For a CPS-IoT Enabled Healthcare Ecosystem
Consider Cognitive Cybersecurity

Anggy Giri Prawiyogi¹, Lista Meria²

¹ University of Buana Perjuangan Karawang, Karawang, Indonesia
² University of Esa Unggul, Jakarta, Indonesia

e-mail: anggy.prawiyogi@ubpkarawang.ac.id, lista.meria@esaunggul.ac.id

ABSTRACT
Cyber-Physical Systems (CPS)-Internet of Things (IoT) enable healthcare services and infrastructure to enhance human lives, but they are vulnerable to various emerging cyber attacks. Cybersecurity specialists struggle to keep up with increasingly sophisticated attack methods. An urgent requirement exists for inventive cognitive cybersecurity in CPS-IoT enabled healthcare ecosystems. This paper presents a framework for cognitive cybersecurity to simulate human cognitive behavior in anticipating and responding to new and evolving cybersecurity and privacy threats to CPS-IoT and critical infrastructure systems. The framework encompasses the conceptualization and description of a layered architecture that integrates Artificial Intelligence, cognitive methods, and innovative security mechanisms.

This is an open access article under the CC BY 4.0 license.

1. INTRODUCTION
There has been a significant increase in the use of various Cyber-Physical Systems (CPS)-Internet of Things (IoT) applications in the eHealth and well-being sector [1]. In recent years, CPS-IoT has evolved to possess cognitive capabilities such as learning, reasoning, and autonomously understanding the physical and social environment. However, with increased complexity, cognitive CPS-IoT also brings new challenges in terms of cybersecurity. The growing interconnectivity in healthcare infrastructure has raised the risk of cybersecurity vulnerabilities concerning data and medical devices [2]. CPS-IoT within the healthcare ecosystem is susceptible to various emerging cyber attacks. Weak cybersecurity can result in user privacy breaches, physical damage, financial losses, and even threats to human lives [3].

However, the existing security solutions have not been able to cope with the complexity, dynamics, and high level of connectivity of CPS-IoT-enabled healthcare
services[4]. Therefore, an innovative approach is needed to establish cognitive cybersecurity within the CPS-IoT-supported healthcare ecosystem. This paper aims to present a methodology and theory of cognitive cybersecurity that enables modeling the behavior of attackers, identifying their intentions, and predicting potential attacks. This methodology relies on a cognitive framework capable of emulating human cognitive patterns to foresee and address emerging security and privacy risks [5]. By incorporating inventive elements such as security, privacy, and dynamic security knowledge metrics, our goal is to bolster measures for prevention, detection, response, and mitigation against threats in the CPS-IoT-enabled healthcare environment.

In this research, we will also explore conscious privacy collaboration, computational techniques, adaptive data collection, and the integration of cross-sectoral techniques such as AI predictive analysis and runtime verification [6]. It is expected that this approach will help enhance cybersecurity in CPS-IoT within the healthcare sector, reduce the risk of attacks, and protect the integrity, privacy, and security of sensitive medical data. With a focus on the urgent need for effective security solutions, this research will contribute to a better understanding of cognitive cybersecurity for CPS-IoT in the context of the healthcare ecosystem. Through collaborative efforts among cybersecurity experts, healthcare practitioners, and researchers, proactive measures are expected to be achieved in protecting critical infrastructure and ensuring the security and privacy of patients in this evolving era [7].

2. METHOD

This research employs a holistic and interdisciplinary approach to address the challenges of cognitive cybersecurity in CPS-IoT systems [8]. The methods used include the development of a cognitive security lifecycle model that resembles human cognitive mechanisms, handling complex temporal feedback loops, modeling complex interactions among entities in CPS-IoT, and solutions for heterogeneous configurations in inter-component communication. Additionally, innovative and intelligent security mechanisms are developed, including cognitive analysis, distributed decision-making, and understanding attacker intentions [9]. Runtime verification is also considered by monitoring and analyzing the system in real-time. Sustainability, privacy, and user awareness are also important focuses in this research [10]. Through this approach, it is expected to build a robust and reliable cognitive cybersecurity system for CPS-IoT [11].

3. RESULTS AND DISCUSSION

3.1. Challenges and Mechanisms

Cognitive cybersecurity faces several complex challenges in protecting dynamic and interconnected CPS-IoT systems [12]. One of the main challenges is designing a cognitive security lifecycle model that can incorporate human-like cognitive mechanisms such as control functions, learning, adaptability, perception, decision-making, and action. This model architecture must be capable of adapting to the diverse limitations and capabilities of CPS-IoT and be able to address dynamic changes in these limitations and capabilities [13]. In facing the complexity of CPS-IoT, there are challenges in modeling different temporal feedback loops [14]. Some activities require tight and fast feedback loops, while others occur over longer time scales. Therefore, cognitive control algorithms must be able to consider factors in slow feedback loops and handle dramatic tempo variations. Additionally, another challenge is capturing and modeling the complex interactions among entities in CPS-IoT that are difficult to analyze manually [15].

