# A Cognitive Digital Twin Architecture for Cybersecurity in IoT-based Smart Homes

Sandeep Pirbhulal[1, *], Habtamu Abie[1], Ankur Shukla[2] and Basel Katt[3]
[1]Norwegian Computing Center, PO Box 114, Blindern, 0314 Oslo, Norway
[2] Department of Risk and Security,
Institute for Energy Technology, 1777 Halden, Norway
[3] Department of Information Security and Communication Technology,
Norwegian University of Science and Technology, 2815 Gjøvik, Norway
*Corresponding Author: Sandeep Pirbhulal (sandeeep@nr.no)

**Abstract.** Cognitive Digital Twin (CDT) is an extension of Digital Twin with cognitive capabilities to monitor and analyse complex and unforeseen behaviours and to ensure critical reasoning and decision-making. Thus, CDT has a potential for enhancing cybersecurity for the Internet of Things (IoT)-based applications such as smart homes. In this paper, we developed a conceptual CDT architecture for improving cybersecurity in smart homes with dynamic threat detection and mitigation capabilities. The proposed approach applies closed feedback loops between cognitive process and cybersecurity using artificial intelligence and machine learning techniques. This will allow continuous monitoring of security-related information and analytics with complex behaviours within a virtual environment. The developed approach allows security testing and simulation in the virtual world for prediction and anticipation of dynamic security threats. It also facilitates dynamic updates to the physical world of attack prevention strategies for the dynamic optimization of smart homes security. Finally, this paper discusses the applicability of the developed CDT architecture in other IoT-based critical sectors.

**Keywords:** Cybersecurity, Cognitive Digital Twins, IoT, Smart Homes

## 1 Introduction

The Internet of Things (IoT) has been widely used in various sectors, including telemedicine, smart homes, smart cities, etc. [1]. IoT-based smart homes and healthcare [2] facilitate a unique way to support people with special needs, suffering chronically ill, elderly, disabled, and even everyone in pandemic situations such as Covid-19 [3]. Millions of embedded devices use new software stacks that significantly increase the threat level of these IoT devices and the likelihood of turning previously-unexploitable vulnerabilities into actively exploitable vulnerabilities. These challenges were also seen during Covid-19, thus raising the necessity for innovative security solutions in IoT-based applications [4, 5].

In recent times, the digital twin (DT) and cognitive digital twin (CDT) concepts have been increasingly used in different critical sectors. DT and CDT are used to develop a

virtual systems to collect real-time data from IoT devices to allow insights into performance and cyber threats [6-10]. CDT is the advancement of DT that will assist in achieving the goal of industry 4.0 [11]. CDT includes cognitive features that brings the critical aspects of cognition such as attention, perception, learning, memory, decision making, etc. [8, 11]. There exist several studies in the areas of cognitive twins such as enhancing cognition [12], adapted model of CDT [13], providing different levels of self-awareness [14], personalized system for smart cities [15], automatizing cognitive science for cybersecurity [16], cognitive cybersecurity analysis [17], etc. Al Faruque et al. [11] developed a CDT framework that focuses on the impact of twin technology on the performance of the product life cycle. Zheng et al. [6] developed a reference architecture for CDT for different applications. However, the above studies did not highlight how CDT can be useful for monitoring and preventing cyber threats. Nguyen, et al. [18] presented an approach which emphasizes the applicability of CDT for cybersecurity using ontology concepts. The main limitation of their approach is that it does not highlight how dynamic updates of the cognitive cycle will be analysed and used for offering adaptive measures to secure systems.

The key limitations of existing CDT approaches can be summarized as follows:

- There is not any systematic CDT framework to enhance cybersecurity which can be used for IoT-based smart home applications.
- There is a lack of automated cyber threats mitigation approach using CDT by analysing complex behaviours, system architectures, and interdependencies of their components and processes.
- Existing CDT approaches for cybersecurity do not apply a feedback loop between cognitive process and cybersecurity, and do not periodically share dynamic updates about security information in a virtual environment, which plays a crucial role in predicting cyber threats.

