BIS INFORMATION TECHNOLOGY AND COMPUTER SCIENCE

Volume 2 2025 | DOI: 10.31603/bistycs.196
6th Borobudur International Symposium on Science and Technology (BIS-STE) 2024

UNIMMA PRESS
UNIVERSITAS MUHAMMADIYAH MAGELANG

Cross-layer analysis of physically unclonable functions in cyber-physical systems

Nuniek Fahriani[1]*

[1] Universitas Muhammadiyah Surabaya, Surabaya, Indonesia
*Corresponding author email: nuniekfahriani@ft.um-surabaya.ac.id

Abstract

Several key factors drive the exploration of PUFs across multiple layers of CPS: rising cybersecurity threats, unique security challenges of CPS, the need for holistic security approaches, scalability, and interoperability. The purposes of this analysis include: comprehensive vulnerability assessment, understanding cross-layer dependencies, ensuring device-level security, and preparing for future threats. Physically Unclonable Functions (PUFs) with Computer-Aided Design (CAD) are used for the design, analysis, and verification of electronic systems. PUF designers may utilize CAD tools for designing and simulating PUF circuits. PUFs are investigated for their integration into Cyber-Physical Systems (CPS) to address security challenges in the convergence of physical and digital components. Cross-layer analyses and evaluations aim to understand how PUFs can contribute to the overall security posture of CPS. There are methods to evaluate the effectiveness of integrating Physically Unclonable Functions (PUF) in enhancing hardware security at the physical level within Cyber-Physical Systems (CPS) is penetration testing, vulnerability analysis, security testing, attack simulation and performance analysis. Here are several domains and disciplines where the findings and implications of this study can be applied: Cybersecurity, Embedded Systems Design, Cryptography, Computer Engineering, IoT (Internet of Things), Information Security, Systems Engineering. The outcomes research on Cross-Layer Analysis of Physically Unclonable Functions in Cyber-Physical Systems include: identification of vulnerabilities, insight into cross-layer dependencies, assessment of PUF integration, Development of security strategies, enhanced security posture.

Published:
April 28, 2025

Selection and Peer-review under the responsibility of the 6th BIS-STE 2024 Committee

Keywords

Cross-layer analysis, Unclonable functions, Cyber-physical systems

Introduction

In the digital era and the realm of Cyber-Physical Systems (CPS), security has become a primary concern due to the increasing interconnectedness of devices and systems. To address these security challenges, Physically Unclonable Functions (PUFs) have emerged as a potential solution. PUFs are security components that leverage natural variations in the physical properties of electronic devices to generate unique identifiers, which can be used for authentication and encryption [1,2]. Physically Unclonable Functions (PUFs) refer to a type of security mechanism implemented in hardware that leverages the inherent variations in the physical characteristics of a device to generate unique values or keys. The uniqueness of PUFs makes them valuable in security applications, such as generating unique cryptographic keys for each device or identifying devices in a way that is difficult or nearly impossible to forge. PUFs are often employed in hardware security design and high-level security systems, including applications in the Internet of Things (IoT), embedded systems, and other security-critical scenarios [3–5]. Furthermore, the application layer scrutinizes the practical implications of PUFs in real-world CPS scenarios, evaluating their effectiveness in ensuring the integrity and authenticity of data and communication. By conducting a cross-layer analysis, this research seeks to identify vulnerabilities, strengths, and potential improvements in the deployment of PUFs in CPS. the Cross-Layer Analysis of Physically Unclonable Functions (PUFs) in Cyber-Physical Systems (CPS) lies in the critical need for robust and comprehensive security measures in the ever-evolving landscape of connected systems. Several key factors drive the exploration of PUFs across multiple layers of CPS: Rising Cybersecurity Threats, Unique Security Challenges of CPS, PUFs as a Security Enabler, Need for Holistic Security Approaches, Real-world Applicability, Scalability and Interoperability. Physically Unclonable Function (PUF) can be applied in various aspects of computer security to enhance the level of security. Here are some applications of PUF in the context of computer security,[4,6–9] in Table 1 [10,11].

