Beyond Posters: A User-Centric Digital Twin Framework for Cybersecurity Awareness

Fhatuwani Makharamedzha, Errol Baloyi, Rendani Mmbodi and Ndabezinhle Hlongwane
Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa

FMakharamedzha@csir.co.za
EBaloyi2@csir.co.za
RMmbodi@csir.co.za
NHlongwane@csir.co.za

Abstract: Traditional cybersecurity awareness (CSA) methods, such as posters, flyers, and static training modules often fail to engage users or drive lasting behavioural change. To address these limitations, this paper proposes a novel, user-centric approach to CSA using Digital Twin (DT) technology integrated with machine learning (ML). The proposed framework introduces the concept of a User-Centric Digital Twin (UCDT)-CSA, a dynamic digital replica of each user modelled on their cybersecurity knowledge, behaviours, and risk profile. While UCDTs have been applied in domains such as construction, aquaculture, and healthcare, this work pioneers their use in the cybersecurity context. The system begins with a pre-assessment to capture individual user responses, which are used to configure a personalized training path. Through ongoing interaction with adaptive simulations and scenario-based learning, the UCDT-CSA evolves in real time, enabling training that continuously adjusts to user performance and behaviour. ML models analyse these interactions to refine each twin's profile, delivering increasingly targeted content and interventions aimed at improving secure behaviours. This approach transforms CSA from a static, compliance-focused exercise into an engaging, data-driven, and behaviourally adaptive learning experience. The paper outlines the architecture of the UCDT-CSA framework, discusses key implementation considerations, and sets the stage for future empirical validation and deployment in government, Small and Medium-Sized Enterprises (SMEs) and academic environment.

Keywords: Digital twin, Machine learning, Cybersecurity awareness

1. Introduction

In today's technologically interconnected world, cybersecurity awareness (CSA) has become a critical component of online security. This change arises at a time when organizations are increasingly dependent on technology for communication, online transactions, and various operational activities. CSA is commonly defined as the knowledge, behaviours, and practices that enable individuals and organizations to identify threats and risks, and to adopt prudent measures within the digital environment (Maqousi, 2023). Nonetheless, CSA often fails to receive the level of attention it warrants, particularly among frequent Internet users who remain vulnerable to cyber threats and attacks due to insecure online practices. It is also important to emphasize that CSA is not solely the responsibility of Information Technology (IT) professionals, but a necessary competency for all organizational employees and individuals.

CSA involves everyone who uses technology, from employees managing sensitive data to individuals using their modern gadgets like smartphones in the cyber space (Maqousi, 2023). Thereby, making cybersecurity both a personal and collective responsibility. Human behaviour remains the biggest threat to cybersecurity. Past research shows that most frequent incidents have occurred because of human error and or negligence, which includes blindly clicking on malicious links, reusing past passwords, and a general lack of social engineering tactics (Tambe-Jagtap, 2023). In most cases, organizations do finance technical defences like encryption and detection systems which end up unsuccessful, as threat actors often exploit the human element, using tactics such as social-engineering and password theft.

Furthermore, modern threat actors are now conducting advanced modern attacks such as weaponizing artificial intelligence (AI), deepfakes and psychological manipulation to power up these scams, which further complicates the threat landscape (Mushtaq, 2019). The results of these attacks expand as far as financial losses and reputational damage. An attempt by some organization to curb the rise of cyber-threats through CSA training has been made, however, this includes CSA programmes delivered through traditional delivery methods such as posters, generic training modules, and compliance-driven campaigns which often fail to engage users effectively or adapt to their evolving risk profiles (Fujs, 2022).

These methods typically rely on one-size-fits-all content, ignoring the diversity in user behaviour, digital literacy, and security attitudes. To address this limitation, a need for personalization CSA is needed. As a such, the current study proposes a baseline user-centric digital twin (UCDT)-CSA framework. To provide a theoretical

foundation and the necessary background for the framework, existing literature on CSA and digital twin technology was reviewed. This involved searching search engines and academic databases such as ScienceDirect and Google Scholar for peer-reviewed publications and related reports.

