

Revue de l'utilisation des Jumeaux Numériques pour la Cybersécurité

Hugo Bourreau

IMT Atlantique, IRISA, Cyber CNI

hugo.bourreau@cybercni.fr

Fabien Dagnat

IMT Atlantique, LabSticc

fabien.dagnat@imt-atlantique.fr

Fehmi Jaafar

UQAC

fjaafar@uqac.ca

Marc-Oliver Pahl

IMT Atlantique, IRISA, Cyber CNI

pahl@cybercni.fr

Abstract—Ce papier étudie l'état de l'art de l'utilisation des jumeaux numériques (JN) dans la cybersécurité des systèmes cyber-physiques (CPS). Les JN permettent une surveillance en temps réel, des analyses prédictives et une prise de décision adaptative. L'étude met en avant les avantages principaux de l'utilisation des JN et identifie les défis principaux, tels que le manque d'évaluation de l'impact des JN et la nécessité de standardiser leur fonctionnement. Le tout, en mettant en avant les avancées basées sur l'intelligence artificielle (IA). Elle souligne également les problématiques ouvertes et les perspectives pour une intégration réussie des JN dans des environnements critiques.

Index Terms—cybersecurity, jumeaux numériques, CPS, IoT, intelligence artificielle

I. INTRODUCTION

Les jumeaux numériques (JN) se répandent de plus en plus dans l'industrie pour les avantages qu'ils apportent, notamment dans la partie contrôle des systèmes cyber-physiques (CPS). Ils permettent un contrôle en temps réel des systèmes tout en incluant une approche dynamique et donc bien plus flexible que les outils de modélisation traditionnels. Ces deux caractéristiques sont liées, permettant à l'outil de s'adapter en temps réel à ce qu'il peut se passer et tout imprévu sur le système réel sera représenté sur son JN. Leurs avantages peuvent aller plus loin que cela et leur potentiel en cybersécurité reste sous-exploré.

En effet, ils offrent des possibilités de prédictions et permettent de guider les agents dans leurs décisions futures ou d'adapter le système automatiquement, en fonction de ce qui se passe en temps réel dans le système. Les JN offrent un cadre permettant d'explorer des scénarios parallèles à la réalité, ce qui pourrait contribuer à mieux anticiper l'impact potentiel d'attaques ou de défaillances et, par conséquent, améliorer la résilience des CPS. Ils peuvent également être utilisés pour la détection proactive des anomalies, la simulation d'attaques sophistiquées, et la mise au point de stratégies de réponse optimales, en intégrant des algorithmes d'intelligence artificielle (IA). En outre, les JN permettent de centraliser et de structurer des données complexes provenant de multiples sources, favorisant ainsi une vision holistique et cohérente des systèmes à protéger.

Ce travail est cofinancé par la chaire industrielle Cybersecurity for Critical Networked Infrastructures (cyberCNI.fr) avec le soutien du fonds de développement FEDER de la région Bretagne, France.

Cette étude offre un panorama de l'état de l'art sur l'intégration des JN et de l'intelligence artificielle (IA) pour améliorer la cybersécurité des CPS, tout en explorant les perspectives et défis associés à leur adoption dans des environnements industriels.

La suite de l'article est structurée de la manière suivante. La section II introduit les travaux existants au sein de la littérature sur les JN appliqués à la cybersécurité. Section III détaille l'architecture des JN en mettant en avant les avantages et les défis apportés. Section IV présente les questions de recherche ouvertes. Enfin, la section V synthétise le travail réalisé.

II. TRAVAUX CONNEXES

Dans cette section, nous discutons des avancées dans le domaine des jumeaux numériques, avec un intérêt particulier sur leur utilisation en cybersécurité. On s'intéresse à leur principales applications, les défis identifiés dans la littérature, et les efforts en cours pour standardiser leur conception.

Les JN constituent un domaine de recherche en forte croissance, avec un intérêt marqué et un nombre important de publications ces dernières années, illustré en figure 1. De nombreuses études de prédiction de l'avenir de la part du marché des JN ont été réalisées par des entreprises comme IBM ou Bpifrance. Bien que la valeur monétaire estimée en milliards d'euro diffère, les études s'accordent en prédisant que leur ascension va continuer pendant les prochaines années.