Table 1. Implementation of PUF in the context of computer security

Process	Implementation
Device authentication	Public key infrastructure, certificate-based authentication, MAC address filtering, Token-based authentication, Mutual transport layer security, Device ID and secret key, Biometric authentication, fingerprinting techniques.
Key generation	Cryptographic hash function, password-based key derivation function, elliptic curve cryptography (ECC), RSA key pair generation, Diffie-helman key exchange, One-time pad (OTP), Hardware security module, Biometric key generation.
Anti-cloning protection	Embedded secure elements, Hardware-based unique identifier, Firmware verification, Remote attestation, Counterfeit detection technologies.
Secure key storage	Cloud-based key management, encrypted file systems, Split key storage, Secret sharing schemes, Password-based key derivation function.
Reverse engineering prevention	Code obfuscation, Binary code protection, Anti-debugging techniques, Dynamic code generation, Memory protection techniques, License checks dan activation, secure boot, Watermarking and tracing, Legal protections.
RFID and smart card protection	Secure elements, Access controls, anti-cloning features, secure communication protocols, Tamper detection.

Cyber-Physical Systems (CPS) refer to integrated systems that blend computational and physical elements, creating an environment where digital systems and physical processes interact closely [12] . These systems seamlessly combine hardware, software, communication networks, and physical components to monitor, control, and respond to the surrounding physical world [13,14]. Key Characteristics of Cyber-Physical Systems (CPS): Integration of Computation and Physical Processes, Use of Sensors and

Actuators, Connected Networks, Real-Time Processing, Autonomy and Decision-Making, Security and Privacy Challenges, Applications Across Industries [15]. Main Objectives of Cyber-Physical Systems (CPS): Optimization and Efficiency, Innovation, Safety and Reliability, Adaptation to Changes [16].

Methods

The operation of integrating Physically Unclonable Functions (PUFs) across different layers to enhance the security of Cyber-Physical Systems (CPS) involves leveraging the unique physical characteristics of hardware for secure authentication, cryptographic key generation, and device identification. Cyber-Physical Systems (CPS) are complex, interconnected systems that integrate computational and physical processes to monitor and control the physical world. CPS typically involve a combination of hardware, software, sensors, actuators, communication systems, and data processing capabilities. Figure 1 are key specifications and components commonly associated with Cyber-Physical Systems [17].

Figure 2 creating a block diagram for the cross-layer analysis of Physically Unclonable Functions (PUFs) in Cyber-Physical Systems (CPS) involves representing the various layers and components involved in the integration of PUFs. Below is a simplified block diagram to illustrate the cross-layer analysis of PUFs in CPS [18–21]. Cross-layer analysis of Physically Unclonable Functions (PUFs) in Cyber-Physical Systems (CPS) often involves various mathematical methods. These methods aid in examining and understanding the contributions of PUFs across different layers of the system. Here are some common mathematical methods used in the cross-layer analysis of PUFs in CPS: Information Theory, Cryptography, Computational Complexity Theory, Statistics and Probability, Control Theory, Graph Theory, Automata Theory, Linear Algebra, Coding Theory, Algorithm Complexity Analysis.

The application of these mathematical methods helps ensure the security and reliability of CPS systems integrating PUFs through a cross-layer approach. At the physical layer, the focus lies on the underlying hardware implementation of PUFs and their susceptibility to environmental variations and potential attacks. The logical layer investigates the integration of PUFs into the overarching system architecture, examining how they interact with other security mechanisms and protocols [22–24]. Identifying the Cross-Layer Analysis of Physically Unclonable Functions (PUFs) in Cyber-Physical Systems (CPS) [25] involves understanding and evaluating the interaction between PUFs and different security layers within a system. PUF generates unique values based on inherent physical variations in semiconductor devices. Identify how information generated by PUF can be used or impact other security layers. PUF integrates with other security technologies in CPS, such as firewalls, IDS/IPS, or other authentication methods. This analysis helps understand the contribution of PUF in the context of cross-layer analysis. Identify the extent to which PUF and other security layers can withstand threats involving coordinated attacks across multiple layers. cross-layer analysis of PUFs contributes to the overall security in the context of Cyber-Physical Systems [26–29].

