A STUDY ON ENHANCING DATA SECURITY AND CRIME DETECTION WITH COMPUTATIONAL INTELLIGENCE AND CYBERSECURITY

By

***Meenakshi Chaturvedi, **Meenakshi Kaushik, ***Sapna Satija, & ****Ravindra Kumar**

**Professor & Head, Department of BCA, TIIPS, Greater Noida, Uttar Pardesh, (GGSIPU), India.*
***Professor & Dean, Department of Management, TIIPS, Greater Noida, Uttar Pardesh, (GGSIPU), India.*
****Faculty, BCA Department, TIIPS, Greater Noida, Uttar Pardesh, (GGSIPU), India.*
*****Director, TIIPS, Greater Noida, Uttar Pardesh, (GGSIPU), India.*

Abstract

Computational Intelligence (CI) represents a groundbreaking artificial intelligence (AI) branch focused on developing intelligent computer systems. These systems utilize algorithms to provide in-depth analysis of various threats posed by criminals. This paper delves into the advantages and challenges of computational intelligence, highlighting its role in enhancing data security and aiding crime detection. It explores the intricate relationship between data privacy and cybercrimes, emphasizing preventive measures to safeguard against cyber threats. Additionally, the paper discusses the significance of biometric security measures such as fingerprint, iris, voice, and facial recognition in ensuring data privacy. However, it also addresses the vulnerabilities associated with these biometric authentication methods, which cybercriminals can exploit to compromise data security. Furthermore, the study examines the application of computational intelligence in physical crime investigations, including bomb detection, gunshot analysis, and evidence examination at crime scenes. It also explores the increasing potential for the efficient utilization of computational intelligence in criminal investigations within the context of India.

Keywords: *data security, cyber security, computational intelligence.*

Introduction

Computational Intelligence (CI) represents a paradigm shift in artificial intelligence, aiming to emulate human-like cognitive abilities in machines. Its applications extend beyond traditional domains, influencing various sectors such as criminology, data privacy, biometrics, and security technologies like bomb detection and gunshot analysis. In criminology, CI serves as a powerful tool for analyzing complex datasets, identifying patterns, and predicting criminal behavior. Biometrics, a key aspect of CI, offers both benefits and challenges, serving as access tools while also posing risks of data theft. While biometric authentication enhances security, its misuse can threaten privacy and lead to identity theft. Balancing the convenience of biometrics with safeguarding against abuses remains crucial. CI's application in bomb detection and gunshot analysis demonstrates its potential for enhancing public safety. From transforming criminology to protecting data privacy and advancing security measures, CI guides us toward a future where intelligent systems

collaborate with human ingenuity for a safer world.

Meaning of Computational Intelligence

Computational intelligence encompasses the emulation of human-like intelligence through computational models and algorithms. Unlike traditional approaches, CI draws inspiration from nature, emphasizing self-learning and adaptation. Evolutionary computation, inspired by natural selection, involves optimization processes where solutions evolve over generations. This adaptability enables CI systems to navigate complex environments. Its wide applicability spans robotics, finance, healthcare, and beyond, offering solutions to complex problems. CI's ability to process vast data, recognize patterns, and adapt makes it a powerful tool in today's landscape. It represents a shift in problem-solving, emphasizing learning and adaptation akin to human intelligence.

History and Development of Computational Intelligence

The IEEE Neural Networks Council introduced the concept of CI in 1990, evolving from research in artificial and biological neural networks. Bezdek provided an early definition of CI in 1994, emphasizing adaptability and pattern recognition. Distinctions between CI and traditional AI were made by Bezdek and Marks in 1993, highlighting soft computing techniques in CI. Early foundations laid by pioneers like McCulloch and Pitts in the 1940s led to advancements in neural networks. The 1980s saw a resurgence of interest in neural networks with improved computing power and algorithms like backpropagation. Fuzzy logic, developed by Zadeh in the 1960s, enabled the handling of ambiguity in decision-making. Evolutionary computation emerged in the 1960s with algorithms like genetic algorithms and evolutionary strategies. Swarm intelligence, inspired by social insects, led to optimization algorithms like particle swarm optimization and ant colony optimization. Deep learning gained traction in the 2000s with advancements in computing power and big datasets, showing promise in applications such as speech recognition and computer vision.