The main contribution of this study is a provision of dynamic and systematic solution for automated cybersecurity using CDT in IoT-based smart homes. The secondary objectives are:

- To develop a CDT-based conceptual architecture that can monitor, analyse and predict cyber threats.
- To apply a dynamic closed-loop solution within a virtual environment using complex behaviours to address varying dynamic cyber security threats in changing environments.
- To present a systematic way of preventing cyber threats within IoT-based smart homes (physically) by allowing simulation and experimentation in CDT (virtually) using the developed architecture.

This paper is organized as follows: Comparisons between DT and CDT are discussed in Section 2. Section 3 describes on the proposed architecture for enhancing cybersecurity in smart homes using CDT. CDT applications, conclusions and future directions are discussed in Section 4.

## 2 Digital Twin vs Cognitive Digital Twin

A DT is a virtual representation of a physical world (system or infrastructure) that captures the system's real-time information, features, and behaviours via physical-virtual world synchronization [10]. The main objective of DT is to empower simulations and testing in the virtual environment to monitor and control the physical system. The advancements in data analytics, i.e., artificial intelligence (AI) and machine learning (ML) offer more capabilities to DT. CDT is self-learning and proactive by incorporating DT and cognitive process (analysing, learning, critical reasoning, planning and decision making) for better understanding and experimenting prediction of unforeseen events of the physical system. An illustration of the comparisons between DT and CDT for smart homes is shown in Fig.1.

There is a need to comprehend the fact that the CDT technology is not developed to substitute DT. However, CDT is an evolved version of the existing DT technology. DT and CDT technologies have their respective benefits and applicabilities. Before implementing any of them for physical systems, their requirements, specifications, and scenarios must be considered. The empowering technologies of DT are more established, and several case studies are also available, which may serve as references. Nevertheless, CDT requires complex hierarchies to understand relationships between entities and components through lifecycle stages to detect complex behaviours and unforeseen situations [6]. There is not any generic framework or architecture of CDT for enhancing cybersecurity in smart applications. Hence, efforts in that direction are required.

