Guest Editorial Preface

Special Issue of Big Data and Computing Security

Lidong Zhai, Institute of Computing Technology, Chinese Academy of Science, China
Tao Han, University of North Carolina, Charlotte, USA
Ning Zang, Texas A&M University at Corpus Christi, USA

With more devices connected to the Internet, cyber attacks are becoming more frequent. Attacks may cause big data loss, information leakage, and network security operations. Big data security threats exist in all aspects of the big data industry chain, such as data production and collection, processing and sharing. These problems will cause many annoyances to people's lives, such as privacy and safety, and even personal safety. Big data technology is a double-edged sword, which can not only benefit society and the people, but also be used by some people to harm the various property of public citizens.

The organizers of this special issue of Big Data and Computing Security is aimed at paying great attention to the security issues in the field of big data, and arouse scholars' research focus on this new topic. As a result, this special issue extends the theory and practice of big data security technological environments. It fulfills the need for stimulating critical debate on and research into theories, approaches, principles, applications and the implementation of big data security learning.

The six papers in this special issue cover a wide range of aspects of big data security, from case studies in recommendation algorithms with nature language, to the designing of cyberspace security talents training system based on knowledge graph. Each of these revised and extended papers has undergone full double blind peer review, prior to being selected for this special issue.

The paper from Xin Liu addresses a critical and entertaining issue problem-SLU (Spoken Language Understanding) for task-oriented SDS (spoken dialogue system). He propose a joint model based attention mechanism, Bi-LSTM and CRF for Intent Detection and Slot Filling, and make an analysis of how the jointly task can benefit from the contextual information of the Chinese queries within a session. To use both past and future input features efficiently, a bidirectional Long Short-Term Memory model (Bi-LSTM) with contextual information is employed to learn the representation of each time step. The experimental results show the joint model outperforms the separate models for both tasks, and achieves competitive performance on both tasks. Overall, this paper, apparently, is suitable for publication in our particular journal.

In "A Light Recommendation Algorithm of We-Media Articles Based on Content", Xin Zheng addresses an important and interesting recommendation system based on wechat official articles. She propose a light recommendation algorithm based on LSTM and LDA, and make an analysis of how to make recommend from the reading history of articles. The experimental results show the light recommendation algorithm outperforms the non-personalized and traditional collaborative filtering recommendation method.

In recent years, the sharing of cyber security threats intelligence has received increasing attention from national network security management organizations and network security enterprises. Academia and industry have conducted research on threat intelligence analysis and sharing. In this paper "A Summary of the Development of Cyber Security Threat Intelligence Sharing", Lili Du first introduces

the value and significance of threat intelligence. Then it introduces the commonly used threat intelligence analysis model. Then it organizes and classifies the threat intelligence sharing norms and threat intelligence vendors. Then it starts from the main problems faced by threat intelligence sharing. A solution to build regional network security capabilities. Finally, the future research direction of threat intelligence sharing is expected.

Prathap Rudra Boppuru examines the news feed data collected from various sources regarding crime in India and Bangalore city. The crimes are then classified on the geographic density and the crime patterns such as time of day to identify and visualize the distribution of national and regional crime such as theft, murder, alcoholism, assault, etc. In total, 68 types of crime-related dictionary keywords are classified into 6 classes based on the news feed data collected for 1 year. Kernel Density Estimation method is used to identify the hotspots of crime. With the help of the ARIMA model, time series prediction is performed on the data.

With the promotion of online education, the adaptive learning system has attracted attention due to its good curriculum recommendation function. In this paper "Research on the Construction of Student Model of Adaptive Learning System Based on Cognitive Diagnosis Theory", Yang Zhao explore the student model between the adaptive learning system and the user, reflecting the individual characteristics, knowledge status, and cognitive ability of the student. The accuracy of the information in the student model directly affects the quality of the system recommendation service. The traditional student model only judges students based on the basic information and simple test scores. This paper introduces the self-adaptive item bank and adaptive item selection strategy based on the cognitive diagnosis theory, and dynamically detects the students' knowledge and analyzes the state according to the answering habits and knowledge mastering status of different students. This paper analyzes and contrasts a variety of traditional cognitive diagnosis theories, and proposes a mixed cognitive diagnosis question bank and a selection strategy model to provide strong support for the construction of student models.

In Xi Chen's paper "Design of Cyberspace Security Talents Training System Based on Knowledge Graph", she explores the development in internet, big data and global society, economy, life, politics, military and culture. Cyberspace security has become the most complex, comprehensive and severe non-traditional security challenge facing all countries in the world. However, the scarcity of talents in the field of cyberspace security cannot satisfy the practical needs of the development of cyberspace security. This paper puts forward the training scheme of network security talents, discusses the relationship between knowledge atlas and network space security, provides the construction and distribution of network space stuffed by knowledge atlas, and then constructs a education big data architecture for cyberspace security based on knowledge graph around the use of knowledge.

As the guest editor of this special issue of Big Data and Computing Security, I'm proud to bring you all these good papers. We hope that reading these high-quality papers will inspire you to make your own submissions to future conferences.

May these contributions pave the way for the broad and open waters ahead with all the new developments in big data and computing security!

Lidong Zhai
Guest Editor
IJDCF