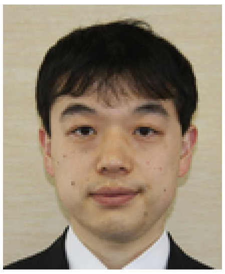
Foundation of Computer Science Laboratory

Takafumi Hayashi
Professor

Akihito Nakamura
Senior Associate Professor



Yodai Watanabe
Associate Professor

Yen Neil Yuwen
Associate Professor

Li Zhenni
Visiting Researcher

Refereed academic journal

[neilyyen-103-002-01:2015] Neil Y. Yen Lei Jing Joseph C. Tsai Yinghui Zhou Tongjun Huang Peng Li Zixue Cheng, Junbo Wang. A Context-aware IoT Middleware for Management of Conflicts Using a Priority Scheme based on Diagram of Situation State Transition. *Journal of Internet Technology*, 16(1):151–162, 2015.

Context-aware service is an extremely important research issue for users to collaborate with multiple smart objects embedded with various sensors in a local ubiquitous computing environment. And it is showing more important position in Internet of Things (shortly IoT) environment, when considering more complex situations happening in different locations. There is a need for IoT middleware to well organize the situations, e.g., creation and deletion of a situation, state transmission of the situation, in order to effectively provide services adaptive to various situations in IoT environment. Meanwhile conflict requests for situation-aware services are really hard to be solved, since many situations happen in the same time period need common resources for the services. In order to tackle the problem, we first propose an IoT middleware based on diagram of situation state transition (DSST), to specify and manage states of a situation. And then a priority scheme based on DSST for resolving conflicts is also presented by considering different states of situations. Experiment results demonstrate the feasibility of proposed method and the performance of situation-aware services based on the conflict resolution scheme.

[neilyyen-103-002-02:2015] Joseph C. Tsai James J. Park Neil Y. Yen, Qun Jin. Intelligent State Machine for Social Ad Hoc Data Management and Reuse. *Multimedia Tools and Applications*, 74(10):3521–3541, 2015.

Recent advances in information technology have turned out World Wide Web to be the main platform for interactions where participants–users and corresponding events–are triggered. Although the participants vary in accordance with scenarios, a considerable size of data will be generated. This phenomenon indeed causes the complexity in information retrieval, management, and resuse, and meanwhile, turns down the value of this data. In this research, we attempt to achieve efficient management of user-generated data and its derivative contexts (i.e., social ad hoc data) for human supports. The correlations among data, contexts, and their hybridization are specifically concentrated. An intelligent state machine is proposed to outline the relations of data and contexts, and applied to further identify their usage scenarios. The performance and feasibility can be revealed by the experiments that were conducted on the data collected from open social networks (e.g., Facebook, Twitter, etc.) in the past few years with size around 500 users and 8,000,000 shared contents from them.

[neilyyen-103-002-03:2015] Neil Y Yen Atsushi Sato, Runhe Huang. Design of fusion technique-based mining engine for smart business. *Human-centric Computing and Information Sciences*, 5(23), 2015.

Keys to successful implementation of smart business require a wide spectrum of domain knowledge, experts, and their correlated experiences. Excluding those external factors-which can be collected by well-deployed sensors-being aware of user (or consumer) has the highest priority on the to-do-list. The more user is understood, the more user can be satisfied from an intuitive point of view, and thus, data plays a rather essential role in the scenario. However, it is never easy to achieve comprehensive understanding as the data requires further processing before its values can be extracted and used. So how the data can be properly transformed into something useful for smart business development is exactly what we pursue in this study. As a pioneer, three major tasks are focused. First, a data mining engine based on the concept of the KID model is designed and developed to be responsible for the universal collection of data and mining valuable information which is primarily from real world, cyber world, and social world. Second, we go further into the fusion process of the collected data and meaningful information extracted and interpreted by algorithms or fused algorithms in the data mining engine (e.g., the consumer purchase data shared by real-world company) and turn them into valuable knowledge about the situation of customers and business situations based on the concept of knowledge, information, and data. A three-layer analysis and mining procedure is designed to enhance the mining engine through conventional RFM (Recency, Frequency, and Monetary Value) model and a set of fusion techniques. And in the end, we make planning-based predictions for a real-world company for expansion of the business interests.

[neilyyen-103-002-04:2015] Zhiwen Yu Yu Wang Neil Y. Yen Runhe Huang Xingshe Zhou Bin Buo, Zhu Wang. Mobile Crowd Sensing and Computing: The Review of an Emerging Human-Powered Sensing Paradigm. *ACM Computing Surveys*, 48(1), 2015.

