Poster: Securing the Virtual Mirror: Blockchain Technology for Digital Twins Security

Rahanatu Suleiman
Department of Computer and Information Sciences
Towson University
Towson, Maryland - 21252
Email:rsuleim1@students.towson.edu

Akshita Maradapu Vera Venkata Sai
Department of Computer and Information Sciences
Towson University
Towson, Maryland - 21252
Email:amaradapuveravenkatasai@towson.edu

***Abstract*—Digital twins have become essential tools for enhancing efficiency and security in various industries. However, their widespread adoption poses significant security challenges, with potential vulnerabilities that could be exploited by attackers. Here we examine some of the security threats faced by digital twins, including bandwidth sniffing, data delay attacks, data injection, and model poisoning. We then propose two blockchain based frameworks to address these security concerns. The first framework leverages blockchain for secure data transmission, while the second utilizes Hyperledger Fabric for enhanced privacy and data integrity. These frameworks offer robust solutions to safeguard digital twins ecosystem, ensuring the reliability and integrity of critical information in the face of evolving cyber threats.**

***Index Terms*—Digital Twins, privacy, Man-in-the-Middle attacks, blockchain CPS, Hyperledger Fabric, IPFS**

I. Introduction

Digital twins (DTs) have emerged as valuable tools for facilitating the development of efficient services, monitoring industrial processes, and ensuring proactive maintenance. These systems are built upon distributed network architectures, where individual electronic systems comprise a multitude of Internet of Things (IoT) devices [1]. A digital twin represents virtual replica of a physical asset, facilitating analysis, prediction, and optimization of operations by leveraging real time and historical data [2]. Within the realm of information security, DT plays a crucial role in fortifying the security of Cyber-Physical-Systems (CPS) through diverse security improving uses, including system testing, system training, and misconfiguration detection [3]. This is achieved by ensuring synchronous operation between digital twins and their physical counterparts, with the objective of identifying any discrepancies in data between the physical and virtual entities [4]. In other to understand the behavior of the physical environment, DT needs to get data from different sources, such as data from various stages of the CPS life cycle, domain expertise, and sensory inputs from the physical environment. It also uses several applications that support security during the system development and CPS. Despite having multiple use cases that support security during the system development and CPS operation stages [5], there are chances for attackers to leverage DTs as attack vectors against CPS due to the rise in hidden attacks. Due to their nature as digital replicas, DT shares functional needs and operational behavior with their physical counterparts. As a result, DTs could unintentionally act as channels for data breaches, increasing the risk of abuse. DTs offer significant advantages over traditional trial-and-error methods by enabling timely resolution of operational challenges in complex environments [1]. However, the efficiency of DTs relies on robust security measures to safeguard the associated data from potential vulnerabilities. Inadequate security protocols for DTs and their associated datasets may expose sensitive business information to risks such as loss or unauthorized use. Unprotected DTs are particularly susceptible to breaches that could compromise operational, security, and design data thus posing significant threats across various sectors. Consequently, there is a pressing need to enhance the security infrastructure surrounding DTs to mitigate potential risks and ensure the integrity of critical information. Blockchain technology has emerged as a promising option, with intrinsic features such as decentralization, immutability, and transparency that can improve the security of digital twin. The data collected using DT is analyzed by AI algorithms to find trends and make predictions. Blockchain technology offers a transparent and secure means of storing and sharing large volumes of data that are generated between parties for instant exchange and validation. Blockchain's decentralized systems provides high level security and resilience while operating independently, making it difficult to hack and attack the systems. Organizations can reduce the risks of data alteration, unauthorized access, and breach of privacy by integrating blockchain into their digital twin ecosystems [**?**].

II. Attacks on Digital Twins

Unprotected DTs may in some circumstances be susceptible to exposing sensitive operational, design, and security data to hostile parties, which could have a catastrophic effect on any sector. Such attacks include bandwidth sniffing and data delay attacks which are examples of man in the middle attacks (MiTM), as well as data injection and model corruption attacks which are examples of data poisoning attacks. Bandwidth sniffing allows attackers to monitor network traffic, identify vulnerabilities, and exploit weaknesses within the CPS and its digital twin counterpart. Data delay attacks disrupt real-time synchronization by introducing communication delays between the digital and physical entities. Data injection attacks use vulnerabilities to gain control over the CPS, potentially causing equipment damage or failure. The attacker can also mislead the DT by sending packets designed to mimic the current state of the CPS, leading to inaccuracies in operations and potentially compromising the reliability of the entire DT ecosystem. On the other hand, model corruption involves corrupting DT models by injecting malicious code, disrupting synchronization between the two. These attacks can lead to inconsistencies in output and degrade the fidelity of the DT in replicating the physical twin.