2. Literature Review

To engineer significant personalization in CSA, innovative methods are needed. Digital Twin (DT) technology offers a novel approach. Digital Twins are dynamic virtual replicas of a physical system, objects that constantly grow in real time-based data from their original counterparts (Azambuja et al, 2024). They have recently been used in fields such as construction, healthcare, business and production (Alhamam, Rahman and Aljughaiman, 2025). As such, the current study intends to apply DTs in a human-centric manner, UCDT can serve as a living model of an individual's cybersecurity behaviors, risk profile and information. Below the current study investigates some of the CSA delivery methods.

2.1 Traditional Cybersecurity Awareness (CSA) Approaches

Traditional CSA often relies on mandatory annual training, posters, and emails. However, these kinds of methods are restricted and limited in impact and widely adopted in both educational and corporate environments (Alam, 2017). Whilst they may be easy to scale and cost-effective, prior studies have consistently demonstrated that their effectiveness in fostering sustainable security behaviour is limited. For instance, Parsons et al. (2017) realized that required training often results in short-term knowledge retention which also fails to create lasting behavioural change, an observation that was also noted by Alshaikh (2020).

2.2 Personalization and Adaptive Learning in CSA

The value of personalization is progressively recognized. For example, GPT-powered CSA has been shown to exceed static programs by dynamically adapting content to user profiles which also improve engagement (Al-Dhamari, 2024). Likewise, adaptive learning in cybersecurity training assists to deliver content suited to students' skill levels by avoiding unnecessary or overly complex material. Research shows that adaptive approaches improve engagement and completion rates, and students report better experiences (Seda, 2022).

2.3 Virtual Reality (VR) in Cybersecurity Awareness

Virtual Reality (VR) has lately been explored as one of the innovative medium for CSA together with training. Far from traditional or gamified approaches, VR gives out interactive environment that gives users a safely experience simulated cyber threats in real time (Sheridan et al, 2020). By creating realistic scenarios such as social engineering encounters, phishing attacks, or password exploitation, VR offers participants opportunity to learn through experiential engagement rather than passive instruction. This fascinating quality assist in overcoming the limitations of static awareness programs, which often fail to translate into real-world behaviour.

Research have also shown that VR-based cybersecurity training enhances both retention and engagement. For example, McGill and Klobas (2020) show that immersive training scenarios significantly enhance users' ability to detect phishing attempts com-pared to text-based learning. Comparably, Kritzinger and Solms (2021) argue that VR provides "situated learning," where students can develop skills within realistic contexts, leading to stronger transfer of knowledge into workplace practices. Further-more, VR can be customized to specific roles and environments, which allows personalized training experiences that account for individual differences in risk perception and cognitive style.

2.4 Digital Twin Technology in Cybersecurity and Beyond

DTs have obtained momentum across diverse domains such as healthcare, manufacturing, and human–machine collaboration, where they are used for predictive maintenance, patient monitoring, and real-time process optimization (Fuller et al, 2020; Tao et al, 2019; Minerva et al, 2020). Their core strength lies in creating dynamic virtual replicas of physical systems, enabling simulation, optimization, and monitoring without interfering with real-world operations.

Even though initially applied in industrial and engineering contexts, researchers have increasingly explored DTs within cybersecurity. For example, DTs have been employed for threat modelling, intrusion detection, and resilience testing in Industrial Control Systems (ICS) and IoT infrastructures (Cimino et al, 2019; Grieves and Vickers, 2017). They allow corporations to simulate red- and blue-team exercises, test incident response strategies, and rehearse chaos scenarios without disrupting production systems. Other works show how DTs

can aid in anomaly detection, forensic analysis, and security control validation by enabling replay and traceability of cyber events (Jones et al, 2020; Yaqoob et al, 2020).

Nonetheless with these promising applications, the user-centric potential of DTs for CSA and education remains underexplored. While DTs have been leveraged to protect infrastructure and validate technical defences, few if any frameworks explicitly focus on enhancing end-user awareness, decision-making, and behavioural adaptation in the face of cyber threats. To the best of the authors' knowledge, no prior work has proposed a digital twin–driven model specifically designed for cybersecurity training and awareness, highlighting a critical gap that this study aims to address.

