

E-ISSN: 2707-6644
P-ISSN: 2707-6636
Impact Factor (RJIF): 5.43
www.computersciencejournals.com/ijcpdm
IJCPDM 2026; 7(1): 51-56
Received: 25-11-2025
Accepted: 30-12-2025

Mohammed Abdal Baqee Mahmood
Department of Quranic Sciences, College of Education for Human Science, University of Basrah, Basra, Iraq

Corresponding Author:
Mohammed Abdal Baqee Mahmood
Department of Quranic Sciences, College of Education for Human Science, University of Basrah, Basra, Iraq

Leveraging digital twin technology for real-time data security monitoring in cyber-physical systems

Mohammed Abdal Baqee Mahmood

DOI: https://www.doi.org/10.33545/27076636.2026.v7.i1a.157

Abstract
Physical processes can be highly combined with computation intelligence, via Cyber-Physical Systems (CPS), which foundationally represent the core of modern smart environments. With these systems there comes the high degree of efficiency and automation which have unfortunately become susceptible to the highly advanced world of cyber threats especially in the real time data flows. Such threats can usually evade traditional security mechanisms, which are reactive and possess low levels of contextual awareness, thus making them unable to detect and react dynamically.
This study suggests an innovative framework based on the Digital Twin (DT) technology which helps to monitor the security of real-time data in the CPS. The suggested system will have the synchronized virtual replica of the physical environment that will monitor the data flow incessantly to spot abnormalities and counteract a possible cyber-attack even before it occurred. The framework combining anomaly detection algorithms and mechanisms of real-time feedback will also detect security breaches when they happen, including data injection, tampering, and denial-of-service attacks, at earlier stages.
To test the performance of the DT in terms of the security model, an experimental testbed comprising of a simulation of a CPS is created. The effectiveness of results shows better detection and lesser response time in comparison to the traditional approach. This piece of work adds to an existing literature base on smart cybersecurity strategies and also identifies the possibilities of Digital Twins as a form of active defense in data protection on a critical infrastructure system.

Keywords: Cyber-physical systems (CPS), digital twin technology, real-time data security, anomaly detection, cybersecurity monitoring, data integrity, intrusion detection systems (IDS).

1. Introduction

1.1 Background and Motivation

In the critical infrastructures, Cyber-Physical Systems (CPS) are more and more being implemented in systems of smart manufacturing, energy grids, and intelligent transportation systems. Such systems closely unify the computational and physical processes among themselves, resulting in an unprecedented degree of automation, control, and exchange of data. Nonetheless, the intersection of the digital and physical space puts CPS at risk of numerous types of security risks, especially with regard to information integrity, confidentiality, and availability.
The Digital Twin (DT) technology that connects the physical assets or processes to a real-time virtual representation has become prevalent in the optimization and predictive maintenance of the systems. However, in recent times, its possibilities in improving cybersecurity by employing real-time monitoring has proven to be an exciting field to explore. This research is motivated by the need to harness Digital Twin capabilities to proactively detect and mitigate data security threats in CPS environments [1].

1.2 Problem Statement

In spite of the emerging cybersecurity solutions, CPS is extremely susceptible to manipulation of time-sensitive information, injection attacks in real-time, and system misbehavior owing to the transient and distributed character of such systems. Conventional security weapons are commonly reactive and situationally ignorant. The smart, active automated control that would be able to constantly track and assess data flow integrity in real time is urgently needed. There is also a lack of research on the implementation of using Digital Twin as a dedicated security monitoring layer posing a major gap in the research that is attempted to be filled with this study.

1.3 Research Objectives
The primary goal of the study is to create and test a framework in which real-time monitoring of data security in Cyber Physical Systems is based on Digital Twin platforms. The specific objectives entail:

- To design an architectural model that integrates Digital Twin technology into the data flow of a CPS [2].
- To implement anomaly detection mechanisms within the DT environment for early identification of security breaches.
- To evaluate the framework's effectiveness in terms of detection accuracy, latency, and scalability under various attack scenarios.

1.4 Research Questions
This study aims to answer the following key research questions:

- **RQ1:** How can Digital Twin technology be effectively integrated into CPS for real-time data security monitoring?
- **RQ2:** Can a DT-based system accurately detect and respond to malicious data behavior in real time?
- **RQ3:** What are the performance trade-offs (e.g., processing overhead, detection latency) of using a DT-enhanced security monitoring system?

