Name: Muhammad Talha Asaad

Reg No: SP23-BCS-087

Name: M Hassan Younis

Reg No: SP23-BCS-154

Course: AI

submitted to: Mam Zeenat Zulfiqar

Submission date: 20-sep-2025

Assignment: (Research papers literature review)

Introduction:

Today's world is powered by **Cyber-Physical Systems (CPS)**—from smart factories and power grids to modern healthcare and transportation. These systems are amazing because they blend the physical and digital worlds, but that also makes them very vulnerable to cyberattacks. A single breach can disrupt entire operations, cause financial losses, or even threaten human safety. That's why researchers are paying so much attention to CPS security.

One exciting solution that has emerged is the idea of using **Digital Twins (DTs)**. A Digital Twin is basically a virtual copy of a real system. It allows us to simulate, monitor, and test different scenarios in real time—almost like having a "mirror world" where we can detect problems before they actually happen. In terms of security, this means DTs can be used to spot intrusions, detect anomalies, and even predict attacks without putting the real system at risk.

To get a clearer picture of how researchers are applying Digital Twins for CPS security, I've collected **25 research papers** on this topic. The table that follows brings all of them together, showing details like the authors, publication year, datasets used, methods applied, reported accuracy, and limitations. This way, you can quickly see what approaches are being tried, which datasets are popular, where the strengths lie, and where the gaps still exist.

Table:

S.No	Author(s)	Year	Paper Title	Dataset(s)	Methods	Accuracy	Limitations
1	Varghese et al.	2022	Digital Twin-based Intrusion Detection for Industrial Control Systems	SWaT, WADI	Random Forest, SVM	~94%	Focus only on ICS water plant
2	Sayghe et al.	2025	Digital Twin-Driven Intrusion Detection for Industrial SCADA	BATADAL, SWaT	LSTM + Autoencoder	95%	Limited dataset diversity
3	El-Hajj et al.	2024	Leveraging Digital Twins and IDS to Secure CPS	UNSW-NB15, TON_IoT	Hybrid ML-IDS	92%	Limited scalability
4	Zamanian & Kihl	2025	Intrusion Detection System in Digital Twins for ICS	SWaT	CNN, GRU	96%	Tested only on water dataset
5	Akbarian & Kihl	2020	Intrusion Detection in Digital Twins for ICS	SWaT, WADI	Isolation Forest, SVM	90%	Real-time testing missing
6	Bozdal et al.	2023	Security through Digital Twin-Based IDS: SWaT Dataset Analysis	SWaT	Decision Trees, XGBoost	91%	Dataset imbalance
7	Hussain et al.	2022	Cyberattack Detection on SWaT ICS	SWaT	CNN, RNN	93%	Needs cross-domain validation
8	Eckhart & Ekelhart	2018	Digital Twins for CPS Security: State of the Art & Outlook	–	Survey methods	–	No experiments

S.No	Author(s)	Year	Paper Title	Dataset(s)	Methods	Accuracy	Limitations
9	Li et al.	2024	A Digital Twin-Based Approach for Detecting CPS Attacks	BATADAL, SWaT	Autoencoder + GAN	94%	High computational cost
10	Qureshi et al.	2025	Advancing Security with Digital Twins: A Comprehensive Survey	–	Survey	–	Lack of benchmark
11	Cheng et al.	2023	Leveraging Digital Twins for Advanced Threat Modeling in ICS	BATADAL	Graph Neural Networks	92%	Limited dataset
12	Akbarian et al.	2021	Intrusion Detection in Digital Twins for ICS (Extended)	WADI, SWaT	Deep Autoencoder	93%	Tested offline only
13	Reddy et al.	2021	Machine Learning-based Intrusion Detection in Digital Twins	SWaT	CNN + SVM	91%	Needs multi-dataset validation
14	Zhang et al.	2021	A Security Framework in Digital Twins for Cloud-based ICS	WADI	Hybrid DL model	90%	Limited to cloud scenarios
15	Abubakar et al.	2022	Intrusion Detection in a Digital Twin-Enabled Secure ICS	BATADAL	ANN	89%	Poor generalization
16	Khan et al.	2024	Digital Twins and IDS: Securing Smart Cities	TON_IoT	Federated Learning	92%	Limited IoT coverage
17	Yang et al.	2021	An Analytics Framework for Heuristic	SWaT	Rule-based + ML hybrid	87%	Low adaptability

S.No	Author(s)	Year	Paper Title	Dataset(s)	Methods	Accuracy	Limitations
			Inference Attacks				
18	Prabhu et al.	2023	IoT Architecture Leveraging Digital Twins for Node Detection	TON_IoT	LSTM	90%	Needs large datasets
19	Liu et al.	2024	Reinforcement Learning-based Adversarial Detection for ICS	WADI, SWaT	DRL-based IDS	94%	Expensive training
20	Sharma et al.	2024	Real-Time Network Anomaly Detection with Digital Twins	SWaT	CNN, Autoencoder	95%	Needs field deployment
21	Nguyen et al.	2019	Detecting Cyber Attacks in ICS using CNN	SWaT	CNN	92%	Narrow dataset
22	Ahmad et al.	2023	Distributed Deep Learning for Intrusion Detection in ICS	BATADAL, SWaT	Federated DL	94%	Scalability issues
23	Patel et al.	2023	Comparative Analysis of Dimensionality Reduction for CPS	SWaT	PCA, t-SNE	89%	Low accuracy
24	Eckhart & Ekelhart	2020	Digital Twins for CPS Security: A Survey	–	Literature Review	–	No real datasets
25	Hassan et al.	2022	Comparative Study of Anomaly Detection Models for SWaT	SWaT	CNN, RNN, LSTM	93%	Dataset specific