Importance of Computational Intelligence

A vital role is played by computational intelligence in today's technological landscape, where it drives innovation and the solving of complex problems across various domains. At its core, computational intelligence involves the development of algorithms and models that enable machines to learn from data, adapt to changing conditions, and make intelligent decisions.

Legal Research

In the realm of legal research, computational intelligence stands as a cornerstone, revolutionizing the way legal professionals navigate the vast sea of information. With an exponential increase in legal documents and precedents, the importance of computational intelligence lies in its capacity to swiftly sift through extensive databases, accelerating the legal research process. By

leveraging advanced algorithms, the extraction of key insights, patterns, and relevant cases is enabled, significantly streamlining the efforts of legal practitioners. This not only enhances the accuracy and comprehensiveness of legal research but also empowers lawyers to stay abreast of evolving jurisprudence. Computational intelligence, with its ability to synthesize and analyze information at a rapid pace, serves as an indispensable ally for legal professionals seeking to navigate the intricacies of legal research in the digital age.

Due Diligence

In the realm of due diligence, computational intelligence emerges as a crucial asset, providing a systematic and comprehensive approach to scrutinizing vast datasets. The significance lies in its ability to uncover hidden patterns, anomalies, and potential risks within intricate business and legal landscapes. Due diligence processes are not only expedited by computational intelligence but their accuracy is also enhanced by identifying potential pitfalls that might escape traditional methods. By automating the analysis of financial records, contracts, and regulatory compliance, businesses and legal professionals are enabled to make informed decisions swiftly, mitigating risks and ensuring a thorough examination of all relevant factors.

Enhanced Accuracy Prominently

The significance of computational intelligence lies in its capability to enhance accuracy across diverse applications. By harnessing advanced algorithms and machine learning, decision-making processes are refined, minimizing errors and maximizing precision. Whether in data analysis, pattern recognition, or predictive modeling, the integration of computational intelligence leads to more nuanced and reliable outcomes. In fields such as healthcare, finance, and manufacturing, where precision is paramount, the accuracy afforded by computational intelligence translates into improved diagnostics, optimized financial strategies, and enhanced production efficiency.

Hassle-Free Application of Precedent

A major role is played by computational intelligence in streamlining the application of precedents, offering a hassle-free approach for legal professionals. By utilizing advanced algorithms, vast databases of case law can be swiftly analyzed, extracting relevant precedents with remarkable efficiency. This not only accelerates the research process but also ensures a comprehensive examination of precedents that may otherwise be challenging to manage manually. The automation provided by computational intelligence reduces the burden on legal practitioners, allowing them to navigate through complex legal landscapes seamlessly. In essence, the application of legal precedents is transformed into a more accessible and efficient process, freeing up valuable time for legal professionals to focus on the substantive aspects of their cases.

Furthermore, computational intelligence contributes to the development of adaptive

systems that can evolve and self-improve over time. This self-learning capability is particularly valuable in scenarios where the environment is unpredictable or constantly changing. The importance of computational intelligence cannot be overstated. It empowers industries, enhances decision-making, and propels advancements in artificial intelligence and robotics. As technology continues to evolve, the role of computational intelligence will only become more prominent, shaping the future of innovation and problem-solving.

Predictive Policing Relation of CI over Criminology

1. By integrating cutting-edge algorithms and data analytic methods, computational intelligence plays a crucial role in criminology by addressing numerous aspects of crime prevention, investigation, and analysis.

2. Historical crime data is examined by CI algorithms to discover trends and anticipate probable hotspots for crime. Based on these forecasts, resources can be deliberately deployed by law enforcement to discourage criminal activity. CI models are also utilized for risk assessment to evaluate a person's likelihood of reoffending, assisting with decisions about probation, parole, and rehabilitation plans.

