Information Sciences 318 (2015) 48–50

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Editorial

Special issue on Security, Privacy and Trust in network-based Big Data

1. Introduction

Recent advances in commoditization of hardware, mobile technologies, large-scale networks and cloud computing, have expedited the generation and collection of data and at the same time they have enhanced the ability to process large amounts of it. Nowadays, researchers in a wide range of fields are seeing great potential in gaining insights by analyzing large-scale data in their entirety. Apart from volume, which is obviously their cardinal attribute, the so called "Big Data" [1] possess a set of common characteristics that normally could not be dealt with existing data processing software and methodologies. On top of that, the analysis of Big Data may involve geographically distributed datasets, where transferring vast amounts of data is not an option.

It is therefore obvious that the variety, velocity and volume of Big Data not only augments security and privacy management challenges, as they are commonly addressed in traditional security management, but also generates new ones that need to be dealt in a special way. For instance, Big Data repositories store information gathered by various sources scattered across an organization. This variety and heterogeneity of data constitutes secure access management a major challenge due to the different access restrictions and security policies that may apply per distinct source, making it cumbersome to balance appropriate security with the need to aggregate and distil meaning from the data. Also, the attack surface for an adversary is increased proportionally to the number of data sources, i.e., one attack vector per source is made available for an aggressor attempting to gain access to a data cluster. It is also to be stressed that due to the large volume of data stored, a breach on such data may bear catastrophic consequences; it will affect a significantly greater number of people, with repercussions spanning from reputational risks to significant legal consequences. Organizations also need to cope with several types of users each one requiring access to a specific subset of information. Hence, for example, the encryption solution one chooses to safeguard the data needs to coincide this new status quo. A high degree of granularity in access control is also required to make sure users are able to only access pieces of data they are authorized to obtain. Having all the above into mind, Big Data is often regarded as a security distress.

Moreover, one of the biggest challenges for Big Data is the protection of end-user's privacy as such systems frequently contain a tremendous amount of Personal Identifiable Information (PII). So, a major question arises; what access policy and privacy-preservation mechanisms should be enforced to ensure adequate security? Removing PII instances from Big Data is not an easy task, especially if the data are unstructured. To do so, one has to firstly identify the sensitive pieces of information contained in their Big Data and then delicately detach or isolate this information to ensure compatibility. For this reason, often security requirements in Big Data realms need to be dealt on a case-by-case basis. According to the work in [2], there are five major considerations for one to take into account when dealing with Big Data from a security point of view: anonymisation; encryption; access control and monitoring; policy; and governance frameworks.

Taking all the above into account there is no room for getting Big Data security and privacy as an afterthought or something you worry about at the end. Instead it is imperative to be addressed and embedded in the rest of each system's components from the beginning. This is sure to lead to a far more secure system overall.

The aim of the special issue was to present leading edge work concerning privacy protection issues and security challenges in the rapidly emerging field of network-based Big Data. Research that addresses organisational and enterprise solutions for privacy protection and information security in Big Data environments was also in scope of the SI. Consequently, all works dealing with fundamental theory, techniques, applications, and practical experiences concerning secure Big Data were considered. It is expected that the special issue will stimulate further related research and technology improvements in this significant and timely subject.

http://dx.doi.org/10.1016/j.ins.2015.05.040

2. Submissions

This special issue presents high-quality articles describing: a graph-based comprehensive reputation model for social commerce, a transmission protocol for secure big data in two-hop wireless networks, a method for obtaining trustworthy answers for queries on uncertain big data in decision making, a method to detect anomalies in big network traffic data, an ID-based generalized signcryption method to obtain confidentiality or/and authenticity in big data, and an efficient trust computation scheme for large-scale mobile social networks, all for use in the network-based big data environment. We received a total of 29 submissions, and after a rigorous review process, we selected 6 articles covering the subject from different perspectives, i.e., 21% of all the submitted papers.

The first manuscript, "A Graph-Based Comprehensive Reputation Model: Exploiting the Social Context of Opinions to Enhance Trust in Social Commerce" by Su-Rong Yan, Xiao-Lin Zheng, Yan Wang, William Wei Song, Wen-Yu Zhang, focuses on social commerce and argues that due to the open and dynamic nature of social media infrastructure, the governance structures of this type of commerce are as a rule of thumb realized via reputation mechanisms. The authors observe that so far the prediction of trust in future interactions are based on personal observations and publicly shared information. The paper proposes a new graph-based reputation model to create trust by fully exploiting the social context of opinions based on the activities and relationship networks of opinion contributors. Their model incorporates the behavioral activities and social relationship reputations of users to combat the scarcity of first-hand information and identifies a set of critical trust factors to mitigate the subjectivity of opinions and the dynamics of behaviors. Moreover, the authors provide experimental results that demonstrate the superiority of their proposal against similar solutions.

In the second paper by H.T.H. Nguyen and Jinli Cao, entitled "Trustworthy answers for top-k queries on uncertain big data in decision making", revolves around the fact that nowadays many organizations or enterprises have realized that the inherent valuable knowledge extracting from large volumes of data can help them to analyse and improve business performance. As a result, effectively extracting reliable and trustable information from big data has become strategically important for large business enterprises. This paper proposes a novel approach which combines the benefits of the skyline and the dominating top-k query semantics to provide trustable and reliable data for ranking queries over big data. The outcome of the research can derive intelligence and useful knowledge to support data analysis and decision making. It is also guaranteed the effectiveness of the proposed algorithms using a number of pruning rules to reduce the search space and terminate the search as early as possible.