2.5 Gaps and Opportunities

While DTs are deep-rooted for systems and network modelling, their use in human-centric CSA, mainly at the isolated level, remains evolving. Existing DT studies focuses on infrastructure, enterprise networks, or cyber-physical systems, not only on modelling user behaviour, knowledge, or learning trajectories (Ghosh, 2024). There's an important opportunity to fill this opportunity by developing UCDTs which is a virtual representation of user cognition, habits, and progression. Similar with UCDTs could enable personal scenario simulation, adaptive feedback, and training personalization driven by ML. This approach shifts CSA from one-size-fits-all modules to one of dynamic, behavioural, and user-specific learning paths bridging current CSA limitations, adaptive learning, and DT capabilities.

3. Conceptual Framework Design: UCDT-CSA

This section outlines the UCDT-CSA framework, as noted, to the best of the author's knowledge, this is the first framework to apply a UCDT approach specifically to CSA. The proposed UCDT-CSA framework is designed to model and influence individual user behaviour through a modular, ML-enhanced CSA system. This section describes the high-level architecture, data flow, and core functional components of the framework. Figure 1 provides an illustration of the UCDT-CSA framework.

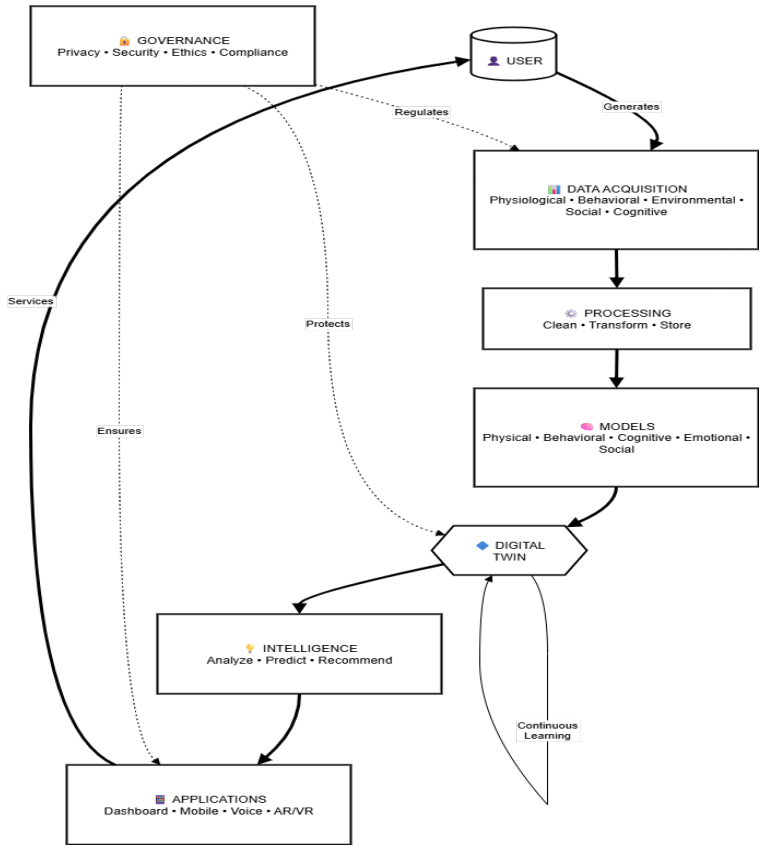

Figure 1: UCDT-CSA Framework Design

As illustrated in Figure 1, the UCDT-CSA framework is designed around a modular, engine-based architecture comprising three layers: data acquisition, processing, and models. Each layer is responsible for specific tasks, enabling independent development, seamless integration, and future scalability. The data acquisition layer

captures initial and ongoing user data to build detailed user profiles. The processing layer cleans, transforms, and stores these profiles, while the model layer applies AI/ML techniques to personalize cybersecurity training and maintain the DT engine through continuous learning. Finally, the framework includes an application layer that delivers adaptive cybersecurity awareness content.

4. Implementation Considerations

The successful deployment of UCDT-CSA framework requires careful attention to multiple implementation dimensions that extend beyond technical architecture. This section examines four critical considerations that organizations must be addressed to ensure effective, ethical, and sustainable UCDT-CSA framework implementation.

