Communications in Computer and Information Science 1186

Commenced Publication in 2007
Founding and Former Series Editors:
Phoebe Chen, Alfredo Cuzzocrea, Xiaoyong Du, Orhun Kara, Ting Liu, Krishna M. Sivalingam, Dominik Ślęzak, Takashi Washio, Xiaokang Yang, and Junsong Yuan

Editorial Board Members

More information about this series at http://www.springer.com/series/7899

Sanjay K. Sahay · Nihita Goel ·
Vishwas Patil · Murtuza Jadliwala (Eds.)

Secure Knowledge Management In Artificial Intelligence Era

8th International Conference, SKM 2019
Goa, India, December 21–22, 2019
Proceedings

Springer

Editors
Sanjay K. Sahay
Birla Institute of Technology and Science
Goa, India

Vishwas Patil
Indian Institute of Technology Bombay
Mumbai, India

Nihita Goel
Information Systems Development Group, TIFR
Mumbai, India

Murtuza Jadliwala
The University of Texas at San Antonio
San Antonio, TX, USA

ISSN 1865-0929 ISSN 1865-0937 (electronic)
Communications in Computer and Information Science
ISBN 978-981-15-3816-2 ISBN 978-981-15-3817-9 (eBook)
https://doi.org/10.1007/978-981-15-3817-9

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The International Conference on Secure Knowledge Management (SKM) in Artificial Intelligence Era (SKM 2019), a multidisciplinary conference, was jointly organized by the Department of Computer Science and Information System, BITS Pilani, K. K. Birla Goa Campus India, with the University of Texas at San Antonio, USA, and the University at Buffalo, USA, held during December 21–22, 2019, to bring together researchers and practitioners from academia, industry, and government on a global scale. SKM is an important research area that deals with methodologies for systematically gathering, organizing, and securely disseminating knowledge and information. The first SKM conference was organized in 2004 at the University at Buffalo, USA, and over the years it has been held every two years in SUNY Albany, SUNY Stonybrook, UT Dallas, Rutgers, Dubai, Tampa, etc. 2019 was the first time that SKM was held in India. Also, in conjunction with SKM, a workshop on Digital Payment Systems was organized. SKM 2019 focused on revolutionary technologies such as artificial intelligence, machine learning, cloud computing, big data, and IoT. In the conference, delegates presented and discussed the most recent innovations, trends, and concerns, including theoretical and practical challenges encountered with an emphasis on artificial intelligence.

Prof. G. Raghurama, Director at BITS Pilani, K. K. Birla Goa Campus, inaugurated the conference and addressed the participants. The conference dignitaries Prof. H. R. Rao (Steering Committee member), Prof. Sanjay K. Sahay (General Chair), BITS Pilani K. K. Birla Goa Campus, Prof. Ram Krishnan, General Co-Chair, UTSA and Dr. Nihita Goel, Program Committee chair, TIFR, Mumbai also welcomed and addressed the participants. The conference started with a keynote talk by Dr. Shriram Revankar, Vice President of Adobe. He addressed the issue of trust and loyalty in artificial intelligence. His talk positioned trust and loyalty as computable entities that can play a significant role in today's human-machine collaborative societies. Prof. Sandeep Shukla, Chair Professor, IIT Kanpur delivered a talk on cyber security of critical infrastructures. Mr. Anil Nair, MD at Cisco, and Mr. K. P. M. Das, Director, Cyber Security and Trust, Cisco discussed the digital transformation in India. They pointed out that India has what is commonly known as the two-third:one-third problem, which is that two-thirds of the population resides in rural areas while they have access to only a third of the country's resources. The government recognizes this, and citizens are realizing too, that India can alleviate the situation rapidly with smart digital interventions. Prof R. K. Shyamsundar, IIT Bombay, India addressed the challenges of ownership and privacy in medical data sharing and how medical data has become vital for society. In addition, an invited talk was delivered by Srihari Muralidhar, Aarhus University, Denmark on "Digital payments adoption by low-income population in Bengaluru: Lessons from the road." Dr. Vishnu Pendyala, Cisco and San Jose State University, USA spoke on security trust in online social networks. Also, a tutorial on "Blockchain for Enterprise" was delivered by Dr. Mani Madhukar, IBM, India.