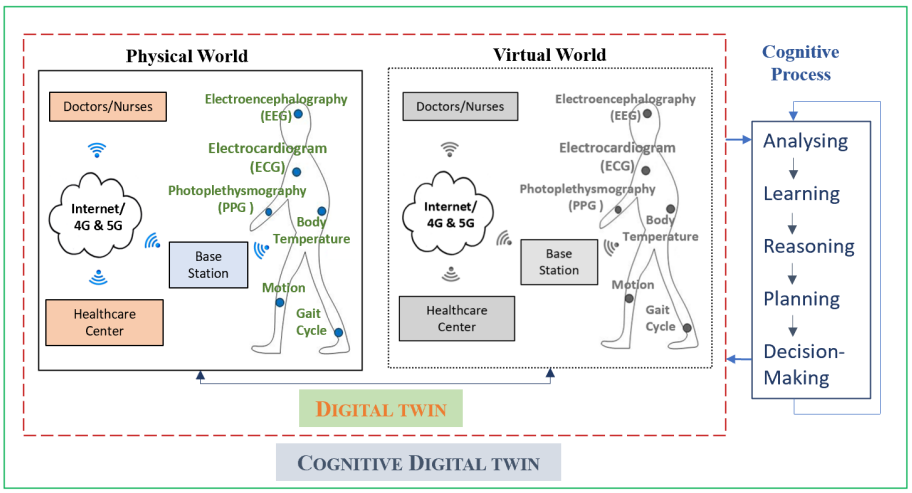


**Fig. 1.** An illustration of comparisons between Digital Twin and Cognitive Digital Twin of Smart Homes

## 3 Proposed Cognitive Digital Twin Architecture for Cybersecurity

This study presents a CDT architecture for cybersecurity. It continuously collects security-related information such as vulnerabilities, security threats from the IoT devices of smart homes in the physical world and integrates dynamic updates from the virtual world. It allows analytics, prediction and anticipation of cyber threats by performing simulation and experimentation virtually, and responses of prevention measures autonomously to the physical world. Fig. 2 depicts our proposed conceptual CDT architecture for enhancing cybersecurity in IoT-based smart homes. The proposed approach uses a closed feedback loop of AI/ML techniques for analysing complex behaviours and adapting to security variations in the cognitive process of smart homes.

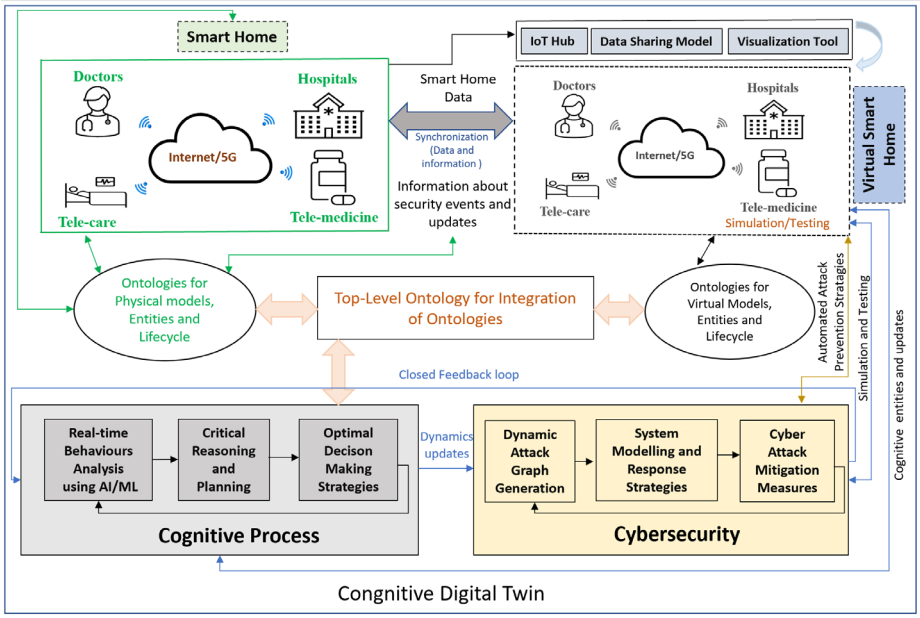


**Fig. 2.** The proposed conceptual cognitive digital twin architecture for enhancing cybersecurity in IoT-based smart homes

There are three stages in the developed architecture, (i) physical world, (ii)virtual world, and (iii) cognitive process and cybersecurity as described below:

**Stage I-Physical World:** This stage develops and monitors the IoT-based smart homes having the capability to offer guidance or prescribe medicine to patients remotely by collecting and analysing health data. The health data from medical IoT devices is stored in the cloud, which can be accessed by the concerned authorities (doctors, nurses and hospitals) remotely using wireless communication (5G or Wi-Fi). Hackers can eavesdrop and modify the communication between source and destination devices which can lead to illegal collection and misuse of secret medical information. Hence, security is one of the major concerns in IoT-based smart homes.

**Stage II-Virtual World:** At this stage, a virtual replica of smart home (physical world) with cognitive properties is developed and visualized to deal with cybersecurity threats efficiently. As depicted in Fig. 2, CDT integrates multiple models to attain more analytical abilities and incorporates expert knowledge to find the optimal solution for avoiding security threats. In our previous research work [19], we developed a framework for reinforcing the cybersecurity in IoT-based healthcare using DT technology. In [20], we discussed the significance of cognitive cybersecurity for anticipating and responding to new and emerging cybersecurity and privacy threats for IoT based critical infrastructures. From this experience, we realized that the cognitive capabilities could learn the behaviour of digital and physical entities to provide better decision-making tool for real operational systems.

