The 7th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2021)

The 7th IEEE International Conference on High Performance and Smart Computing (IEEE HPSC 2021)

The 6th IEEE International Conference on Intelligent Data and Security (IEEE IDS 2021)

May 15-17, 2021
New York, USA

Conference Program and Information Booklet

Organized By
IEEE BIGDATASECURITY/HPSC/IDS 2021 Committee

Sponsored By
IEEE Longxiang High Tech
IEEE Computer Society
IEEE TCSC
IEEE STC Smart Computing
North America Chinese Talents Association
Welcome to IEEE Computer Society Smart Computing Special Technical Community (SCSTC)

IEEE SCSTC is built up for changing people’s future work and life; attracting intelligent computing talents in smart computing field; producing high quality research work and services in human-centric technologies to change the world; leading the research of smart computing by solving challenging problems; and expanding the smart computing community in a self-sustainable financial way. Two main layers are involved in the concept of smart: one is the traditional optimization; the other one is the intelligent living.

Vision: IEEE Computer Society Smart Computing STC is to enable smart life with smart data, smart cloud, and smart security and become a community leader in these technical fields.

We will create a smart computing society for changing people’s future work and life; attract intelligent computing talents in smart computing field; produce high quality research work and services in human-centric technologies to change the world; lead the research of smart computing by solving challenging problems; and expand the smart computing community in a self-sustainable financial way. Two main layers are involved in the concept of smart: one is the traditional optimization; the other one is the intelligent living.

Mission: IEEE Computer Society Smart Computing STC is to utilize smarting computing technologies to increase humans’ life by integrating smart data, smart cloud, and smart security in both optimizations and intelligences. We will build up the largest professional and academic community in smart computing and aim to enhance humans’ life by utilizing smart computing technologies. This expected community will be providing an integrative research platform for global researchers who are interested in smart computing that covers both optimizations and intelligent living. The target area is a convergence of three novel dimensions at the collaborative application layer, namely smart data, smart cloud, and smart security. This is a social network-based community that is planned to be a long-term self-sustaining organization.

Purpose: The main purpose of this proposed STC is to serve the smart computing research community and advance the research by covering three dimensions, including smart data, smart cloud, and smart security. Current existing STCs cannot satisfy the demands of research interests in convergences of multiple disciplines, which include data, cloud computing, and security. Most existing STCs only have isolative focus in one specific field. However, data, cloud computing, and security are becoming strongly tied techniques, which are hard to separately considered for many contemporary researches or future technical development. Therefore, building up a STC in Smart Computing has an urgent demand for both smart computing research and professional practices.

Scope: the scope of Smart Computing STC is a technical group within the Computer Society. Term Smart in “Smart Computing” mainly covers two aspects, including optimizations and intelligence, by which smart concept will be adopted for new networking-oriented technologies. We are looking for intelligent approaches gaining optimal performances by high-speed data mining and data analysis throughout all aspects in distributed computing and integrated systems. Both aspects are strongly relevant to the performance of the system at the application layer during the process of data transmissions within the distributed environment. This concentration emphasizes the optimizations and intelligences of networking performances and empowers the capabilities of the connected computing devices in distributed systems, which distinguishes from other societies or communities.

Activities: IEEE Computer Society Smart Computing STC organizes a bunch of research community-oriented activities. We aim to unionize scholars or students who have similar or relevant research interests in smart computing and grow the research community globally. Our memberships owners will have a great opportunity to build up an active social network and strengthen the knowledge scope throughout the following activities:

- Improve communications and interconnections between peers.
- Explore the theory, applications, implementations, and research of smart computing.
- Publish whitepapers, reports, technical manual, and handbooks on research, policies, standards, products, services, and applications.
- Organize conferences and workshops that are related to smart computing.
- Release newsletters with updated news regularly.
- Host academic publications focusing on smart computing.
- Develop smart computing standards.
- Standardize the mechanisms, operating principles, and industrial manual guidelines.

