Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications

Sandeep Pirbhulal and Habtamu Abie
Norwegian Computing Center,
P.O. Box 114, Blindern, 0314 Oslo, Norway
Emails: sandeep@nr.no
abie@nr.no

Ankur Shukla
Department of Information Security and Communication Technology, Norwegian University of Science and Technology,
2815 Gjøvik, Norway
Email: ankur.shukla@ntnu.no

***Abstract*— In recent years, the cybersecurity attacks on the internet of things (IoT)-based healthcare systems became the major concern for researchers and health organizations. With time, the sophistication of these attacks is increasing. Therefore, healthcare service providers must implement efficient security mechanisms carefully while taking the advantages of connected devices without compromising the patient safety and disturbing the real-time health services. A digital twin (DT) is a virtual representation of a real-time counterpart of a physical world. DT offers significant advantages to cybersecurity experts, empowering them to predict risks without entering the physical world, and to simulate and test cyber-attacks that would otherwise be infeasible to do in real-time in the physical environment. DT in healthcare helps to identify security vulnerabilities, conduct attack simulations, and potential security breaches by creating a virtual replica of the targeted healthcare systems. In this paper, a novel and automated conceptual framework is developed for reinforcing the cybersecurity in IoT-based healthcare using DT technology. It includes the conceptualization and analysis of the proposed framework which can provide dynamic and adaptive security solution to identify real-time threats and vulnerabilities in IoT-based healthcare applications.**

Keywords—cybersecurity, digital twins, IoT, healthcare

I. Introduction

A. Overview

Security of the IoT-based healthcare systems is crucial because individual medical information needs to be safeguarded against potential threats and risks. Although IoT overcomes critical difficulties in telecare, it is vulnerable to all sorts of physical and wireless attacks [1].

In modern era, the Digital Twins (DTs) have been widely applied to provide the interaction between physical and virtual worlds. DT is a virtual representation of the physical world by mapping the physical components throughout the life cycle of the process utilizing both physical and virtual information, and interaction between both worlds. DT communicates with the physical world without altering anything in both worlds [2]. This brings several benefits to different applications, particularly in the IoT-basedhealthcare applications, which saves costs, predicts potentialthreats, and enhances decision-making processes [3][4]. COVID-19 has witnessed a need for DT in public and privatesectors since virtual interaction has been significant for smooth operations [5]. Various industries such as energy, healthcare, and transportation are applying DT technology to solve cybersecurity-related issues. Furthermore, the healthcare sector is also expected to demonstrate an essentialincrement in adopting DT technology post-COVID-19 [5]. A DT technology itself has a great potential to perform risk assessment to understand and mitigate security threats available in the IoT-based healthcare systems. DT provides the following features for reinforcing cybersecurity:

- Improves the understanding of cyber attacks
- Gives a continuous overview of vulnerabilities, threat landscape, attack space, and mitigates them before they happen
- Allows the design of new prevention, detection, and response methods without disturbing the physical world.

In view of the above advantages of DT technology, this study develops an innovative and automated conceptual framework for enhancing cybersecurity using DT for IoT-based healthcare applications. This research work provides a novel and efficient methodology which can have a potential to provide more reliable, secure and rapid healthcare. It also proposes automated solution which will have great impact to be used in different IoT-based applications.

B. Related work

Several authors have discussed the applicability of DT to be used for enhancing cybersecurity in different aspects such as cyberattack prediction [2], vulnerability detection & cyber resilience [4], data security and privacy [6], and cyber-range [7]. Fig.1 demonstrates the potential application areas for enhancing cybersecurity using DT technology in IoT-based healthcare applications. Mittal et al. [7] discussed the importance of DT in testing and evaluating IoT security and developed a DT-based engineering methodology. The authors conducted a case study considering the Nest thermostat (www.nest.com), a device used to access and control the house temperature, occupancy information, weather report, etc. The key benefit of DT is that the virtual world gets updated continuously based on the input data received from the physical world. This characteristic of DT plays an essential role in enhancing cybersecurity in different applications [2]. Azzaouiet et al. [8] presented a blockchain-based approach for improving data security. Authors developed a secure blockchain-based DT approach for asmart healthy city composed of layered model to maintain privacy, security, and trust.

In [9], the authors presented the state-of-the-art applicability of using Augmented Reality (AR) and DT for cybersecurity. The insights realized in their research are useful to design a conceptual approach by integrating AR and DT for improving cybersecurity. The physical and DT layers are extensively suitable for several use-cases of the AR-DT integration. Nevertheless, the application layer is highly dependent on which infrastructure it will be applied. Different cyber security measures can be enhanced, such as Intrusion Detection (IDS), cyber range, Security Information and Event Management (SIEM) systems, Intrusion Prevention Systems (IPS), etc. DT has potential to become an essential part of enhancing cyber security in IoT applications.