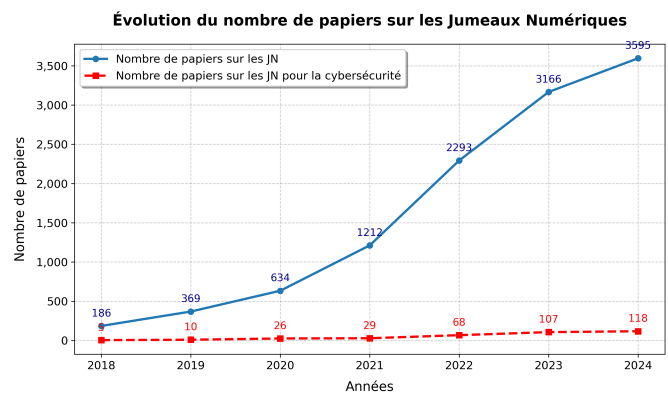


Fig. 1. Nombre de papiers sur IEEEXplore mentionnant les JN

La majorité des publications ne s'intéressent pas à la cybersécurité ainsi le nombre de papiers traitant de ce domaine

passé de 12005 articles à seulement 373, toutes années confondues.

Ces publications se concentrent sur des applications industrielles, telles que la maintenance prédictive, la conception de produits ou la gestion d'infrastructures complexes. L'approche dominante consiste à utiliser les JN pour simuler et optimiser des systèmes physiques. Cependant, on voit apparaître des travaux soulignant les intérêts de cette technologie pour la cybersécurité. Notamment Homaei et al. [1] souligne le rôle important des JN dans le cadre de la cybersécurité, notamment lorsqu'ils sont couplés à l'IA. Cette intégration peut améliorer la détection des anomalies, fournir des capacités de réaction adaptative aux cybermenaces et prédire les vulnérabilités potentielles des systèmes.

On retrouve aussi des cas d'usage avec la détection d'attaques de déni de service (DoS) sur des contrôleurs programmables [2]. Le JN est utilisé comme environnement d'analyse de sécurité et d'évaluation des méthodes d'atténuation des menaces. Ici l'auteur met en avant le JN pour faire de l'analyse de comportement et réussir à détecter s'il y a une attaque ou non.

Dans le secteur de la santé, les JN sont utilisés pour sécuriser les dispositifs médicaux connectés et les données des patients, en simulant des scénarios d'attaques potentielles sans compromettre les systèmes réels. Au sein de [3], Pirbhulal et al. décrivent la nécessité de protéger les infrastructures de santé possédant des objets connectés. Dans le modèle présenté ils ajoutent la couche de cybersécurité comme lien entre le monde physique et le JN. Ils en concluent que les JN permettent de lutter contre des brèches de sécurité en proposant une analyse active et améliorent la précision du système, s'adaptant aux menaces en temps réel.

Dans le domaine énergétique, les JN contribuent à la cybersécurité des réseaux intelligents en détectant les attaques ainsi que les manipulations de données. Qian et al. [4] proposent une nouvelle architecture intégrant une couche de données dédiée aux systèmes cyber-physiques, facilitant l'utilisation des JN pour la surveillance et la protection des infrastructures critiques. Leur modèle permet de structurer et d'analyser en temps réel les données issues des capteurs du réseau, améliorant ainsi la détection des anomalies et la réponse aux menaces. Ils démontrent que les JN peuvent non seulement anticiper les attaques en simulant divers scénarios tel que de l'injection de données modifiées, mais aussi optimiser la gestion des ressources énergétiques pour minimiser les impacts d'éventuelles intrusions. Leur approche met en évidence la capacité des JN à renforcer la sécurité des réseaux intelligents en fournissant une vision dynamique et actualisée de l'état du système, facilitant ainsi une réponse proactive aux cyber menaces.

On remarque tout de même un effort avec une volonté de standardiser les pratiques [5]. La fragmentation des protocoles limite leur scalabilité et leur sécurité, soulignant la nécessité de développer des cadres standardisés [1].

