Journal of Cybersecurity and Privacy

MDPI

Editorial

Journal of Cybersecurity and Privacy: A New Open Access Journal

Danda B. Rawat

Data Science and Cybersecurity Center, Department of Electrical Engineering and Computer Science, Howard University, Washington, DC 20059, USA; db.rawat@ieee.org or danda.rawat@howard.edu

Received: 1 March 2021; Accepted: 17 March 2021; Published: 19 March 2021

check for updates

The Cybersecurity and Privacy field has been one of the most critical parts of our lives and modern society at large. With the evolution of computing, communications, lightweight handheld devices and smart things/devices in the Internet of Things (IoT), we have networked services with anywhere-at-anytime connectivity for different applications such as smart transportation, production and manufacturing, logistics, energy, healthcare, utility, recreation, social and many other domains [1–3]. Furthermore, advancements in computing, communications and control engineering help cyber systems to monitor and control physical systems/operations in a real time manner for emerging cyber physical systems (CPS) [1,4–6]. However, the massive number of connections in IoT/CPS brings new security vulnerabilities and privacy challenges [1,2,5,7–10]. Thus, cybersecurity and privacy are critical to such connected systems to offer secure and trustworthy networked services [2,5,7].

When the Internet was created, cybersecurity was not part of the initial requirements, since the fundamental Internet protocols did not include measures against users attacking one another using communications and computing devices [11]. However, lately, hundreds of billions of dollars are spent on cybersecurity every year to combat cyber-attacks. People's lives are relying on smart sensors and connected systems, such as water infrastructure [8], smart energy grid [4,12,13], smart transportation [1,9,14,15], e-health [7] and wireless systems [16], among others, more new security and privacy challenges are emerging. In some applications, security and privacy are contradicting to each other, such as in vehicular communications; when the identity of vehicles (which is linked with driver/owner/renter) is used, the privacy of the driver/owner/renter could be easily compromised, and when anonymous identity is used for vehicular communications to provide privacy, achieving authentication and trustworthy secure communication becomes challenging. Thus, we need to consider a tradeoff while designing such techniques for privacy-aware security. Furthermore, many emerging applications need a real-time response to control the operations; to address these issues related to latency, cyber defense solutions should be light-weight and usable for such systems.

Cyber-attacks can be launched from anywhere through connected systems and the highly interconnected systems apart from the obvious advantages bring major issues too as a higher number of easily accessed malware targets. Meanwhile, the jurisdiction authorities need to obtain legitimate access to the systems/data under the laws ruling the specific region. Thus, it is very important to protect networked systems by considering all aspects of cyber-attacks. Furthermore, networked systems can be used by enemies for cyber-warfare, state-sponsored intelligence activities and criminal activities. If, or when, World War III happens, it is predicted to be in the cyber-space, or it will be leveraging cyber-attacks to destroy or disable the nation's critical infrastructure. For example, instead of destroying a country's energy grid systems by physical bombs to disable the enemy's power systems, coordinated cyber-attacks will be launched to disable the smart energy grid [12,13]. Similarly, instead of closing the main sources of water supply of the country/city/military-facility, the enemy could contaminate the water with deadly chemicals though connected water infrastructure [8]. Likewise, smart vehicles can be used to create traffic jams and scaled traffic accidents. Thus, the country's

smart critical infrastructure could be easily used against the country by enemies through cyber-attacks. National defense agencies such as law enforcement, national security, private or public agencies must, thus, work together to deter, protect, prevent and respond to a multitude of cyber-attacks targeted to a variety of the nation's critical networked systems and infrastructure.

Recently, we have seen several machine learning (ML) and artificial intelligence (AI) applications such as game, machine vision, image processing, natural language processing, self-driving car, robotics and data analytics, where AI exhibits better machine cognition than the human cognition system. This result attracts the cyber defense teams to leverage data-driven techniques with AI for cybersecurity, where AI learns and enhances its knowledge base more quickly to better detect, predict and respond to cyber-attacks. At the same time, ML algorithms and AI systems can be controlled, dodged, biased and misled through flawed ML/AI learning models, input training/actual data or decision classifier; thus, ML algorithms and AI systems need robust security for trustworthy AI. Emerging networked systems and applications are expected to rely on AI/ML; it is essential to consider cybersecurity for AI for trustworthy AI systems.