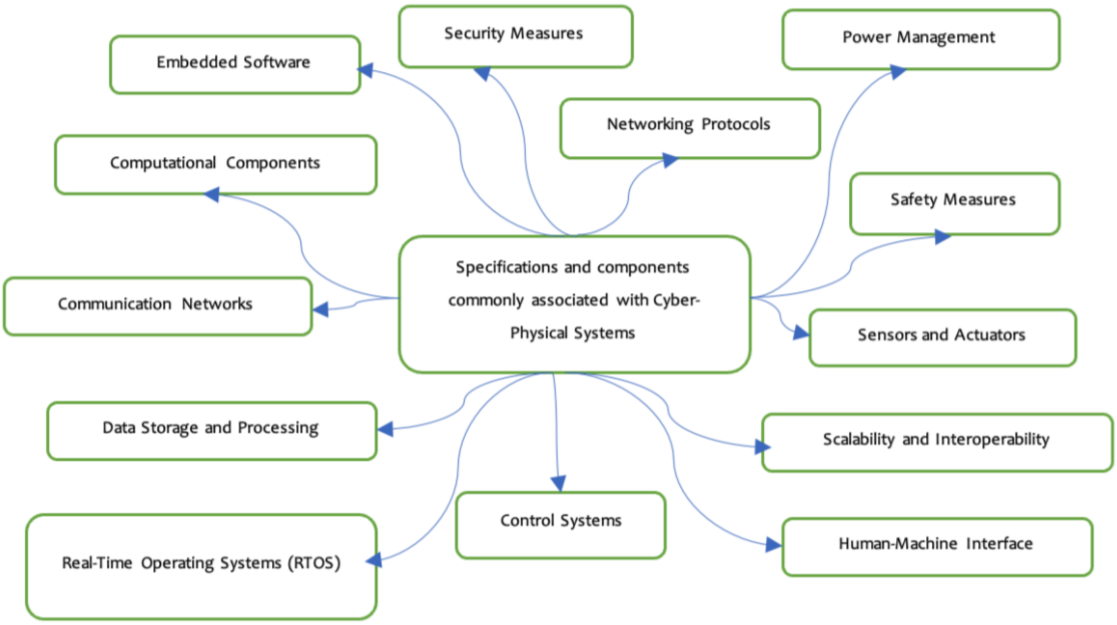

Figure 1. key specifications and components commonly associated with Cyber-Physical Systems

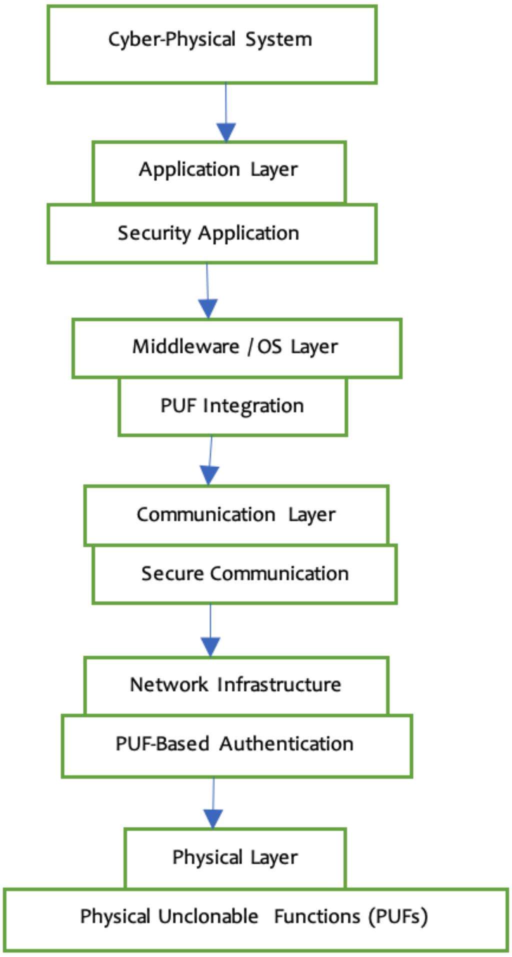

Figure 2. Block diagram for the cross-layer analysis of Physically Unclonable Functions (PUFs) in Cyber-Physical Systems (CPS)

Explanation Figure 2:

1. Cyber-Physical System (CPS): Represents the overall system, combining the cyber (software, algorithms) and physical (hardware, actuators) components.
2. Application Layer: Houses security applications that utilize the unique properties of PUFs for various security purposes like authentication, key generation, and intrusion detection.
3. Middleware / OS Layer: Manages the integration of PUFs into the system. This layer ensures that PUF functionalities are seamlessly incorporated into the operating system and middleware.
4. Communication Layer: Facilitates secure communication within the system. PUFs may contribute to the encryption and integrity verification of communication channels.
5. Network Infrastructure: Represents the network components and protocols that support PUF-based authentication mechanisms, ensuring secure communication between different nodes.
6. Physical Layer: Encompasses the hardware components, including the actual PUFs. PUFs generate unique identifiers based on physical characteristics, contributing to device authentication and secure key generation.