Therefore, we focused on CDT for enhancing cybersecurity due to the advantages acquired from integrating human behaviours with the DT models for critical reasoning, planning and decision-making strategies. Our CDT approach will connect the real-time smart home to IoT Hub and cloud to use data models for IoT devices and digital twins using visualization tools, i.e., 2D or 3D to visualize and understand CDT data. Once the virtual setup is visualized and connected with the physical setup, it is essential to check that both worlds have synchronization so that smart home data (i.e., bio-signals or physiological features) or information about vulnerabilities and cyber security events can be shared. In CDT, the integration of human behaviour with twin models can be ensured in numerous ways, such as semantic technologies (category tagging, ontologies, knowledge graphs, natural language processing, etc.), fuzzy logics, and lifecycle methodologies. Ontologies provide a clear understanding of entities, knowledge-sharing capabilities, and reusability. Thus, in this study, the ontology concepts are used for developing interrelationships between entities, models and lifecycle for monitoring heterogeneous smart home data and cyber security information.

**Stage III-Cognitive Process and Cybersecurity:** This stage discusses how a closed feedback loop between cognitive process and cybersecurity within a virtual environment brings an efficient way to monitor, control, analysis, predict and anticipate security threats in smart homes. Fig. 2 shows the outcomes of the top-level integrated ontologies (physical and virtual) are input to the cognitive process. Initially, the AI/ML models analyse the health data and security information to comprehend potential security threats. After that, careful planning and critical reasoning are done to understand the dynamic environments and the plan is carefully monitored and checked for sustainable accuracy. The specific decision is taken by observing security threats in varying conditions. The cognitive updates are sent to the virtual world and communicated with the physical world via synchronization. This helps monitoring dynamic security threats and understanding entities' relationships and updating ontologies. Secondly, the self-learning feature is achieved through the internal closed feedback loop of cognitive process. The outer closed feedback loop between cognitive process and cybersecurity module enables the dynamic detection of security threats by sharing varying updates between two modules. Thirdly, twin models are used to per-

form simulation and testing in the virtual world. The dynamic attack graphs, response strategies and attack mitigation measures are generated using internal closed feedback loop. Finally, the response strategies and attack mitigation measures are shared with the physical world so that actions against potential threats can be taken sharply.

## 4 Conclusions, Applicability and Future Directions

Robust and accessible home care is a critical service in today's society. To improve the efficiency of such services, the adoption of IoT to collect patients' data and analysis of collected data are becoming more prevalent amongst healthcare providers and citizens. Unfortunately, IoT devices can be seriously compromised that can breach the privacy of patients' medical data and violate the security of the infrastructures they connect to. To detect cyber-attacks in the IoT-based smart homes and to take quick prevention measures against them are difficult, because security testing and experimentation cannot be performed on functioning real-time medical devices and services since stopping them may affect tele-monitoring of patients. Therefore, our study provides CDT architecture for automated cybersecurity for IoT-based homecare which allows simulation and security testing using twin models and cognitive features via the closed feedback loops. This study can be extended and applied to different critical sectors of Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) [21] such as smart cities, smart healthcare, smart electricity systems, and industry 4.0. NORCICS is working towards pushing the boundaries of research-based innovation to enhance the capability of private and public sector stakeholders to respond to the current and future cybersecurity risks by developing, validating, and operationalizing innovative socio-technical solutions [21]. It is believed that the proposed architecture will offer new insights into the critical sectors because the virtual representations of real-world systems or products can be innovative backbone for analysing and predicting future events even before they happen. There is a lot of interest in conducting research on the cyber threat landscape of IoT [22] and structuring AI/ML-based security techniques [23] for intelligent applications. However, there is a lack of an efficient approach which not only offers automated detection of threats for IoT networks but also offers threat prevention strategies and measures. The real strength of the proposed CDT solution lies in its ability to learn, anticipate, detect, identify, and protect automatically against cyber threats over time.