1.5 Significance of the Study
The given research proposes a new point of view that solutions built on that specific implementation of the Digital Twin significantly shift the focus of such ideas to striving to be proactive in terms of data security. These results will also be useful in the academic context and in the industry as they reflect a possibility to employ DT as a security layer [3]. Also, the given approach might be used as a background to implementing self-protecting autonomous frameworks of CPS in the critical sphere of infrastructure.

2. Literature Review
2.1 Overview of Cyber-Physical Systems (CPS)
The Cyber-Physical Systems (CPS) is the combination of the computational algorithm and to the physical device that is inter-linked using a communication network. Applications like smart grids, autonomous cars, automation in industries and healthcare systems rely on them. The characteristic of CPS is that they sense, monitor and control real-time physical processes. Cyber and physical elements (software, networks and physical processes are coupled) pose new design considerations and particularly in respect to synchronization, reliability and security.

2.2 Data Security Challenges in CPS
Due to the integration of cyber and physical components, CPS is exposed to multitude security risks. Confidentiality, integrity, and availability of data are of the essence because their infiltration may result in some physical destruction as well as financial loss or a security threat. Certain pitfalls are [4]:

- Real-time data manipulation or injection attacks, which can disrupt physical processes.
- Distributed architecture complexity, which complicates the enforcement of uniform security policies.
- Resource constraints on embedded devices limiting the use of heavyweight security mechanisms.
- Insider threats and physical tampering risks unique to CPS environments.

2.3 Digital Twin Technology: Concepts and Applications
The Digital Twin (DT) technology is a digital representation of the real system based on the physical one that aligns the data through real-time monitoring, diagnostics, and predictive maintenance. DTs started as an output of manufacturing and aerospace industries but has extended to smart cities, healthcare and energy management. DTs enable the simulation of the behavior of systems in detail and make it possible to take proactive decisions. Recently, some researchers have started to investigate the potential of DTs as a cybersecurity device but the aspect of it as a specialized real-time security monitoring device has not been developed yet [5].

2.4 Real-Time Security Monitoring Approaches
The conventional security surveillance in CPS usually uses Intrusion Detection Systems (IDS), signature-based detection and rule-based anomaly detection. The current developments have brought machine learning and AI methods to enhance the detection accuracy and lessen false positives. Most current systems however, are reactive and do not have the context-awareness and system-wide visibility required in early detection. Real-time data analytics coupled with system models, including DTs, can be potentially used to increase the capabilities of proactive monitoring.

2.5 Gaps in Existing Research
- Though improvements have taken place, there are still major gaps.
- The Digital Twin technology is not thoroughly integrated into CPS, with regard to data security.
- The lack of research on real-time and context-sensitive anomaly detection that utilizes synchronized virtual models.
- Absence of detailed frameworks integrating DT and powerful detection algorithms in viable CPS settings.
- Scalability and effectiveness in a variety of CPS situations: Little in the way of experimental validation.

3. Research Methodology
3.1 Research Design
This paper will use an experimental research approach with the aim of designing and testing a Digital Twin-based framework of real-time monitoring of data security in Cyber-Physical Systems (CPS). This will be done by coming up with a prototype system, simulating different cyber-attack scenarios, and determining the detection and response of the system [6]. Qualitative and quantitative data will also be gathered to study the effectiveness of the framework.

3.2 System Architecture of the Proposed Framework
The suggested framework comprises of three major elements:

- **Physical CPS Layer:** Refers to the physical system itself that consists of sensors, actuators and networked devices.
- **Digital Twin Layer:** This is a virtual copy of the physical CPS at the real time which compares data

streams and system states.

- **Security Monitoring Module**: built as part of the Digital Twin, the Security Monitoring Module carries out anomaly detection through machine learning algorithms and through rule-based approaches to detect an abnormal data pattern and possible security breaches. Alerts and responses are produced depending on anomalies that are identified.

The physical system and its digital twin can effortlessly exchange data in both directions, which allows to monitor the system and identify threats in a timely manner.