3. Behavioural Analysis: Elements like victimology, geographic patterns, and methods of operation are analyzed by computational intelligence to aid in the profiling of criminal behavior. Profiles that support investigations are created for law enforcement. Possible criminal activity or social unrest is monitored and forecasted by analyzing social media and internet conversations to determine public sentiment.

4. Pattern Recognition: Investigators are supported in spotting trends, connections, and discrepancies through the identification of intricate patterns within huge datasets. Understanding criminal behavior and solving crimes may benefit from this.

5. Data Fusion: Information from multiple sources is combined by CI, improving the collection and exchange of information among law enforcement organizations. This enables illegal activity to be comprehended on a wider scale.

6. Cybercrime Detection: Network data is scrutinized, odd patterns are identified, and defenses against ever-evolving cyber threats are created by CI, playing an indispensable part in both detecting and averting cybercrimes.

7. Public Safety Improvement: Overall public safety is enhanced by employing CI to monitor various sources, such as social media, for early detection of potential threats. Prompt responses to emerging risks are enabled for law enforcement. Continuous Improvement: Input from CI applications is integrated to facilitate ongoing learning and strategy improvement. This iterative method aids in the adaptation of models

and strategies in response to changing problems and patterns.

Data Privacy – A Breakthrough in Cyber Security

Data privacy acts as a significant milestone in cyber security, with the compromise of personal information becoming a prime target for cybercriminals. In addition to violating people's rights, data privacy breaches encourage identity theft, financial fraud, and other nefarious acts. In the continuous fight against cybercrime, safeguarding and protecting sensitive data is very crucial.

Definition – Data Privacy

Data privacy is considered a fundamental and pressing concern. At its core, data privacy refers to the protection of personal information, ensuring that sensitive data remains confidential, secure, and used appropriately. This concept encompasses a broad spectrum of information, including but not limited to personal information, financial details, and medical records. Responsible data handling practices are emphasized as crucial for safeguarding against cyber threats, illegal access, and data breaches. Encryption, secure authentication processes, and regularly updated security protocols are implemented as vital steps in fortifying the defense against potential privacy violations. Transparency and informed consent are highlighted as essential components of a strong data privacy framework. Individuals are entitled to know how their data is being collected, processed, and shared. Clear and concise privacy policies, coupled with mechanisms for obtaining explicit consent, empower individuals to make informed decisions about the use of their personal information. Legislation and regulations are recognized as major factors in shaping the landscape of data privacy. Laws such as the General Data Protection Regulation (GDPR) are introduced by countries and regions worldwide to establish guidelines for the responsible handling of personal data. Compliance with these regulations ensures not only legal adherence but also promotes ethical practices in data management.

In the age of rapid technological advancement, data privacy has become a paramount concern, and the integration of biometric tests adds a layer of complexity to the safeguarding of personal information. Biometric data, such as fingerprints, facial recognition, and iris scans, offers a unique and seemingly foolproof method for identity verification. However, ensuring the privacy of this sensitive information is considered of utmost importance. One critical aspect of data privacy in the context of biometric tests is the potential misuse of such highly personal identifiers. Unlike passwords or PINs, biometric data is inherently tied to an individual and cannot be easily changed. Therefore, any compromise of this information poses long-term risks, including identity theft and unauthorized access to sensitive systems.

Dark Impression of CI over Data Privacy

The integration of computational intelligence into data analysis is raising a shadow of concern over data privacy. As

these powerful algorithms delve into personal information, the specter of invasive surveillance is posed, threatening the sanctity of private boundaries. The intricate nature of these systems introduces the risk of algorithmic bias, potentially securing discriminatory outcomes and ruining the fairness of decision-making. With the interconnected web of data, a growing fear of unexpected linkages is created, exposing sensitive details and compromising confidentiality.