Nous avons répertorié dans la table I l'ensemble des papiers

sélectionnés dans cette étude afin de classifier les types de contributions qu'ils apportent aux JN en matière de cybersécurité. Ils sont ordonnés par date de publication et classifiés selon quatre niveaux :

- × Le sujet n'est pas abordé
- ◌ Le sujet est abordé, par exemple dans le contexte
- ◐ Le sujet est couvert partiellement
- ● Le sujet est entièrement couvert

TABLE I
SUJETS COUVERTS PAR LA LITTÉRATURE

Ref.	Année	Définition		Avenir des JN		Mesure de la performance
		Taxonomie	Domaine d'application	Challenges actuels	Tendances futures	
[6]	2019	●	◐	◌	×	×
[5]	2020	●	●	◐	◌	◌
[2]	2021	◐	●	◌	×	●
[7]	2021	●	×	◐	◌	×
[3]	2022	◐	●	●	◐	×
[8]	2022	●	◌	◐	◌	×
[9]	2022	◌	●	×	×	×
[10]	2023	◌	◐	◐	×	◌
[1]	2024	●	●	◐	◌	×
[4]	2024	◐	×	◐	◐	◌
[11]	2024	◐	×	◐	◐	◌
Observation		●	◐	◐	◐	◌
Notre article		●	●	●	●	×

Certains articles, comme [6], ne répondent que partiellement aux défis liés aux JN, car ils les étudient de manière générale, sans se focaliser sur leur application à la cybersécurité. Concernant la définition, la taxonomie est tout d'abord étudiée, c'est-à-dire la définition des concepts et des principales composantes des JN. Cette analyse est complétée par l'étude du domaine d'application, qui clarifie si la définition est appliquée à un cas d'usage particulier. Ensuite, les pistes futures des JN sont abordées, examinant d'abord les défis actuels, puis les tendances émergentes afin d'identifier les orientations des travaux à venir. Enfin, nous analysons les évaluations de performance des jumeaux numériques, bien que cette dimension reste peu explorée dans la littérature.

Nous observons que la définition des JN est largement étudiée et appliquée à divers domaines tels que les réseaux intelligents d'énergie (smart grids) [5], les infrastructures critiques [2] ou encore le secteur de la santé [3]. De plus, les défis actuels sont bien identifiés, et plusieurs études proposent des pistes pour l'évolution des JN. Cependant, les mesures de performance restent en marge des travaux existants, et l'impact concret des JN sur les systèmes demeure insuffisamment exploré. Certains articles soulignent la nécessité d'étudier cet impact, et [2] constitue l'une des rares études à s'y intéresser spécifiquement.

En bas du tableau vous trouverez une observation globale sur la couverture de la littérature sur les aspects étudiés. Notre étude vient compléter les aspects de définition de perspectives d'avenir des JN, cependant l'aspect de mesure de la performance n'est pas traité.

III. CONSTATS

Au sein de cette section, nous présentons les principales observations et conclusions issues de l'analyse des jumeaux numériques existants. En commençant par présenter les propriétés des JN, les avantages à leur utilisation et enfin les défis qu'ils suscitent.

A. Propriétés

Les propriétés des JN reposent sur une structure modulaire qui permet de représenter et d'interagir avec des systèmes physiques en temps réel. Une architecture typique est composée des éléments présentés en figure 2.

- **Architecture.** D'une part, il y a l'architecture du JN, avec les composants essentiels à sa conception. On retrouve une entité physique connectée à son jumeau virtuel avec un échange de données entre les deux parties. Le jumeau virtuel, le JN, est lui une modélisation dynamique de l'état du système mis à jour en temps réel grâce aux données [6].
- **Type.** Ensuite il faut s'intéresser au type de JN que l'on souhaite, le type étant grandement relié au cas d'usage étudié. Il ne faut pas oublier que la conception d'un JN est là pour répondre à un besoin, qu'il est nécessaire d'analyser pour voir ce qui doit être fait. Une fois le besoin identifié, il définit le périmètre qu'englobe le JN afin de sélectionner les aspects à modéliser [6].
- **Traitement des données.** Enfin, une architecture incluant l'acquisition, le traitement, la modélisation des données, la prédiction et la prise de décision est mise en place. Ce processus s'effectue en temps réel afin d'assurer une synchronisation constante entre le jumeau numérique et son entité physique. Il s'agit d'un cheminement nécessaire pour mettre en place et tirer profit du JN. La notion de temps réel peut différer en fonction du contexte, ils peuvent être inférieur à la seconde pour certains, et de l'ordre de la minute pour d'autres en fonction de l'échelle de temps utilisée. Les points de synchronisation peuvent aussi être bloquants, c'est-à-dire que les deux systèmes doivent nécessairement attendre d'avoir le même état, ou non [3].