Official Permanent Site: https://stc.computer.org/smart-stc/
### IEEE BigDataSecurity/HPSC/IDS 2021 Program at a Glance

#### Saturday, May 15th, 2021

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:45 – 9:00</td>
<td>Opening</td>
<td>Conference Room</td>
</tr>
<tr>
<td>9:00 – 10:00</td>
<td>Keynote 1</td>
<td></td>
</tr>
<tr>
<td>10:00 – 10:10</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>10:10 – 11:10</td>
<td>Keynote 2</td>
<td></td>
</tr>
<tr>
<td>11:10 – 11:20</td>
<td>Award Session</td>
<td></td>
</tr>
<tr>
<td>11:20 – 12:20</td>
<td>BDS Session 1</td>
<td></td>
</tr>
<tr>
<td>12:20 – 13:30</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>13:30 – 14:30</td>
<td>BDS Session 2</td>
<td></td>
</tr>
<tr>
<td>14:30 – 15:30</td>
<td>BDS Session 3</td>
<td></td>
</tr>
<tr>
<td>15:30 – 15:50</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>15:50 – 16:50</td>
<td>HPSC Session 1</td>
<td></td>
</tr>
<tr>
<td>16:50 – 17:50</td>
<td>IDS Session 1</td>
<td></td>
</tr>
</tbody>
</table>

#### Sunday, May 16th, 2021

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 – 10:00</td>
<td>BDS Session 4</td>
<td></td>
</tr>
<tr>
<td>10:00 – 11:00</td>
<td>BDS Session 5</td>
<td></td>
</tr>
<tr>
<td>11:00 – 12:00</td>
<td>HPSC Session 2</td>
<td></td>
</tr>
<tr>
<td>12:00 – 13:00</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>13:00 – 14:00</td>
<td>IDS Session 2</td>
<td></td>
</tr>
<tr>
<td>14:00 – 15:00</td>
<td>IDS Session 3</td>
<td></td>
</tr>
</tbody>
</table>

### Registration:


### Presentation Online Rooms:

Zoom
([https://zoom.com.cn/j/83365988614?pwd=TIZEK3FLa3JsTDJoUFZ6d2hTNktpUT09](https://zoom.com.cn/j/83365988614?pwd=TIZEK3FLa3JsTDJoUFZ6d2hTNktpUT09))

### Important Notice:

Due to the outbreak of COVID-19, this year the IEEE BigDataSecurity/HPSC/IDS will be a virtual conference online. For all participants, please do notice all the time mentioned in this booklet is based on the time zone of east USA which is **Eastern Daylight Time (EDT)**, UTC -4.
May 15th, 2021, 9:00 AM, Eastern Daylight Time (EDT), UTC -4

Topic: Privacy in the Era of Big Data, Machine Learning, IoT, and 5G

Prof. Elisa Bertino
Purdue University, USA

Bio: Elisa Bertino is the Samuel D. Conte Professor of Computer Science at Purdue University. She serves as Director of the Purdue Cyberspace Security Lab (Cyber2SLab). In her role as Director of Cyber2SLab she leads multi-disciplinary research in data security and privacy. Prior to joining Purdue, she was a professor and department head at the Department of Computer Science and Communication of the University of Milan. She has been a visiting researcher at the IBM Research Laboratory (now Almaden) in San Jose and visiting professor at the Singapore Management University and the National University of Singapore. Her recent research focuses on cybersecurity and privacy of cellular networks and IoT systems, and edge analytics and machine learning for cybersecurity. Elisa Bertino is a Fellow member of IEEE, ACM, and AAAS. She received the 2002 IEEE Computer Society Technical Achievement Award for "For outstanding contributions to database systems and database security and advanced data management systems", the 2005 IEEE Computer Society Tsutomu Kanai Award for "Pioneering and innovative research contributions to secure distributed systems", the 2014 ACM SIGSAC Outstanding Contributions Award with citation "For her seminal research contributions and outstanding leadership to data security and privacy for the past 25 years", and the 2019-2020 ACM Athena Lecturer Award. She is currently serving as ACM Secretary-Treasurer.