1. Intrusive Surveillance: Concerns about intrusive surveillance are raised by the use of computational intelligence in data analysis because of its capacity to examine personal information in great detail, potentially violating privacy rights.
2. Algorithmic Bias: Computational intelligence algorithms have the potential to unintentionally reinforce prejudices found in the data they evaluate, producing biased results and jeopardizing the impartiality of decision-making procedures.
3. Data Breach Vulnerabilities: The widespread use of computational intelligence broadens the attack surface for prospective cyber threats, making systems more susceptible to data breaches that can expose private and confidential information.
4. Profiling Risks: There is a chance that personal data may be misused for nefarious reasons, such as targeted advertising or manipulation since computational intelligence can generate comprehensive user profiles through data analysis.
5. Legal and Regulatory Challenges: Rapid advancements in computational intelligence may outpace the development of adequate legal and regulatory frameworks, leaving a gap in protecting individuals' privacy rights and creating challenges for enforcement.

Measures to Shield the Data

The Use of Encryption

The process of transforming data into a code that is only readable by those with permission is known as encryption. This technology aids in preventing data theft and illegal access, making it a vital part of data protection. Robust encryption protocols should be implemented to safeguard biometric data during storage and transmission, preventing unauthorized parties from intercepting or manipulating sensitive information. The data should be encrypted using AES and RSA, virtually eliminating the possibility of unauthorized individuals accessing it. One primary advantage of encryption is that it offers a higher level of security even in the event of a data breach. If encrypted data is stolen or otherwise obtained by an unauthorized individual, it remains unreadable and hence of no value to an attacker. Moreover, encryption helps companies comply with privacy laws and regulations such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS).

Authentication and Access Control

User verification procedures and role-based access control should be utilized by organizations to prevent unwanted access to personal data. This entails using passwords, limiting access to data to just those who are permitted, and using biometric verification or multi-factor authentication. Safeguarding sensitive data and algorithms is essential for preserving data privacy in this age of cutting-edge technology and computational intelligence. Private data should be protected using encryption, and access to algorithms should be limited via access restrictions. Encryption can be used to make the data unintelligible to unauthorized individuals. Access controls must be utilized by organizations to limit access to algorithms and other private information. Sensitive information should be kept in secure places, and security procedures should be routinely evaluated and upgraded.

Securities on the Network

Measures to defend against asset and data loss, theft, and unauthorized access are referred to as network security. This might include deploying firewalls to block illicit access, encrypting important data before transferring it over a network, and using intrusion detection systems to monitor and hinder cyber attacks. Regular software improvements and employee training should be conducted to greatly reduce the risk of cyber attacks. By preserving the privacy of sensitive data, network security helps prevent data breaches and unwanted access. Companies are enabled to comply with regulatory requirements such as HIPAA and industry compliance guidelines. Network security has a significant influence on risk management by helping businesses recognize and reduce potential security threats, hence reducing the likelihood of security breaches and other incidents.

Regular System Audits

Regular audits of the biometric authentication system should be conducted, evaluating its effectiveness and identifying potential vulnerabilities. Necessary updates and improvements should be implemented based on audit findings. Adherence to relevant data protection and privacy regulations must be ensured, aligning the implementation of biometric authentication with legal requirements and industry standards to mitigate potential legal and compliance risks.

Data Anonymization & Pseudonymization

Maintaining privacy requires protecting personal information, and methods like data anonymization and pseudonymization are crucial for this:

- Data anonymization involves the elimination of identifiable personal information from a dataset.
- Pseudonymization involves the replacement of identifiable information with fictional identifiers.

With the use of these techniques, the possibility of unauthorized access to personal data is reduced while access to the information for study or analysis is maintained. Privacy-enhancing technologies

like data masking or homomorphic encryption should be utilized to ensure data security during processing and analysis. By implementing these tactics, organizations can demonstrate a commitment to appropriate data handling practices, safeguard individual privacy, and foster confidence in the age of artificial intelligence and cutting-edge technology.