III. Proposed Solutions

To mitigate these security concerns, two blockchain based frameworks are proposed. In the first solution, both the DT and the CPS send and receive data through the blockchain. The physical twin generates a blockchain fingerprint for the intended data file before sending it to the DT. Subsequently, upon receiving the data, the DT attempts to send back the data, but blockchain authenticates the data and finds out the blockchain fingerprint is not present and sends it back to the DT. This process is further enhanced by time stamping each block within the blockchain, facilitating authentication of data origin, destination, participants involved, timing as well as the nature and method of data exchange. These measures establish a high degree of trust and security in data transmission, rendering the process tamper-proof [**?**]. Blockchain offers security, transparency, and decentralization,which differentiates it from classic authentication techniques like digital signatures.

In the second solution, Hyper-ledger Fabric (HF) is utilized as a private permissioned blockchain, offering robust privacy features where access and validation are restricted to authorized users. Fig 2 illustrates how stakeholders of the DT interact with HF through Application Programming Interfaces (APIs), which serves as front-end decentralized applications. Depending on the state of the DT, stakeholders can execute specific functional calls via these APIs. Additionally, stakeholders have the capability to monitor the DT's state, access logs, and the stored in IPFS servers. IPFS serves an important role in ensuring the reliability, integrity, and accessibility of stored data within the ecosystem. Each file uploaded to IPFS servers is uniquely hashed, providing a secure reference point for data integrity. All data pertaining to the creation of the DT and its subsequent processes are associated with a unique hash within IPFS. In the event of an attack aimed at stealing and corrupting data, any tampered data would fail to match the hash stored in IPFS, thereby alerting stakeholders of potential breaches and maintaining the integrity of the DT ecosystem.

IV. Conclusion

In conclusion, this research aims to improve understanding of blockchain solutions for DT security, offering practical insights int mitigating Cyber security threats within DT environment. By leveraging blockchain technology, organizations can maintain the dependability and integrity of simulated asset data and strengthen the robustness of their DT deployments. This project aims to pave the path for more robust and secure implementation of DT technologies across diverse industries by fostering trust and security in DT ecosystems.

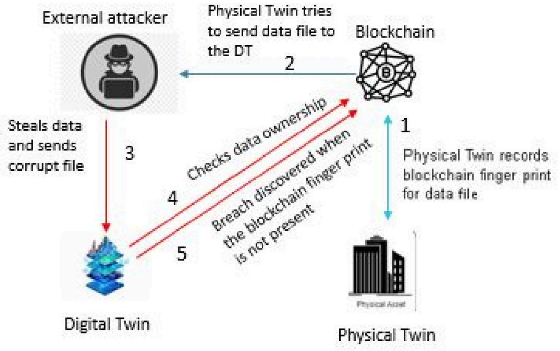

External attacker
Physical Twin tries to send data file to the DT
2
Blockchain
1
Physical Twin records blockchain finger print for data file
Steals data and sends corrupt file
3
Checks data ownership
4
Breach discovered when the blockchain finger print is not present
5
Digital Twin
Physical Asset
Physical Twin

Fig. 1. Blockchain for Data Authentication

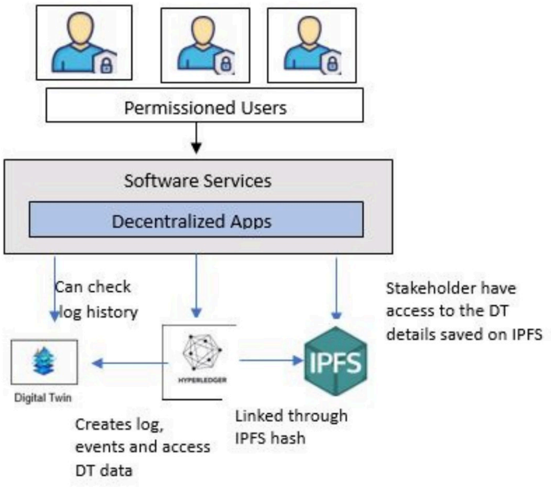


Fig. 2. Solution using Hyperledger Fabric and IPFS

References

[1] Juarez, M. G., Botti, V. J., and Giret, A. S. 2021. Digital Twins: Review and Challenges. ASME. J. Comput. Inf. Sci. Eng. June 2021;21(3):030802. https://doi.org/10.1115/1.4050244

[2] Yaqoob, I. et al. (2020) 'Blockchain for Digital Twins: Recent Advances and future research challenges', IEEE Network, 34(5), pp.290–298. doi:10.1109/mnet.001.1900661.