SKM 2019 received many high-quality submissions. Authors comprised a mix from India, US, Canada, and Italy. A total of 34 research papers were received by the Technical Program Committee (TPC). The TPC of SKM 2019 comprised of researchers and industry practitioners from all corners of the world. Each of the submitted papers received at least two reviewers. The review process was double-blind, and after the careful review process, the top 12 papers were selected for publication in this proceedings volume, with an acceptance rate of 35%. The conference was organized over two days with a very compact schedule. Beyond the technical program of the research papers, the conference was enriched by many other items. For young researchers, a five-minute innovation challenge was organized in which students presented their idea in five minutes. The winner and runner-up were awarded cash prizes.

We are very much thankful to the delegates, speakers, and the authors for their active participation in SKM 2019, especially with regards to the sharing of innovative ideas and view. We are also thankful to Ms. Kamiya Khatter (Associate Editor at Springer Nature), for providing continuous guidance and support. Also, we extend our heartfelt gratitude to the reviewers and TPC members for their efforts in the review process. We are indeed thankful to everyone who was directly or indirectly associated with the organizing team of the conference leading to a successful event. We also gratefully acknowledge Indo-U.S. Science and Technology Forum for partially funding the workshop and the conference via grant No. IUSSTF/AUG/WS/162/2019. We hope the proceedings will inspire more research in Secure Knowledge Management, Digital Payments, and the application of artificial intelligence.

December 2019

Sanjay K. Sahay
Nihita Goel
Vishwas Patil
Murtuza Jadliwala

Organization

Chief Patron

Raghurama G.	BITS Pilani, Goa Campus, India

General Chair

Sahay Sanjay K.	BITS Pilani, Goa Campus, India

General Co-Chair

Krishnan Ram	University of Texas at San Antonio, USA

Program Committee Chairs

Goel Nihita	Tata Institute of Fundamental Research, Mumbai, India
Jadliwala Murtuza	University of Texas at San Antonio, USA
Patil Vishwas	IIT Bombay, India

Steering Committee

Kwiat Kevin	Air Force Research Laboratory, USA
Memon Nasir	New York University, USA
Rao Raghav	University of Texas at San Antonio, USA
Thuraisingham Bhavani	University of Texas at Dallas, USA
Upadhyaya Shambhu	University at Buffalo, The State University of New York, USA

Program Committee

Agarwal Swati	BITS Pilani, Goa Campus, India
Agrawal Manish	University of South Florida, USA
Bano Wajeeda	Mangalore University, India
Bedi Punam	Delhi University, India
Chakraborty Tanmoy	IIIT Delhi, India
Cheng Yuan	California State University, USA
Chowdhury Dipanwita	IIT Kharagpur, India
Das Debasis	IIT Jodhpur, India
Dhal Subhasish	IIIT Guwahati, India
Geethakumari G.	BITS Pilani, Hyderabad Campus, India
Halder Raju	IIT Patna, India
Husain Mohammad	California State Polytechnic University, USA
Jain Shweta	John Jay College of Criminal Justice, USA