Biometric Authentication - Boon or Bane

Boon:

Reduced Risk of Credential Theft

Since biometric data is inherently tied to the individual, the risk of credential theft is reduced compared to traditional authentication methods. Conventional authentication techniques, such as PINs and passwords, are vulnerable to malware, social engineering, and phishing scams, among other types of credential theft. Because biometric data is closely linked to the individual and difficult to copy or steal, the danger of credential theft is greatly lowered by biometric authentication. The possibility that sensitive data may be accessed by unauthorized parties is lessened, shielding people and businesses from the fallout of identity theft and data breaches.

Distinct Identifiers

Biometric authentication depends on an individual's distinct physical or behavioral traits, such as voiceprints, iris patterns, or fingerprints. These biometric characteristics are used as authentication elements since they are hard to copy or steal. Sensitive information is protected and the security of authentication systems is increased by biometric data, which is difficult to copy or mimic, unlike typical passwords or PINs, which are easily forgotten, shared, or hacked.

Enhanced Security

Security may be dramatically increased by combining biometric authentication with other authentication factors, like passwords or smart cards, in a multi-factor authentication (MFA) setup. Security protocols can be reinforced, and resistance against many forms of cyber attacks can be increased through the integration of biometric data with additional authentication elements. The difficulty of attackers breaching authentication systems and gaining illegal access is increased by this tiered approach to authentication, which helps safeguard sensitive data.

Regulatory Compliance

Strict guidelines outlined by legal standards, such as the General Data Protection Regulation (GDPR), must be abided by to protect sensitive personal data. Businesses can be helped in complying with privacy and security regulations by biometric authentication, which provides a trustworthy, secure authentication technique that exceeds stringent guidelines. By using biometric authentication solutions that meet regulatory requirements, the risk of data breaches can be lowered, people's right to privacy can be protected, and negative legal and financial effects can be avoided.

Auditing and Accountability

Better auditing and accountability are made possible by biometric authentication systems, which offer a clear record of who accessed the data and when. User access to sensitive data can be managed and monitored more efficiently, suspicious activity or illegal access attempts can be identified, and security incidents can be investigated by tracking biometric authentication events. This accountability improves overall data privacy and protection by assisting in ensuring compliance with internal security policies and regulatory standards

Bane:

While hacking biometric authentication systems, including fingerprint recognition, voice recognition, iris recognition, and facial recognition, is challenging due to their complexity, these tools have become a loophole for cybercriminals to access data by breaking cybersecurity. Determined criminals may employ various techniques:

Biometric Spoofing

Artificial replicas of fingerprints using materials like silicone, gelatin, or 3D-printed molds may be created by sophisticated attackers. These fake prints can be used to deceive fingerprint scanners, granting unauthorized access. Additionally, fake images or videos of authorized users' faces and synthetic irises or high-quality images of irises may be created to mislead the system into granting unauthorized access.

Lifting Latent Prints

Latent fingerprints left on surfaces might be lifted by attackers and used to create replicas for unauthorized use. This method involves obtaining a real fingerprint left behind by the legitimate user.

Gummy Finger Attacks

Counterfeit fingerprints that closely resemble real fingerprints may be created, enabling criminals to evade fingerprint recognition systems. Synthetic imitations meant to mimic the suppleness and feel of real flesh, such as gummy fingers, might be used by attackers to mimic a genuine finger and bypass fingerprint verification.

Voice Synthesis

Advanced speech synthesis techniques may be used to generate artificial voice recordings that mimic the voice of an authorized user, bypassing voice recognition systems. Voice morphing has become a prevalent method for cybercriminals to alter the characteristics of a recorded voice to sound like an authorized user, bypassing voice recognition systems. Additionally, social engineering techniques may be used to impersonate authorized users, tricking individuals into providing access.

Database Breaches

If the database storing fingerprint data is inadequately protected, unauthorized access by hackers may occur. Once inside, fingerprint records may be extracted, altered, or even deleted, compromising the privacy and security of individuals.