5. Privacy and Ethical Concerns

The implementation of user-centric digital twins raises fundamental privacy and ethical challenges that must be addressed proactively. Data sovereignty represents a primary concern, as users must maintain control over their personal information while enabling the system to function effectively (Minerva et al., 2020). The principle of informed consent becomes complex when dealing with continuous data collection and evolving model capabilities, requiring dynamic consent mechanisms that adapt to changing data uses (Tao et al, 2019). Algorithmic transparency poses another critical challenge. Users have the right to understand how their digital twin makes predictions and recommendations, necessitating explainable AI approaches that balance model complexity with interpretability (Fuller et al, 2020). The implementation must address data minimization principles, collecting only necessary information while maintaining model effectiveness (El Saddik, 2018).

Organizations must implement differential privacy techniques to protect individual privacy while enabling population-level insights (Qi et al, 2021). This includes implementing privacy-preserving federated learning approaches that allow model training without centralizing sensitive data (Zhang et al, 2022). The framework must also address algorithmic bias through continuous monitoring and correction mechanisms, ensuring equitable outcomes across diverse user populations (Barricelli et al, 2019). Ethical AI governance structures must be embedded within the implementation, including ethics review boards, regular audits, and clear accountability frameworks (van der Valk et al, 2021). The system should implement right to explanation capabilities, allowing users to understand and challenge automated decisions that significantly affect them (Liu et al, 2021).

5.1 System Integration

Successful digital twin implementation requires seamless integration with existing organizational infrastructure and third-party systems. Legacy system compatibility presents a significant challenge, as organizations must bridge modern digital twin architectures with established enterprise systems (Kritzinger et al., 2018). This requires developing robust middleware solutions and API standardization to ensure interoperability across heterogeneous technology stacks (Tao et al, 2018). Data integration complexities arise from the need to harmonize information from multiple sources with varying formats, quality levels, and update frequencies (Zheng et al, 2021). Organizations must implement master data management strategies and data governance frameworks to ensure consistency and reliability across integrated systems (Semeraro et al, 2021).

The implementation must address real-time synchronization requirements, ensuring that the digital twin maintains temporal coherence with physical world changes (Jones et al, 2020). This necessitates event-driven architectures and stream processing capabilities that can handle high-velocity data flows while maintaining system stability (Rasheed et al, 2020). Semantic interoperability represents another critical challenge, requiring the development of common ontologies and data models that enable meaningful information exchange between systems (Jacoby and Usländer, 2020). Organizations must implement service-oriented architectures that support loose coupling and enable gradual migration from legacy systems (Singh et al, 2021).

Security integration across systems requires implementing consistent authentication and authorization mechanisms while maintaining zero-trust principles (Alcaraz and Lopez, 2022). This includes establishing secure API gateways, identity federation, and encrypted communication channels across all integrated components (Dietz and Pernul, 2020).

5.2 Scalability

Digital twin implementations must be designed to scale efficiently as user bases grow, and data volumes expand exponentially. Horizontal scalability requires architectures that can distribute processing across multiple nodes without degrading performance (VanDerHorn and Mahadevan, 2021). This necessitates implementing microservices architectures with container orchestration platforms that enable dynamic resource allocation (Minerva et al, 2020). Data scalability challenges emerge as systems must process and store massive volumes of heterogeneous data while maintaining query performance (Lehner and Sattler, 2020). Organizations must implement distributed storage solutions, data partitioning strategies, and intelligent caching mechanisms to manage growing data repositories effectively (Qi and Tao, 2018).

Model scalability becomes critical as the number of concurrent digital twins increases, requiring efficient model serving infrastructure that can handle thousands of simultaneous predictions (Lim et al, 2021). This includes implementing model compression techniques, edge computing strategies, and federated learning approaches that distribute computational load (Park et al, 2022). Network scalability must accommodate increasing data transmission requirements while maintaining low latency for real-time applications (Lu et al, 2020). Organizations should implement content delivery networks, edge caching, and 5G integration to ensure responsive system performance at scale (Minerva et al, 2021).

Cost scalability represents a crucial consideration, as infrastructure costs can grow non-linearly with system expansion (Cimino et al, 2019). Implementation strategies must include cloud-native architectures, serverless computing, and auto-scaling policies that optimize resource utilization while controlling expenses (Alam and El Saddik, 2017).

5.3 Content Development

The creation and maintenance of digital twin content require sophisticated development frameworks and continuous refinement processes. Model development pipelines must support iterative refinement, version control, and A/B testing capabilities to ensure model quality and relevance (Zheng et al, 2022). This includes establishing MLOps practices that standardize model development, testing, and deployment workflows (Rathore et al, 2021).