Jaiswal Raj	BITS Pilani, Goa Campus, India
Krishnan Ram	University of Texas at San Antonio, USA
Kumar Kuldeep	NIT Jalandhar, India
Maiti Anindya	University of Texas at San Antonio, USA
Maity Soumyadev	IIIT Allahabad, India
Masoumzadeh Amirreza	University at Albany, NY, USA
Medrano Carlos	Arizona State University, USA
Narang Pratik	BITS Pilani, Pilani Campus, India
Narendra Kumar	IDRBT, Hyderabad, India
Ninglekhu Jiwan	University of Texas at San Antonio, USA
Niyogi Rajdeep	IIT Roorkee, India
Pal Abhipsa	IIM Bangalore, India
Park Jaehong	University of Alabama in Huntsville, USA
Paul Souradyuti	IIT Bhilai, India
Raghu	Arizona State University, USA
Ramanujam R.	IMSc Chennai, India
Rana Nripendra	Swansea University, USA
Rao Raghav	University of Texas at San Antonio, USA
Rathore Heena	Hiller Measurements, USA
Rathore Hemant	BITS Pilani, Goa Campus, India
Sahay Sanjay K.	BITS Pilani, Goa Campus, India
Samtani Sagar	University of South Florida, USA
Shan J.	Miami University, USA
Sharma Ashu	Mindtree, Hyderabad, India
Shekhar	Mangalore University, India
Shetty Rathnakara	Mangalore University, India
Shukla Sandeep	IIT Kanpur, India
Shyamasundar R. K.	IIT Bombay, India
Srinathan Kannan	IIIT Hyderabad, India
Subramanyan Pramod	IIT Kanpur, India
Thakur Rahul	IIT Roorkee, India
Upadhyay Nitin	Goa Institute of Management, India
Upadhyaya Shambhu	University at Buffalo, The State University of New York, USA
Vaish Abhishek	IIIT Allahabad, India
Valecha Rohit	University of Texas at San Antonio, USA
Wang J.	University of Texas at Arlington, USA

External Reviewers

Dutta Hridoy	IIIT Delhi, India
N. Naren	IIT Kanpur, India
Samant Abhay	University of Texas at Austin, USA
Santanam Raghu	Arizona State University, USA
Sureshkanth Nisha	University of Texas at San Antonio, USA
Wijewickrama Raveen	University of Texas at San Antonio, USA
Xu Liwei	University of South Florida, USA

Abstracts

Challenges of Ownership and Privacy in Medical Data Sharing

R. K. Shyamasundar

Department of Computer Science and Engineering,
Indian Institute of Technology Bombay, India
rkss@cse.iitb.ac.in

Sharing of medical data has become vital for the society. Three common usage patterns are:

1. Information sharing among the medical community is immensely important both from the perspective of growth of medical science and patient treatment. Medical wisdom is realized through a large number of experiments by multiple parties. In the creation of such datasets, privacy, provenance, and ownership play a vital role. Privacy is very important as the medical information of individual patient needs to be kept private, while the data is used for purposes of individual treatment and also warnings to the community. Provenance and ownership play a vital role in constructing intermediate results or new experiments from intermediate ones across groups of researchers or laboratories.
2. Medical information is being standardized in the form of Electronic Health Record (EHR). EHR systems enable easier and faster sharing of medical information among different health care providers serving the same patients. It is also expected to eliminate duplicate medical tests, like pathology tests, X-rays, EEG, etc., that are often repeated by different health-care providers. EHR systems are provided as a service by health care providers. Currently, EHR systems are fragmented and are incompatible with one another. Thus, collaboration among different health care providers becomes a challenge if the same patient seeks care from different providers. Privacy is an important concern when multiple providers share health information of any patient. It must be ensured that the patient consents before her data is shared and owns the data for sharing. Of course, the patient has the right to selectively share information with the provider of her choice; this has to be guaranteed by the service provider. Currently, health care providers are responsible for storing and managing the data and need to be trusted for first sharing the information with the patient and no one else without the consent of the patient.
3. Medical databases like Hippocratic databases accept responsibility for the security and privacy of information they manage without impeding legitimate use and disclosure. Sharing and privacy is usually realized through restricted views of the database in these systems.

We shall discuss various security architectures that promote sharing of medical data satisfying the various requirements without a centralized trust and enables interoperability, based on information flow security models, blockchain technology, and various cryptographic encryption techniques.

Cyber Security of Critical Infrastructures: A C3I Perspective

Rohit Negi and Sandeep K. Shukla

National Interdisciplinary Center for Cyber Security and Cyber Defense
of Critical Infrastructures, Indian Institute of Technology Kanpur,
Uttar Pradesh, India
{rohit,sandeeps}@cse.iitk.ac.in

Critical Infrastructures are infrastructures such as power grids, water/sewage systems, industrial manufacturing, air-traffic control, and railway signaling systems – which if compromised, could harm a nation's economic security as well as the health and lives of people. Most critical infrastructures are cyber-physical systems which have physical dynamics controlled by centralized or distributed software-based controllers – that are aided by sensors carrying information on the current physical state of such systems, and by actuators to effect changes in the physical dynamics of the systems. The sensors, actuators, the information flow through communication network, and the controllers themselves are the cyber components of critical infrastructures. In recent years, an increasing trend of making these components targets of cyber attacks have necessitated research and development of cyber-security methods, tools, and manpower training.