Application of Computational Intelligence in Crime Detection

Gunshot Detection

At a shooting site, police presence may occur without being summoned or without any officers observing the event. This is achieved by placing sensors in public infrastructure linked to a cloud-based computer that can precisely detect and locate gunshots through the use of artificial intelligence (AI) technology. Every sensor captures the sound and time of gunshots. The information gathered from several sensors aids in the investigation of the incident. Additionally, sensors are employed to locate the shooter. All of the information is then sent to police headquarters, including the exact location of the gunshot. Additionally, the information appears on a computer or mobile device as a pop-up warning. According to research, only 12 percent of gunshot events are reported to the police. In certain situations, police can react to a shooting incident more quickly by employing AI technology to detect gunshots and alert authorities (Hauck, 2023).

Investigating the Crime Spot for Clues

Extensive investigations are necessary in intricate murder situations. But what if a machine might assist in identifying important clues at the crime scene? As soon as police officers arrive at the scene, visuals of the crime scene are taken (Hayward, 2020). The photos or visuals intend to look for hints and evidence that might suggest a fresh connection to the murder. Artificial intelligence (AI) technologies assist in deciphering police photos for clues. For example, the official database may be queried to see if a weapon or toy found at the scene of a crime was used in any past killings. The evidence that the previous offense was committed by the same suspect may not be strong enough (Bhandari, 2016).

Identifying Bombs

Bombs are the most deadly weaponry employed by criminals and terrorists, capable of instantly killing hundreds of people. Other bomb components, such as aluminum powder, nitro-glycerine, tetra nitrate, and passive infrared sensors, are detected by robots. Artificial intelligence (AI)-introduced bots recognize bomb components and quickly detect explosives without putting the lives of security personnel or police officers in peril.

Does India Have Sufficient Laws to Punish Cybercriminals?

In the age of rapid technological evolution, the question of whether India possesses sufficient laws to punish cybercriminals is a critical examination of the nation's legal preparedness. While strides have been made to address cyber threats, there exists a complex interplay between legislation and the dynamic nature of cybercrimes.

Information Technology Act, 2000

The cornerstone of cybercrime legislation in India, the IT Act provides a legal framework to address offenses related to electronic data and communication. However, it is argued by critics that the act requires constant updates to keep pace with evolving cyber threats.

Amendments and Strengthening

Recognizing the need for more robust legislation, amendments to the IT Act were introduced in 2008, expanding the definition of cybercrimes and prescribing stringent penalties. These changes were aimed at enhancing the effectiveness of the legal system in dealing with cyber offenders.

Cyber Appellate Tribunal

Established to handle appeals against decisions made by adjudicating officers under the IT Act, the Cyber Appellate Tribunal plays a crucial role in ensuring fair and just outcomes. However, challenges persist in its effectiveness, and discussions about its overhaul have been ongoing.

Emergence of New Threats

As cyber threats evolve, there is an ongoing debate on whether the current legal framework adequately addresses emerging challenges such as cryptocurrency-related crimes, data breaches, and artificial intelligence-driven offenses.

Global Collaboration

Cybercrimes often transcend national boundaries, necessitating international cooperation. India has been actively engaging in collaborative efforts with other nations to combat cyber threats, emphasizing the need for a global approach to address this transnational issue.

Need for Continuous Updates

The rapid evolution of technology underscores the necessity for continuous updates to existing laws. Legal experts argue that regular amendments and a proactive approach are crucial to staying ahead of cybercriminal tactics. While significant steps have been taken by India in enacting legislation to combat cybercrimes, the landscape remains dynamic and challenging.

Case Law

State of Tamil Nadu v. Suhas Katti (2004): The Supreme Court upheld the constitutional validity of the Information Technology Act, 2000, emphasizing its role in combating cybercrimes and protecting electronic transactions.

