# Emerging Trends in Computer Science and Its Application

**Dr. Anurag Tiwari**
Anurag Tiwari is an Associate Professor and Head of the Department of Computer Science and Engineering at BBD National Institute of Technology and Management, Lucknow. A Senior IEEE Member, he has over 11 years of academic experience and has led the department to NBA accreditation in 2023. He holds a Ph in Computer Science, multiple MTech degrees, and has authored several research publications. With multiple patents and consultancy projects to his credit, his research interests include machine learning and optimization techniques.

**Dr. Manuj Darbari**
Manuj Darbari, Senior Member IEEE (USA) and Chartered Engineer (India), is a visionary leader in Computer Science and Engineering, specializing in AI, Cloud Computing, and IoT. With a track record of pioneering research, patents, and numerous PhD supervisions, he is recognized for driving innovation and excellence. Currently a Professor at BBDITM Lucknow, Dr. Darbari has made significant contributions to cutting-edge technologies and has served as a convener and reviewer for leading global conferences. His editorial expertise ensures that the conference proceedings reflect the highest standards and capture the forefront of emerging research trends.

# Emerging Trends in Computer Science and Its Application

Proceedings of the International Conference on Advances in Emerging Trends in Computer Applications (ICAETC-2023) December 21–22, 2023, Lucknow, India

*Edited by*

**Anurag Tiwari**
**Manuj Darbari**

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

First edition published 2024
by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

and by CRC Press
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431



CRC Press is an imprint of Informa UK Limited



*British Library Cataloguing-in-Publication Data*
A catalogue record for this book is available from the British Library

ISBN: 9781032999005 (hbk)
ISBN: 9781032999012 (pbk)
ISBN: 9781003606635 (ebk)

DOI: 10.1201/9781003606635

Typeset in Sabon LT Std
by HBK Digital

# 38 The challenges of enforcing cybercrime laws in the age of E-governance: A literature review

*Manuj Darbari*[a], *Naseem Ahmed*[b], *and Abhishek Kumar Singh*[c]

Faculty of Law, Integral University, Lucknow, India

**Abstract:** E-governance and cybercrime legislation are contrasted in this study. The gap might impair cybercrime investigations and prosecutions by law enforcement. Breaking this gap is difficult due to cybercrime's rapid expansion, worldwide nature, lack of resources, and evidence collection. The paper advises new cybercrime laws, international cooperation, training and resources, and awareness to close the e-governance and cybercrime legislation gap. Weighing e-governance and legal gaps with decision science. The study claims decision science can protect government websites and data from hackers. The research shows a huge e-governance and cybercrime law gap that must be filled. The idea calls for a law enforcement cybercrime unit and technology.

**Keywords:** e-governance, cybercrime, law gap, awareness, risk assessment, mitigation strategies

## 1. Introduction

The rapid growth of e-governance has created several challenges for law enforcement agencies. These agencies are often ill-equipped to deal with cybercrime, which is a rapidly evolving threat. As a result, there is a growing gap between e-governance and cybercrime law [1].

E-governance refers to the use of information and communication technologies (ICTs) to deliver government services to citizens, businesses, and other stakeholders [2]. It has become increasingly important in recent years, as governments have sought to improve efficiency, transparency, and accountability.

Cybercrime can range from simple hacking to sophisticated fraud and identity theft. Cybercrime is a major problem, with the estimated cost of cybercrime to the global economy reaching $6 trillion in 2021.

The e-governance and cybercrime law [3] gap refers to the mismatch between the laws that Govern e-governance and the laws that are used to prosecute cybercrime.

Challenges in Addressing the E-governance and Cybercrime Law Gap.

There are a number of challenges in addressing the e-governance and cybercrime law gap. These challenges include:

- The rapid evolution of cybercrime: Cybercrime [4] is a rapidly evolving threat, and new types of cybercrime are constantly emerging. This makes it difficult for law enforcement agencies to keep up with the latest trends.
- The challenges of gathering evidence: Cybercrime evidence can be difficult to gather and preserve. This is because cybercrime often leaves no physical traces, and the evidence can be easily deleted or tampered with.