Abstract: Technological advances, such as IoT devices, cyber-physical systems, smart mobile devices, data analytics, social networks, and increased communication capabilities are making possible to capture and to quickly process and analyze huge amounts of data from which to extract information critical for many critical tasks, such as healthcare and cyber security. In the area of cyber security, such tasks include user authentication, access control, anomaly detection, user monitoring, and protection from insider threat. By analyzing and integrating data collected on the Internet and the Web one can identify connections and relationships among individuals that may in turn help with homeland protection. By collecting and mining data concerning user travels, contacts and disease outbreaks one can predict disease spreading across geographical areas. And those are just a few examples. The use of data for those tasks raises however major privacy concerns. Collected data, even if anonymized by removing identifiers such as names or social security numbers, when linked with other data may lead to re-identify the individuals to which specific data items are related to. Also, as organizations, such as governmental agencies, often need to collaborate on security tasks, data sets are exchanged across different organizations, resulting in these data sets being available to many different parties. Privacy breaches may occur at different layers and components in our interconnected systems. In this talk, I first present an interesting privacy attack that exploits paging occasion in 5G cellular networks and possible defenses. Such attack shows that achieving privacy is challenging and there is no unique technique that one can use; rather one must combine different techniques depending also on the intended use of data. Examples of these techniques and their applications are presented. Finally, I discuss the notion of data transparency – critical when dealing with user sensitive data, and elaborate on the different dimensions of data transparency.
IEEE BigDataSecurity/HPSC/IDS 2021 Keynotes

May 15th, 2021, 10:10 AM, Eastern Daylight Time (EDT), UTC -4

**Topic: SecAI: Integrating Cyber Security and Artificial Intelligence**

**Prof. Bhavani Thuraisingham**
The University of Texas at Dallas, USA

**Bio:** Dr. Bhavani Thuraisingham is the Founders Chaired Professor of Computer Science and the Executive Director of the Cyber Security Research and Education Institute at the University of Texas at Dallas. She is also a visiting Senior Research Fellow at Kings College, University of London and a Fellow of the ACM, IEEE, the AAAS, the NAI and the BCS. She has received several awards including the IEEE CS 1997 Technical Achievement Award, ACM SIGSAC 2010 Outstanding Contributions Award, and the ACM SACMAT 10 Year Test of Time Awards for 2018 and 2019. She co-chaired the Women in Cyber Security Conference (WiCyS) in 2016 and delivered the featured address at the 2018 Women in Data Science (WiDS) at Stanford University and has chaired several conferences for ACM and IEEE. Her 39 years career included industry (Honeywell), federal laboratory (MITRE), US government (NSF) and US Academia. Her work has resulted in 130+ journal articles, 300+ conference papers, 140+ keynote and featured addresses, six US patents, fifteen books as well as technology transfer of the research to commercial and operational systems. She received her PhD from the University of Wales, Swansea, UK, and the prestigious earned higher doctorate (D.Eng) from the University of Bristol, UK.