Emerging networked systems are expected to collect, store and share personally identifiable information (PII) to some extent, to offer accountability and non-repudiation. Cyber attackers could steal PII or related information such as bank account number, utility account number, date of birth, credit card numbers, medical records, social security numbers, drivers' license numbers and state IDs to compromise the privacy of the person. Moreover, cloud-based storage can easily lead to personal information being inferred about individuals. When cloud storage happens outside the country, it adds more privacy challenges because different laws are applied on different countries. Similarly, GPS traces can be used to track vehicles and thereby the drivers/owners/renters of the vehicles. Medical records are essential for personal health and medication. Recently, caused by medical IoT devices, healthcare system breaches affected nearly one million us patients [17]. When medical record or data is compromised, it is a life-or-death situation when medication information is compromised [7,17]. Smart home systems could be exploited to understand the lifestyle of a person and/or could provide the means to track individuals and their personal activities. While addressing these challenges related to cybersecurity and privacy in smart networked systems and critical infrastructure, it is essential to explore and study the systems and solutions from legal, ethical and policy point of view, to make the systems acceptable, usable and trustworthy.

All in all, it is crucial to have security and privacy for emerging networked systems and critical infrastructure, considering the importance and constraints imposed by such systems. The goal of the *Journal of Cybersecurity and Privacy* is to provide a venue for practitioners and researchers from academia, governments and industries, to advance the state of the art in security and privacy research and practice, present new results and provide future visions on these topics for an increasingly connected cyber world. The technical scope of this journal is interdisciplinary, involving contributions from different technical disciplines addressing both cybersecurity and privacy, such as cryptography, wireless security, computer security, network security, information security, socioeconomic aspects of cybersecurity and privacy, legal/ethical/policy aspects of cybersecurity and privacy, signal processing for secure systems, information and communications theory for secure communications, game theoretic security and AL/ML for security, security for AI/ML, data mining and data analytics. From this perspective, the journal's goal is to strategically attract and publish articles on topics including, but not limited to:

- articles that convey new cybersecurity and privacy solutions and technologies;
- articles bridging different technologies with cybersecurity and privacy such as cybersecurity for AI and AI for cybersecurity, technology and public policy for cybersecurity and privacy;
- articles that discuss the, ethical, policy and legal implications of cybersecurity and privacy;
- position articles with new ideas and paradigm shifts for cybersecurity and privacy;
- articles containing implementation of basic and applied research into real-world applications;
- survey and tutorial articles that cover emerging cybersecurity and privacy challenges and solutions.

Journal of Cybersecurity and Privacy is a scholarly archival journal published quarterly.

Funding: This research is funded by the Data Science & Cybersecurity Center (DSC2) at Howard University, Washington, DC, USA.

Conflicts of Interest: Declare conflicts of interest or state.