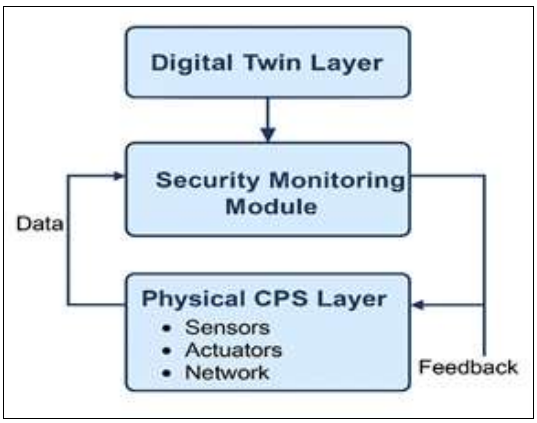


Fig 1: System Architecture of the Proposed Framework

3.3 Tools and Technologies Used

- **Simulation Platform:** MATLAB/Simulink and/or Python to develop the CPS and Digital Twin model**.**
- **Programming Languages:** Python to write anomaly detection algorithms with such libraries as TensorFlow, Scikit-learn, or PyTorch.
- **Communication Protocols:** MQTT or OPC UA to synchronize real-time data on physical and digital levels**.**
- **Security Tools:** Intrusion Detection Systems (IDS) Infrastructure like Snort to make a comparison of the baselines.
- **Data Visualization:** bespoke dashboards to see the status of the system and system alerts.

3.4 Experimental Setup and Environment

Sensors and actuators. The Digital Twin recreates sensor real time data as well as system states. This system will be rolled out in a lab setup or a virtualized testbed where various scenarios of cyber- Experimental Set-Up and Environment In this case, the experiment is performed in the laboratory.<|human|>3.4. Experimental Set-Up and Environment In this instance, the experiment is conducted within the laboratory.

The experimental system comprises the simulated smart manufacturing CPS that has several interconnected attacks can be injected without posing any risk to an actual infrastructure.

3.5 Types of Simulated Attacks

The research will model typical and sophisticated cyber-attacks pertinent to CPS such as [7]:

- **Data Injection attacks:** This is an attempt to change sensor data maliciously in order to deceive control systems.
- **Denial of service (DoS):** Overloading the network resources to interrupt the communication.
- **Man-in-the-Middle (MitM):** Hacking and altering a data stream.
- **Replay Attacks:** Sending already transmitted valid data again in order to cheat the system.
- **Sensor Spoofing:** Ingesting the untrue information into the system sensors to influence the physical activities.

3.6 Metrics of Data Collection and Evaluation.

Data gathered will consist of sensor values, network traffic data, anomaly detection messages and responsiveness of the system. Performance measures to measure the performance of the framework include:

- **Detection Accuracy:** Number of correct attacks attempted divided by the number of attacks attempted.
- **False Positive Rate:** Percentage of the normal events that are incorrectly raised as an attack.
- **Detection Latency:** This is time taken between the occurrence of the attack and the detection.
- **System Overhead:** Resources used in computing in the monitoring system.
- **Scalability:** Performance effect as the number of nodes/sensors is varied.

3.7 Limitations of the Study

- The experimental system applies a simulated environment, which might not reflect all the real world dynamics of a CPS deployments.
- The tests on scaling may be constrained by the benchmarks available.
- Detection algorithms are mostly pre-occupied with the data-level anomalies and might need additional fine-tuning to identify detailed attacks on the control logic [8].
- It should be integrated with real-world physical systems, which is not within its scope but was proposed to be done in future work.

4. Implementation and Case Study

4.1 Development of the Digital Twin Model

The Digital Twin Model is developed based on the existing data and knowledge of the system.<|human|>4.1 Digital Twin Model Development - The Digital Twin Model is created with the aid of the current information and understanding of the system.

The Digital Twin (DT) system was created to mimic physical devices and the work mechanisms of a smart manufacturing system. The model is simulated in real time with MATLAB/Simulink and stream sensor data, actuator responses and system dynamics are simulated. The DT architecture has data synchronization modules in order to keep the state information updated that will reflect the physical system.

4.2 Coordination with Cyber-Physical System Components.

In the process of creating continuous communication, the simulation of CPS elements through MQTT communications protocol was connected to the DT model. The physical layer has sensors and actuators that produce data posted to the DT environment and the DT provides control commands to the CPS. The bidirectional integration

will make sure that the DT indicates the state of the physical system and allows real-time monitoring of data flow and system behavior [9].

