energy required to meet the unforeseen rise in demand. Given the common architectures that the smart grid has adopted, if unsecured communication is used or physical access to the smart meter is too weak, attackers may purposefully alter the data that this device acquires or alter it while it is being transmitted. This research focuses on a specific type of smart grid architecture that uses a federated approach to estimate energy provisioning and detect anomalies in collected data. A typical attack scenario, caused by a malicious node, will be described in the manuscript. Relevance of these attacks can lead to an overall deterioration of the model. To effectively prevent these attacks we present a novel system leveraging blockchain technology. Our framework not only addresses the critical issue of data modification but also provides a mechanism to prevent attacks aimed at disrupting data-driven applications. Through validation in a real-world energy forecasting use case, we demonstrate the efficacy and reliability of our approach.

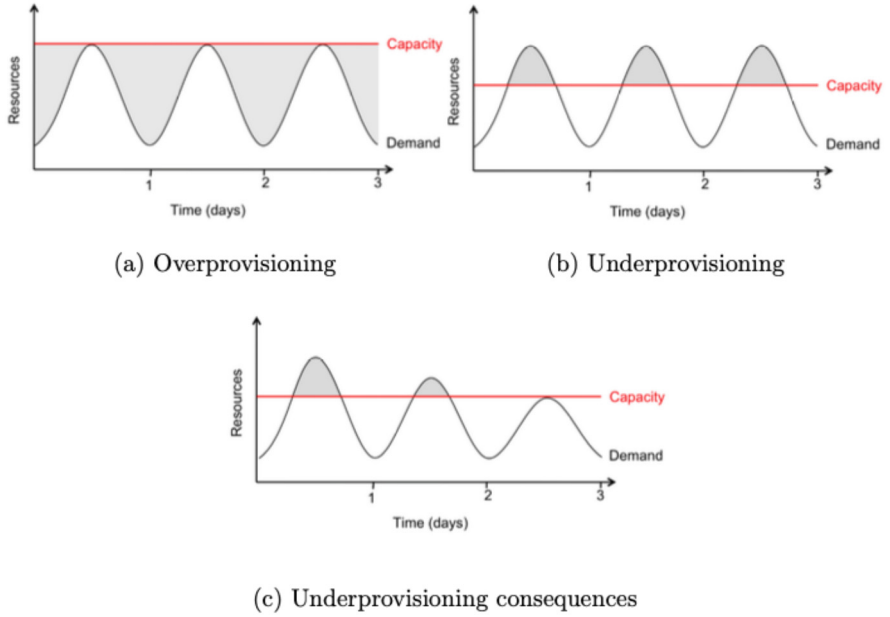


Fig. 1. Energy consumption prediction

The manuscript is structured into five sections. In the second section, we discuss the current research in the field of DTs to enhance the performance of smart grids. In the third section, we discuss of the proposed system, able to prevent attacks related to data poisoning and data modification. In the fourth section we demonstrate the efficacy of the proposed method by discussing results. We conclude the manuscript with the future works and limitations of the proposed approach.

2 State of the Art

In recent years, the increased performance of IoT Nodes, as well as edge devices, paved the way for more advanced applications within the CPS context. Anyway, this particular field introduces multiple challenges that must be take into account when designing a solution. Table 1 describes the most relevant challenges according to a recent review in the field [15]. CPS is usually associated with the DTs concept due to the characteristics of these elements to reproduce the current status of the physical counterpart. Multiple applications have been discussed in the literature, such as predictive [4,11] or prognostics [3] maintenance. An interesting application has been also presented within the automotive field, where a solution able to predict brake pad malfunctions has been presented in [10]. The improvements introduced by this technology are not limited to the economical aspect, but can easily be found also within the medical one [9]. The usage of

Machine Learning (ML) algorithms in combination with DTs can easily speed up almost every process [14], by reducing costs and preventing possible threats to humans.