**Abstract:** Artificial Intelligence (AI) emerged as a field of study in Computer Science in the late 1950s. Researchers were interested in designing and developing systems that could behave like humans. This interest resulted in substantial developments in areas such as expert systems, machine learning, planning systems, reasoning systems and robotics. However, it is only recently that these AI systems are being used in practical applications in various fields such as medicine, finance, marketing, defense, and manufacturing. The main reason behind the success of these AI systems is due to the developments in data science and high-performance computing. For example, it is now possible collect, store, manipulate, analyze and retain massive amounts of data and therefore the AI systems are now able to learn patterns from this data and make useful predictions. While AI has been evolving as a field during the past sixty years, the developments in computing systems and data management systems have resulted in serious security and privacy considerations. Various regulations are being proposed to handle big data so that the privacy of the individuals is not violated. For example, even if personally identifiable information is removed from the data, when data is combined with other data, an individual can be identified. Furthermore, the computing systems are being attacked by malware resulting in disastrous consequences. In order words, as progress is being made with technology, the security of these technologies is in serious question due to the malicious attacks. Over the decade, AI and Security are being integrated. For example, machine learning techniques are being applied to solve security problems such as malware analysis, intrusion detection and insider threat detection. However, there is also a major concern that the machine learning techniques themselves could be attacked. Therefore, the machine learning techniques are being adapted to handle adversarial attacks. This area is known as adversarial machine learning. Furthermore, while collecting massive amounts of data causes security and privacy concerns, big data analytics applications in cyber security is exploding. For example, an organization can outsource activities such as identity management, intrusion detection and malware analysis to the cloud. While AI techniques are being applied to solve cyber security problems, the AI systems have to be protected. For example, how can the machine learning systems be protected from the attacks? What are the threats to the planning systems? How can expert system carry out their functions in the midst of malware attacks? What are the appropriate access control models for AI systems? How can we develop appropriate security policies for AI systems? These are questions that researchers are beginning to provide answers to. To assess the developments on the integration of AI and Security over the past decade and to determine future directions, the presentation will focus on two major questions: (i) how can the developments in AI techniques be used to solve security problems and (ii) how can we ensure that the AI systems are secure and (iii) what are the security and privacy considerations for AI systems. Second, it will describe the application of AI including machine learning for cyber security applications such as insider threat detection. Third, it will discuss the trends in areas such as adversarial machine learning that take into consideration the attacker’s behavior in developing machine learning techniques. Fourth, it will discuss some emerging trends in carrying out trustworthy AI so that the AI techniques can be secured against malicious attacks. Fifth, it will focus on the privacy threats due to the collection of massive amounts of data and potential solutions. Finally, it will discuss the next steps.
The 7th IEEE International Conference on Big Data Security on Cloud (IEEE BigDataSecurity 2021)

**BIGDATASECURITY 1:** 15/05/2021, Online Conference, 11:20 - 12:20
- Aidong Xu, Tao Wu, Yunan Zhang, Zhiwei Hu and Yixin Jiang. Graph-Based Time Series Edge Anomaly Detection in Smart Grid
- Dae-young Kim and Karuna Pande Joshi. A Semantically Rich Knowledge Graph to Automate HIPAA Regulations for Cloud Health IT Services
- Lixia Li, Wei Peng, Yonglu Li, Huifang Liu, Ying Wang, Zhijie Chen, Xiuping Ouyang, Min Lin and Haining Ye. Community detection of mobile Internet delivery users
- Zhuoyi Wang, Yu Lin, Yifan Li, Feng Mi, Zachary Tian, Latifur Khan and Bhavani Thuraisingham. Unsupervised Perturbation based Self-Supervised Adversarial Training

**BIGDATASECURITY 2:** 05/15/2021, Online Conference, 13:30 - 14:30
- Shuang Xie, Yujie Hong, Xiangdie Wang and Jie Shen. Research on data security technology based on blockchain Technology
- Mingyue Xie, Shuyu Chen and Jun Liu. Improvement of the DPoS Consensus Mechanism in Blockchain Based on PLTS
- Ankur Nagar, Lavanya Elluri and Karuna Pande Joshi. Automated Compliance of Mobile Wallet Payments for Cloud Services
- Xiaoyan Chen. Research on Big Data Value Creation System Applied to CPS

**BIGDATASECURITY 3:** 05/15/2021, Online Conference, 14:30 - 15:30
- Ziheng Zhou, Lin Li and Xu Zhao. Webshell Detection Technology Based on Deep Learning
- Wenyi Yang, Wenhui Hu, Yingjie Liu, Yu Huang, Xueyang Liu and Shikun Zhang. Research on Bootstrapping Algorithm for Health Insurance Data Fraud Detection Based on Decision Tree
- Hong Guo, Yining Li, Fang Liu, Tianyi Liu and Wei Hu. Machine-Learning based MOOC learning data analysis