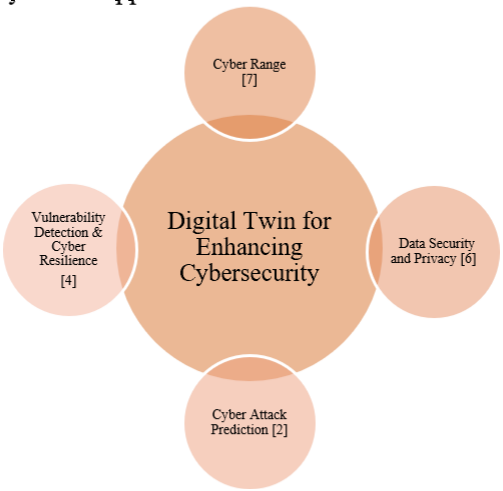
Cyber Range [7]
Vulnerability Detection & Cyber Resilience [4]
Digital Twin for Enhancing Cybersecurity
Data Security and Privacy [6]
Cyber Attack Prediction [2]

Figure1. Potential Application Areas for Enhancing Cybersecurity using Digital Twins in IoT-based Healthcare Applications

However, there is still a lack of DT technology-based real-time approach for enhancing cybersecurity in healthcare applications. IoT-based healthcare enables healthcare providers to do remote monitoring to improve patient outcomes and comfort, to enhance efficiency of healthcare services, to increase decision making capabilities, and to increase safety for patients, health professionals and staffs. [10][11]. On one hand IoT-based healthcare offers numerous benefits, but it also poses many security risks that needcareful attention. Therefore, this paper develops a novel and automated cybersecurity framework using DT which includes attack and response strategies for preventing cyberthreats for IoT-based healthcare systems.

C. Our contribution

This research work studies the impacts of DT technology for improving cybersecurity concerns of IoT-based healthcare applications. The foremost objective is to investigate the applicability of DT for cyber-attacks prevention, and to present strategic procedure for enhancing cybersecurity. Secondly, to develop a novel framework for reinforcing cybersecurity of healthcare systems. These objectives will be attained by introducing innovative healthcare security techniques, including system modelling, traffic and attack generation, impact assessment, attack and responsestrategies, and cyber-attacks prevention process to handle cyber threats and potential vulnerabilities.

D. Organization

This paper is organized as follows: Section 2 presents how DT technology can be applied to enhance cybersecurity for IoT-based applications. In Section 3, the strategic procedure for risk mitigation using DT in IoT-based healthcare systems is described. Section 4 elaborates the proposed framework. Finally, in Section 5, concluding remarks and future research directions are stated.

II. Applicability of Digital Twins for Reinforcing Cybersecurity

DT technology can be used to mitigate security attacks in IoT-based healthcare systems by using risks simulation and testing capabilities in virtual world or improved perceptibility of the system behaviours. DT plays a significant role in solving the following cybersecurity challenges [12].

- *Enhanced Security Patch Management*: One of the main limitations of the patching operation technology (OT) is recognizing the impact of using the security patch on the overall system. Testing a single device independently is either costly or time-consuming. This challenge can be addressed by applying DT technology to simulate the OT infrastructure to assist in security patch management.
- *Improved Security Testing Opportunities*: Cyber Digital Twins (CDTs) help in the smooth management and testing of security operations. Security threats are dynamic and fast evolving depending on several circumstances, including availability exploitation, vulnerability identification, and threat intelligence. DT and CDT enable service providers to offer comprehensive evaluations of potential vulnerabilities and attacks of the system, also study and assess possible attack vectors.
- *Improved Risk Management:* DT can be valuable in improving risk management since it presents an opportunity to test and simulate the impact of configuration changes on the security components of the healthcare systems to prevent potential risks. Moreover, through automated investigation of DT records, the points of failures are instantly recognized, thus facilitating a risk mitigation response on time.
- *Active Cyber Defence:* DT technology empowers incident responders with the knowledge to assess and evaluate any cyber threats in the system. Thus, DT helps in cyber defence by reducing the attack vectors and providing support for incident preparation.
- *Advanced Training for Cybersecurity Experts*: DT and cyber-range are beneficial to strengthen the skill development of cybersecurity experts to enable risk detection and prediction.
- *Anomaly Detection:* DT helps in detecting attacks by allowing modelling the system and performing simulation in a virtual environment. DT and digital shadows may also improve the runtime verification, a specification-based method connecting anomaly detection and dynamic testing.
- *Virtual Commissioning*: DTs are performance enablers because of fault forecasting and virtual commissioning capabilities. The data produced by the DT as the result of the commissioning procedure can be applied to develop training strategies for detecting anomalies and making cybersecurity defence profiles.
- *Ensuring Autonomy*: DT is also fundamental for developing autonomous systems that have potential to provide timely and effective response to system faults, anomalies, errors, and cybersecurity threats.