Results and Discussion

Cyber-Physical Systems (CPS) security poses unique challenges due to the integration of physical processes with computational and communication elements. Addressing these challenges requires a comprehensive understanding of potential threats and the implementation of effective countermeasures [30,31]. Here are some key security challenges in CPS along with corresponding countermeasures, security challenges:

Integration of cyber and physical domains

1. Challenge: The convergence of cyber and physical components creates vulnerabilities where cyber-attacks can have direct physical consequences.
2. Countermeasure: Implement strong access controls, encryption, and authentication mechanisms to protect cyber-physical interfaces. Use intrusion detection systems for early threat detection.
3. The workings of the system: integrating between the cyber domain (digital components such as software, computer networks, servers, and IoT devices) and the physical domain (such as sensors, computer hardware, and machinery). Data from physical sensors is processed by a computer system, covers data acquisition, analog to digital conversion (if necessary), data transmission, data reception, data processing, interpretation and action, visualization or reporting.

Interconnectedness and Interoperability

1. Challenge: Increased connectivity between CPS components can lead to a broader attack surface and potential propagation of threats.
2. Countermeasure: Employ secure communication protocols, isolate critical systems, and apply network segmentation. Regularly update and patch software to address vulnerabilities.
3. The workings of the system: involve the following aspects is interconnectedness (establishing connections, data transmission, network Protocols, scalability), Interoperability (compatibility, data Standardization, application programming interfaces (APIs) and interfaces, plug-and-play integration), operation (data exchange, resource sharing, cross-domain functionality), management and governance (monitoring and control, standards and policies, collaboration and partnerships).

Real-Time requirements

1. Challenge: Many CPS applications require real-time processing, making it challenging to implement traditional security measures without impacting performance.
2. Countermeasure: Implement lightweight and efficient security protocols. Consider the use of real-time operating Systems (RTOS) for critical applications.
3. The workings of real-time requirements in Physically Unclonable Functions (PUFs) involve several key aspects: response time, latency, reliability, integration, security, testing and validation, scalability, adaptability.

Safety and security conflict

1. Challenge: Security measures may conflict with safety requirements in CPS, as actions taken for security reasons might jeopardize system safety.
2. Countermeasure: Develop a holistic approach to address both safety and security concerns. Conduct thorough risk assessments and prioritize measures based on criticality.
3. The operation of the Safety and Security Conflict in Physically Unclonable Functions (PUFs) involves complex considerations related to data protection, hardware security, and user safety. PUFs should have strong self-recovery capabilities to address attacks or failures that may occur. Additionally, systems can use redundancy to ensure the availability and reliability of PUF operations. PUF implementations must comply with applicable security and safety regulations, including stringent data protection and privacy requirements. This includes compliance with standards such as GDPR, HIPAA, or ISO 27001.

Physical attacks

1. Challenge: CPS systems are susceptible to physical attacks such as tampering with sensors or actuators.

2. Countermeasure: Employ tamper-resistant hardware, secure physical access points, and monitor physical components for signs of tampering.
3. Physical attacks on Physically Unclonable Functions (PUFs) involve various techniques aimed at compromising the security and integrity of the PUF hardware, for example side-channel attacks, fault injection attacks, tampering attacks, reverse engineering, temperature and environmental attacks, acoustic attacks, side-channel leakage reduction techniques.

Supply chain vulnerabilities

1. Challenge: The global and complex supply chain for CPS components introduces the risk of compromised or counterfeit hardware.
2. Countermeasure: Establish a secure supply chain, perform rigorous vetting of suppliers, and ensure the integrity of components through cryptographic verification.
3. Supply chain vulnerabilities in Physically Unclonable Functions (PUFs) occur when the manufacturing or distribution process of PUFs is disrupted or infiltrated by malicious actors. How supply chain vulnerabilities in PUFs work: substitution or counterfeiting, theft of design information, replacement of firmware or software, integration with fake devices, manipulation in the production process, vulnerability to physical Attacks

Lack of security standards

1. Challenge: The absence of universally accepted security standards for CPS can lead to inconsistent security practices.
2. Countermeasure: Advocate for and adhere to industry-specific and international security standards. Develop best practices and guidelines for CPS security.
3. The lack of security standards in Physically Unclonable Functions (PUFs) refers to the absence or inadequacy of established guidelines or regulations governing the security aspects of PUF technology. Lack of security standards in PUFs is undefined security criteria, vulnerability to exploitation, interoperability challenges, Lack of Assurance, Regulatory Compliance Issues, Limited Adoption.