Anyway, not all the properties can be satisfied by traditional DTs if considering the landscape of attacks which is possible to perform targeting an IoT device and the overall flow of communication between edge devices and servers [1]. A challenge in the development and design of CPS is represented by the significant differences among the various engineering disciplines involved, such as software and mechanical engineering. In fact, they require a highly skilled workforce, encouraging multidisciplinary collaborations between universities and industry. Some solutions, such as [2] proposed the usage of blockchain as a valuable technology to prevent data modification or to prevent unauthorized access to the system, anyway most of the works described do not cover all the challenges currently existing in a CPS. Our work aims at solving all these challenges by providing a strong framework able to prevent data tampering while ensuring the data heterogeneity and real-time data from sensors.

Table 1. Properties of a strong Cyber-Physical Systems (CPS)

Property	Description
Data heterogeneity	Systems must be able to support a large number of different applications and devices. Digital devices use different communication protocols such as Bluetooth, Zigbee, RF, and infrared
Reliability	Reliability and security are fundamental requirements due to how actuators influence the environment. Any failure of CPS components can lead to system degradation, resulting in serious harm to people and things
Data management	It is necessary to store and analyze big data from various connected devices, process them, and display the results in real-time
Privacy	Since CPS manage large amounts of data, including sensitive information such as health, gender, religion, and many others, significant data privacy issues are raised
Security	CPS rely on heterogeneous applications and wireless communications, which often raise security issues. Security has become a global concern
Real-time	CPS must ensure they have the necessary bandwidth or system capacity to meet critical time-sensitive functions because failures at the time of actions can cause permanent damage

3 Methodology

From SOTA section we have demonstrated the efficacy of ML algorithms applied to DTs in Smart Grid, as well as possible attacks on these systems, particularly concerning the data poisoning or data modifications. In this section, we will present our system with the first aim of detecting and recovering datasets from possible attacks on the system. The discussion of the proposed system is limited to an architecture containing a single device, instead of a federation of them, but it can be easily extended to include additional devices. In order to reflect the changes in a physical system in our model we implemented a DT-based approach,

where each smart meter is identified by a digital twin. Upon these, as depicted in Fig. 2, we created an ML model based on a digital twin able to detect the request of energy from one source. Blockchain acts as a backup registry where it is possible to restore previous versions of the model whenever an attack on the data has been detected. In the following subsections, we will go deeper in describing the components of the proposed system.