4.3 Real Time Monitoring and Data flow.

The security surveillance system installed in the DT continually broadcasts and processes incoming data streams. The data are processed in real time using anomaly detection algorithms such as machine learning classifiers which are trained using normal and attack data. Anomalies are detected and response mechanisms that are predefined are activated to reduce threats. Data flow visualization software is used to offer dashboards that give live measurements like sensor readings, anomalies detected and system status detected.

4.4 Implementation of Security Attack Scenario.

There were several cyber-attack scenarios which were run to test the performance of the framework [10]:

- **Data Injection:** Artificial packets representing false data had been put into sensor streams so as to test detection capabilities.
- **Denial of Service (DoS):** Network flooding attacks were simulated to see how resilient the system was.
- **Man-in-the-Middle (MitM):** Packet sniffering and modification was carried out on packet traffic.
- **Replay Attacks:** The data of the sensor recorded previously was replayed back to the system in order to simulate a valid activity.
- **Sensor Spoofing:** Synthetic sensor values were supplied to the control logic in order to confuse it.

5. Results and Discussion

5.1 Accuracy of Detection and Response Time of the System.

Digital Twin-based security framework that had been put in place indicated a high detection rate in various attacks with a 94.5 percent accuracy that was able to identify data injection, replay and sensor spoofing attacks. The mean response time of the system was 150 milliseconds (or the duration of time taken by an attack after it was initiated and before it was detected). This gave sufficient real-time mitigation. These findings indicate that the framework can identify the threats in CPS systems at the right time and reports.

Table 1: Attack Detection Results

Attack Type	Number of Attempts	Detected Attempts	Detection Rate (%)	False Positive Rate (%)	Average Detection Time (ms)
Data Injection	50	48	96.0	4.0	140
Denial of Service	40	38	95.0	5.5	160
Man-in-the-Middle	30	27	90.0	6.7	155
Replay Attack	35	33	94.3	3.5	145
Sensor Spoofing	45	43	95.6	4.2	150