The heterogeneous configuration in inter-component communication is also a challenge that needs to be addressed. In this regard, solutions are needed to enhance network performance and overcome this heterogeneity. Another challenge is understanding the trade-offs and factors that affect the limitations of cognitive models and related security mechanisms. This is crucial to stay ahead of the attacker's cognitive decision cycle by considering uncertainty and preventing adaptive attacks.
In developing innovative security mechanisms, cognitive analysis, distributed decision-making, and understanding attacker intentions are required. These mechanisms should be able to integrate trust-based cognitive security to learn attacker behavior and predict their intentions. Another obstacle involves creating flexible metrics that align dynamic security risks with security goals and verifying the real-time efficacy of adaptable security measures. Additionally, it is important to pay attention to user privacy and personal interests. In this regard, appropriate privacy policies, strict access controls, and transparency in the use of user data need to be developed. This will help ensure that the cognitive cybersecurity system remains effective over time and can address new threats and vulnerabilities that may arise [16].

In achieving these goals, it is important to develop skills and awareness in dynamic forensic analysis. New methods and tools need to be developed to effectively and reliably collect and track evidence in the face of rapidly growing volumes of evidence. Additionally, runtime verification should be integrated to ensure the achievement of adaptive security and privacy [17]. By addressing these challenges, cognitive cybersecurity can provide intelligent and effective solutions in protecting CPS-IoT and its critical components [18]. Through the use of a combination of cognitive methods and artificial intelligence, along with control theory and game analysis, efficient and adaptive security mechanisms can be implemented [19].

3.2. Artificial Intelligence for Cognitive Cybersecurity

Cognitive systems are autonomous learning systems designed to emulate the functioning of the human brain. Cognitive cybersecurity aims to anticipate and respond to security threats in ways that emulate human thinking and behavior [20]. In this regard, artificial intelligence (AI) technology plays a crucial role by utilizing techniques such as machine learning, natural language processing, and sentiment analysis. Cognitive security systems can learn autonomously and automate security problem-solving. Moreover, cognitive security can also help prevent cyber attacks that manipulate human perception, such as cognitive hacking. The cognitive security approach involves both technical and non-technical solutions, including approaches that reduce individuals' vulnerability to manipulation, as well as technical solutions for detecting and preventing the spread of deceptive data and disinformation.

In the context of cognitive cybersecurity, AI technology plays a significant role. Certain pertinent AI methodologies encompass knowledge engineering, planning and scheduling, machine learning, distributed AI, and multi-agent systems. Knowledge engineering is used to capture complex knowledge in security problem-solving. Machine learning empowers cognitive systems to continually extract insights and gain knowledge through sophisticated analytics. Deep learning allows the identification of complex attack patterns. Planning and scheduling techniques are used to organize and coordinate security tasks. Distributed AI and multi-agent systems seek distributed solutions and address the characteristics of dynamic, decentralized, and diverse environments[21].

These AI techniques are also relevant in addressing the network communication characteristics in the context of CPS-IoT, such as being dynamic, partially observable, having ambiguous observations, resource constraints, diversity, large scale, and complex access policies. The use of AI and machine learning in cybersecurity solutions can expedite threat detection and enhance real-time incident response. These solutions are capable of managing large volumes of structured and unstructured data to identify relationships and trends that may be beyond human capacity.

3.2.1. Dynamic

AI methodologies for making plans in uncertain environments are designed to make decisions that remain effective even amidst evolving conditions within the domain.

3.2.2. Partially observable

AI methods demonstrate proficiency in deducing absent data and extrapolating scenarios, thereby enabling informed decisions to be reached based on present circumstances.
3.2.3. Ambiguous observations
AI methods exhibit competence in identifying ambiguity or low confidence and have the capability to gather additional information for clarification or to arrive at suitable decisions for both scenarios.

3.2.4. Resource constraints
AI methods prove their effectiveness in adapting solutions to the platforms they operate on, as well as in devising tasks that efficiently utilize the available resources.

3.2.5. Diversity
AI methodologies regard diversity as a strength, enabling resources to be managed in various adaptive approaches.