**BIGDATASECURITY 4:** 05/16/2021, Online Conference, 9:00 - 10:00
- Weihang Cui and Pan Gao. Filtration method of DDoS attacks based on time-frequency analysis
- Fatema Rashid and Ali Miri. User and Event Behavior Analytics on Differentially Private Data for Anomaly Detection
- Hong Guo, Liu Tianyi, Fang Liu, Yining Li and Wei Hu. Chinese text classification model based on Bert and capsule network

**BIGDATASECURITY 5:** 05/16/2021, Online Conference, 10:00 - 11:00
- Qiang Wang, Jiawei Jiang, Yongxin Zhao, Weipeng Cao, Chunjiang Wang and Jiyong Zhang. Algorithm selection for software verification based on adversarial LSTM
- Guidong Wu, Hang Li, Xiaqiao Liao, Yuemeng Li, Yu Huang and Xiang Chen. An Automatic and Unified Consistency Verification Rule and Method of SG-CIM Model
The 7th IEEE International Conference on High Performance and Smart Computing (IEEE HPSC 2021)

**HPSC 1:** 05/15/2021, Online Conference, 15:50 – 16:50
- Yihang Gao, Peng Su, Hui Zhao and Meikang Qiu. Research On Sentiment Dictionary Based On Sentiment Analysis In News Domain
- Jun Liu, Sule Tang, Chuang Ma, Sishi Qin, Wei Li and Aidong Xu. A community detection algorithm based on discrete mixed fruit fly optimization

**HPSC 2:** 05/16/2021, Online Conference, 11:00 - 12:00
- Sudiksha Das. A Smart Solution with Ignition Interlock Device to Prevent Drunk-Driving Accidents
- Qiaohong Wu, Weidong Xiao, Peiyuan Zhu and Xihua Chen. A Data Privacy and Authentication Scheme Based on Internet of Vehicles
- Xiao Chen. Energy-efficient Smart Parking for Self-driving Vehicles

The 6th IEEE International Conference on Intelligent Data and Security (IEEE IDS 2021)

**IDS 1:** 05/15/2021, Online Conference, 16:50 - 17:50
- Han Deng, Zhechon Wang and Yazhen Zhang. Overview of privacy protection data release anonymity technology
- Jack D’Agostino and Gokhan Kul. Toward Pinpointing Data Leakage from Advanced Persistent Threats
- Xiaoyan Chen. Research on Secret Sharing Scheme in CPS Environment

**IDS 2:** 05/16/2021, Online Conference, 13:00 - 14:00
- Alan Hong, Weidong Xiao and Jiangling Ge. Big Data Analysis System Based on Cloudera Distribution Hadoop
- Han Deng, Fei Fang and Yazhen Zhang. A Cloud Data Storage Technology for Alliance Blockchain Technology
- Zihan Zhang, Jianfei Jiang, Qin Wang, Zhigang Mao and Naifeng Jing. A Mapping Method for Reconfigurable Array based on Decoupled DataFlow
- Angel Castro and Alexander Perez-Pons. Virtual Assistant for Forensics Recovery of IoT Devices

**IDS 3:** 05/16/2021, Online Conference, 14:00 - 15:00
- Xiyue Liu, Xin Feng and Pan Pan. GANN: A Graph alignment neural network for video partial copy detection
- Daniyar Sultan. Cyberbullying and Hate Speech Detection on Kazakh-Language Social Networks
- Yue Wang, Xinlian Zhou, Shiwen Zhang and Wei Liang. Human Mobility Model in Mission-Oriented Opportunistic Networks
- Griffith Samore, Jonah Bates and Xiao Chen. Improving Satisfaction in Crowdsourcing Platforms