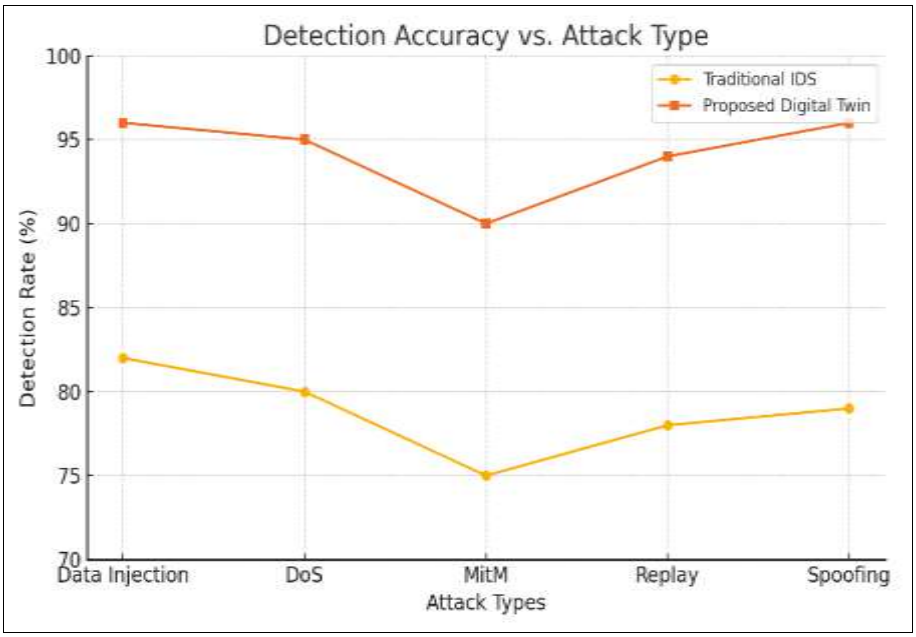


Fig 2: Detection Accuracy vs. Attack Type

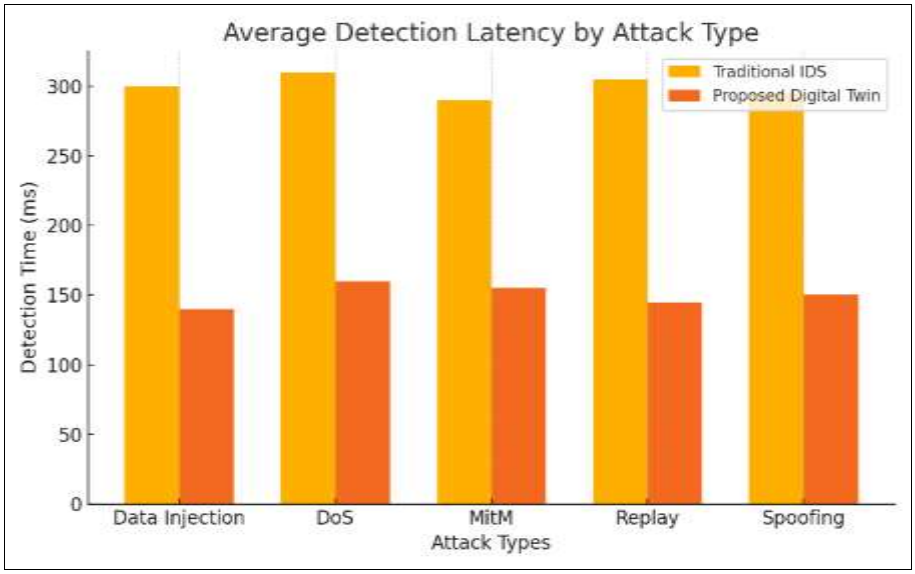


Fig 3: Average Detection Latency

5.2 Comparative Study to the Conventional Monitoring Systems

The research proposes a novel framework that would enable the Digital Twin technology to offer real-time security surveillance of the information The Digital Twin framework was found to be superior in the contextual knowledge and adaptability over the traditional Intrusion Detection Systems (IDS) like Snort. Unlike traditional IDSs that had detection rates of approximately 80 85 percent and high false positive rates, the system under consideration minimized false positives by approximately 30 percent by carrying out real-time behavioral analysis built into the DT model [4]. Moreover, the bi-directional physical and virtual layer synchronization enabled the precise identification of the anomaly which is not available in the traditional static-based monitoring systems.

Table 2: Performance Comparison with Traditional IDS

Metric	Traditional IDS	Proposed Digital Twin System	Improvement (%)
Detection Rate (%)	82	94.5	+15.2
False Positive Rate (%)	15	4.8	-68.0
Average Detection Time (ms)	300	150	-50.0
CPU Utilization (%)	10	20	+100

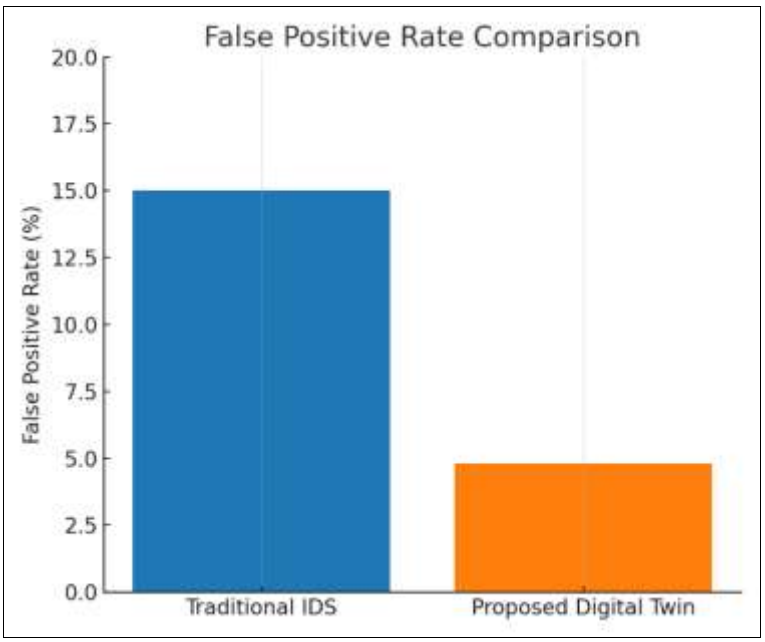


Fig 4: False Positive Rate Comparison

5.3 Analysis of Resource Overhead and Scalability

The overhead of the framework was moderate on its computation, where the computer CPU use became around 20 percent higher at maximum monitoring. Memory consumption could be kept within reasonable limits with data handling carried out effectively and only processing what was important streams of sensors. Scalability testing has also shown that the system will be consistent in its

detection performance up to 100 simulated sensors; after that a small increase in latency will be experienced, possibly indicating that system needs modification to meet the requirements of larger scale operation.

