SPECIAL ISSUE on Cybersecurity applications for improving data management: trends and challenges

GUEST EDITORS

Haris M. Khalid, University of Johannesburg, South Africa.

Taha Zoulagh, University if Santiago, Chile.

Mohammad Abuashour, Hashemite University, Jordan.

DESCRIPTION

This special issue in Open Computer Science focuses on the Cybersecurity applications for improving data management

Vulnerability concerns have grown due to incorporation of Information and Communication Technology (ICT) technologies into mechanical components used regularly in the travel industry. As the amount of integration rises, so do the inherent problems in the software applications that power these organizations. Additionally, as the business shift towards implementing automated aero planes and intelligent terminals picks up speed, these worries are growing much more important. An analysis of aerospace hacking attempts and assault interfaces over the past years reveals patterns and lessons that can be used to plan future approaches to safeguard the development of a crucial business. Advanced persistent threat groups that are working together with a specific government entertainer to grab intellectual assets and intellectual ability in hopes of improving their residential airframe functionality as well as supervising, easily penetrating, and undermining another nations functionality are demonstrated to be the biggest contenders to the economy, according to the facts offered. The Information Technology (IT) infrastructures are a part of civil aviation that is frequently assaulted, with hostile intrusion to gain unauthorized, proving to be the most attack patterns method. Potential cyber patterns have already been predicted by evaluating the variety of attack vectors and the national threat characteristics. The survey conclusions will assist in establishing and executing preventative measures to safeguard essential facilities from computer security, undermining consumer sentiment in a vital customer sector. The Internet of Things (IoT), a new technology, has completely changed how individuals, intelligence items, smart watches, data, and knowledge are connected globally. IoT innovation remains in its early stages, and numerous connected problems require being resolved. IoT is an all-encompassing idea of integrating anything. A significant increase in transparency, authenticity, availability, flexibility, security, and compatibility could be achieved in the country thanks to IoT. IoT security, unfortunately, is a hard process. IoT innovation is founded based on security systems. IoT vulnerability is methodically analyzed in this piece. The connection and safeguarding of various connected devices and modern informational communications are the primary concerns (ICT). Academics and professionals willing to engage in IoT cyberattacks will benefit from the Survey& data and conclusions. Important topics include current IoT internet security investigations, IoT cyberwarfare structures, and categorizations, important empowering preventive actions and methodologies, effective business implementations, and data analysis patterns and obstacles. Several academics and experts have recently discovered that modern communications systems and equipment are vulnerable to various cyberattacks. These cyberattacks damage and damage private corporations as well as governmental entities. In light of the preceding, we welcome academics to submit original research articles and review papers for the current Special Issue that will address the topic of Cybersecurity applications for enhancing data management: trends and difficulties.

Potential topics include but are not limited to the following:

- An overview of current and anticipated developments for cybersecurity in the transport sector.
- Overview of existing technologies, needs, issues, and patterns in using big data analytics for security.
- An overview of present study problems in the context of Internet of Things (IoT) protection.
- Social psychology and computers were attempting to learn about developments in security administration.
- Improvements in cybercrime judgement call for assistance in visualisation and data authenticity.
- Current products and future possibilities in machine learning and defence.
- Review the literature and upcoming advances in authorization techniques for big data management platforms.
- An analysis of vulnerability problems in significant industrial infrastructure.
- Big data implications and recent technologies in protection.
- Challenges and advancements in data security as these apply to a multitude of platforms and information management.
- Information security and forensic investigations are emerging problems for pervasive computing.
- The architecture uses and upcoming recent developments for a supervised learning architecture for security.

Authors are requested to submit their full revised papers complying the general scope of the journal. The submitted papers will undergo the standard peer-review process before they can be accepted. Notification of acceptance will be communicated as we progress with the review process.

HOW TO SUBMIT

Before submission authors should carefully read the Instruction for Authors, available online.

Manuscripts can be written in TeX, LaTeX (strongly recommended) - the journal's LATEX template. Please note that we do not accept papers in Plain TEX format. Text files can be also submitted as standard DOCUMENT (.DOC) which is acceptable if the submission in LATEX is not possible. **For an initial submission, the authors are strongly advised to upload their entire manuscript, including tables and figures, as a single PDF file.**

All submissions to the Special Issue must be made electronically via online submission system Editorial Manager: http://www.editorialmanager.com/opencs/

All manuscripts will undergo the standard peer-review process (single blind, at least two independent reviewers). **When entering your submission via online submission system please choose the option "SI: Cybersecurity applications for improving data management".**

Submission of a manuscript implies that the work described has not been published before and it is not under consideration for publication anywhere else.

The deadline for submissions is November 15, 2023 but individual papers will be reviewed and published online on an ongoing basis.

Contributors to the Special Issue will benefit from:

- Critical peer-review
- no space constraints
- quick online publication upon completing the publishing process (continuous publication model)
- better visibility due to Open Access – free, unrestricted and permanent access to all the content
- liberal policies on copyrights (authors retain copyrights) and on self-archiving (no embargo periods)
- promotion of published papers to readers and citers
- long-term preservation – content archiving with Portico

We are looking forward to your submission!

In case of any questions please contact Editorial Office (opencomputerscience@degruyter.com)