B. Avantages

- **Réponse en temps réel et dynamique.** Contrairement à une approche traditionnelle, ici chaque modification de l'état du système est représentée. Une analyse fonctionnelle ou dysfonctionnelle préalable permet même d'aller plus loin et d'anticiper les états suivants du système. Toute l'évolution étant suivie en direct, diminuant drastiquement le temps de réponse à incident [6].

- **Intégration de l'IA.** L'intelligence artificielle est utilisée pour apprendre des schémas d'attaque et pouvoir détecter des anomalies. Ce qui permettrait de détecter une attaque en cours ou d'identifier des vulnérabilités. Un usage plus poussé ouvrirait le champ des possibles sur la prédiction des effets en cascade. Ces pistes, encore peu explorées, offrent un potentiel considérable pour renforcer la résilience du système face à des menaces émergentes et adapter les réponses en fonction de l'évolution des attaques. L'intégration des JN dans ce cadre permettrait de simuler ces scénarios d'attaques en environnement contrôlé, d'affiner les algorithmes de détection et d'améliorer la précision des modèles prédictifs [1].
- **Prédiction d'incidents.** Ici on s'intéresse autant à un problème de sûreté que de sécurité. On assure le bon fonctionnement du système aussi bien sur l'aspect technique que pour la sécurité des opérateurs humains. Cette phase incluse dans la partie de prédiction du JN, permet de renforcer ses capacités et d'étendre son utilisation. Il est nécessaire de le prendre en compte lors de la mise en place du JN pour voir la portée de ce qui veut être réalisé [11].
- **Substitution du système.** Le JN peut aussi se substituer à l'entité physique dans certains cas d'usage afin de travailler avec le JN. Cela permet, par exemple, de tester des paramètres comme une configuration différente, comme des règles différentes sur un pare-feu, ce qui serait trop dangereux ou coûteux à tester sur le système réel. On peut aussi substituer le système à des fins de formation, permettant de travailler sur un aspect du système pour un opérateur. C'est ce que l'on peut retrouver couplé à de la réalité augmentée dans [9].

C. Défis

- **Manque d'outils et plateformes standardisés.** La mise en place de JN nécessite des outils, aussi bien pour la partie technique que pour toutes les étapes préalables. À l'heure actuelle il n'existe pas de plateforme facilitant la mise en place de JN, ce qui constitue un frein à leur développement [8]. Les JN sont tout de même utilisés lors de projets européen tel qu'au sein du projet Praetorian ou du projet ELEGANT, sans la mise à disposition de tous d'une plateforme commune à l'issue des projets. On voit cependant apparaître des outils de modélisation pouvant servir de base pour la conception de JN tel que PyCATSHOO qui est un logiciel propriétaire mais gratuit à l'utilisation.
- **Les JN peuvent être la cible d'attaque.** Ajouter un JN dans son infrastructure présente de nombreux avantages mais peut être tout aussi difficile. Étant donné qu'il s'agit d'une réplique d'un aspect de notre système. Si un attaquant parvient à y avoir accès, il a accès à une partie de notre infrastructure ainsi qu'aux données qui peuvent y transiter [7].