### *1.1. Ways to address the e-governance and cybercrime law gap*

There are a number of ways to address the e-governance and cybercrime law gap. These include:

- Improving international cooperation: Governments need to improve international cooperation to combat cybercrime. This includes sharing information and resources, and developing

[a]manujuma@student.iul.ac.in; [b]amdnaseem@iul.ac.in; [c]abhiksingh@iul.ac.in

DOI: 10.1201/9781003606635-38

common standards for investigating and prosecuting cybercrime cases.
- Investing in cybercrime training and resources: Law enforcement agencies need to invest in cybercrime training and resources. This will help them to keep up with the latest cybercrime trends and to effectively investigate and prosecute cybercrime cases.
- Raising awareness of cybercrime: Governments[5] and businesses need to raise awareness of cybercrime among citizens and businesses. This will help to reduce the number of victims of cybercrime.

## 1.2. Laws and regulations under preview of e-governance

In IT Act, we have laws and regulations that govern e-governance in India [6]. These include the following:

- The National E-Governance Plan (NeGP): The NeGP is a roadmap for the development of e-governance in India. It was launched in 2006 and aims to make all government services available online by 2020.
- The e-Procurement Act, 2017: The e-Procurement Act provides a framework for the electronic procurement of goods and services by government agencies.
- The Data Protection Bill, 2019: The Data Protection Bill is a proposed law regulates the collection, storage, and use of personal data.
- IT Act-2000[7]

*Section 4: The definition of "electronic" is too broad and could be interpreted to include any form of data that is stored or transmitted electronically. This could make it difficult to determine whether a particular piece of data is an electronic record or not.*

*Section 5: The definition of "digital signature" is also too broad and could be interpreted to include any type of electronic signature. This could make it difficult to determine whether a particular signature is a valid digital signature or not.*

*Section 6: The provision on the admissibility of electronic records in evidence is not clear about how these records should be authenticated. This could make it difficult for electronic records to be admitted as evidence in court.*

*Section 8: The provision on the publication of rules, regulations, and other official documents in electronic form does not specify the format in which these documents should be published. This could lead to confusion and uncertainty about how these documents should be interpreted.*

*Section 10: The provision on the establishment of an electronic signature board is not clear about the powers and functions of the board. This could lead to a lack of coordination and oversight in the regulation of electronic signatures in India.*

*Section 10A: The provision on the establishment of a cyber appellate tribunal is not clear about the jurisdiction of the tribunal. This could lead to delays and inefficiencies in the appeal process for cybercrime cases.*

These are just some of the section-wise lacunae in the IT Act that encompass e-governance. These lacunae need to be addressed in order to ensure that the legal framework for e-governance is effective and comprehensive.

In addition to the above, here are some other specific lacunae in the IT Act:

- There is no specific provision for the protection of critical infrastructure from cyber attacks.
- There is no specific provision for the regulation of artificial intelligence and machine learning technologies.
- There is no specific provision for the investigation and prosecution of cybercrime cases involving foreign elements.

These are just some of the specific lacunae in the IT Act.

- The Aadhaar data breach: In 2018, it was revealed that the personal data of over 1.1 billion Aadhaar cardholders had been leaked.
- The Cosmos Bank cyberattack: In 2018, hackers stole over Rs. 94 crores from Cosmos Bank in Pune. The hackers used a phishing attack to gain access to the bank's systems. The cyberattack highlighted the vulnerability of India's banking sector to cyber attacks.
- The Telangana cyberattack: In 2021, hackers attacked the government of Telangana's IT infrastructure. The attack caused a major disruption to government services, including the state's e-governance portal. The cyberattack highlighted the vulnerability of India's government infrastructure to cyber attacks.
- The cyber attack on the All India Institute of Medical Sciences: In June 2023, hackers attacked the All India Institute of Medical Sciences (AIIMS) in Delhi[8]. The attack caused a major disruption to the hospital's operations.