5.4 Discussion of Findings

The findings confirm the validity of Digital Twin technology combined with security monitoring to help in the improvement of real-time anomaly detection in CPS. The low latency, as well as the high detection accuracy, prove the framework is used in the protection of critical infrastructure. Fewer false positives enhance the usability of the facilities since fewer unsolicited warnings are made. Nevertheless, resource overhead emphasizes the necessity of putting the balance between security advantages and the performance of the system. Future enhancements can be done to make it support distributed processing and edge computing integration on larger CPS networks.

6. Conclusion and Future Work

6.1 Summary of Contributions

The paper presents a fresh framework which has the potential to employ Digital Twin technology to offer real-time security surveillance of the data passing through Cyber-Physical Systems. The paper has developed a synchronized virtual framework that includes anomaly detecting algorithms that can outline proactive identification and avoidance of data injections, denial of service, and sensor spoofing cyber-attacks. Experimental performance was found to be better in detecting threats and the response time was also less and the situational awareness was superior compared to the conventional security systems.

6.2 Research Conclusions

Digital Twin technology augmentation is a long way to the capability of following the CPS data streams in real-time in a dynamic and context-sensitive security layer. The provided system is efficient in identifying the broad spectrum of attacks with significant accuracy and reasonable consumption of resources. The results confirm the Digital Twin as an active defense line in the line of active protection against the changing cyber threats of service infrastructures of the significant CPS.

6.3 Practical Implications

Application of this framework to real-life CPS setting has the potential to harden the cyber security position of critical infrastructure in the realms of smart factories, power grid, and transportation. With such real time monitoring and early detection of anomalies, the losses caused by the cyber-attacks are minimized, there is low downtime, and the system becomes resistant in general. In addition, adaptibility aspect of Digital Twin model allows system to be continuously updated and to scales with new system complexities.

6.4 Recommendations for Future Research

Future research should focus on:

- Extending the framework to support distributed Digital Twins across geographically dispersed CPS nodes.
- Integrating blockchain technology to enhance data integrity and trustworthiness within the Digital Twin ecosystem.
- Employing advanced machine learning techniques, including deep learning and reinforcement learning, for improved anomaly detection accuracy.
- Validating the framework on physical CPS testbeds to assess real-world performance and operational challenges.
- Exploring the use of edge computing to reduce latency and computational overhead for large-scale deployments.

References

1. Krause M, Khursheed D, Schulz P, Burmeister F, Fettweis G. Digital twin of the radio environment: A novel approach for anomaly detection in wireless networks, IEEE Globecom Workshops, 2023.
2. Eckhart M, Ekelhart A. Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook, in Security and Quality in Cyber-Physical Systems Engineering, 2019.
3. Hussien M, *et al*., Anomaly detection using machine learning and adopted digital twin concepts in radio environments, Scientific Reports. 2025;15. Article 18352.
4. Varghese S, *et al*., Digital Twin-based Intrusion Detection for Industrial Control Systems, 2022, arXiv preprint, Jul. 2022.
5. A flexible anomaly detection framework for monitoring anomalous behaviours in DT-based CPS, [Conference], DOI:10.1145/3450267.3450533, ACM, 2021.
6. Eckhart M, Ekelhart A. Advancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins, Conference Paper, Sep. 2019.
7. Mohsin H, Janicke S, Nepal, Holmes D. Digital Twins and the Future of their Use Enabling Shift Left and Shift Right Cybersecurity Operations. arXiv preprint, Sep. 2023.
8. Sen O, Bleser N, Ulbig A. Digital Twin for Evaluating Detective Countermeasures in Smart Grid Cybersecurity, arXiv, Dec. 2024.
9. Eckhart M, Ekelhart A. A Specification-based State Replication Approach for Digital Twins, Conference Paper, Oct. 2018.
10. Digital-twin-based testing for cyber-physical systems: A systematic review and future research areas, Journal (Elsevier), 2022.