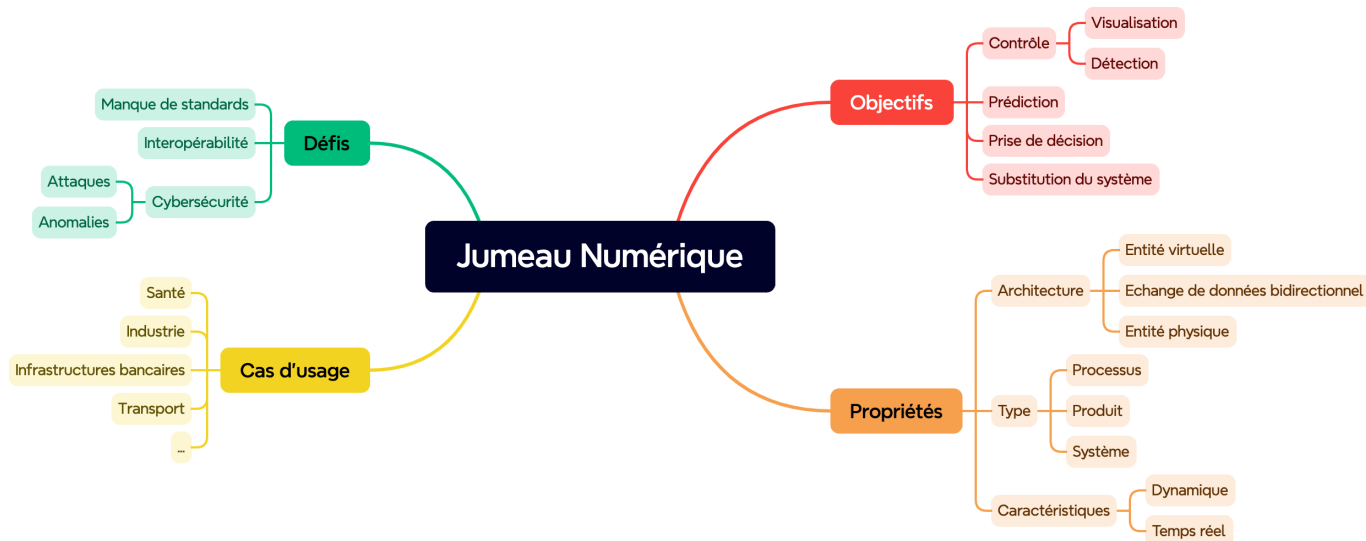


Fig. 2. Composantes d'un jumeau numérique

- **Confidentialité.** L'essence même des jumeaux numériques est d'utiliser les données du système réel. Ces données étant sensibles au sein des infrastructures critiques, il est nécessaire de prendre des précautions pour que celles-ci ne puissent pas fuir [10]. Ces précautions peuvent concerner la classification des données selon leur sensibilité, ce qui est mis en avant par la norme ISO 27001:2022 ou encore la mise en place de plusieurs niveau de sécurité. Les niveaux de sécurité doivent respecter les mêmes critères pour le système réel que pour le JN.

IV. QUESTIONS OUVERTES

Cette section présente les questions de recherche qui restent ouvertes quant aux jumeaux numériques pour la cybersécurité.

Le manque de standards et d'outils se fait ressentir. Des initiatives ont déjà été prises pour essayer de pallier ces manques mais les efforts sont encore loin d'être aboutis. Notamment avec l'apparition de normes ISO telles que la norme ISO/IEC 30173:2023 définissant les concepts et la terminologie des JN ou encore la norme ISO 23247-1:2021 présentant un cadre (framework) pour la fabrication industrielle. Ces efforts ne doivent pas se limiter à un champ d'application ou à un usage spécifique. Le besoin de méthodes concerne la mise en place des JN indifféremment de leur usage, sur l'ensemble de leur cycle de vie.

L'adoption de standard permet d'avoir un point de vu plus uniforme du JN, et si l'ensemble des parties prenantes, ou du moins une majorité venait à se mettre d'accord, alors il serait plus simple de sortir des outils permettant de répondre au besoin du plus grand nombre. Ces outils faciliteront les implémentations de par une plateforme commune et permettront d'obtenir des résultats concrets sur leur utilisation en entreprise et sur la recherche des différences structurelles entre les JN industriels et ceux consacrés à la cybersécurité. L'avenir

des JN passe également par leur capacité à se conformer aux contraintes de sécurité et de confidentialité, en protégeant les données critiques tout en restant efficaces.

Les défis rencontrés ouvrent un nouveau champ de recherche sur l'utilisation de l'IA dans le domaine et notamment avec des modèles prédictifs. Ces efforts contribueront à faire des jumeaux numériques un outil de choix à même d'assurer la résilience des systèmes.

V. CONCLUSION

Les jumeaux numériques représentent une avancée pour la cybersécurité des CPS, offrant des opportunités pour l'analyse prédictive et la réaction aux cyberattaques, notamment celles en cascade. Ce qui permettrait d'anticiper davantage les actions des attaquants et d'être mieux préparé. Cependant, des efforts de collaboration entre chercheurs et industries sont nécessaires pour surmonter les défis techniques. Cette étude fournit une base pour orienter les recherches vers des solutions durables et standardisées.

