



OPEN ACCESS

EDITED AND REVIEWED BY
Nicola Zannone,
Eindhoven University of
Technology, Netherlands

*CORRESPONDENCE
Eduard Babulak
✉ babulak@yahoo.com

RECEIVED 14 August 2025
ACCEPTED 04 September 2025
PUBLISHED 22 September 2025
CORRECTED 24 September 2025

CITATION
Babulak E, AL_Dabass D and Tomar G (2025)
Editorial: Cyber security prevention, defenses
driven by AI, and mathematical modelling and
simulation tools.
Front. Comput. Sci. 7:1685873.
doi: 10.3389/fcomp.2025.1685873

COPYRIGHT
© 2025 Babulak, AL_Dabass and Tomar. This is
an open-access article distributed under the
terms of the [Creative Commons Attribution
License \(CC BY\)](#). The use, distribution or
reproduction in other forums is permitted,
provided the original author(s) and the
copyright owner(s) are credited and that the
original publication in this journal is cited, in
accordance with accepted academic practice.
No use, distribution or reproduction is
permitted which does not comply with these
terms.

Editorial: Cyber security prevention, defenses driven by AI, and mathematical modelling and simulation tools

Eduard Babulak^{1*}, David AL_Dabass² and Geetam Tomar³

¹National Science Foundation (NSF), Alexandria, VA, United States, ²Nottingham Trent University, Nottingham, United Kingdom, ³Rajkiya Engineering College Sonbhadra, Gwalior, Madhya Pradesh, India

KEYWORDS

cyber security, applied AI, Mathematical Modeling and Simulation, smart cyberspace, Internet

Editorial on the Research Topic

Cyber security prevention, defenses driven by AI, and mathematical modelling and simulation tools

The rise of the Smart Computation driven by the Artificial Intelligence with the ubiquitous access to Data Computer Communication Technologies and Internet by anyone, from anywhere at any time, has become a working, learning and socializing platform for people worldwide and is often known as Cyberspace.

The past century technological advancements in the Data Communications Technologies, Semiconductor Industry (SI) and a Very Large Scale Integration (VLSI) contributed to significant increase of computer systems performance and computational capacity of small portable computers and cell phones that have become available at low cost for people anywhere in the world.

Due to relatively low cost, anyone and anywhere in the world may purchase a PC, Laptop, Smart Phone, or Tablet. These smart-computational devices are capable of powerful computation and connecting to almost any computer system in the world via Internet 24/7.

Given the current unstable geopolitical ecosystem in conjunction with the dynamic development in the artificial intelligence (AI), smart computation and fast Internet with the ubiquitous access to Internet 24/7, the reliable and secure provision of confidentiality, integrity and accessibility of data available via Internet, has become essential for governments, businesses, industries and individuals worldwide.

The fast developments in the field of AI gave rise to a new era of smart computation that can easily be utilized by the governments, special groups or very well-trained and skilled individuals with malicious intend due to their political, economic or personal motivation.

Given the rise of next generation of smart cyberattacks, the use of AI and Mathematical Modeling and Simulations Tools has become essential part of cybersecurity tool kit, to make sure that contra cyber measures are most effective and reliable in real-time 24/7.

The Research Topic was received with great interest in the scholastic and professional community worldwide. The paper selection was very competitive based on rigorous reviews presenting seven papers.

The Research Topic presents a collection of selected peer reviewed papers presenting most recent advances and the state-of-the-art in the field of Applied AI and Mathematical Modeling in Cyber Security.

The papers show evidence that cyberattacks are becoming much more sophisticated, computationally complex, and challenging for the current cyber security mechanisms, which drives the research, innovation, and development of the next generation of AI assisted Cyber Security embedded with the Mathematical Modeling and Simulations tools.

The first paper presents practical application of eXplainable AI (XAI) in cybersecurity while enabling a machine-human interaction (Moyle et al.).

The second paper discusses effective use of AI applied in the cyberattacks prevention utilizing Intrusion Detection and Prevention Systems (IDPS) (Karmous et al.).

The third paper presents use of deep learning and machine learning algorithms to identify the malicious malware (Miraoui and Belgacem).

The fourth paper discusses the use of encryption and cryptographic algorithms in creating an effective cyber defenses in the Internet of Thing Cyber Infrastructures (Rasheed and Satheesh Kumar).

The fifth paper presents effective methods to identify possible cyberattacks utilizing the noisy audio evidence (Iqbal et al.).

The sixth paper illustrates utilization of simulation based on the dropout mechanisms to identify obfuscated malicious traffic (Ye et al.).

The seventh paper (Jain and Achuthan) presents effective applications of Generative AI Influenced Spread, Extended Models and Awareness Spread Models to analyze fake news propagation and enable the intervention strategy assessment.

The Research Topic brings to light most recent developments in the field of applied AI and Mathematical Modeling and Simulations in Cyber Security, while presenting current and future challenges presented by ongoing challenges in the field of studies. Given the current dynamic advancements in the field of AI, Smart Computation and AI, we are yet at the very beginning of new era of new generation of ultra-smart and most sophisticated cyberattacks that will require a new ultra-smart cyber defenses to make sure that the future cyberspace will be safe, reliable and beneficial to the betterment of mankind for future generations for many years to come. The Research Topic promotes creation of the AI Inspired Cyber Security Center, bringing together multidisciplinary research teams working together while seeking best solutions and mechanism to make the current and future cyberspace safe, secure and reliable 27/7 in the nation and worldwide.

The Topic Editors would like to use this opportunity to express most sincere gratitude to contributors, reviewers, to Dr. Enrique Morillas, Dr. Nicola Zannone, Mr Sean O'Reilly Ms Alice Gooch,

and Colleagues at Frontiers in Computer Science for their strong support, kind guidance and good counsel provided during the course of the project.

Author contributions

EB: Writing – original draft, Writing – review & editing. DA: Writing – original draft, Writing – review & editing. GT: Writing – review & editing, Writing – original draft.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Correction note

This article has been corrected with minor changes. These changes do not impact the scientific content of the article.

Generative AI statement

The author(s) declare that no Gen AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.