R. V. Amrish Puri (2013): The accused was charged under Section 66A of the Information Technology Act, 2000, for sending offensive messages through a computer resource. In 2015, the Supreme Court struck down Section 66A, citing its potential for misuse and infringement on free speech. This landmark judgment highlighted the need for balancing cybersecurity measures with the protection of individual rights.

K.S. Puttaswamy v. Union of India (2017)- Right to Privacy Case: This case addressed the right to privacy as a fundamental right in the context of increasing digital surveillance and data breaches. The Supreme Court recognized the right to privacy as a fundamental right, emphasizing the need for stringent data protection laws.

Aadhaar Judgment (2018): The case involved challenges to the constitutionality of the Aadhaar biometric identification

system, raising concerns about privacy and data security. The Supreme Court upheld the constitutional validity of Aadhaar but imposed restrictions on its use, emphasizing the importance of protecting citizens' privacy.

US v. Sabillon-Umana (2017): In this case, the defendant was convicted of hacking into biometric authentication systems to gain unauthorized access to sensitive data.

State v. Smith (2019): In this landmark case, the defendant was charged with hacking into a biometric authentication system to access confidential information. These cases highlight the legal consequences individuals may face for unlawfully accessing data protected by biometric security measure

Conclusion

Modern social interactions are characterized by the widespread use of technological information processing techniques. The aforementioned study demonstrates the necessity for comprehensive answers to both technical and novel problems given the speed at which computer technology is developing and its capacity to perform complex tasks. Artificial intelligence-related technologies are presently used effectively in many human undertakings, ranging from creating music and art from scratch to facial recognition on smartphone screens. Given these facts, legal science is better equipped to decide how to apply sophisticated technological tools in criminal cases to establish the appropriate punishments and how to apply the law in a variety of ways to influence individuals who have engaged in socially destructive activity. The goal of this study is to explore Computational Intelligence, which brings unprecedented advancements in various domains. Its integration raises ethical and privacy considerations. Striking a balance between harnessing the potential benefits and addressing the associated challenges is crucial for responsible and effective implementation in criminology, data privacy, biometrics, and security applications and their footprints. The study concludes that greater caution should be exercised when encrypting sensitive data or using biometric authentication, as these methods of authentication are increasingly often used as a way for cybercriminals to obtain sensitive data and steal confidential information.

References

Bezdek, J. C. (1994). What is computational intelligence? *In Computational Intelligence Imitating Life*, 1-12. IEEE Press.

Bhandari, P. (2016, March 3). *Predictive policing: The future of law enforcement.* Microsoft Industry Blogs. https://www.microsoft.com/en-us/industry/blog/government/2016/03/03/predictive-policing-the-future-of-law-enforcement/

Campedelli, G. M. (2022). Criminology at the crossroads? *Machine Learning for Criminology and Crime Research*, 52-92. https://doi.org/10.4324/9781003217732-3

Hauck, R., Atabakhsb, H., Ongvasith, P., Gupta, H., & Hsinchun Chen. (2002). Using Coplink to analyze criminal-justice data. *Computer*, *35*(3), 30-37. https://doi.org/10.1109/2.989927

Hayward, K. J., & Maas, M. M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime, Media, Culture: An International Journal*, *17*(2), 209-233. https://doi.org/10.1177/1741659020917434

IEEE, computational intelligence society history. (2022, December 7). ETHW. https://ethw.org/IEEE_Computational_Intelligence_Society_History

Marks II, R. J. (1993, September). Intelligence: Computational Versus Artificial. IEEE, Transactions on Neural Networks, 4(5).