Starting with the Maroochy Sewage treatment plant attack in early 2000, there has been a steady increase in cyber attacks, for example with the most recent attacks on the Ukraine power grid and an attack on a Nuclear plant in India – thus one can find many examples of cyber attacks on critical infrastructures. In most cases, these attacks are attributed to nation state sponsored actors – who have deep financial and technology access, making sophisticated attacks plausible.

In response to the Stuxnet attack on the Nuclear facilities in Iran, there was a presidential executive order in the US in 2013, and a corresponding enactment of a legislation in 2014 – leading to the development of a cyber-security framework for adoption by utilities of various critical infrastructure sectors. Even though it is voluntary to implement such a framework – it provides a very succinct description of basic structures, processes, and measures for risk-assessment based cyber-security strategy and implementation.

The basic functions prescribed in this framework by NIST are identify-protect-detect-respond-recover. The identification of cyber assets and the risk analysis of their exposure, as well as strong cryptographic authentication for both equipment and human actors are the goals of the 'identify' function. The 'protect' function includes various protection mechanisms starting from perimeter defense, zone division, authenticated communication, access control, etc. The 'detect' function entails intrusion detection, malware detection, vulnerability assessment, and penetration testing. The 'respond' function is activated when an attack is detected – followed by containment, localization, and possibly islanding to reduce the extent of damage. The

'recovery' function entails recovering from an attack by bringing back the system to its full functionality – and better implementation of a recovery plan should minimize the downtime due to an attack.

Depending on how well these functions are implemented and well strategized – an organization (e.g., utility), is placed in various tiers of cyber readiness (partial, risk-informed, repeatable, and adaptive). An organization has to profile itself – accordingly, and a better profile is to be targeted with a measurable pathway to achieve a better tier and profile in terms of cyber readiness.

With this framework in mind, the national interdisciplinary center for cyber security and cyber defense of critical infrastructure (aka C3I center at IIT Kanpur) has a research program that enables the development of various tools, methods, and information required by utilities to implement the NIST framework, and also become better positioned for cyber attacks. In a recent survey by Siemens and Ponemon Institute – it was found that in 2019, only about 42% of respondents involved in utilities claim that they have good readiness for cyber security. 54% of the respondents believe that there will be a major cyber attack on their installation within the next 12 months. This shows the urgency and immediacy for such developments.

C3I has developed various industry scale test beds that are the – first of their kind in India, for example – power distribution, power generation and synchronization of renewables with the grid, power transmission, multi-stage water treatment plants, and industrial manufacturing plants with discrete control testbeds on which cyber-security research is being carried out. These test-beds are controlled by multiple PLCs, various industrial protocols, as well as SCADA supervision and control. There are industrial automation products from all well-known manufacturers. This allows the center to do vulnerability assessment and penetration testing experiments (VAPT) – leading to the disclosure of over 15 critical to high vulnerabilities in industry products such as PLC, SCADA, RTU, etc. 8 of these disclosed vulnerabilities are already in the NVD database or ICSA database. More vulnerabilities are being discovered at the center. The penetration testing techniques being used are being automated into tools so that engineers can easily repeat such processes on their own industrial set up.

C3I also developed intrusion detection tools – both model driven – implemented on the PLC itself for detecting false data injection attacks – and data-driven – using machine learning models detecting anomalies in the physical signals of the plant dynamics themselves.

Malware analysis especially for zero-day malware has to be taken seriously. C3I has developed a multitarget malware analysis tool leveraging memory forensics, static and dynamic information of the executables, and network activity monitoring – which would allow all new executables to be first pass through malware detection/classification tool before being put into any equipment such as PLC/RTU or SCADA workstations. This malware analysis tool along with intrusion detection tools form the backbone of a 'detect' function.