Personalization algorithms must balance individual customization with computational efficiency, requiring adaptive learning mechanisms that evolve with user behaviour (Wang et al., 2022). Organizations must implement transfer learning and meta-learning approaches that enable rapid personalization for new users while maintaining model accuracy (Lv et al., 2022). Content validation processes must ensure that digital twin outputs remain accurate, relevant, and beneficial to users (Boje et al., 2020). This requires implementing continuous monitoring systems, feedback loops, and quality assurance frameworks that detect and correct model drift (Errandonea et al, 2020).

Knowledge representation challenges arise in encoding complex human behaviours and contexts within computational models (Leng et a., 2021). Organizations must develop multi-modal representation learning approaches that capture the richness of human experience while maintaining computational tractability (Kang et al, 2021). User experience design for digital twin interfaces requires careful attention to information presentation, interaction paradigms, and cognitive load management (Kaur et al., 2020). Implementation must include adaptive interfaces, progressive disclosure patterns, and context-aware visualizations that make complex information accessible to diverse user populations (Madni et al, 2019).

5.4 Implementation Framework Integration

These implementation considerations must be integrated holistically within the overall digital twin architecture. The following framework illustrates how these considerations interact with the technical layers:

Privacy-Preserving Architecture

- Implement homomorphic encryption for sensitive data processing.
- Deploy differential privacy mechanisms at data aggregation points.
- Establish consent management systems with granular control options.
- Enable data portability and deletion capabilities per GDPR requirements.

Integration Architecture

- Deploy enterprise service bus (ESB) for system communication.

- Implement API management platforms with versioning support.
- Establish data transformation services for format harmonization.
- Create adapter patterns for legacy system connectivity.

Scalable Infrastructure

- Utilize Kubernetes for container orchestration and auto-scaling.
- Implement Apache Kafka for distributed event streaming.
- Deploy distributed databases with sharding capabilities.
- Establish CDN and edge computing nodes for global reach.

Content Management System

- Create model registries for version control and governance.
- Implement feature stores for consistent feature engineering.
- Establish A/B testing frameworks for model evaluation.
- Deploy continuous integration/continuous deployment (CI/CD) pipelines.

6. Use Cases

The proposed UCDT-CSA framework offers versatile applications in CSA, addressing diverse needs across various organizational environments. The key potential use cases outlined below demonstrate its practical value. It should be noted that while this framework is primarily intended for adoption by organizations in South Africa, its applicability is not limited to this context and can be extended globally. However, the focus of these use cases remains on the South African environment.

6.1 Government Agencies

Government agencies are responsible for safeguarding sensitive information and delivering public services efficiently, involving employees at all levels from general staff to technical personnel, all of whom need to possess a basic understanding of CSA to ensure effective service delivery (Ngoma, Keevy and Rama, 2021). Government departments are frequent targets of cyberattacks. In South Africa, Siphambili et al (2024) noted that since 2019, the government sector has been predominantly targeted by ransomware attacks, with ten different departments affected and one department attacked twice. The study recommended implementing a comprehensive CSA programme as a first line of defence against such threats. This is where the UCDT-CSA framework becomes relevant, as it is well-suited for this environment and can tailor CSA content to meet the needs of different user groups.

6.2 Educational Institutions

Tertiary institutions and schools often deliver CSA to a diverse user base with varying technical backgrounds. The UCDT-CSA framework is well-suited for these environments, as it can differentiate content for students, faculty, and administrative staff. If adopted, it could also increase engagement through interactive content, which, according to Nkongolo (2024), is often preferred by this demographic. Furthermore, it can be used as a standardized framework across different Higher Education Institutions (HEIs), which could make a significant difference. Masenya's (2023) study, which investigated the CSA of students within South African HEIs, where this framework will also probable be implemented found that while students are aware of some cybersecurity terms, there is a lack of collaboration within these institutions on the best approach to CSA training.

6.3 Small and Medium-Sized Enterprises (SMEs)

A study by Eybers and Mvundla (2022) investigated CSA among managers in fifteen small and SMEs in South Africa. The findings revealed that most SME managers are aware of cybersecurity threats, as they are currently facing them within their organizations. However, the challenge lies with employees, many of whom lack such awareness. Furthermore, SMEs often lack the financial resources to provide comprehensive cybersecurity training programs, and many outsource their IT and security functions. In this context, the framework is particularly valuable, as it enables the customization of CSA content to address the specific needs of different roles within an organization, such as management, technical staff, and general employees. The framework can therefore offer a scalable and cost-effective solution for enhancing cybersecurity awareness across various organizational levels.