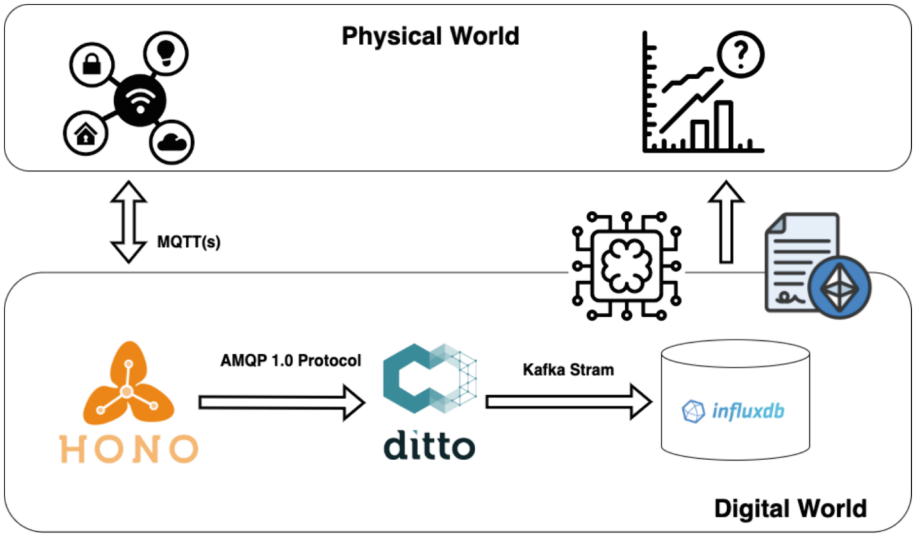


Fig. 2. Architecture of the Proposed System

3.1 Heterogenous Data Collections

One of the main challenges when considering typical DTs smart grid systems is related to the way in which IoT nodes are connected to the gateway. In the proposed system we choose Hono framework, which offers multiple communication protocols through the usage of adapter. Some example of supported protocol are HTTP, MQTT, CoAP, AMQP, and so on. In our system we will leverage this framework to create a reliable MQTT connection between the IoT node and the gateway. More in detail, to secure this communication we defined a Distributed Public Key Infrastructure (DPKI) approach, where each device holds an asymmetric key pair released by the authority. The management of certificates is done through the usage of a smart contract, as demonstrated in multiple approaches already existing in the literature described in [13]. The IoT Node will publish in a given topic served by Hono, authenticating itself using a TLS handshake. This handshake can be easily implemented in HTTP and MQTT, by securing the exchange of data between parties.

3.2 Digital Twin

We proposed a model where smart grid is represented by a digital twin. Particularly, we considers the architecture proposed in [5], where different aspects have been taken into account for representing the physical object. The idea is to have physical objects, all connected to the same gateway responsible for representing the current status. In our case it is implemented by Eclipse Ditto, which is able to include all the metadata connected to the physical entity. Before to define the digital twin, it is necessary to define a policy to assoicate with the physical thing that will be created with Ditto. An example is depicted in Fig. 3, where a policy called *my.test:policy* describes which is the owner of the policy and the permissions related with the operations. Each thing implementing this policy will follow all the permissions defined here. In this way it is possible to implement a mechanism of fine-grined policies, able to enhance the privacy of operations which is possible to perform on the physical object.

```
{"policyId": "my.test:policy","entries": {
   "owner": {
       "subjects": {
           "nginx:ditto": {
               "type": "nginx basic auth user"
           }
       },
       "resources": {
           "thing:/": {
               "grant": ["READ","WRITE"],
               "revoke": []
           },
           "policy:/": {
               "grant": ["READ","WRITE"],
               "revoke": []
           },
           "message:/": {
               "grant": ["READ","WRITE"],
               "revoke": []
           }
       }
   },
}
}
```

Fig. 3. Policy of IoT Node

Once defined policies, we defined attributes for the IoT node for the scope of our research, related to the power consumption. Notice that we want to forecast the overall consumption of energy within a smart home, which can be seen as a sum of the singular power consumption.

3.3 Real-Time Series Database

Managing huge quantity of data it is not an easy task and must be carefully implemented. The usage of InfluxDB, which is a real-time series database completely meet this requirement by providing a tool for collecting huge series of data. InfluxDB is a popular time-series database, plays a crucial role in the realm of energy prediction by efficiently storing and managing vast amounts of time-stamped data generated from various energy sources. In the context of energy prediction, data series refer to the sequential collection of energy consumption, production, and related metrics over time, forming the basis for predictive modeling and analysis. InfluxDB excels in handling the high volume and velocity of time-series data characteristic of energy systems, offering scalability, flexibility, and robust querying capabilities tailored to time-stamped datasets.

The integration of InfluxDB with data series for energy prediction enables organizations to leverage historical energy data to train machine learning models, develop statistical algorithms, and deploy predictive analytics solutions. By ingesting data from diverse sources such as smart meters, IoT sensors, weather stations, and renewable energy assets, InfluxDB provides a unified platform for aggregating, processing, and analyzing heterogeneous data streams critical for accurate prediction models.

One of the key advantages of using InfluxDB for energy prediction lies in its ability to handle real-time data ingestion and querying, facilitating timely insights and adaptive forecasting models. By leveraging continuous querying and retention policies, organizations can retain relevant historical data while efficiently managing storage costs and ensuring data accessibility for predictive analytics tasks.

3.4 Machine Learning Model

Typical smart grid architectures include a Machine Learning (ML) model able to perform predictions about a given task or behavior. Considering the case of energy forecasting and anomaly detection, we moved our focus to a Long-Short Term Memory (LSTM) model able to capture the correlation between time and trends in data. The model obtains the data read by the IoT sensors through the mechanism described before.