The third paper, "Detecting Anomalies from Big Network Traffic Data Using an Adaptive Detection Approach" by Ji Zhang, Qigang Gao, Hai Wang, Yonglong Luo. In this paper, authors study the problem of anomaly detection in big network connection data sets and propose an outlier detection technique, called Adaptive Stream Projected Outlier deTector (A-SPOT), to detect anomalies from large data sets using a novel adaptive subspace analysis approach. A case study of A-SPOT is conducted in this paper by deploying it to the 1999 KDD CUP anomaly detection application. Innovative approaches for training data generation, anomaly classification and false positive reduction are proposed in this paper as well to better tailor A-SPOT to deal with the case study. Experimental results demonstrate that A-SPOT is effective and efficient in detecting anomalies from network data sets and outperforms existing detection methods.

The fourth contribution, entitled "Obtain Confidentiality or/and Authenticity in Big Data by ID-based Generalized Signcryption" by Guiyi Wei, Jun Shao, Yang Xiang, Pingping Zhu, Rongxing Lu.

In this paper, authors propose a new identity-based generalized signcryption scheme to solve the above problems. In particular, it has the following two properties to fit the efficiency requirement. (1) It can work as an encryption scheme, a signature scheme or a signcryption scheme as per need. (2) It does not have the heavy burden on the complicated certificate management as the traditional cryptographic schemes. Furthermore, our proposed scheme can be proven-secure in the standard model.

The fifth paper, "K-FuzzyTrust: Efficient Trust Computation for Large-scale Mobile Social Networks using a Fuzzy Implicit Social Graph" by Shuhong Chen, Guojun Wang, Weijia Jia. The paper proposes an algorithm for detection of community structure in complex networks under fuzzy degree κ and construct a fuzzy implicit social graph. It then constructs a mobile social context including static attributes (such as user profile and prestige) and dynamic behavioural characteristics (such as user interaction partners, interaction familiarity, communication location and time) based on the fuzzy implicit social graph. Authors discuss the aggregation and propagation of trust values for overlapping users and indirect connected users. Further, they evaluate the performance of κ-FuzzyTrust in simulations. The results show the validity of our fuzzy inference mechanism for behavioural trust relationships in MSNs. They also demonstrate that κ-FuzzyTrust can infer trust values with high precision.

The last paper "Universal Designated Verifier Transitive Signatures for Graph-based Big Data" by Shuquan Houa, Xinyi Huanga, Joseph K. Liuc, Jin Li and Li Xu. Authors propose a new type of digital signatures which is specifically designed for graph-based big data system. The properties of the proposed signatures are twofold. On one side it possesses the features of transitive signatures: One can sign a graph in such a way that, given two signatures on adjacent edges, anyone with public information can compute a signature on edge. On the other side, it is universal designated verifiable: It allows any signature holder to prove to a designated verifier that a message has been signed by the signer, but the verifier cannot convince (even sharing all secret information) any other third party of this fact. The signature method can efficiently address privacy issues associated with dissemination of transitive signatures of graph-based big data.

Acknowledgements

The guest editors would like to express their thanks to the Elsevier's Information Sciences Editor in Chief Professor Witold Pedrycz for giving them the opportunity to edit this special issue on "Security, Privacy and Trust in network-based Big Data". Also, we gratefully thank the authors for submitting their work as well as the tireless reviewers who have constructively evaluated the papers within the stipulated time. Finally, we sincerely hope the reader will share our view and find this special issue very useful.

References

[1] Min Chen, Shiwen Mao, Yunhao Liu, Big Data: a survey, Mobile Networks Appl. 19 (2) (2014) 171–209.
[2] Guillermo Lafuente, The Big Data security challenge, Network Security 2015 (1) (2015) 12–14.

Guest Editors

Hua Wang
Centre for Applied Informatics, College of Engineering and Science, Victoria University, Australia
E-mail address: hua.wang@vu.edu.au

Xiaohong Jiang
School of Systems Information Science, Future University Hakodate, Japan
E-mail address: jiang@fun.ac.jp

Georgios Kambourakis
Dept. of Information and Communication Systems Engineering, University of the Aegean, Greece
E-mail address: gkamb@aegean.gr

Hua Wang is a full time professor in Victoria University, Australia. Dr Wang awarded a PhD degree in Computer Science from the University of Southern Queensland in 2004. He has been active in the areas of Information Systems Management, Distributed Database Management Systems, Access Control, Software Engineering and Electronic Commerce. He has participated in research projects on mobile electronic system, Web service, and role-based access control for Electronic service system, and has already published over 155 research papers.

Xiaohong Jiang is currently a full professor of Future University Hakodate, Japan. Before joining Future University, Dr.Jiang was an Associate professor, Tohoku University, from Feb.2005 to Mar.2010. Dr. Jiang's research interests include computer communications networks, mainly wireless networks and optical networks, reliable network design, interconnection networks for massive parallel computing systems, routers/switches design for high performance networks, etc. He has published over 260 technical papers at premium international journals and conferences including 60 papers published in top IEEE journals and top IEEE conferences. He is a Senior Member of IEEE, a Member of ACM and IEICE.

Georgios Kambourakis received Ph.D. in Information and Communication Systems Engineering from the dept. of Information and Communications Systems Engineering, University of the Aegean. He also holds a Master of Education degree from the Hellenic Open University. Currently, he is an Assistant Professor at the department of Information and Communication Systems Engineering, University of the Aegean, Greece. His research interests are in the fields of mobile and wireless networks security and privacy, VoIP security, DNS security, and m-learning and he has more than 100 publications in the above areas. He has been involved in several national and EU funded R&D projects in the areas of Information and Communication Systems Security.