7. Conclusion and Future Work

This paper addresses the identified gap by proposing a baseline UCDT-CSA framework that builds a dynamic digital profile of the user through initial assessment and continuous behavioural input, integrates AI/ML components to personalize awareness delivery over time, offers a scalable and modular approach for use across organizational settings and positions the user as an active participant in the cybersecurity lifecycle, not just a passive recipient of awareness content. By bridging concepts from DT technology, adaptive learning, and cybersecurity behaviour modelling, this work introduces a novel paradigm for CSA, one that is personalized, data-driven, and continuous.

For future work, a working prototype of the UCDT framework incorporating the core engines, Pre-Assessment, Digital Twin Management, AI/ML Adaptation, and Awareness Delivery will be developed. This will enable practical experimentation and refinement of the system components. This framework will be deployed within diverse organizational settings to assess its effectiveness in improving cybersecurity knowledge and behaviour.

Ethics Declaration: Ethical clearance was not obtained, since the current study did not involve human participants.

AI Declaration: AI tools were not used in the current study.

References

Alam, M., and El Saddik, A. (2017) "A digital twin architecture reference model for the cloud-based cyber-physical systems" *IEEE Access*, Vol. 5, 2050-2062.

Al-Dhamari, R. (2024). AI-driven adaptive cybersecurity awareness using GPT models: A user-focused approach. Computers & Security, 141, 103365. https://doi.org/10.1016/j.cose.2024.103365

Alcaraz, C., and Lopez, J. (2022) "Digital twin: A comprehensive survey of security threats", *IEEE Communications Surveys & Tutorials*, Vol. 24, No. 3, pp 1475-1503.

Alhamam, N., Rahman, M. M. H. and Aljughaiman, A. (2025) "A comprehensive review on cybersecurity of digital twins: Issues, challenges, and future research directions", *IEEE Access*, Vol. 13, pp 45106–45124.

Azambuja, A. J. G. de, Giese, T., Schützer, K., Anderl, R., Schleich, B., and Almeida, V. R. (2024) "Digital twins in Industry 4.0 – Opportunities and challenges related to cyber security", *Procedia CIRP*, pp 25–30.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003

Barricelli, B. R., Casiraghi, E., and Fogli, D. (2019) "A survey on digital twin: Definitions, characteristics, applications, and design implications" *IEEE Access,* 7, 167653-167671.

Boje, C., Guerriero, A., Kubicki, S., and Rezgui, Y. (2020) "Towards a semantic Construction Digital Twin: Directions for future research" *Automation in Construction*.

Cimino, C., Negri, E. and Fumagalli, L. (2019) "Review of digital twin applications in manufacturing", *Computers in Industry*.

Dietz, M., and Pernul, G. (2020) "Digital twin: Empowering enterprises towards a system-of-systems approach" *Business & Information Systems Engineering*, Vol. 62, Vol. 2, pp 179-184.

El Saddik, A. (2018) "Digital twins: The convergence of multimedia technologies", *IEEE Multimedia*, Vol. 25, No. 2, pp 87-92.

Errandonea, I., Beltrán, S., & Arrizabalaga, S. (2020) "Digital twin for maintenance: Data-driven approach", *Procedia Manufacturing*, Vol. 42, pp 362–369.

Eybers, S. and Mvundla, Z. (2022) "Investigating Cyber Security Awareness (CSA) Amongst Managers in Small and Medium Enterprises (SMEs)" *Comprehensible Science. ICCS 2021. Lecture Notes in Networks and Systems*, Vol. 315.

Fujs, D., Vrhovec, S. and Vavpotič, D. (2022) "Towards personalized user training for secure use of information systems", *The International Arab Journal of Information Technology*, Vol. 19, No. 3.

Fuller, A., Fan, Z., Day, C., and Barlow, C. (2020) "Digital twin: Enabling technologies, challenges and open research" *IEEE Access*, Vol. 8, 108952-108971.