The model architecture is designed to accept input data in the format of (*number of features*, 1). In our scenario, as illustrated in Fig. 4, where the violet and black lines exhibit lower values, showcasing the influence of the day of the week on energy demand; we incorporated features such as day of the week, month, and hour of the day into our model. Then we placed two Convolutional Layers with ReLU activation, each followed by MaxPooling and Dropout layers. After that, flatten the output from the convolutional layers into a 1D vector. At the end of the model, we have one dense layer with a single neuron, serving as the output layer for regression.

Once we have added this information to the model, we have set up the model, and it is possible to proceed with the training phase. In this case, we proceed

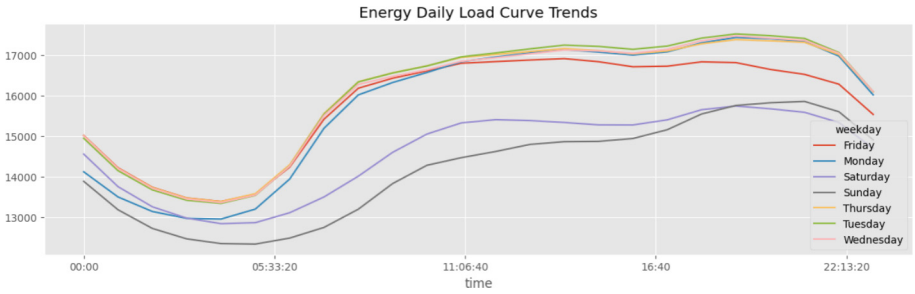


Fig. 4. Daily Load Trends

with a 80:20 split in order to validate the model and check for the initial accuracy. We will go deeper into analyzing the performance of the model in the results section, while now we focus on the mechanism used to gather data from DT and how to restore a previous version of the model in case of attacks.

3.5 Blockchain Backup

Although the described system effectively prevents attacks on communication, IoT nodes often remain susceptible to physical attacks. In such instances, attackers can manipulate the normal behavior of sensors or the microcontroller itself to transmit malicious data. In order to prevent possible attacks on the DTs and data poisoning attacks, aimed at disrupting the current knowledge available at the level of the digital world, it is necessary to implement a resilient mechanism able to provide data backup on possible attacks. Blockchain provides an immutable registry and a mechanism for the validation of the transaction which is highly resilient to attacks thanks to the distributed nature of the system.

Anyway, blockchain cannot be directly applied as storage due to the not permissive fee to pay for the transaction and for the storage of sensitive data, and we will leverage IPFS to store weights of the model as follows. To better explain the mechanism proposed, let us consider a constant time w. We set up a timer, which elapse each w minutes. In the case of the energy consumption model it is reasonable to think that this corresponds to a minute. At this time, the model will read the data from the DT and will store them in InfluxDB. After passing the entire day, it is ready to transmit the newer data to the model in order to perform reinforcement learning and improve the performance. At this point, in a traditional system, if the data received by the model have been poisoned or modified, then the accuracy of the model will decrease and the future predictions will be worse than the current ones. We will see an attack in the results section.

To prevent these attacks we proposed an architecture that include blockchain as a system to register the new weights of the ML model in IPFS. At the end of the day, whenever the InfluxDB need to transmit data to ML model, the model will contact the blockchain in order to assess the quality of current data and decide if accept the newer data. This can be done by performing a test

prediction in order to evaluate the quality of the new incoming data. If the current accuracy is found to be lower, indicating a potential poisoning attack, the backup mechanism will take place. This is done through a smart contract responsible for registering all the statuses of the ML model with the help of IPFS. As depicted in Fig. 5, the ML Model will upload the model parameters in IPFS as soon as it has a new value and performs reinforcement learning. Then it transmits the new Content ID (CID) to the Smart Contract, which will store the CID and will evaluate for the performance of the current model. To be more precise, this operation is performed by the ML Model which sends an accuracy value together with the new CID. Smart Contract saves all the accuracy values and will respond with the best weights between the newer and the previous one. As a note, the model under attack tends to overestimate the actual power consumption of the network yet it still manages to identify the underlying pattern of the dataset. The model, which leverages a backup mechanism, instead, achieves a good prediction with some underestimation in some phases, caused by the attacks received by the node.