The developed CDT architecture can be extended and incorporated with our existing platforms and methodologies to be applied to critical sectors in the NORCICS project: **Smart Healthcare:** In our previous research, we developed adaptive security for smart Internet of Things in eHealth (ASSET) platform [24] which can monitor the health data remotely collected from the Raspberry Pi and Shimmer motes. The health data from the medical IoT devices is stored in the cloud, which can be securely accessed by the concerned authorities remotely using wireless communication. In [20], we developed the DT of the ASSET platform [25] which includes the steps for creating virtual system, executing and examining the data sharing model, configuring the function app, analysing and implementing twin models, and performing real-time synchronisation between the physical and virtual systems. Our real-time DT platform can be extended to CDT for enhancing cybersecurity in smart healthcare.

**Smart Cities**: In [26], we developed resource-efficient approach for data transmission in IoT-enabled smart cities. The resource-efficiency was measured regarding power drain, standard deviation, battery lifetime, delay, and packet loss ratio. The resource-efficient solution can be integrated into CDT for providing balance energy-efficiency and security in smart cities.
**Industry 4.0 and Cyber Physical Electrical Systems (CPES):** In [20], we developed cognitive cybersecurity framework for ensuring security and privacy in CPS-IoT enabled critical systems based on cognitive cycle of observe and orient, learn, plan, decide and act. This framework can be one of the main pillars to our CDT approach to enhance security in critical sectors (industry 4.0 and CPES).

In the future, we plan to implement the developed CDT architecture on our existing e-healthcare platform [27] and developed prototype [25] to ensure performance analysis regarding automated cyber-attack monitoring and prevention. Moreover, to research how our proposed approach will prevent new cyber threats that may arise due to the advancement of technologies such as 5G and beyond, Information Technology (IT) and Operational Technology (OT) integration.

## Acknowledgment

This work has received funding from the Research Council of Norway through the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS), project no. 310105, and basic institute funding at Norwegian Computing Center (Norsk Regnesentral), RCN grant number 194067.

## References

1. Nimmy, K., Dilraj, M., Sankaran, S., & Achuthan, K. Leveraging power consumption for anomaly detection on IoT devices in smart homes. Journal of Ambient Intelligence and Humanized Computing, pp.1-12, 2022.
2. Pirbhulal, S., Pombo, N., Felizardo, V., Garcia, N., Sodhro, A. H., & Mukhopadhyay, S. C. (2019, December). Towards machine learning enabled security framework for IoT-based healthcare. In 2019 13th International Conference on Sensing Technology (ICST) (pp. 1-6). IEEE.
3. Li, W., Su, Z., & Zhang, K. Security Solutions for IoT-Enabled Applications Against the Disease Pandemic. IEEE Internet of Things Magazine, 4(4), pp.100-106, 2021.
4. Nina Pappot , Gry Assam Taarnhøj and Helle Pappot. Telemedicine and e-Health Solutions for COVID-19: Patients' Perspective, Journal of "Telemedicine and e-Health", Vol. 26, No. 7, 2020.
5. Judd E. Hollander, MD, and Brendan G. Carr, MD. Virtually Perfect? Telemedicine for Covid-19. Commentary in the "New England Journal of Medicine", 2020.
6. Zheng, Xiaochen, Jinzhi Lu, and Dimitris Kiritsis. "The emergence of cognitive digital twin: vision, challenges and opportunities." International Journal of Production Research (2021): 1-23.
7. Pokhrel, A., Katta, V., & Colomo-Palacios, R. (2020, June). Digital twin for cybersecurity incident prediction: A multivocal literature review. In Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops (pp. 671-678).
8. Nguyen, T. N. (2022). Toward Human Digital Twins for Cybersecurity Simulations on the Metaverse: Ontological and Network Science Approach. JMIRx Med, 3(2), e33502.