Data integrity and trustworthiness

1. Challenge: Ensuring the integrity and trustworthiness of data is crucial in CPS applications.
2. Countermeasure: Implement data encryption, digital signatures, and integrity checks. Utilize trusted computing techniques to verify the integrity of software components.
3. The operation of Data Integrity and Trustworthiness in Physically Unclonable Functions (PUFs) involves utilizing the unique physical properties of PUFs to secure and ensure the integrity of data. Here are the common steps in maintaining data

integrity and reliability in PUFs : unique identifier generation, encryption and authentication, anti-cloning properties, data integrity checking, protection against physical attacks, application in system Security.

Human factor

1. Challenge: Human errors, negligence, or malicious actions can compromise CPS security.
2. Countermeasure: provide security training for personnel, implement strict access controls, and enforce the principle of least privilege. Conduct regular security audits.
3. The role of the human factor in Physically Unclonable Functions (PUFs) involves aspects related to human interaction, perception, and behavior that can influence the security and effectiveness of PUFs. Here are several key aspects of the human factor in relation to PUFs: user authentication, training and education, usability and user experience (UX), human error and vulnerabilities, social engineering attacks, policy and compliance, human-centric security measures.

Scalability

1. Challenge: As CPS scale, managing security across a large number of interconnected devices becomes complex.
2. Countermeasure: Implement centralized security management systems, automate security processes, and employ scalable cryptographic solutions.
3. The security scalability system in Physically Unclonable Functions (PUFs) is designed to ensure that the security of PUFs remains intact and effective even when deployed at a large scale or in complex environments. Here's how the security scalability system operates in PUFs: implementation of strong security algorithms and protocols, efficient key management, capability for mass updates or management of PUFs, integration with existing security infrastructure, monitoring and auditing, user training and Awareness.

Physically Unclonable Functions (PUFs) with Computer-Aided Design (CAD) are used for the design, analysis, and verification of electronic systems. PUF designers may utilize CAD tools for designing and simulating PUF circuits. There are several ways to evaluate the effectiveness of integrating Physically Unclonable Functions (PUF) in enhancing hardware security at the physical level within Cyber-Physical Systems (CPS) [32,33]. Here are some commonly used methods in Table 2.

Conclusion

The escalating integration of Cyber-Physical Systems (CPS) across diverse domains has accentuated the imperative for robust security measures. Physically Unclonable Functions (PUFs) have emerged as a promising solution to fortify the security of CPS by providing unique and inherent hardware fingerprints. A comprehensive understanding of PUFs, spanning various layers of the system, is crucial for ensuring their effective deployment. This study delves into the Cross-Layer Analysis of Physically Unclonable Functions in Cyber-Physical Systems, aiming to explore the intricacies of PUFs across multiple layers of CPS. At the physical layer, the focus lies on the underlying hardware implementation of PUFs and their susceptibility to environmental variations and potential attacks. The logical layer investigates the integration of PUFs into the overarching system architecture, examining how they interact with other security mechanisms and protocols. Furthermore, the application layer scrutinizes the practical implications of PUFs in real-world CPS scenarios, assessing their efficacy in ensuring data integrity and the authenticity of communications. By conducting a cross-layer analysis, this research seeks to identify vulnerabilities, strengths, and potential enhancements in the deployment of PUFs in CPS. The outcomes of this study aim to contribute valuable insights to the development of resilient security strategies for Cyber-Physical Systems. By examining PUFs across different layers, the research endeavors to provide guidance for designing, implementing, and optimizing PUF-based security mechanisms.

Table 2. Commonly used methods

Methods	Explanation
Penetration Testing	Conducting penetration testing on CPS systems using PUF to assess how difficult it is for attackers to breach the hardware security through cloning or physical attacks on the device.
Vulnerability Analysis	Identifying and analyzing potential vulnerabilities that may occur in the implementation of PUF in CPS hardware. This can be done by examining various attack scenarios and determining whether PUF can protect the device from these attacks
Security Testing	Performing security testing on CPS systems using PUF to evaluate the strength of the security mechanisms implemented with PUF. This may include testing the cryptographic strength of PUF and its resilience against various types of physical attacks
Attack Simulation	Simulating various types of attacks that may occur on CPS hardware using PUF to assess how effective PUF is in protecting the device from these attacks.
Performance Analysis	Measuring the performance of PUF in enhancing hardware security at the physical level within CPS by comparing the results of tests and analysis with systems that do not use PUF or use other security methods.