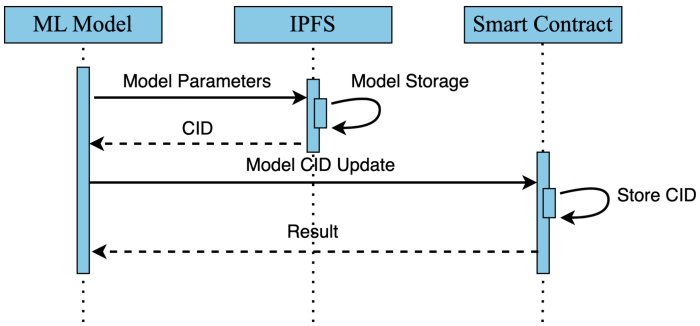


Fig. 5. Interaction between ML Model, IPFS and Smart Contract

4 Results

In order to evaluate the quality in terms of the security of the proposed system, we first introduce a possible attack aimed at disrupting the global model. Once the attack model is discussed, we validate the proposed approach by considering the Hourly Dataset [12]. It offers multiple sources of data, such as American Electric Power (AEP), Commonwealth Edison (ComEd), The Dayton Power and Light Company, Duke Energy Ohio/Kentucky (DEOK), and so on. We will focus on the first one, the AEP. It contains energy consumption from American citizens collected between 2004 and 2018. Despite this being an old dataset, we aim to validate attack detection and the backup system put in place through the usage of blockchain. The attack model outlined here pertains to the system discussed in the previous section and aims to demonstrate the impact of an attacker who intentionally alters the data collected by a smart meter within a federation. As

depicted by Fig. 6, we have two genuine smart meters performing local training and exchanging weights with the aggregator, and a third smart meter that acts as a malicious node (on the right). In this scenario, the attacker either gains access to the federation or physically compromises an authorized node. The implementation of the second attack involves the attacker disconnecting the wires and deliberately altering the data from the sensor to reduce its stability. At this point, InfluxDB will store the new data and according to the description given in the previous section, at the end of the day, it will transmit these data to the aggregator to update the global weights. If the incoming data does not reflect the current status of the system, then the novel weights and consequential local models will start to perform training on malicious data and will start to predict with less accuracy.

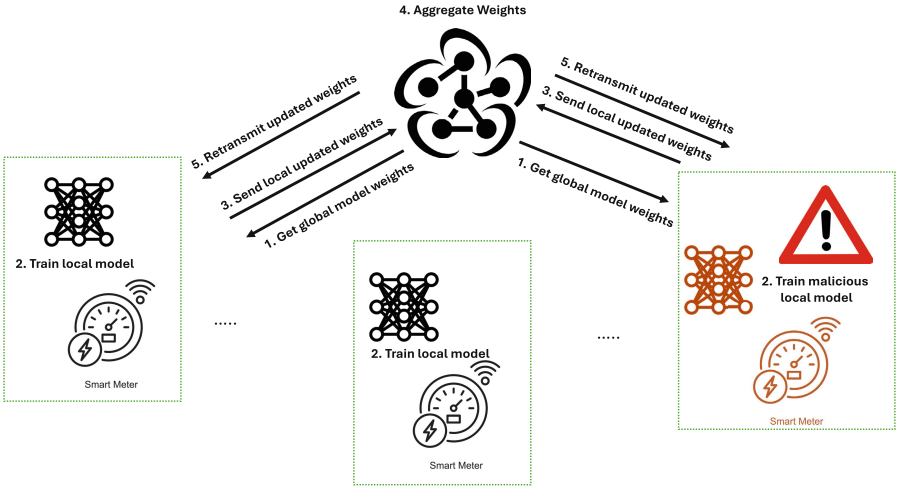


Fig. 6. Attack performed by malicious node (on the right) on the overall FL architecture.