III. Strategic Process for Risk Mitigation using Digital Twins In Healthcare

DTs can play a significant role in enhancing cybersecurity, because they allow us to simulate risks in a virtual environment of IoT-based applications that exactly mirror their real systems [13]. There are three key elements for developing the strategic process for enhancing cybersecurity in DT technology for healthcare applications, as shown in Fig. 2.

- *Attack Graphs Generation:* At this stage, it will be demonstrated what could be the possible ways that attackers may use to enter the system. DT allows analysing asset-by-asset of healthcare systems by providing a continuous overview of vulnerabilities, threat landscape, and attack space. At every step, one can monitor the potential of attackers for entering the system and evaluate what kind of security threats they may bring.

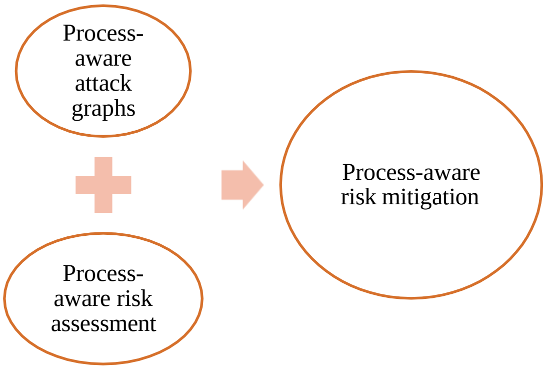
Process-aware attack graphs
Process-aware risk assessment
Process-aware risk mitigation

Figure 2. Strategic Process for Risk Mitigation using Digital Twins in IoT-based Healthcare Applications

- *Risk Assessment:* The learning from the first step will provide insights into the healthcare systems, and their potential vulnerabilities, risks and threats. Later, acquired knowledge and simulation from DT can be useful for risk assessment and management at each level at individual or operational stage.
- *Risk Mitigation:* After identifying risks and vulnerabilities at each process in IoT-based healthcare, testing can be performed on DT, and different strategies can be developed to prevent risks. Overall, DT can empower smart applications to minimize risks across each process. IoT-based healthcare systems are prone to several risks and cyberattacks, if not addressed, they may possibly have devastating consequences. Further, the effects of cyber-attacks on healthcare services are not only restricted to data confidentiality and integrity but may also endanger precious lives. Health service providers must identify which processes are more vulnerable. CDT can be helpful to fight against intruders and improve cybersecurity.

IV. Proposed Framework Using Digital Twins for Enhancing Cybersecurity

The proposed conceptual framework includes contextual computing and simulation technologies for healthcare to forecast and mitigate security threats in real-time. This framework can be helpful to update access control policies and enhance cybersecurity. Fig. 3 illustrates the proposed framework for improving cybersecurity services in IoT-based healthcare. Our framework provides an automated cybersecurity solution by incorporating the system model and resolving known vulnerabilities and threats. The proposed solution using DT will be useful to:

- Analysis vulnerabilities and threats in the healthcare system.
- Automate prediction and mitigation of potential security threats using testing and simulation.
- Develop attack and response strategies for enhancing cybersecurity in IoT-based healthcare systems