References

[1] Wachsmann, C.; Sadeghi, A.-R. Basics of Physically Unclonable Functions. In; 2015.

[2] Helfmeier, C.; Boit, C.; Nedospasov, D.; Seifert, J.P. Cloning Physically Unclonable Functions. In Proceedings of the Proceedings of the 2013 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013; 2013.

[3] Maes, R. *Physically Unclonable Functions*; 2013;

[4] Labrado, C.; Thapliyal, H. Design of a Piezoelectric-Based Physically Unclonable Function for IoT Security. *IEEE Internet Things J* **2019**, 6, doi:10.1109/JIOT.2018.2874626.

[5] Zhao, B.; Zhao, P.; Fan, P. Epuf: A Lightweight Double Identity Verification in IoT. *Tsinghua Sci Technol* **2020**, 25, doi:10.26599/TST.2019.9010072.

[6] Tiplea, F.L.; Hristea, C.; Bulai, R. Privacy and Reader-First Authentication in Vaudenay's RFID Model with Temporary State Disclosure. *Computer Science Journal of Moldova* **2022**, *30*, doi:10.56415/csjm.v30.18.

[7] Kim, D.; Im, S.; Kim, D.; Lee, H.; Choi, C.; Cho, J.H.; Ju, H.; Lim, J.A. Reconfigurable Electronic Physically Unclonable Functions Based on Organic Thin-Film Transistors with Multiscale Polycrystalline Entropy for Highly Secure Cryptography Primitives. *Adv Funct Mater* **2023**, *33*, doi:10.1002/adfm.202210367.

[8] Kraleva, L.; Mahzoun, M.; Posteuca, R.; Toprakhisar, D.; Ashur, T.; Verbauwhede, I. Cryptanalysis of Strong Physically Unclonable Functions. *IEEE Open Journal of the Solid-State Circuits Society* **2022**, *3*, doi:10.1109/ojsscs.2022.3227009.

[9] Zhu, F.; Li, P.; Xu, H.; Wang, R. A Lightweight RFID Mutual Authentication Protocol with PUF. *Sensors (Switzerland)* **2019**, *19*, doi:10.3390/s19132957.

[10] Nguyen, K.T.; Laurent, M.; Oualha, N. Survey on Secure Communication Protocols for the Internet of Things. *Ad Hoc Networks* **2015**, *32*, doi:10.1016/j.adhoc.2015.01.006.

[11] Kurniawan, R.A.Z.; Wahjuni, S.; Neyman, S.N. Secure Communication Protocol for Arduino-Based IoT Using Lightweight Cryptography. *Int J Adv Sci Eng Inf Technol* **2022**, *12*, doi:10.18517/ijaseit.12.2.8601.

[12] Liu, Y.; Peng, Y.; Wang, B.; Yao, S.; Liu, Z. Review on Cyber-Physical Systems. *IEEE/CAA Journal of Automatica Sinica* **2017**, *4*, doi:10.1109/JAS.2017.7510349.

[13] Lu, Y. Cyber Physical System (CPS)-Based Industry 4.0: A Survey. *Journal of Industrial Integration and Management* **2017**, 2, doi:10.1142/S2424862217500142.

[14] Oks, S.J.; Jalowski, M.; Lechner, M.; Mirschberger, S.; Merklein, M.; Vogel-Heuser, B.; Möslein, K.M. Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook. *Information Systems Frontiers* **2022**, doi:10.1007/s10796-022-10252-x.

[15] Raisin, S.N.; Jamaludin, J.; Mohd Rahalim, F.; Jamal Mohamad, F.A.; Naeem, B. Cyber-Physical System (CPS) Application- A REVIEW. *REKA ELKOMIKA: Jurnal Pengabdian kepada Masyarakat* **2020**, *1*, doi:10.26760/rekaelkomika.v1i2.52-65.

[16] Saudi, M.M.; Sukardi, S.; Aziz, N.A.A.A.; Ahmad, A.; Husainiamer, M. 'Afif Malware Classification for Cyber Physical System (CPS) Based on Phylogenetics. *Int J Eng Adv Technol* **2019**, *9*, doi:10.35940/ijeat.A2711.109119.