Threat intelligence collection from open source feeds, and local honeypots, has provided us with a protect functionality – whereas a cyber-asset registration, management, and patching tool developed at C3I gives us part of the identify functional capability.

A http traffic monitoring and payload classification tool developed at C3I provides basic protection from manipulation of web services – noting the fact that web services form the basis of today's automation tools for remote configuration and monitoring.

In summary, the C3I center is aiming to develop comprehensive solutions with novel technological innovations so tools and methods are made available to implement the entire NIST framework. This talk will provide a glimpse of the research and development of translatable technologies at the C3I center.

Trust and Loyalty in AI

Shriram Revankar

Adobe Systems, Bengaluru, India
shriram.revankar@gmail.com

Trust and loyalty are common topics of social discourse and have been of great interest throughout the recorded history of our civilization. Although trust and loyalty have been explored well before the information technology era, they are often seen as extensions of each other and sometimes intertwined with faith and morality. The intent of this talk is to position them as computable entities that can continue to play as significant a role in today's human-machine collaborative societies as they played in human only environments. The importance of exploring computational mapping of trust and loyalty has increased owing to pervasive adoption of artificial intelligence (AI) in our social and work environment.

Trust plays a pervasive role in removing friction from a wide variety of social transactions. Without trust, the simplest of our day-to-day activities such as driving on roads or buying groceries become cumbersome activities. Early initiatives in establishing trust in a digital environment were based on assumptions of an adversarial world. Perimeter and network security, encryption, authentication, authorization, and access control were extensively used as means to establish trust and trusted environments. However, the prior art is sparse on computational mapping of loyalty. Stephen Marsh provides a formalism to trust as a computational concept. One may argue that this formalism incorrectly mixes aspects of loyalty with trust. In this talk, I explore both trust and loyalty as separable computational constructs in the context of AI.

Trust is defined as "willingness to be vulnerable under conditions of risk and interdependence." Although, there is no universal agreement on this definition of trust, the concept of 'risk and interdependence' provides us effective means to understand the state of the art in computational adaptation of trust. Trust in information technology has become important because people and societies extensively rely on IT for many day-to-day transactions.

I argue that the essential nature of risk and interdependence changes drastically with ubiquity of AI. Hence, much of the traditional trust mechanisms need to be explored anew. I propose that trust building mechanisms need to be integral to design of AI systems. An AI system should make the 'risk of dependence' learnable and explicit for humans to trust it. The trust building mechanism should assist a human to build an introspectable model of the AI system. The model in turn will enable humans to assess the risk of dependence and hence help establish the appropriate level of trust. I will illustrate this through examples and use cases.

Loyalty, on the other hand, has been either ignored or often confused as an extension of trust. Loyalty is defined as never mere emotion, but practical action for a cause. Hence loyalty comes into play when there is an action taken by an AI system on

our behalf. The action may yield a positive or a negative payoff. A loyal AI system therefore is expected to always achieve a positive payoff. While we may not usually ask if a piece of software is loyal to us, we should do so in the case of an AI system. Our dependence on AI systems is bidirectional, and an AI agent may proxy for us in making decisions. Kate Crawford described some of the negative payoffs (e.g. allocation harm and representational harm) an AI system may impart. There have been several studies that have exposed negative impacts of biases in AI systems.

The Simple assertion that AI systems should be loyal to whoever owns it or pays for it is not very useful for implementation and explicit evaluation of loyalty. Practical implications of a system being loyal and to who, and the problems loyalty poses are many. I will illustrate this through some practical examples and then argue for a game theory based computational realization for loyalty. I will also briefly talk about other efforts involved in minimizing the discriminatory negative payoffs from AI systems.