3.2.6. Large scale
Data mining and machine learning methods demonstrate their efficacy even with exceptionally large datasets. Moreover, planning and incremental learning techniques are also highly effective in such contexts.

3.2.7. Complex access policies
In knowledge engineering, policies can be represented as constraints. Through the utilization of constraint reasoning techniques, satisfactory solutions can swiftly be identified by seamlessly integrating newly acquired information. Overall, the use of AI technology in cognitive cybersecurity holds significant potential to enhance security and response to evolving threats. In complex environments such as CPS-IoT, these AI techniques can assist in analyzing security trends, processing large volumes of data, and rapidly identifying threats. However, it is important to note that human assessment and oversight remain necessary in validating and measuring the accuracy of AI solutions, as well as in making final decisions.

3.3. The Proposed Approach
The aim of the suggested method is to establish a unified cognitive framework capable of resiliently handling dynamic and adaptive threats within the CPS-IoT-enabled healthcare ecosystem. This framework aims to contribute to global cybersecurity challenges in the healthcare domain. To fulfill this aim, a multidisciplinary approach is necessary, integrating expertise from cognitive computing, optimization, formal methods, cybersecurity, trust, forensics, artificial intelligence, and mathematics. Figure 1 depicts the comprehensive architecture of cybersecurity for the CPS-IoT-enabled healthcare ecosystem. It outlines the building blocks structured within four layers: Healthcare Stakeholder Collaboration Layer, Perception and Knowledge Layer, Adaptive Data Collection and Actuation Layer, and Healthcare Stakeholder Infrastructure Layer. Subsequent sections provide concise explanations of the primary functions of the key building blocks within each layer.
3.3.1. Privacy-Aware collaboration

To effectively address threats and minimize risks within the intricate healthcare ecosystem, it is imperative to implement dynamic, evidence-based risk management. This necessitates an approach that is privacy-aware and emphasizes collaboration among stakeholders through secure information exchange, reporting, and visualization. Data exchange in healthcare is driven by interoperability, interaction, and collaboration, which also present new challenges in terms of security, privacy, technology, incentives, and governance[22].

One promising solution is the use of blockchain technology with a decentralized approach. This technology can facilitate collaboration through mechanisms such as digital access rules, data aggregation, data liquidity, patient identity, and data immutability. By leveraging blockchain, data can be shared in a decentralized manner, and privacy can be protected through clear access rules. This facilitates productive and streamlined cooperation in cybersecurity and privacy throughout the diverse layers of the intricate healthcare ecosystem, all with the aim of bolstering cognitive cybersecurity and privacy measures.

3.3.2. Cognitive security cycle model

The cognitive security cycle model for CPS-IoT is designed with the objective of completing the cognitive loop in both countering attacks and assimilating insights from the measures undertaken. This methodology encompasses the utilization of trade-offs, artificial intelligence (AI), controllers, and inventive mechanisms. Moreover, the model comprehends the dynamics of CPS-IoT, human behavior, and the broader social context. It then employs
this understanding to enact appropriate measures and glean valuable knowledge from the process.

This model consists of four steps in the cycle: Observe & Orient, Learn, Plan, and Decide & Act. In the Observe & Orient step, adaptive data collectors are used to monitor and understand stimuli such as configurations, user activities, vulnerabilities, threats, and interactions with the physical environment. In the Learn step, the model learns from perceptions, observations, decisions, and actions. In the Plan step, the model generates plans by identifying desired goals and considering timing. In the Decide & Act step, the model selects the appropriate security plan and implements it through physical actions or modifications to CPS-IoT devices[23].

The challenges in this model include capturing human cognitive mechanisms, quickly learning from attackers, and considering the complexity and dynamics of the CPS-IoT environment. Techniques such as AI, big data processing, and accurate decision-making are employed in this model. The cognitive model is also used to understand users in various contexts and maintain security and privacy in their interactions.

3.3.3. The importance of a dynamic security knowledge base

In the CPS-IoT environment, a dynamic security knowledge base plays a critical role in capturing information regarding the ever-evolving vulnerabilities and threats. Within the intricate healthcare ecosystem, ontologies prove to be invaluable tools for formally and expressively modeling and managing contexts[24]. By harnessing ontologies, one can employ reasoning techniques to effectively facilitate the dynamic modeling and management of contexts. Additionally, the integration of dynamic vulnerability scanning and penetration testing offers a means to consistently assess and monitor alterations in vulnerabilities, threats, security measures, privacy safeguards, and other pertinent attributes. This ongoing vigilance ensures the proper functioning of the cognitive intelligence within the complex healthcare ecosystem.