A clear impact of the data poisoning attack is represented in Fig. 7. In Fig. 7a it is possible to notice a model applied to non-attacked data that behaves as a good model with interesting results on anomaly detection. Mean Square Error (MSE) scaled with the MinMax approach reveals a result of 0.002310 from the first model, indicating a pretty accurate prediction, with a really low error with respect to the actual values.

On the contrary, for the Fig. 7b, the model creates situations of overprovisioning and underprovisioning, leading to an increase in costs for the energy provider. MSE for the attacked model is 0.020164, which is 10 times higher with respect to the genuine model. Finally, the efficacy of our approach is depicted in Fig. 7c, where an MSE of 0.002780 has been obtained. Such an error validates our approach by marginally increasing the error faced with the genuine model.

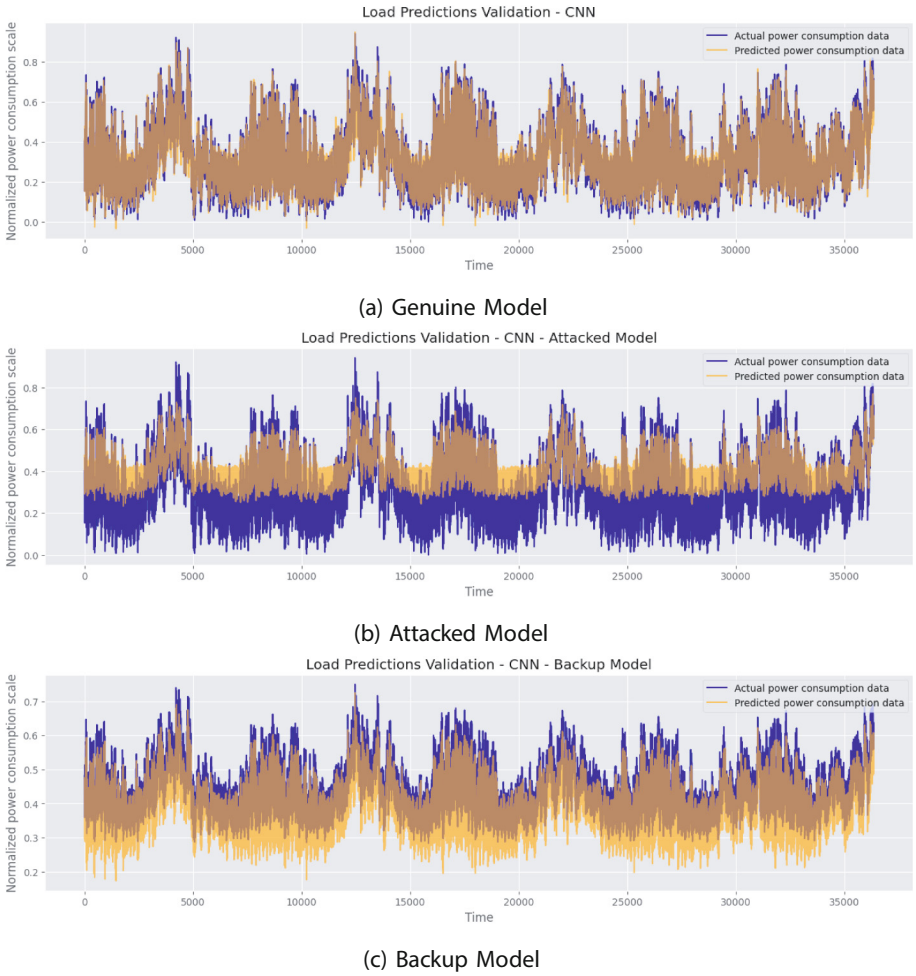


Fig. 7. Power Consumption Predictions

5 Conclusion

The current research demonstrated the efficacy of an interoperable and device-agnostic system to manage smart grid, able to manage threats related to data modification. Blockchain is a powerful technology that is able to restore previous versions of data efficiently. Results validate the proposed approach, by demonstrating a marginal error with respect to the genuine model. The limitations of the proposed approach are related to the data used to test the model, which is restricted to a dataset and might be enhanced with more recent data and data coming from the sensors. In the future, we aim to assess the quality of