With the surging of smartphone sensing, wireless networking, and mobile social networking techniques, Mobile Crowd Sensing and Computing (MCSC) has become a promising paradigm for cross-space and large-scale sensing. MCSC extends the vision of participatory sensing by leveraging both participatory sensory data from mobile devices (offline) and user-contributed data from mobile social networking services (online). Further, it explores the complementary roles and presents the fusion/collaboration of machine and human intelligence in the crowd sensing and computing processes. This article characterizes the unique features and novel application areas of MCSC and proposes a reference framework for building human-in-the-loop MCSC systems. We further clarify the complementary nature of human and machine intelligence and envision the potential of deep-fused human–machine systems. We conclude by discussing the limitations, open issues, and research opportunities of MCSC.

[neilyyen-103-002-05:2015] James J. Park Neil Y. Yen Chia-Chen Chen, Tien-Chi Huang. Real-time Smartphone Sensing and Recommendations towards Context-Awareness Shopping. *Multimedia Systems*, 21(1):61–72, 2015.

This study investigates a smart environment, namely 'Intelligent Shopping-aid Sensing System (iS3)' for online shopping support in the next era by developing a context-aware automated service system. Sensors, radio frequency identification (RFID), are applied for the recognition, collection, and delivery of user contexts. Following the collected contexts from sensors, integrated mining and analysis techniques (i.e., customized clustering analysis and association rules) were implemented for the provision of instant and personal information to users. Information of products, such as locations, specifications, and characteristics can be collected quickly through the deployed RFID reader and display. Moreover, local applications on mobile devices offer real-time interactions between central system and end users. The system is expected to prompt the product promotion, inquiry and online marketing to shopping malls (and related companies as well). In the empirical results, the quality of recommendations with the proposed approach reaches 70 percent accuracy rate. The traditional and non-clustering approaches are 56 and 46 percent, respectively. This study reduces long-term operation costs of retailers, stimulates service innovation and experience economy and enhances corporate operational performance.

[yodai-103-002-01:2015] Takao Maeda, Yodai Watanabe, and Takafumi Hayashi. Parameterization of High-Dimensional Perfect Sequences over a Composition Algebra over R. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E98-A(12):2439–2445, 2015.

To analyze the structure of a set of high-dimensional perfect sequences over a composition algebra over R, we developed the theory of Fourier transforms of the set of such sequences. We define the discrete cosine transform and the discrete sine transform, and we show that there exists a relationship between these transforms and a convolution of sequences. By applying this property to a set of perfect sequences, we obtain a parameterization theorem. Using this theorem, we show the equivalence between the left perfectness and right perfectness of sequences. For sequences of real numbers, we obtain the parameterization without restrictions on the parameters.

Refereed proceedings of an academic conference

[yodai-103-002-02:2015] Keisuke Tamoi, Takafumi Hayashi, and Yodai Watanabe. Security analysis of audio secret sharing scheme encrypting audio secrets. In *Proceedings of IEEE 7th International Conference on Awareness Science and Technology (iCAST2015)*, pages 130–134, Qinhuangdao, China, September 2015. IEEE.

Secret sharing is a method of encrypting a secret into multiple pieces called shares so that only qualified sets of shares can be employed to reconstruct the secret. Audio secret sharing (ASS) is an example of secret sharing whose decryption can be performed by human ears. This paper investigates the security of an audio secret sharing scheme encrypting audio secrets by numerical experiments based on simple statistical tests.

Unrefeered proceedings of an academic conference

[nakamura-103-002-01:2015] Shinji Kikuchi, Daishi Yoshino, Joseph C Tsai, Jiro Yamazaki, Hideyuki Fukuhara, Masanari Murasawa, Yuya Ito, Kyouhei Shiozawa, Takafumi Hayashi, Akihito Nakamura, and Jiro Iwase. Design and Implementation of an Overlaid Sensor Data Management Platform. In *IEICE Technical Report SC2015-11*, volume 115, pages 13–22, October 2015.

[nakamura-103-002-02:2015] Yodai Watanabe, Akihito Nakamura, Jiro Yamazaki, Shinji Kikuchi, Toshiaki Miyazaki, Jiro Iwase, and Takafumi Hayashi. Implementation of Robust Cyber Physical System using Mathematical

Engineering Method. In *Proc. of the Japan Society for Industrial and Applied Mathematics (JSIAM) Annual Conference*, September 2015.