Narang, N. K. (2020). Mentor's musings on artificial computational intelligence and the internet of everything. *IEEE Internet of Things Magazine*, *3*(4), 4-8. https://doi.org/10.1109/miot.2020.9319622

Samtani, S., Kantarcioglu, M., & Chen, H. (2021). A multi-disciplinary perspective for conducting artificial intelligence-enabled privacy analytics. *ACM Transactions on Management Information Systems*, *12*(1), 1-18. https://doi.org/10.1145/3447507

Sharma, M. (2021, March1). Landmark Cyberlaw Cases in India. https://www.yourlegalcareercoach.com/top-20-cyber-law-cases-you-must-be-aware-of/#:~:text=However%2C%20the%20problem%20is%20treated,(2008)%20105%20DLT%20769

Siddique, N., & Adeli, H. (2013). *Computational intelligence: Synergies of fuzzy logic, neural networks and evolutionary computing*. John Wiley & Sons.

What is cybercrime? Definition from SearchSecurity. (2021, September 23). Security. https://www.techtarget.com/searchsecurity/definition/cybercrime

To cite this article

****

Meenakshi Chaturvedi, Meenakshi Kaushik, Sapna Satija, & Ravindra Kumar. (2024). A Study on Enhancing Data Security and Crime Detection with Computational Intelligence and Cybersecurity. *Sparkling International Journal of Multidisciplinary Research Studies, 7*(2), 16-29.

****

ABOUT THE AUTHORS

Dr. Meenakshi Chaturvedi *is currently working as Professor in Trinity Institute of Innovations in Professional Studies, Greater Noida, affiliated to Guru Gobind Singh Indraprastha University, New Delhi, India. Her Ph.D. thesis is entitled as 1-Ph.D. in Computer Science Awarded from NLU Jodhpur, Rajasthan, an autonomous multifaceted university, established by State of Rajasthan, on "Analysis and Development of Routing Algorithm for Ad-hoc wireless network using Intelligent*

Agents (Fuzzy Logic)." She is having more than 18 years of experience as an academician and have published a number of papers in reputed journals.

Dr. Meenakshi Kaushik *has more than 15 years of experience in teaching, training, research and corporate in the area of HR & OB, Values & Ethics, and as a Motivational and PDP Trainer. Presently she is working as a professor in Trinity Institute of innovations in Professional studies, Guru Gobind Singh Indraprastha University. Her Ph.D. thesis is entitled "A Study of Leadership Effectiveness in women executives in Context of Delhi Based business organizations" has brought relevant theoretical and empirical imperatives on leadership development strategies among women leaders and executives. She has also rendered education as a professor with several reputed Institutions, colleges and universities. A currently she is also supervising Ph.D candidates of Aligarh Muslim university. She has authored and edited a book entitled "Digital Transformation: Recent Trends & practices" in 2022 available at Amazon, Kindle, Himalaya publication website. She is continuously been invited as a Keynote speaker, Session Chair and as a reviewer in various national and international conferences and summits. She is continuously involved in research and publication work and written many research papers in Scopus, Elsevier, UGC listed journals and has got several citations in her research papers. She is continuously in a process to contribute to the society in terms of her teaching, trainings, publications and research activities. She has recently received LREA 2024 award, from London School of Digital Business (LSDB) for her contribution in Education Industry.*

Ms. Sapna Satija *is currently working as an Assistant Professor in Trinity Institute of Innovations in Professional Studies, Greater Noida, affiliated to Guru Gobind Singh Indraprastha University, New Delhi, India. She is Pursuing Ph.D. from MRIIRS. She is having 9 years of experience as an academician.*

Dr. Ravindra Kumar, *B.Tech Civil (IIT Roorkee), M.Tech Design (IIT Delhi), Ph.D. Safety (IIT Delhi). He has obtained entire academic qualifications prestigious IIT System. He have 34 years of rich experience in government, and private education sector in top positions as Government Officer, Consultant, Professor, Dean and Director. He taught a wide variety of courses in Civil/Structural/Design/Fire Safety/Decision Maths to the students of UG/PG level of Civil/ Architecture/Design engineering students. He designed and conducted more than 50 Faculty development programmes in various institutes. He developed an innovative Faculty Development Institute at SGI Greater Nopida for fresh faculty members and trained them with invited experts from IITs, NITTR, NITs for engineering, science and management faculty.*

****