

Takuya Kataiwa

Undergraduate Student, Faculty of Informatics, Shizuoka University

[takuyakataiwa@gmail.com] Portfolio | GitHub | LinkedIn | Google Scholar | ORCID

Research Interests

Usable Security, LLM Security, Human–AI Interaction, Trustworthy AI Systems, Natural Language Processing, and Computational Cognitive Science.

I am an undergraduate student in informatics with experience in research, software development, and student-led projects. My current interests focus on usable security and LLM security, especially in settings where AI agents act on behalf of users across browsers, external systems, and personal contexts.

Education

Shizuoka University Japan *Undergraduate Student, Faculty of Informatics, Department of Socio-Information Studies* Expected bachelor's degree.

Peer-Reviewed Publications

1. Ryota Saito, **Takuya Kataiwa**, and Tetsushi Ohki. “Enhancing LLM4Decompile with Obfuscated Source Code for Optimized Assembly.” *Network and Distributed System Security Symposium (NDSS)*, 2025.
2. Ryota Saito, **Takuya Kataiwa**, Minato Takashima, and Tetsushi Ohki. “Invisible Consent: Browser Automation by LLM Agents is Not Privacy-aware.” *Extended Abstracts of the ACM CHI Conference on Human Factors in Computing Systems (CHI EA)*, 2026.
3. Natsuki Nagai, Tetsuro Takahashi, **Takuya Kataiwa**, Masakatsu Nishigaki, and Tetsushi Ohki. “Secure and Usable Authentication Using Avatar Expression Blendshapes in Virtual Reality.” *Extended Abstracts of the ACM CHI Conference on Human Factors in Computing Systems (CHI EA)*, 2026.

Preprints

1. **Takuya Kataiwa**, Hakaze Cho, and Tetsushi Ohki. “Measuring Intrinsic Dimension of Token Embeddings.” *arXiv preprint arXiv:2503.02142*, 2025.

Conference Presentations in Japan

1. Ryota Saito, **Takuya Kataiwa**, Masakatsu Nishigaki, and Tetsushi Ohki. “Invisible Consent: LLM Agents’ Browser Automation is Not Privacy-aware.” *Computer Security Symposium (CSS)*, 2025.
2. **Takuya Kataiwa**, Hakaze Cho, and Tetsushi Ohki. “Measuring Intrinsic Dimension of Token Embeddings.” *The 39th Annual Conference of the Japanese Society for Artificial Intelligence (JSAI)*, 2025.
3. Jun Tajima, **Takuya Kataiwa**, Kenya Sasaki, and Junya Morita. “A Simulator for the Formation of Social Norms Through the Aggregation of Individual Behavioral Decisions.” *The 39th Annual Conference of the Japanese Society for Artificial Intelligence (JSAI)*, 2025.
4. **Takuya Kataiwa**, Hakaze Cho, and Tetsushi Ohki. “Measuring Intrinsic Dimension of Embedding Representations.” *The 31st Annual Meeting of the Association for Natural Language Processing*, 2025.
5. **Takuya Kataiwa** and Junya Morita. “A Dynamic Graph Neural Network Approach to Emotional Contagion in Local Communities.” *The 21st Workshop on Informatics*, 2023.

Poster Presentations

1. Natsuki Nagai, Tetsuro Takahashi, **Takuya Kataiwa**, Masakatsu Nishigaki, and Tetsushi Ohki. “Effects of Facial Expression Types on Authentication Accuracy and Usability in VR Facial Expression Recognition.” *Symposium on Cryptography and Information Security (SCIS)*, 2026.
2. Ryota Saito, **Takuya Kataiwa**, Shin Yamaguchi, Yoshinobu Kano, and Tetsushi Ohki. “Evaluating Scalability Using Source Code Obfuscation in LLM-based Decompilation.” *The 20th Young Researchers’ Symposium on Natural Language Processing*, 2025. Sponsor Award.
3. Shin Yamaguchi, **Takuya Kataiwa**, and Yoshinobu Kano. “Does Training Order Affect Transfer Performance and Internal Representations in Multilingual Continual Pretraining?” *The 20th Young Researchers’ Symposium on Natural Language Processing*, 2025.
4. Shiori Shiratori and **Takuya Kataiwa**. “Hypothesis Exploration for Man’yōshū Volumes Written Mainly in Kunji Using KL Divergence of n-gram Models.” *The 20th Young Researchers’ Symposium on Natural Language Processing*, 2025.

Selective Programs and Grants

- **IPA MITOU IT Human Resources Development Program**, 2026. Selected for Japan's national talent development program for young creators with original and innovative IT projects. Project: Communication augmentation through a haptic gel interface. Acceptance rate: 7.5
- **Kansai Tech Creator Challenge (K-TCC)**, 2025. Selected for a regional creator development program under METI's AKATSUKI Project. Project: Holoprax, connecting cognition and bodily action.

Awards and Honors

University Honors

- **President's Award**, Shizuoka University, 2026.

National and Domestic Awards

- **Gold Award, General Division**, Urban Data Challenge 2025, 2026. Project: Churin Watch. Top 0.6

Selected Projects

- **Communication Augmentation through a Haptic Gel Interface**. Project selected for the IPA MITOU IT Human Resources Development Program 2026. Explores a haptic interface that makes affective and social signals more tangible through material changes and AI-based interpretation.
- **Churin Watch**. Civic-tech project addressing bicycle-parking issues around urban areas. Received the Gold Award in the General Division at Urban Data Challenge 2025.
- **Holoprax**. Project selected for Kansai Tech Creator Challenge 2025. Explores the augmentation of cognition and bodily action by connecting thought and action.

Competitive Experience

- **AtCoder Algorithm**: User name *MoonStep*; Green-level rating; Rating 879; Rank 18,843rd; top 14.7As of June 2026.
- **AtCoder Heuristic**: User name *MoonStep*; Cyan-level rating; Rating 1448, provisional; Rank 1,106th; top 16.4As of June 2026.
- **Competitive Mathematics**: Online Math Contest, Blue.
- **Capture The Flag / OSINT**: Member of team *teapp*. Selected results include DIVER OSINT CTF 2025, top 2.4
- **iGEM HG-Tokyo**: Advisor, 2025. Gold Medal; Presentation Award, top 6.8

Leadership and Community Activities

- **Executive Committee Member**, CPC Spring Camp, 2024–present.
- **Member**, Symbol Emergence Outreach Team, 2024–present.
- **Advisor**, IYNA Japan Chapter, 2024–present.
- **Advisor**, iGEM HG-Tokyo, 2025.

Technical Skills

- **Programming**: Python, C++, JavaScript/TypeScript, Java, Swift, R.
- **Research**: LLM security, usable security, natural language processing, machine learning, human–AI interaction, graph neural networks.
- **Tools**: Git/GitHub, L^AT_EX, web application development, data analysis, experimental design.