Igniting Digital Transformation

Anil Nair[1] and K P M Das[2]

[1] Cisco Systems, Mumbai, India
[2] Cisco Systems, Bengaluru, India
{nairanil,kpmdas}@cisco.com

Digital transformation: As the second fastest digitizing nation in the world, India has what can is commonly known as the two-third:one-third problem, which is that two thirds of the population resides in rural areas while they have access to only a third of the country's resources. The government recognizes this, and citizens are realizing too that India can alleviate the situation rapidly with smart digital interventions. Cisco too believes that digitization is implicit in the transformation of India and has invested substantially to advocate this in an initiative: CDA (Country Digital Acceleration). This is a part of a global program in 31 countries touching half the population of the globe. Under this program in India, Cisco invests in POCs (proof of concepts) that are aligned with the national agenda and include several projects under Digital India, Skill India, Start-up India, as well as Defence and Cyber Security. These POCs showcase digital possibilities to address the rapid/explosive/exponential and inclusive growth that India needs for accelerated growth. Some of the key themes in Cisco's CDA program are Education, Transportation, Agriculture, Rural Connectivity, Telemedicine, Smart Cities, Innovation Labs, Cyber Security, and Government. For each of the digital themes mentioned above, the foundation rests on an end-to-end Secure Knowledge Management architecture framework. Five key security architecture considerations to ponder are:

1. Is the architecture designed to stop threats at the perimeter of the knowledge system?
2. Can architecture protect knowledge workers and users wherever they are? (work and home environments are merging)
3. Can the architecture control who has access to the components of the knowledge system?
4. Is the architecture simple and integrated – not too fragmented?
5. Can security issues be discovered quickly and contained effectively?

Design of the secure knowledge management framework will rest on a few principles. These principles include, but are not limited to, the following:

- Zero Trust
- Never Trust – Always Verify
- Threats Pervasive, Persistent
- Default Least Privilege Access
- Dynamic Policies

The digital transformation of India has begun and our POCs under the CDA (Country Digital Acceleration) program showcase digital possibilities. Cisco is fully invested in this journey and aspires to spearhead the agenda not only to digitize India but secure it as it leapfrogs to a new level of prosperity as a Smart Nation.

Digital Payments Adoption by Low-Income Populations in Bangalore: Lessons from the Road

Srihari Hulikal Muralidhar[1] and Jacki O'Neill[2]

[1] Department of Digital Design and Information Studies, Aarhus University, Aarhus, Denmark
srihari@cc.au.dk
[2] Microsoft Research India, Bengaluru, India
jaoneil@microsoft.com

Digital payments, in recent years, have increasingly been promoted as a key driver of financial inclusion by various interests such as governments, philanthropic foundations, banks, and private players. Mobile money, it is argued, reduces transaction costs associated with physical banking and enables real-time transactions such as P2P transfers, bill payments, and so on. However, the actual successes of mobile money deployments at scale are limited. M-PESA in Kenya, which has been claimed to be the biggest success to date, has itself come under critique in recent times for various reasons. Nonetheless, the belief that "cashless technologies are the way to achieve an inclusive economy" has been guiding the Indian government as well and was, in fact, argued to be one of the main motivations for undertaking the controversial 'demonetization exercise'. On the one hand, we have macro-level data showing a steady increase in the use of UPI-based payments over the last three years. On the other, we are also confronted with data that shows we have not become less-cash, let alone 'cashless'. What are the ground realities on the adoption and use of digital payments in the country, especially among the low-income populations? What do we even mean by 'financial inclusion'? How can digital payments help achieve it? In this talk, we aim to shed light on some of these issues from our work with auto-rickshaw drivers in Karnataka, India. Our experiences have taught us that auto-rickshaw drivers, as low- and semi-literate, low-income, first-time smartphone, and digital money users, can tell us a lot about poverty, exclusion, and technology-use, and we aim to share some of them. We argue that the dominant understanding of 'financial inclusion' needs rethinking, a shift in emphasis towards 'why' or 'what for' from 'how'. The means by which we achieve financial inclusion should not make us lose sight of what we want to ultimately achieve with/by financial inclusion. It is also our contention that structural problems such as poverty and marginalization should not be reduced to a problem of 'lack of access' to bank accounts or technology. Digital payments, therefore, do not represent a 'magic bullet' that will help us achieve financial inclusion.

Contents

Social Networks