the proposed approach in a federation of IoT devices where multiple devices are responsible for sensing the power requested by different sources guaranteeing non-IID property. Moreover, we planned to investigate another kind of attack aimed at disrupting smart grid communication or stealing sensitive information.

Acknowledgements. This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government (MOTIE) (RS-2023-00303559, Study on developing cyber-physical attack response system and security management system to maximize real-time distributed resource availability).

References

1. Alcaraz, C., Lopez, J.: Digital twin: a comprehensive survey of security threats. IEEE Commun. Surv. Tutorials **24**(3), 1475–1503 (2022)
2. Altun, C., Tavli, B.: Social internet of digital twins via distributed ledger technologies: application of predictive maintenance. In: 2019 27th Telecommunications Forum (TELFOR), pp. 1–4. IEEE (2019)
3. Cattaneo, L., Macchi, M.: A digital twin proof of concept to support machine prognostics with low availability of run-to-failure data. IFAC-PapersOnLine **52**(10), 37–42 (2019)
4. Centomo, S., Dall'Ora, N., Fummi, F.: The design of a digital-twin for predictive maintenance. In: 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), vol. 1, pp. 1781–1788. IEEE (2020)
5. Fujii, T.Y., et al.: A digital twin architecture model applied with mlops techniques to improve short-term energy consumption prediction. Machines **10**(1), 23 (2021)
6. Ghenai, C., Husein, L.A., Al Nahlawi, M., Hamid, A.K., Bettayeb, M.: Recent trends of digital twin technologies in the energy sector: a comprehensive review. Sustainable Energy Technol. Assess. **54**, 102837 (2022)
7. Hashmi, M.H., Ullah, Z., Asghar, R., Shaker, B., Tariq, M., Saleem, H.: An overview of the current challenges and issues in smart grid technologies. In: 2023 International Conference on Emerging Power Technologies (ICEPT), pp. 1–6 (2023). https://doi.org/10.1109/ICEPT58859.2023.10152331
8. Javaid, M., Haleem, A.: Digital twin applications toward industry 4.0: A review. Cognitive Robotics (2023)
9. Liu, Z., Zhang, Z., Xu, G., Jin, W., Lee, J.: Design of cyber-physical systems architecture for prognostics and health management of high-speed railway transportation systems. Int. J. Prognostics Health Manage. **9**(3) (2018)
10. Rajesh, P., Manikandan, N., Ramshankar, C., Vishwanathan, T., Sathishkumar, C.: Digital twin of an automotive brake pad for predictive maintenance. Procedia Comput. Sci. **165**, 18–24 (2019)
11. Rossini, R., Conzon, D., Prato, G., Pastrone, C., dos Reis, J.P.C., Gonçalves, G.: Replica: a solution for next generation IoT and digital twin based fault diagnosis and predictive maintenance. SAM IoT **2739**, 55–62 (2020)
12. Sahay, K.B., Tripathi, M.M.: Day ahead hourly load forecast of pjm electricity market and iso new England market by using artificial neural network. In: ISGT 2014, pp. 1–5. IEEE (2014)

13. Sivakumar, P., Singh, K.: Privacy based decentralized public key infrastructure (pki) implementation using smart contract in blockchain. National Institute of Technology, p. 6 (2017)
14. Soori, M., Arezoo, B., Dastres, R.: Digital twin for smart manufacturing, a review. Sustainable Manufacturing and Service Economics, p. 100017 (2023)
15. Tyagi, A.K., Sreenath, N.: Cyber physical systems: analyses, challenges and possible solutions. Internet Things Cyber-Phys. Syst. **1**, 22–33 (2021)