[3] Suhail, S. and Jurdak, R., 2021. Towards trusted and intelligent cyber-physical systems: A security-by-design approach. arXiv preprint arXiv:2105.08886.

[4] Eckhart, M. and Ekelhart, A., 2018, May. Towards security-aware virtual environments for digital twins. In Proceedings of the 4th ACM workshop on cyber-physical system security (pp. 61-72).

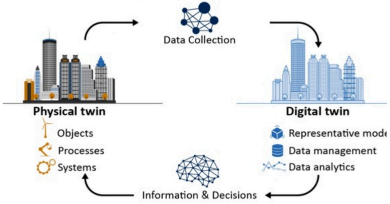
[5] Eckhart, M. and Ekelhart, A., 2019. Digital twins for cyber-physical systems security: State of the art and outlook. Security and Quality in Cyber-Physical Systems Engineering: With Forewords by Robert M. Lee and Tom Gilb, pp.383-412.

1. Motivation

One major challenge in deploying digital twins is ensuring the integrity of data transmitted between the physical and digital components of the twin. Cyber-attacks, system faults, or unauthorized access can all cause difficulties data integrity. Due to its decentralized and immutable nature, blockchain technology has emerged as a promising solution for improving security in a wide range of domains.

2. Digital Twin

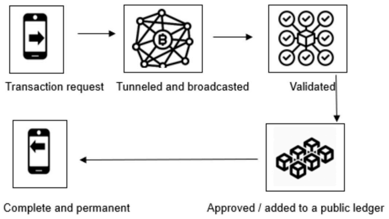
Digital Twins are virtual replicas of their physical counterparts that share essential system knowledge. They enable real-time monitoring, analysis, and optimization of assets, leading to improved efficiency and decision making.



Src:Gao;Ladoga/stock.adobe.com

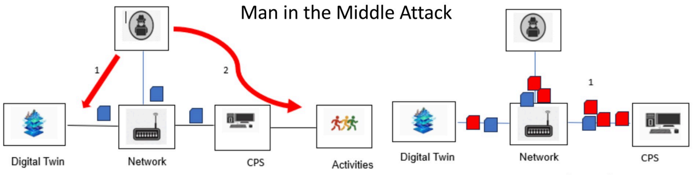
3. Blockchain Technology

How a Blockchain works



4. Cyber Attacks on Digital Twins

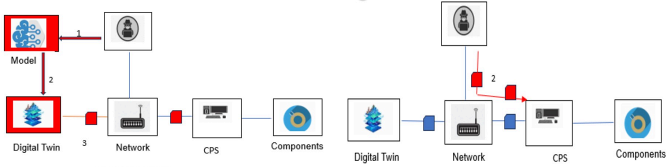
Man in the Middle Attack



Bandwidth Sniffing

Data Delay Attack

Data Poisoning Attacks

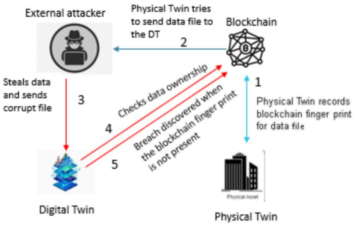


Model Corruption

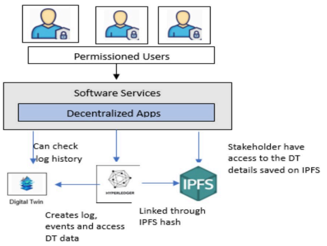
Data Injection Attack

5. Blockchain Solutions for Digital Twins Data

a. Blockchain for data authentication


External attacker
Physical Twin tries to send data file to the DT
2
Blockchain
Steals data and sends corrupt file
3
Checks data ownership
4
Breach discovered when the blockchain finger print is not present
5
1
Physical Twin records blockchain finger print for data file
Digital Twin
Physical Asset
Physical Twin

b. Using Hyperledger Fabric and IPFS



6. Conclusion

Blockchain technology presents a transformative approach to security against diverse data attacks targeting digital twins. Hyperledger fabric, a permissioned private blockchain, supports complex privacy by allowing only specific users to validate and access the blockchain.