[nakamura-103-002-03:2015] Takafumi Hayashi, Akihito Nakamura, Jiro Yamazaki, Shinji Kikuchi, Daishi Yoshino, Hitoki Matsuda, Masayuki Hisada, Yodai Watanabe, Yasuhiro Abe, and Jiro Iwase. A Novel Anonymization Scheme by Using Experimental Design. In *Proc. of the Society of Socio-Informatics (SSI) Annual Meeting*, volume 4, pages 253–256, September 2015.

[yodai-103-002-03:2015] Keisuke Tamoi, Takafumi Hayashi, and Yodai Watanabe. Security analysis of audio secret sharing scheme encrypting audio secrets (in Japanese). In *Proceedings of Tohoku-section Joint Convention of IEIE*, pages 130–134, Iwate, Japan, August 2015. IEIE.

Secret sharing is a method of encrypting a secret into multiple pieces called shares so that only qualified sets of shares can be employed to reconstruct the secret. Audio secret sharing (ASS) is an example of secret sharing whose decryption can be performed by human ears. This paper investigates the security of an audio secret sharing scheme encrypting audio secrets by numerical experiments based on simple statistical tests.

Research grants from scientific research funds and public organizations

[yodai-103-002-04:2015] Yodai Watanabe. JSPS Grant-in-Aid for Scientific Research (C), 2015-2018.

Academic society activities

[nakamura-103-002-04:2015] Akihito Nakamura, 2016.

Member

[nakamura-103-002-05:2015] Akihito Nakamura, 2016.

Member

[nakamura-103-002-06:2015] Akihito Nakamura, 2016.

Reviwer, IEEE TENCON 2016

Advisor for undergraduate research and graduate research

[yodai-103-002-05:2015] Shinya Washio. Master Thesis: Contributory Broadcast Encryption with Personalized Message, University of Aizu, 2016.

Thesis Advisor: Y. Watanabe

[yodai-103-002-06:2015] Shutaro Kato. Graduation Thesis: Sound classification by use of similarity distance based on audio compression, University of Aizu, 2016.

Thesis Advisor: Y. Watanabe

[yodai-103-002-07:2015] Mao Nozaki. Graduation Thesis: The Algorithmic Design Having a Mental Effect, University of Aizu, 2016.

Thesis Advisor: Y. Watanabe

[yodai-103-002-08:2015] Yuto Miura. Graduation Thesis: Image Classification by Use of Similarity Distance Based on Lossy Compression, University of Aizu, 2016.

Thesis Advisor: Y. Watanabe

Others

[nakamura-103-002-07:2015] COCN Project, Privacy and Innovation in IoT Era, Final Report. http://www.cocn.jp/thema84-L.pdf, March 2016.

[yodai-103-002-09:2015] Yuto Miura. Image Classification by Use of Similarity Distance Based on Lossy Compression, 2015.

2015 IPSJ Tohoku Section Student Award (Yuto Miura)

Contributions related to syllabus preparation

[nakamura-103-002-08:2015] L6 Information Security

[nakamura-103-002-09:2015] CSC01 Information Security

[nakamura-103-002-10:2015] O3-043 SCCP Open Data Hacks

Proposal/implementation of a future industry plan

[nakamura-103-002-11:2015] Takafumi Hayashi, Fumiaki Yamazaki, Akihito Nakamura, Yasuhiro Abe, Makoto Yashiro. In-Vehicle Infortainment Systems Security. Collaboration with ALPINE and Aizu Lab, AOI Meetings.

Did you participate in Public Lectures, and/or Open Campus? (Yes or No) If yes, please describe what you did.

[nakamura-103-002-12:2015] Akihito Nakamura. Software Vulnerability Management. UoA Open Labs 2015 Autumn Session, October 2015.

[nakamura-103-002-13:2015] Akihito Nakamura and Yasuhiro Abe. Continuous Security Management in Organizations. Cyber Attack Protection and Information Security Seminar, January 2015.

[nakamura-103-002-14:2015] Akihito Nakamura. Software Vulnerability Assessment based on Open Data. Keynote address in T4U Partner Meeting, Tokyo, April 2015.

[nakamura-103-002-15:2015] Akihito Nakamura. Cyber Security Trends and Continuous Security Management. Keynote address in My-Number Seminar, organized by NTT Advanced Technology Corporation, Kawasaki, February 2016.

[yodai-103-002-10:2015] Open Laboratory at Open Campus 2015 (Summer and Autumn Sessions)