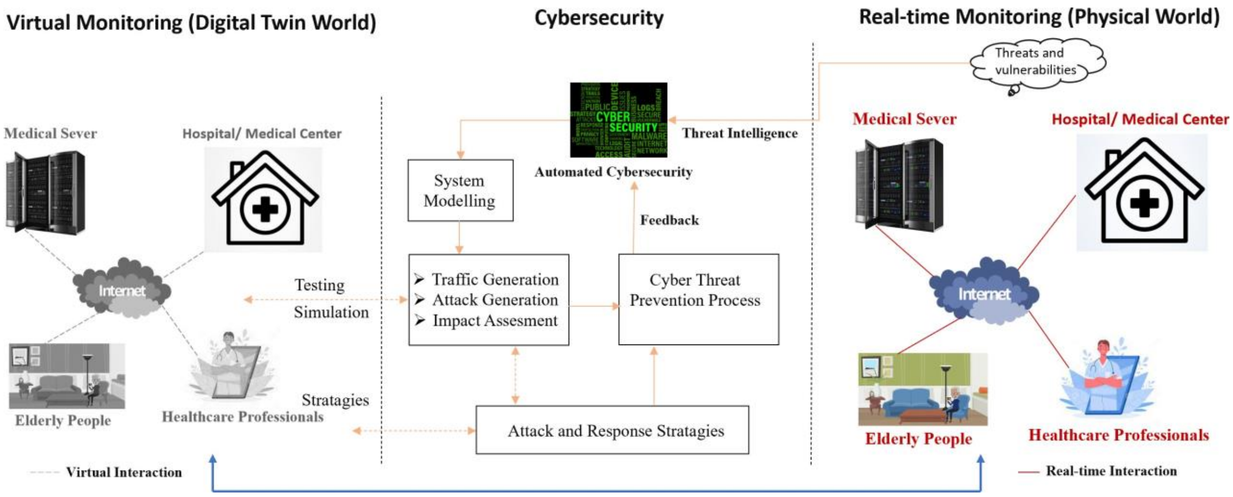

Figure 3. Proposed Conceptual Framework for Enhancing Cybersecurity in IoT-based Healthcare

The proposed framework is divided into three modules: physical world, digital twin world and cybersecurity. The ensuing sections briefly describe these:

A) Physical World

This module is the physical healthcare system which is equipped with IoT devices that process data from patients, elder persons, healthcare professionals, staff, and medical centres. A real-time security monitoring system is integrated with the physical healthcare to identify security threats and vulnerabilities. This provides real-time security inputs and visibility into how users and their devices interact within the healthcare systems. It also provides the initial inputs for the system modelling, threat intelligence to the automated cybersecurity system to respond proactively and quickly to potential threats and compromises.

B) *Digital Twin World*

This module is exactly the replica of the physical IoT-based healthcare system (physical world module) and leverages a model to simulate different processes of physical world dynamically adapt to environmental changes. To achieve this, it has a connection with the target physical system so that up to date communication with physical module can occur. In this framework, the Digital Twin World enables the Cybersecurity module to develop different cyber-attack prevention strategies to predict the potential attacks and vulnerabilities and optimizes the protection mechanisms.

C) *Cybersecurity*

This module communicates with Digital Twin World for developing strategies to prevent the cyber threats before they happen and update the physical world about potential threats. The proposed framework is automated and has the following processes:

- *System Modelling:* The system modelling deals with the layered architecture of the healthcare system and flow of information between layers. It also takes inputs from the real-time continuous monitoring module and outcomes of the automated cybersecurity system. The security of each layer is considered.
- *Testing/Simulation:* Based on the input data and system model, a threat scenario is designed and integrated with the DT world. The DT module runs simulations and performs tests on the simulated environment of the healthcare system. The testing includes traffic generation on the existing network that helps to identify the bugs and vulnerabilities such as drop loss of packets and connection drops. Network traffic determines the flow of data and how effectively the IoT-based healthcare systems interact, which is crucial for successful operation of healthcare systems. The next component of testing is attack generation. This is an automated process that considers the attack patterns and potential attacks and generates the test cases accordingly. The attack patterns are based on the potential threats and vulnerabilities from the real-time monitoring system of the physical world module. The potential vulnerabilities can be considered from the OWASP top vulnerabilities [14]. The next component of the testing is impact assessment that includes three stages: impact identification, impact evaluation and impact prediction. Impact identification provides list of potential attacks, guidelines, data collection processes and predictive techniques. Impact evaluation provides the magnitude and likelihood of an attack. This evaluation process may consider other factors such as cost associated with an attack and recovery time. Impact prediction uses the output of the impact evaluation and predicts the magnitude and likelihood of an attack. It can also be useful to predict the extent and duration of the impact. The DT module then analyses the current performance of the system and suggests improvements accordingly which can be applied to the physical world.
- *Cyber Threat Prevention Process:* This process implements the measures and technology to prevent the security threats of the IoT-based healthcare system based on attack and response strategies. The cyber threat prevention process is adaptive and considers the potential threats, attack strategies, environmental factors that change over time to dynamically adapt and update the defences mechanisms and measurements in real-time to make the healthcare system secure. Based on the inputs from the testing and simulation processes the cyber threat prevention process will be continuously up to date.