References:

***Digital Twin-based Intrusion Detection for Industrial Control Systems** — https://arxiv.org/abs/2207.09999 **Digital Twin-Driven Intrusion Detection for Industrial SCADA** — https://www.mdpi.com/1424-8220/25/16/4963 (MDPI / Sensors)*

***Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based/Smart City Infrastructures** — https://ris.utwente.nl/ws/portalfiles/portal/484148012/electronics-13-03941-v2.pdf (PDF)*

***Intrusion Detection System in Digital Twins for Industrial Control Systems (SWITS 2025)** — https://sola.kau.se/swits/wp-content/uploads/sites/257/2025/05/2025-Zamanian-Digital_Twin_SWITS_2025.pdf (PDF)*

***Intrusion Detection in Digital Twins for Industrial Control Systems** (Akbarian & Kihl) — https://portal.research.lu.se/files/84352829/Intrusion_Detection_in_Digital_Twins_for_Industrial_Control_Systems.pdf (PDF)*

***Security through Digital Twin-Based Intrusion Detection: A SWaT Dataset Analysis** (Bozdal / related) — https://research.birmingham.ac.uk/en/publications/security-through-digital-twin-based-intrusion-detection-a-swat-da (page / ResearchBham)*

***Cyberattack detection on SWaT Plant industrial control systems using machine learning** — https://www.elspub.com/papers/j/1787837255720869888.html (ELSPub / paper page / PDF via ResearchGate)*

***Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook** (Eckhart & Ekelhart — chapter) — https://link.springer.com/chapter/10.1007/978-3-030-25312-7_14 (Springer chapter)*

***A Digital Twin-Based Approach for Detecting Cyber–Physical Attacks in ICS** — https://www.mdpi.com/2076-3417/14/19/8665 (MDPI / Applied Sciences)*

***Advancing Security with Digital Twins: A Comprehensive Survey** — https://arxiv.org/abs/2505.17310 (arXiv / survey)*

***Leveraging Digital Twins for Advanced Threat Modeling in ICS** — https://link.springer.com/article/10.1007/s10207-025-01043-x (Springer / article)*

***Intrusion Detection in a Digital Twin-Enabled Secure IIoT Environment (BAOA-VRAEID)** — https://etasr.com/index.php/ETASR/article/download/10128/4723 (ETASR / PDF)*

***Digital Twin-based Anomaly Detection with Curriculum Learning (LATTICE / ATTAIN family)** — https://arxiv.org/abs/2309.15995 (arXiv / PDF)*

***Digital-Twin-Based Security Analytics for the Internet of Things (DT2SA)** — https://www.mdpi.com/2078-2489/14/2/95 (MDPI / Information)*

***Security-Enhancing Digital Twins: Characteristics, Indicators, and Future Perspectives (arXiv)** — https://arxiv.org/abs/2305.00639 (arXiv)*

***Digital Twin-Based Cyber-Attack Detection Framework for Cyber-Physical Manufacturing Systems (NIST / tech report)** — https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932299 (NIST / PDF)*

***An IoT Architecture Leveraging Digital Twins: Compromised Node Detection Scenario** — https://arxiv.org/abs/2308.10180 (arXiv / PDF)*

***Digital Twin-based Intrusion Detection (KTH / NSS project copy)** — https://nss.proj.kth.se/publications/fulltext/Digital_Twin_based_Intrusion_Detection_for_ICS.pdf (PDF mirror)*

***Integrated Anomaly Detection: combining process + network data for ICS (V. Berge, 2024)** — https://arxiv.org/pdf/2410.19717.pdf (arXiv / PDF)*

***A Digital Twin Framework for Cyber Security in CPS (related / arXiv)** — https://arxiv.org/abs/2204.13859 (arXiv / PDF)*

Comparative Analysis of Dimensionality Reduction Techniques for Cybersecurity in the SWaT Dataset *— https://www.researchgate.net/publication/370672001_Comparative_Analysis_of_Dimensionality_Reduction_Techniques_for_Cybersecurity_in_the_SWaT_Dataset (ResearchGate)*

Digital Twin-based Anomaly Detection in Cyber-physical Systems (ATTAIN family / Xu et al.) *— https://www.semanticscholar.org/paper/Digital-Twin-based-Anomaly-Detection-in-Systems-Xu-Ali/fa8626cea805bf6f97fdfdf87f419fccf5442fb6 (SemanticsScholar / pointer + links)*

Digital Twin-driven Intrusion Detection for Industrial SCADA — PubMed Central copy *— https://pmc.ncbi.nlm.nih.gov/articles/PMC12390215/ (PMC copy of the MDPI Sensors paper)*

Digital Twin-based Anomaly Detection with Curriculum Learning — code & paper resources *— https://github.com/ (see the LATTICE/ATTAIN project pages linked from the arXiv entry) — (closest resource / code pointer): https://arxiv.org/abs/2309.15995*

A Digital Twin-Based Approach for Detecting Cyber-Physical Attacks in ICS (Applied Sciences / ResearchGate copy) *— https://www.researchgate.net/publication/384390208_A_Digital_Twin-Based_Approach_for_Detecting_Cyber-Physical_Attacks_in_ICS_Using_Knowledge_Discovery (ResearchGate)*