[17] Moreno, J.; Rosado, D.G.; Sánchez, L.E.; Serrano, M.A.; Fernández-Medina, E. Security Reference Architecture for Cyber-Physical Systems (Cps). *Journal of Universal Computer Science* **2021**, *27*, doi:10.3897/JUCS.68539.

[18] Valentini, R.; Marco, P. Di; Alesii, R.; Santucci, F. Cross-Layer Analysis of Multi-Static RFID Systems Exploiting Capture Diversity. *IEEE Transactions on Communications* **2021**, 69, doi:10.1109/TCOMM.2021.3096541.

[19] Liu, B.; Han, S.; Peng, H.; Xiang, Z.; Sun, G.; Liang, Y.C. A Cross-Layer Analysis for Full-Duplex Ambient Backscatter Communication System. *IEEE Wireless Communications Letters* **2020**, 9, doi:10.1109/LWC.2020.2987792.

[20] Vuran, M.C.; Akyildiz, I.F. Error Control in Wireless Sensor Networks: A Cross Layer Analysis. *IEEE/ACM Transactions on Networking* **2009**, *17*, doi:10.1109/TNET.2008.2009971.

[21] Venkatachalam, K.; Prabu, P.; Balaji, B.S.; Kang, B.G.; Nam, Y.; Abouhawwash, M. Cross-Layer Hidden Markov Analysis for Intrusion Detection. *Computers, Materials and Continua* **2022**, *70*, doi:10.32604/cmc.2022.019502.

[22] Stanciu, A.; Cirstea, M.N.; Moldoveanu, F.D. Analysis and Evaluation of PUF-Based SoC Designs for Security Applications. *IEEE Transactions on Industrial Electronics* **2016**, 63, doi:10.1109/TIE.2016.2570720.

[23] Maes, R. Physically Unclonable Function (PUF). In *Encyclopedia of Cryptography, Security and Privacy*; 2023.

[24] Halak, B. *Physically Unclonable Functions*; 2018;

[25] Gebali, F.; Mamun, M. Review of Physically Unclonable Functions (PUFs): Structures, Models, and Algorithms. *Frontiers in Sensors* **2022**, 2, doi:10.3389/fsens.2021.751748.

[26] Wachsmann, C.; Sadeghi, A.-R. Physically Unclonable Functions (PUFs): Applications, Models, and Future Directions. *Synthesis Lectures on Information Security, Privacy, and Trust* **2014**, *9*, doi:10.2200/s00622ed1v01y201412spt012.

[27] Al-Haidary, M.; Nasir, Q. Physically Unclonable Functions (PUFs): A Systematic Literature Review. In Proceedings of the 2019 Advances in Science and Engineering Technology International Conferences, ASET 2019; 2019.

[28] Arjona, R.; Prada-Delgado, M.Á.; Arcenegui, J.; Baturone, I. A PUF-and Biometric-Based Lightweight Hardware Solution to Increase Security at Sensor Nodes. *Sensors (Switzerland)* **2018**, *18*, doi:10.3390/s18082429.

[29] Xiong, W.; Schaller, A.; Katzenbeisser, S.; Szefer, J. Dynamic Physically Unclonable Functions. In Proceedings of the Proceedings of the ACM Great Lakes Symposium on VLSI, GLSVLSI; 2019.

[30] Shamsoshoara, A.; Korenda, A.; Afghah, F.; Zeadally, S. A Survey on Physical Unclonable Function (PUF)-Based Security Solutions for Internet of Things. *Computer Networks* 2020, *183*.

[31] McGrath, T.; Bagci, I.E.; Wang, Z.M.; Roedig, U.; Young, R.J. A PUF Taxonomy. *Appl Phys Rev* 2019, 6.

[32] Fernández Aragón, J.; Diez-Senorans, G.; Garcia-Bosque, M.; Celma, S. Ring Oscillator PUF on FPGA: Design and Characterisation by Using Second-Order Compensated Measurement. *Jornada de Jóvenes Investigadores del I3A* **2022**, *10*, doi:10.26754/jjii3a.20227004.

[33] Swati; Roy, S.; Singh, J.; Mathew, J. Design and Analysis of DDoS Mitigating Network Architecture. *Int J Inf Secur* **2023**, 22, doi:10.1007/s10207-022-00635-1.