3.3.4. Cross-Sectoral techniques

Within the cognitive security cycle model, AI techniques play a pivotal role in predictive analysis and the incorporation of cognitive methodologies like contextual analysis, machine learning, and reasoning. These methods have proven highly effective in the early detection of cybersecurity incidents. The concept of runtime verification encompasses four distinct types of verification seamlessly integrated into the adaptive feedback control loop: Models@run-time, Requirements@run-time, Dynamic Context Monitoring, and Runtime Verifier. This integrated approach enables ongoing verification throughout system operation, ensuring steadfast adherence to cybersecurity requisites. Specifically, Dynamic Context Monitoring is employed to oversee the constantly evolving contexts, including threat scenarios and monitoring prerequisites. This capability facilitates agile adaptation to context shifts and facilitates runtime verification aligned with pertinent monitoring criteria.

Continuous evidence collection and tracing are conducted to analyze and identify the origins of crimes or incidents. This involves dynamic evidence gathering, tracing, and mapping, as well as the application of AI techniques and deep learning in forensic investigations. This approach aids in crime reconstruction, establishing evidence-based risk management approaches, and improving efficiency and reliability in capturing and tracing the dynamics of evidence. Therefore, the use of AI techniques, runtime verification, dynamic context monitoring, and continuous evidence collection and tracing are crucial in ensuring effective security and risk management in complex healthcare ecosystems.

3.3.5. Adaptive Data Collection and Actuation

The practice of adaptive data collection involves the gathering of security-related data, strategically optimized to enhance efficiency, precision, and minimize the impact of data collection. Its goal is to ensure precise data collection, reduce the amount of collected data, and automate the collection process by adapting to different contexts and situations. The data collection platform should be designed with high speed and scalability for
real-time and historical security analysis. In the realm of crucial healthcare infrastructure and services, gathering and analyzing security data necessitates intelligence, resilience, reliability, and timeliness. It must also adhere to communication standards and requirements to effectively identify potential attacks. For adaptive and efficient analysis strategies, one can employ predictive/regression algorithms like linear regression, Support Vector Regression (SVR), logistic regression, and KNN regression. Additionally, the utilization of deep learning mechanisms will play a pivotal role in discerning intricate attack patterns and potential risks.

3.3.6. Roadmap for Implementation

The outlined approach encompasses the incorporation of several components within the research project. Four distinct modules have been introduced: (i) the implementation of adaptive intelligent monitoring and the collection of security information, (ii) the application of AI-driven predictive analysis utilizing deep learning mechanisms on the gathered data, (iii) fostering stakeholder collaboration in activities such as vulnerability assessment, risk analysis, threat identification, threat mitigation, and compliance, and (iv) the development of a comprehensive security knowledge base. These modules are adaptable for utilization and further enhancement in the proposed approach, facilitating adaptive data collection and movement, multi-sector predictive analysis services, privacy-conscious collaboration, and the dynamic evolution of the security knowledge base[25].

Early studies have demonstrated the effectiveness of pioneering the creation and integration of advanced mechanisms for security, privacy, metrics, and runtime verification. This method can be readily embraced and further enriched through the development of additional innovative mechanisms. Techniques for situational awareness and fortification against evolving adversarial activities, with a specific emphasis on IoT forensics, are currently in progress. These can be adopted and refined to facilitate dynamic cross-sector forensic services. The ongoing development of adaptive data collection for real-time security analytics is set to be seamlessly incorporated into the adaptive data collection module within this approach. Finally, a framework for emulating human cognitive behavior is also slated for development.

4. CONCLUSION

This research introduces a cognitive cybersecurity architecture, aimed at emulating human cognitive responses to evolving cybersecurity and privacy threats within the CPS-IoT healthcare ecosystem. This architecture is crafted by seamlessly integrating artificial intelligence, cognitive techniques, forensics, and innovative security mechanisms, offering cross-sectoral services. Comprising four primary layers collaborative, perception and knowledge, data collection and movement, and infrastructure this architecture builds upon concepts derived from diverse research projects. The upcoming phases of this research involve delving into the intricate specifics of each architecture component, substantiating them through a series of simulations and practical system demonstrations in real-world usage scenarios. Additionally, our future research endeavors are set to incorporate human cognitive perspectives, encompassing both cognitive advantages and potential biases.

ACKNOWLEDGEMENTS

The authors would like to thank Department of Computer Science, Chung-ang University and Department of Computer Science, University of California, Berkeley, who have provided resource persons for the successful implementation of this research. The authors would also like to thank Alphabet Incubator for providing facilities and financial support during this research.

REFERENCES