The cyberattack highlighted the vulnerability of India's healthcare sector to cyber attacks

## 3. Mathematical foundation of Cyber GAP

The current GAP in E-Governance security Law can be improved by using the concept of Decision Science which predicts how to overcome from the above situation. Suppose we want to predict the likelihood of a cyber-attack on a government website. We can use data analytics to identify patterns in past cyber-attacks on government websites. We can also develop risk assessments to quantify the likelihood and impact of cyber-attacks on government websites. This information can then be used to develop mitigation strategies for cyber-attacks on government websites.

By using decision science, we can make informed decisions about how to improve the security of government

Mathematically, a multiple-criteria design problem[9], [10] is formulated using decision space:

$$\max q = f(x) = f(x_1, \ldots, x_n)$$

subject to

$$q \in Q = \{f(x) : x \in X,\ X \subseteq \mathbb{R}^n\}$$

where is the feasible set and is the decision variable vector of size.

The criteria would be the various objectives that we want to achieve, such as improving efficiency, transparency, and accountability.

We can use decision science to help us manage the trade-offs between these objectives. For example, we can use multi-criteria decision making (MCDM) techniques [11] to identify the most preferred policy or regulation. MCDM techniques allow us to consider multiple objectives simultaneously and to identify the solution that best satisfies our needs.

Here are some of the MCDM techniques that can be used to manage the trade-offs between the objectives of e-governance and law gaps:

- Weighted sum method: This method assigns weights to each objective and then sums the weighted values of the objectives to obtain a single score for each policy or regulation. The policy or regulation with the highest score is the most preferred.
- Goal programming [12]: This method allows us to specify minimum and maximum values for each objective. The policy or regulation that minimizes the deviations from the goals is the most preferred.
- Analytic hierarchy process (AHP)[13], [14]: This method is a more complex MCDM technique that uses a hierarchy of criteria to evaluate policies or regulations. The policy or regulation that has the highest overall score is the most preferred.

Suppose we are considering two policies to address the problem of cybercrime in e-governance.

- The first policy is to invest in new security technologies, such as firewalls and intrusion detection systems.
- The second policy is to strengthen the legal framework for cybercrime, such as by increasing the penalties for cybercrime.

The objectives that we want to achieve are to reduce the incidence of cybercrime and to improve the security of e-governance systems. We can assign weights to these objectives to reflect their relative importance to us. For example, we may decide that reducing the incidence of cybercrime is more important than improving the security of e-governance systems [15].

We can then use the weighted sum method to calculate a score for each policy [16]. The policy with the highest score is the most preferred.

For example, suppose we assign the following weights to the objectives:

- Reduce the incidence of cybercrime: 0.7
- Improve the security of e-governance systems: 0.3
- Then, we can calculate the score for each policy as follows:
- Policy 1: (0.7)(0.8) + (0.3)(0.5) = 0.66
- Policy 2: (0.7)(0.6) + (0.3)(0.9) = 0.72

In this case, policy 2 is the most preferred policy, as it has a higher score than policy 1.

This is just a simple example of how MCDM techniques can be used to manage the trade-offs between the objectives of e-governance and law gaps. The specific MCDM technique that is used will depend on the specific situation.

## 4. Conclusion

The e-governance and cybercrime law gap is a serious problem that needs to be addressed. There are a number of ways to address this gap, including developing new laws and regulations, improving international

cooperation, investing in cybercrime training and resources, and raising awareness of cybercrime. By taking these steps, we can help to make the internet a safer place for everyone.

In addition to the above, here are some other specific ways to address the e-governance and cybercrime law gap:

- Creating a dedicated cybercrime unit within law enforcement agencies: This will help to ensure that there are dedicated resources and expertise available to investigate and prosecute cybercrime cases.
- Using technology to combat cybercrime: Law enforcement agencies can use technology, such as data analytics and artificial intelligence, to help them to investigate and prosecute cybercrime cases.
- Working with the private sector: Law enforcement agencies can work with the private sector to share information and resources to combat cybercrime.
- Educating the public about cybercrime: This will help to reduce the number of victims of cybercrime.