Jacoby, M. and Usländer, T. (2020) "Digital twin and internet of things—Current standards landscape", *Applied Sciences*, Vol. 10, No. 18, 6519.

Grieves, M., & Vickers, J. (2017). Digital twin: Mitigating unanticipated failures in complex systems. In Proceedings of the ASME 2017.

Ghosh, S. (2024). User-centric digital twins for adaptive cybersecurity awareness: A conceptual framework. IEEE Internet of Things Journal, 11(2), 1454–1466. https://doi.org/10.1109/JIOT.2023.3312345.

Jones, D., Snider, C., Nassehi, A., Yon, J. and Hicks, B. (2020) "Characterising the Digital Twin: A systematic literature review", *CIRP Journal of Manufacturing Science and Technology,* 29, pp 36-52.

Kang, J., Wang, D., and Chen, Y. (2021) "Multimodal digital twin: A conceptual framework for human-centric applications", *Journal of Manufacturing Systems*, 61, pp 424-435.

Kaur, S., Singh, A., & Kumar, P. (2020) "User-centric visualization for digital twins" *International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 5, pp 233–241.

Kritzinger, W., Karner, M., Traar, G., Henjes, J. and Sihn, W. (2018) "Digital Twin in manufacturing: A categorical literature review and classification", *IFAC-PapersOnLine,* Vol. 51, No. 11, 1016-1022.

Lehner, W. and Sattler, K. U. (2020) "Database support for data-driven digital twins", *Datenbank-Spektrum*, Vol. 20, No. 2, pp 119-126.

Leng, J., Wang, D., Shen, W., Li, X., Liu, Q. and Chen, X. (2021) "Digital twins-based smart manufacturing system design in Industry 4.0: A review" *Journal of Manufacturing Systems*, 60, 119-137.

Lim, K. Y. H., Zheng, P., and Chen, C. H. (2021) "A state-of-the-art survey of Digital Twin: Techniques, engineering product lifecycle management and business innovation perspectives" *Journal of Intelligent Manufacturing*, Vol .31, No. 6, 1313-1337.

Liu, M., Fang, S., Dong, H. and Xu, C. (2021) "Review of digital twin about concepts, technologies, and industrial applications", *Journal of Manufacturing Systems*, 58, 346-361.

Lu, Y., Liu, C., Kevin, I., Wang, K., Huang, H. and Xu, X. (2020) "Digital Twin-driven smart manufacturing: Connotation, reference model, applications and research issues", *Robotics and Computer-Integrated Manufacturing*, 61, 101837.

Lv, Z., Xie, S., Li, Y., Hossain, M. S. and El Saddik, A. (2022) "Building the metaverse by digital twins at all scales, state, relation" *Virtual Reality & Intelligent Hardware*, Vol. 4, No. 6, 459-470.

Madni, A. M., Madni, C. C., and Lucero, S. D. (2019) "Leveraging digital twin technology in model-based systems engineering" *Systems*, Vol. 7, No. 1, 7.

Maqousi, A. A. (2023) "A proposed framework for user cybersecurity awareness" *24th International Arab Conference on Information Technology (ACIT)*, 1–6.

Masenya, T. M. (2023) "Awareness and knowledge of cyber ethical behaviour by students in higher education institutions in south africa", *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems*, pp 33–48.

McGill, T. J., & Klobas, J. E. (2020). Immersive cybersecurity training using VR: Improving phishing detection skills. Behaviour & Information Technology, 39(12), 1343–1358. https://doi.org/10.1080/0144929X.2019.1699691.

Minerva, R., Crespi, N., Awan, F. M. and Rotondi, D. (2021). Digital Twins: Properties, Software Frameworks, and Application Scenarios. *IT Professional*, Vol. 23, No. 1, pp 51-56.

Minerva, R., Lee, G. M., and Crespi, N. (2020) "Digital twin in the IoT context: A survey on technical features, scenarios, and architectural model" *Proceedings of the IEEE*, Vol. 108, No. 10, pp 1785-1824.

Mushtaq, S. (2019) "Modern cyber-attacks and cloud security: Strengthening information security in emerging technologies".

Ngoma, M. L., Keevy, M., and Rama, P. (2021) "Cyber-security awareness of South African state-mandated public sector organisations" *Southern African Journal of Accountability and Auditing Research*, Vol. 23, No. 1, pp 53–64.