9. Zhang, J., & Tai, Y. (2022). Secure medical digital twin via human-centric interaction and cyber vulnerability resilience. Connection Science, 34(1), 895-910.
10. Unal, P., Albayrak, Ö., Jomâa, M., & Berre, A. J. (2022). Data-driven artificial intelligence and predictive analytics for the maintenance of industrial machinery with hybrid and cognitive digital twins. In Technologies and Applications for Big Data Value (pp. 299-319). Springer, Cham.
11. Al Faruque, M. A., Muthirayan, D., Yu, S. Y., & Khargonekar, P. P. (2021, February). Cognitive digital twin for manufacturing systems. In 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 440-445). IEEE.
12. P. Eirinakis et al., "Enhancing Cognition for Digital Twins," 2020 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), 2020, pp. 1-7, doi: 10.1109/ICE/ITMC49519.2020.9198492.
13. Yitmen, I., Alizadehsalehi, S., Akıner, İ., & Akıner, M. E. (2021). An Adapted Model of Cognitive Digital Twins for Building Lifecycle Management. Applied Sciences, 11(9), 4276.
14. N. Zhang, R. Bahsoon and G. Theodoropoulos. (2020). Towards Engineering Cognitive Digital Twins with Self-Awareness. In 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2020, pp. 3891-3891. doi: 10.1109/SMC42975.2020.928335
15. [Du 2020] Du, J., Zhu, Q., Shi, Y., Wang, Q., Lin, Y., & Zhao, D. (2020). Cognition digital twins for personalized information systems of smart cities: Proof of concept. Journal of Management in Engineering, 36(2), 04019052
16. [Andrade 2022] Andrade, Roberto O., et al. "An Exploratory Study of Cognitive Sciences Applied to Cybersecurity." Electronics 11.11 (2022): 1692.
17. [Jiang 2021] Yuning Jiang and Yacine Atif. 2021. A selective ensemble model for cognitive cybersecurity analysis. J. Netw. Comput. Appl. 193, C (Nov 2021). https://doi.org/10.1016/j.jnca.2021.103210
18. Nguyen, T. N. (2021). Cybonto: Towards Human Cognitive Digital Twins for Cybersecurity. arXiv preprint arXiv:2108.00551.
19. Pirbhulal, S., Abie, H., & Shukla, A. (2022, June). Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications. In 2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring) (pp. 1-5). IEEE.
20. Abie, Habtamu. "Cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems." In 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), pp. 1-6. IEEE, 2019.
21. https://www.ntnu.edu/norcics, access date:21-09-2022.
22. Mavroeidakos, T., & Chaldeakis, V. (2020, June). Threat landscape of next generation IoT-enabled smart grids. In IFIP International Conference on Artificial Intelligence Applications and Innovations (pp. 116-127). Springer, Cham.
23. Memos, V. A., Psannis, K., & Lv, Z. (2022). A Secure Network Model against Bot Attacks in Edge-enabled Industrial Internet of Things. IEEE Transactions on Industrial Informatics.
24. Berhanu, Y., Abie, H., and Hamdi, M. (2013). A testbed for adaptive security for iot in ehealth. In Proceedings of the International Workshop on Adaptive Security, pages 1–8
25. V Orlauskis, S Pirbhulal, Real-time Implementation of Digital Twin for IoT based Smart Homes, NR-Notat, DART/14/22, 2022.
26. Sodhro, A. H., Pirbhulal, S., Luo, Z., & De Albuquerque, V. H. C. (2019). Towards an optimal resource management for IoT based Green and sustainable smart cities. Journal of Cleaner Production, 220, 1167-1179.
27. Abie, H., & Balasingham, I. (2012, February). Risk-based adaptive security for smart IoT in eHealth. In Proceedings of the 7th International Conference on Body Area Networks (pp. 269-275)