V. Conclusion and future Research Directions

This paper discussed how testing cybersecurity in smart IoT-based healthcare applications becomes difficult in many cases because it is not viable to stop the running ecosystem for testing security threats and risks. DT has a potential for solving this problem by providing an opportunity to work on networks virtually without directly interfering in the normal activities of the physical world. The paper presents a novel and automated conceptual framework using DT which aims to enhance cybersecurity for IoT-based healthcare systems. This paper aimed to demonstrate the impact of DT onimproving cybersecurity in healthcare systems. Our researchuses DT for enhancing cybersecurity because it providesanalysis, design, optimization of systems to improve accuracy,speed, and effectiveness. A DT may also be used to simulate a security breach and develop decision-making and mitigative responses to simulated cyberattacks. Thus, we believe that DT is a valuable tool in developing solutions to determine the extent of the threat and the appropriate response. It can provide a real-time responsive environment to simulate various types of control system compromises.

DT is an emerging technology requiring further study from the perspective of effective innovation regarding its ethical impacts. DTs incorporate numerous developing technologies, including big data, robotics, AI, IoT and Quantum. Therefore, in the future, we are planning to develop an ethical method for DT regarding the socio-ethical characteristics of various technologies and the digital artifacts they create in the virtual world. Finally, we are also planning to validate the effectiveness of the proposed framework through set of experiments and simulations.

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] Olivares-Rojas, J. C., Reyes-Archundia, E., Gutiérrez-Gnecchi, J. A., Molina-Moreno, I., Cerda-Jacobo, J., & Méndez-Patiño, A. (2021). Towards Cybersecurity of the Smart Grid using Digital Twins. *IEEE Internet Computing*.

[2] Azzaoui, A. E., Kim, T. W., Loia, V., & Park, J. H. (2021). Blockchain-Based Secure Digital Twin Framework for Smart Healthy City. In

Advanced Multimedia and Ubiquitous Engineering (pp. 107-113). Springer, Singapore.

[3] S.Pirbhulal, H.Abie (2021), Digital Twins for Enhancing Cybersecurity in Smart Homes, NR-Notat, pp.1-23.

[4] Zhang, J., Li, L., Lin, G., Fang, D., Tai, Y., & Huang, J. (2020). Cyber Resilience in Healthcare Digital Twin on Lung Cancer. IEEEAccess, 8, 201900-201913.

[5] https://medium.com/@pradasr/digital-twins-for-critical-businesses-and-cyber-preparedness-fe14cac1f644

[6] Mittal, S., Tolk, A., Pyles, A., Van Balen, N., & Bergollo, K. (2019, December). Digital twin modeling, co-simulation and cyber use-case inclusion methodology for IoT systems. In 2019 Winter Simulation Conference (WSC) (pp. 2653-2664). IEEE.

[7] Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Braghin, C., Damiani, E., Koshutanski, H., Tsakirakis, G., Hildebrandt, T. and Goeke, L., 2021, July. The THREAT-ARREST Cyber Range Platform. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 422-427). IEEE.

[8] Ahmadi-Assalemi, G., Al-Khateeb, H., Maple, C., Epiphaniou, G., Alhaboby, Z. A., Alkaabi, S., & Alhaboby, D. (2020). Digital twins for precision healthcare. Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity; Springer Nature Switzerland AG: Cham, Switzerland, 133-158.

[9] Mokliakova, K., & Srivastava, G. (2022). Privacy Issues in Smart IoT for Healthcare and Industry. In Intelligent Internet of Things for Healthcare and Industry (pp. 307-326). Springer, Cham.

[10] Koren, A., & Prasad, R. (2022). IoT Health Data in Electronic Health Records (EHR):

[11] Security and Privacy Issues in Era of 6G. Journal of ICT Standardization, 63-84.

[12] Böhm, F., Dietz, M., Preindl, T., & Pernul, G. (2021). Augmented Reality and the Digital Twin: State-of-the-Art and Perspectives for Cybersecurity. *Journal of Cybersecurity and Privacy*, *1*(3), 519-538.

[13] D. Holmes, M. Papathanasaki, L. Maglaras, M. A. Ferrag, S. Nepal and H. Janicke, "Digital Twins and Cyber Security – solution or challenge?," 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2021, pp. 1-8, doi: 10.1109/SEEDA-CECNSM53056.2021.9566277.

[14] https://www.accenture.com/us-en/blogs/technology-innovation/klein-engelberg-get-ahead-of-cyberattacks-with-digital-twins

[15] T. OWASP, 2004-2017, The Most Critical Web Application Security Risks (2018)