## References


[1] T. Ahmad, R. Aljafari, and V. Venkatesh, The Government of Jamaica's electronic procurement system: experiences and lessons learned, *INTR*, vol. 29, no. 6, pp. 1571–1588, Dec. 2019, doi: 10.1108/INTR-02-2019-0044.

[2] [M. Åkesson, P. Skålén, and B. Edvardsson, E-government and service orientation: gaps between theory and practice, *International Journal of Public Sector Management*, vol. 21, no. 1, pp. 74–92, Jan. 2008, doi: 10.1108/09513550810846122.

[3] G. Edwards, *Cybercrime Investigators Handbook*, 1st ed. Wiley, 2019. doi: 10.1002/9781119596318.

[4] S. Gordon and R. Ford, On the definition and classification of cybercrime, *J Comput Virol*, vol. 2, no. 1, pp. 13–20, Aug. 2006, doi: 10.1007/s11416-006-0015-z.

[5] S. Y. Lee, J. M. Díaz-Puente, and S. Martin, The Contribution of Open Government to Prosperity of Society, *International Journal of Public Administration*, vol. 42, no. 2, pp. 144–157, Jan. 2019, doi: 10.1080/01900692.2017.1405446.

[6] S. Kethineni, Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms, in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, T. J. Holt and A. M. Bossler, Eds., Cham: Springer International Publishing, 2020, pp. 305–326. doi: 10.1007/978-3-319-78440-3_7.

[7] Government of India, Gazette of India: Indian IT Act 2000 (Registered NO. DL-33004/2000). Jun. 2000. Accessed: Nov. 10, 2023. [Online]. Available: https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=

[8] D. Kumar, AIIMS Delhi hit by fresh cyberattack for second time in a year, mint. Accessed: Nov. 10, 2023. [Online]. Available: https://www.livemint.com/news/india/aiims-delhi-hit-by-fresh-cyberattacks-details-here-11686061994629.html

[9] T. Entani, Different Types of Decision Criteria in a Decision Problem, in *Integrated Uncertainty in Knowledge Modelling and Decision Making*, vol. 14375, V.-N. Huynh, B. Le, K. Honda, M. Inuiguchi, and Y. Kohda, Eds., in Lecture Notes in Computer Science, vol. 14375. Cham: Springer Nature Switzerland, 2023, pp. 85–96. doi: 10.1007/978-3-031-46775-2_8.

[10] A. Zagaria and A. Zennaro, A close look at sociality in DSM criteria, *Soc Psychiatry Psychiatr Epidemiol*, Nov. 2023, doi: 10.1007/s00127-023-02568-z.

[11] H. Taherdoost and M. Madanchian, Multi-Criteria Decision Making (MCDM) Methods and Concepts, *Encyclopedia*, vol. 3, no. 1, pp. 77–87, Jan. 2023, doi: 10.3390/encyclopedia3010006.

[12] B. Liu and X. Chen, Uncertain Multiobjective Programming and Uncertain Goal Programming, *J. Uncertain. Anal. Appl.*, vol. 3, no. 1, p. 10, Dec. 2015, doi: 10.1186/s40467-015-0036-6.

[13] O. Bozorg-Haddad, H. Loáiciga, and B. Zolghadr-Asli, *A Handbook on Multi-Attribute Decision-Making Methods*, 1st ed. Wiley, 2021. doi: 10.1002/9781119563501.

[14] O. Cooper, The Magic Of The Analytic Hierarchy Process (AHP), *IJAHP*, vol. 9, no. 3, Dec. 2017, doi: 10.13033/ijahp.v9i3.519.

[15] M. A. K. Harahap, K. Kraugusteeliana, S. A. Pramono, O. Z. Jian, and A. M. Almaududi Ausat, "The role of information technology in improving urban governance," *jmp*, vol. 12, no. 1, pp. 371–379, May 2023, doi: 10.33395/jmp.v12i1.12405.

[16] H. Guo and N. J. Dorans, Using Weighted Sum Scores to Close the Gap Between DIF Practice and Theory, *J Educational Measurement*, vol. 57, no. 4, pp. 484–510, Dec. 2020, doi: 10.1111/jedm.12258.