Nkongolo, M. (2024). CyberMoraba: A game-based approach enhancing cybersecurity awareness. International Conference on Cyber Warfare and Security, 19(1), 240–250. https://doi.org/10.34190/iccws.19.1.1957

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee cybersecurity behavior: The role of awareness training. Computers & Security, 68, 24–34. https://doi.org/10.1016/j.cose.2017.04.005

Park, K. T., Nam, Y. W., Lee, H. S., Im, S. J., Noh, S. D., Son, J. Y. and Kim, H. (2022) "Design and implementation of a digital twin application for a connected micro smart factory*", International Journal of Computer Integrated Manufacturing*, Vol. 32, No. 6, pp 596-614.

Qi, Q. and Tao, F. (2018) "Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison", *IEEE Access*, 6, 3585-3593.

Qi, Q., Tao, F., Hu, T., Li, F. and Cheng, J. (2021) "Enabling technologies and tools for digital twin" *Journal of Manufacturing Systems*, 58, pp 3–21.

Rasheed, A., San, O. and Kvamsdal, T. (2020) "Digital twin: Values, challenges and enablers from a modeling perspective" *IEEE Access*, 8, 21980-22012.

Rathore, M. M., Shah, S. A., Shukla, D., Bentafat, E. and Bakiras, S. (2021) "The role of AI, machine learning, and big data in digital twinning: A systematic literature review, challenges, and opportunities" *IEEE Access*, 9, 32030-32052.

Seda, P. (2022). Adaptive learning for cybersecurity awareness in higher education. Education and Information Technologies, 27(8), 10721–10739. https://doi.org/10.1007/s10639-022-11035-2

Semeraro, C., Lezoche, M., Panetto, H. and Dassisti, M. (2021) "Digital twin paradigm: A systematic literature review", *Computers in Industry,* 130, 103469.

Singh, M., Fuenmayor, E., Hinchy, E. P., Qiao, Y., Murray, N. and Devine, D. (2021) "Digital twin: Origin to future" *Applied System Innovation*, Vol. 4, No. 2, 36.

Siphambili, N., Mahlasela, O., Baloyi, E., & Mukondeleli, E. (2024) "A Review of the South African Public Sector's Capability in Combating Ransomware", *4th International Multidisciplinary Information Technology and Engineering Conference (IMITEC),* pp 493-499.

Sheridan, T. B., Williams, C., & Farooq, S. (2020). Immersive VR for cyber threat education. Computers & Security, 94, 101860. https://doi.org/10.1016/j.cose.2020.101860.

Tambe-Jagtap, S. N. (2023) "Human-centric cybersecurity: Understanding and mitigating the role of human error in cyber incidents" *SHIFRA*, 53–59.

Tao, F., Cheng, J., Qi, Q., Zhang, M., Zhang, H., and Sui, F. (2018) "Digital twin-driven product design, manufacturing and service with big data" *The International Journal of Advanced Manufacturing Technology*, 94(9), 3563-3576.

Tao, F., Zhang, H., Liu, A. and Nee, A. Y. (2019) "Digital twin in industry: State-of-the-art" *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 4, 2405-2415.

van der Valk, H., Haße, H. and Breitner, M. H. (2021) "Ethical governance for AI-driven digital twins", *AI and Ethics*, 1, pp 303–315.

VanDerHorn, E., & Mahadevan, S. (2021) "Digital Twin: Generalization, characterization and implementation" *Decision Support Systems*, 145, 113524.

Wang, B., Zhou, H., Li, X., Yang, G., Zheng, P., Song, C., ... and Wang, L. (2022) "Human Digital Twin in the context of Industry 5.0" *Robotics and Computer-Integrated Manufacturing,* 85, 102626.

Zhang, H., Liu, Y. and Zhou, D. (2022) "Privacy-preserving federated learning for digital twins*", IEEE Internet of Things Journal*, Vol. 9, No. 10.

Zheng, P., Lin, T. J., Chen, C. H., & Xu, X. (2021). A systematic design approach for service innovation of digital twin-based services. European Journal of Operational Research, 295(2), 646-661.

Zheng, Y., Yang, S., and Cheng, H. (2022) "An application framework of digital twin and its case study", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 10, No. 3, 1141-1153.