References

1. Ljungholm, D.P. Regulating Autonomous Vehicles in a Smart Urban Transport System: Safety, Security, and Privacy Issues. *Contemp. Readings L. Soc.* **2020**, *12*, 9–15.
2. Rawat, D.B.; Ghafoor, K.Z. *Smart Cities Cybersecurity and Privacy*; Elsevier Press: Amsterdam, The Netherlands, 2018.
3. Jeschke, S.; Brecher, C.; Song, H.; Rawat, D.B. *Industrial Internet of Things: Cyber-Manufacturing Systems*; Springer: Cham, Switzerland, 2016.
4. Rawat, D.B.; Rodrigues, J.; Stojmenovic, I. *Cyber Physical Systems: From Theory to Practice*; CRC Press: Boca Raton, FL, USA, 2015.
5. Olowononi, F.; Rawat, D.B.; Liu, C. Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS. *IEEE Commun. Surv. Tutor.* **2021**. [CrossRef]
6. Rawat, D.B.; Reddy, S. Software Defined Networking Architecture, Security and Energy Efficiency: A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 325–346. [CrossRef]
7. Wu, J.M.-T.; Srivastava, G.; Jolfaei, A.; Fournier-Viger, P.; Lin, J.C.-W. Hiding Sensitive Information in Ehealth Datasets. *Futur. Gener. Comput. Syst.* **2021**, *117*, 169–180. [CrossRef]
8. Peiser, J. A Hacker Broke into a Florida Town's Water Supply and Tried to Poison it with Lye, Police Said, 2021. Available online: https://www.washingtonpost.com/nation/2021/02/09/oldsmar-water-supply-hack-florida (accessed on 25 February 2021).
9. Hackers Remotely Kill a Jeep on the Highway—With Me in It. Available online: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway (accessed on 25 February 2021).
10. Uprety, A.; Rawat, D.B. Reinforcement Learning for IoT Security: A Comprehensive Survey. *IEEE Internet Things J.* **2020**. [CrossRef]
11. The Real Story of How the Internet Became so Vulnerable, The Washington Post. Available online: https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/ (accessed on 25 February 2021).
12. Rawat, D.B.; Bajracharya, C. Cyber security for smart grid systems: Status, challenges and perspectives. *SoutheastCon* **2015**, 1–6. [CrossRef]
13. Rawat, D.B.; Bajracharya, C. Detection of False Data Injection Attacks in Smart Grid Communication Systems. *IEEE Signal Process. Lett.* **2015**, *22*, 1652–1656. [CrossRef]
14. Rawat, D.B.; Bajracharya, C. *Vehicular Cyber Physical Systems: Adaptive Connectivity and Security*; Springer: Berlin/Heidelberg, Germany, 2016.
15. Safavat, S.; Rawat, D.B. On the Elliptic Curve Cryptography for Privacy-Aware Secure ACO-AODV Routing in Intent-Based Internet of Vehicles for Smart Cities. *IEEE Trans. Intell. Transp. Syst.* **2020**. [CrossRef]
16. Sharma, R.; Rawat, D.B. Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1023–1043. [CrossRef]
17. Healthcare Breaches Affected Nearly One Million US Patients: The Security Risks of Medical IoT URL. Available online: https://blog.checkpoint.com/2019/05/29/ultrasound-iot-hack-security-risks-healthcare-medical-device-michigan-ransomware/ (accessed on 25 February 2021).

Biography

Dr. Danda B. Rawat is a Full Professor at the Department of Electrical Engineering & Computer Science (EECS), Founder and Director of the Howard University Data Science and Cybersecurity Center (DSC2), Director, DoD Center of Excellence in Artificial Intelligence & Machine Learning, Director of Cyber-security and Wireless Networking Innovations (CWiNs) Research Lab, Graduate Program Director of Howard CS Graduate Programs and Director of Graduate Cybersecurity Certificate Program at Howard University, Washington, DC, USA. Dr. Rawat is engaged in research and teaching in the

areas of cybersecurity, machine learning, big data analytics and wireless networking for emerging networked systems, including cyber-physical systems, Internet-of-Things, multi-domain battle, smart cities, software defined systems and vehicular networks. He has secured over USD 16 million in research funding from the US National Science Foundation (NSF), US Department of Homeland Security (DHS), US National Security Agency (NSA), US Department of Energy, National Nuclear Security Administration (NNSA), DoD and DoD Research Labs, Industry (Microsoft, Intel, etc.) and private foundations. Dr. Rawat was the recipient of NSF CAREER Award in 2016, Department of Homeland Security (DHS) Scientific Leadership Award in 2017, Researcher Exemplar Award 2019 and Graduate Faculty Exemplar Award 2019 from Howard University, the US Air Force Research Laboratory (AFRL) Summer Faculty Visiting Fellowship in 2017, Outstanding Research Faculty Award (Award for Excellence in Scholarly Activity) at GSU in 2015, the Best Paper Awards (IEEE CCNC, IEEE ICII, BWCA) among others. Dr. Rawat has published over 200 scientific/technical articles and 10 books. He has been serving as an Editor/Guest Editor for over 50 international journals, including the Associate Editor of IEEE Transactions of Service Computing, Editor of IEEE Internet of Things Journal, Associate Editor of IEEE Transactions of Network Science and Engineering and Technical Editors of IEEE Network. He has been on Organizing Committees for several IEEE flagship conferences, such as IEEE INFOCOM, IEEE CNS, IEEE ICC, IEEE GLOBECOM and so on. He has served as a technical program committee (TPC) member for several international conferences. He served as a Vice Chair of the Executive Committee of the IEEE Savannah Section from 2013 to 2017. Dr. Rawat received his PhD from Old Dominion University, Norfolk, Virginia. Dr. Rawat is a Senior Member of IEEE and ACM, a member of ASEE and AAAS and a Fellow of the Institution of Engineering and Technology (IET).