Parmi les directions prometteuses, il apparaît essentiel d'explorer les distinctions entre les JN à vocation industrielle et ceux conçus pour des applications en cybersécurité. Etudier la différence de paradigme dans leur conception et ce, dès l'étude définissant les besoins avant même de penser à leur réalisation. Ce qui permettrait de mettre en avant les différences de conception et les besoins des JN à usage pour la cybersécurité. Ces axes de recherche contribueront à consolider la place des jumeaux numériques comme pilier central de la cybersécurité des CPS.

REFERENCES

- [1] M. Homaei, O. M. Gutierrez, J. C. S. Nunez, M. A. Vegas, and A. C. Lindo, "A Review of Digital Twins and their Application in Cybersecurity based on Artificial Intelligence," *Artificial Intelligence Review*, vol. 57, no. 8, p. 201, Jul. 2024, arXiv:2311.01154 [cs]. [Online]. Available: <http://arxiv.org/abs/2311.01154>

- [2] B. Sousa, M. Arieiro, V. Pereira, J. Correia, N. Lourenço, and T. Cruz, "ELEGANT: Security of Critical Infrastructures With Digital Twins," *IEEE Access*, vol. 9, pp. 107 574–107 588, 2021, conference Name: IEEE Access. [Online]. Available: <https://ieeexplore.ieee.org/document/9499077>
- [3] S. Pirbhulal, H. Abie, and A. Shukla, "Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications," in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, Jun. 2022, pp. 1–5, iSSN: 2577-2465. [Online]. Available: <https://ieeexplore.ieee.org/document/9860581>
- [4] C. Qian, Y. Guo, A. Hussaini, A. Musa, A. Sai, and W. Yu, "A New Layer Structure of Cyber-Physical Systems under the Era of Digital Twin," *ACM Trans. Internet Technol.*, Jun. 2024, just Accepted. [Online]. Available: <https://dl.acm.org/doi/10.1145/3674974>
- [5] M. Atalay and P. Angin, "A Digital Twins Approach to Smart Grid Security Testing and Standardization," in *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*, Jun. 2020, pp. 435–440. [Online]. Available: <https://ieeexplore.ieee.org/document/9138264>
- [6] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital Twin in Industry: State-of-the-Art," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 4, pp. 2405–2415, Apr. 2019, conference Name: IEEE Transactions on Industrial Informatics. [Online]. Available: <https://ieeexplore.ieee.org/document/8477101>
- [7] E. Karaarslan and M. Babiker, "Digital Twin Security Threats and Countermeasures: An Introduction," in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, Dec. 2021, pp. 7–11. [Online]. Available: <https://ieeexplore.ieee.org/document/9654360>
- [8] S. Mihai, M. Yaqoob, D. V. Hung, W. Davis, P. Towakel, M. Raza, M. Karamanoglu, B. Barn, D. Shetve, R. V. Prasad, H. Venkataraman, R. Trestian, and H. X. Nguyen, "Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2255–2291, 2022, conference Name: IEEE Communications Surveys & Tutorials. [Online]. Available: <https://ieeexplore.ieee.org/document/9899718/?arnumber=9899718>
- [9] H. Orsolits, S. F. Rauh, and J. G. Estrada, "Using mixed reality based digital twins for robotics education," in *2022 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, Oct. 2022, pp. 56–59, iSSN: 2771-1110. [Online]. Available: <https://ieeexplore.ieee.org/document/9974561/?arnumber=9974561>
- [10] E. Shaikh, N. Mohammad, A. Al-Ali, and S. Muhammad, "A Probabilistic Model Checking (PMC) Approach to Solve Security Issues in Digital Twin (DT)," in *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Jan. 2023, pp. 192–197. [Online]. Available: <https://ieeexplore.ieee.org/document/10053389>
- [11] J. Luzzi, R. Naha, A. Arulappan, and A. Mahanti, "SoK: A Holistic View of Cyberattacks Prediction with Digital Twins," in *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*. Vellore, India: IEEE, Feb. 2024, pp. 1–7. [Online]. Available: <https://ieeexplore.ieee.org/document/10493514/>