

## Research Interests

---

Security, Cloud-Native, Distributed Networked System, Anomaly Detection, eBPF-based Provenance

## Education

---

<b>Zero Trust Cloud Security Research Center</b> <i>Researcher</i>	Busan, Republic of Korea <i>Feb. 2026</i>
<b>Pusan National University</b> <i>M.S. in Computer Engineering</i>	Busan, Republic of Korea <i>Mar. 2024 – Feb 2026</i>
<b>Pusan National University</b> <i>B.S. in Computer Sciences and Engineering</i> <i>Served mandatory military service</i>	Busan, Republic of Korea <i>Mar. 2018 – Feb. 2024</i> <i>May. 2020 – Nov. 2021</i>

## Publications

---

- **Container-Specific Service Mesh-based System for Mitigating Lateral Movement Attacks**  
*Geonwoo Yoon, Jinmyeong Shin, Jae-Seok Kim, Seunghyuk Kim, Jaeyoung Jeong, Yoon-Ho Choi*  
IEEE Transactions on Cloud Computing, 2026. [Paper]
- **Lightweight Service Mesh for Intrusion Detection using KD-CNN in Cloud-Native Environments**  
*Geonwoo Yoon, Jae-Seok Kim, Seunghyuk Kim, Jaeyoung Jeong, Millati Pratiwi, Yoon-Ho Choi*  
ACM Cloud Computing Security Workshop (CCSW in conjunction with the ACM CCS), 2025. [Paper] [Video]
- **Automated Cybersecurity Risk Assessment and Visualization Framework for Resilient Cloud IT Asset Management**  
*Joonho Seo, Jinmyeong Shin, Geonwoo Yoon, Jae-Seok Kim, Yoon-Ho Choi*  
ACM/SIGAPP Symposium on Applied Computing (SAC), 2025. [Paper]

## Under Review

---

- **Hybrid Session-Based UEBA for AWS Environment**  
*Doo-Hwan Choi, Geonwoo Yoon, Yoon-Ho Choi*  
Under review (double-blinded)
- **SCALE: Risk-aware Distributed System Call Audit Framework for Cloud-Native Environments**  
*Geonwoo Yoon, Seunghyuk Kim, Jaeyoung Jeong, Jae-Seok Kim, Yoon-Ho Choi*  
Under review (double-blinded)
- **Context-Preserving Adversarial System Call Injection for Cloud Anomaly Detection Evasion**  
*Jae-Seok Kim, Geonwoo Yoon, Seunghyuk Kim, Joonho Seo, Yoon-Ho Choi*  
Under review (double-blinded)

## Projects

---

<b>Inhancing VPD Control Web Framework (SCOPE)</b> <i>Developer</i>	In collaboration with LG Electronics <i>Aug. 2025 – Dec. 2025</i>
<ul style="list-style-type: none"><li>• Optimized SCOPE framework architecture to improve scalability, stability, and code quality.</li><li>• Enhanced security and accessibility through testing and user-centered UI/UX improvements.</li><li>• Improved maintainability with technical documentation and framework refinement.</li></ul>	
<b>PNU ZeroTrust CSRC CASB (Cloud Access Security Broker) [Web]</b> <i>Developer</i>	Developed by S3Lab <i>Jul. 2024 – May. 2025</i>

- Designed and developed a CASB to address multi-cloud access control, data leakage, and anomaly behavior.
- Implemented CASB Client (VPN Client), CASB Server (Web, Logging, and Anomaly Detection Server), and CASB Agent (VPN Client, Logging).
- Developed synchronization logic for AWS and Azure clouds, and monitoring functionality.

**Industrial Coating Film Defect Detection and Monitoring System** In collaboration with GBLIGHT  
Developer Jul. 2024 – Dec. 2024

- Implemented logic for the analysis server to control the PLC module via OPC UA communication.
- Preprocessed coating film datasets, trained detection models using YOLOv5, and deployed them to production.
- Developed the analysis server for real-time monitoring and reporting.

**Web-based Psychoeducational Platform [Web]** In collaboration with the Dept. Psychology, PNU  
Project Manager & Developer May. 2024 – Nov. 2024

- Planned development schedules, roles, and scope as a project manager.
- Set up the initial development environment and contributed to frontend, backend, and database development.
- Deployed the platform to production and performed ongoing maintenance.

**PNU Cloud RMF (Risk Management Framework).v1** Developed by S3Lab  
Developer Dec. 2023 – May. 2024

- Analyzed NIST SP 800-37, SP 800-53, and SP 800-30 standards and devised strategies for cloud application.
- Designed and developed the *Select*, *Implement*, and *Assess* steps of the RMF according to NIST standards.
- Implemented automated report generation functionality.

## Teaching Experience

**Operating Systems** Pusan National University  
Teaching Assistant 1st Semester 2024

## Employment

**ERUTY** Busan, Republic of Korea  
Software Engineer Dec. 2022 – Mar. 2023

- Contributed as an early-stage developer to backend development of a 3D graphic design marketplace platform.

## Honors and Awards

**Spear-phishing response training mini-challenge** Dec. 2023

- Awarded **Third Place** in the spear-phishing response training mini-challenge, hosted by the Ulsan Information Security Center and Korea Internet & Security Agency (KISA).

**4th PATH-HACK Makerthon** Feb. 2023

- Awarded **First Place** in the PATH-HACK Makerthon for developing an integrated software-hardware prototype, hosted by pathfinder & Korean Institute of Startup and Entrepreneurship Development.

**Academic Excellence Scholarship** 1st & 2nd Semester. 2022

**National Science & Technology Scholarship** 1st Semester 2018

- Merit-based national STEM scholarship awarded for outstanding scores in math and science on the Korean CSAT.

## Patents

---

- **Geonwoo Yoon**, Yoon-Ho Choi, "Risk-aware and Differentiated Distributed System Call Collection Framework for Cloud-Native Environments". Korean Patent (Under review)
- **Geonwoo Yoon**, Yoon-Ho Choi, "Dispatcher-Based Distributed System Call Collection System for Cloud-Native Environments". Korean Patent (Under review)
- **Geonwoo Yoon**, Yoon-Ho Choi, "METHOD AND SYSTEM FOR DETECTING ABNORMAL BEHAVIOR TO PREVENT LATERAL MOVEMENT ATTACKS IN KUBERNETES ENVIRONMENT". Korean Patent Application No. 10-2025-0067413 (Pending)
- **Geonwoo Yoon**, Yoon-Ho Choi, "ZERO-COPY BASED MAIN CONTAINER'S SYSTEM CALL COLLECTION DEVICE AND METHOD FOR USING EBPF IN KUBERNETES SECONDARY CONTAINER". Korean Patent Application No. 10-2025-0067396 (Pending)
- Jae-Seok Kim, **Geonwoo Yoon**, Yoon-Ho Choi, "EQUIPMENT CONTROL BASED VISION METHOD AND SYSTEM FOR AI-BASED DEFECT DETECTION AND DATA COLLECTION IN HIGH-SPEED AND WIDE-AREA REFLECTIVE FILMS". Korean Patent Application No. 10-2024-0133547

## Skills

---

<b>Languages</b>	C/C++, Python, JavaScript
<b>Libraries</b>	Pytorch, TensorFlow, scikit-learn, React, FastAPI
<b>Tools</b>	Docker, Kubernetes, eBPF, PostgreSQL, pgAdmin