Page 625 - 637 **DOI:** *https://doij.org/10.10000/IJLMH.1112080*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

Current Trends in Digital Forensics with special emphasis on Digital Arrest: An Opinion

NITASHA AGARWAL*, PRERANA** AND PREETI MALIK***

ABSTRACT

Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting on data stored electronically. The main goal of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence and present the findings for prosecution. Digital forensics can be used for a variety of investigations such as cybercrimes, corporate frauds, intellectual property thefts, and so many others. Amongst all the above, what is significantly emerging as the most common financial frauds is the Digital Arrest. The phenomenon termed "Digital Arrest" represents an emerging cyber-scam wherein perpetrators manipulate online data and communication systems under the guise of law enforcement operations. Victims are coerced into remaining on video calls with the scammers, who impersonate officials, until their financial or other demands are fulfilled. This paper presents current trends of digital arrest. Implication of digital arrest on victim also discussed in this article along with precautions to be taken or how it can be minimized. Challenges faced in combating with digital arrest are also included in this article.

Keywords: *Forensic, Digital Forensic, Digital Arrest, Machine Learning, Artificial Intelligence.*

I. INTRODUCTION

It is evident in history that any invention and improvisation in scientific field comes with its costs and benefits. Digitalization is one such exposed concern that we are coping up in 21st century. Digital forensics is the tool that is used to combat the digital frauds which includes the identification, collection, processing, investigation and reporting of all the data which is electronically stored. In today's scenario, digital evidences are the essential component of

* Author is an Assistant Professor at School of Forensic Science, Uttar Pradesh State Institute of Forensic Science, Lucknow, U.P., India.

** Author is an Assistant Professor at School of Cyber Security and Digital Forensics, Uttar Pradesh State Institute of Forensic Science, Lucknow, U.P., India

*** Author is an Assistant Professor at School of Cyber Security and Digital Forensics, Uttar Pradesh State Institute of Forensic Science, Lucknow, U.P., India

 [ISSN 2581-5369]

almost all fraudulent activities. The digital or electronic evidence can be gathered from sources such as computers, mobile phones, tablets, storing devices such as hard disks, pen drives, unmanned aerial systems, digital equipment and much more. The significance of these digital evidences for law enforcement applications has increased many folds in the recent years. It is because of the excessive use of electronic devices and data transmission in many incidents that are under police investigations and trials [1]. Digital forensics' major aim is to extract the information from the digital or electronic evidence, processing it with intelligence and presenting the observations for the court of law. The evolution of technology widened the canvas of digital forensics beyond petty computer crimes. The use of smart phones, digital devices, use of internet, and cloud data has expanded the area of digital forensics, which includes cybercrimes, corporate, digital and engineering enabled frauds.

II. HISTORICAL BACKGROUND OF DIGITAL CRIMES

The emergence of digital forensics can be linked to the Florida Computer Crimes Act, 1978, which came as the primary acknowledgement of computer associated crimes. The book, Crime by Computer by Donn Parker in 1976, was the very first source of descriptive knowledge related to digital information investigation and prosecution in crimes related to computer and its assistance [2]. Initially, around 1990's it was known as computer forensics to what we call as digital forensics now. In USA, the work began in the FBI Computer Analysis and Response Team in the year 1984. Sooner, in UK also a computer related crime unit was setup which was known as the Fraud squad. The expansion of this field began in 1990s. The investigators and law enforcement agencies which operated around the world, along with the specialists of digital world, realized that digital forensics computer forensics required standard protocols, methodology and techniques. It was not just required as the informal guidelines but an urgent need to formalize and to legalize the standards for investigating such digital evidences combating. It was then series of conferences took place around 1995-96 with an agenda to develop methodologies for digital forensics. In UK, the association of chief police officers brought the first draft of its Good Practice Guide for Digital Evidence around 1998, the guidelines made here detailed the main principles applicable to all digital forensics law enforcement facilities.

III. TYPES OF DIGITAL CRIMES

The use of technology based digital communications has given new opportunities to the criminals and investigators simultaneously, who can use the information to track the history related to transactions, messages, and other types of digital data by demographic locations, or

 [ISSN 2581-5369]

an individual's address, account details, bank passwords or any other such official data [3].The increasing network of cyber threats and the complexity of digital footprints and the expansion of advancements in digital forensic techniques are more critical than ever. The field of digital forensics primarily deals with the identification, preservation, analysis and presentation of evidence for legal purposes to uncover and interpret the data obtained electronically for ensuring regulatory compliance and support court proceedings, but now it encompasses much more than just digital world expanding up to sub-disciplines such as mobile-device forensics, network forensics and cloud forensics. It is true to state that now the field of digital forensics has become an indispensable part of law enforcement agencies, professionals from cyber security and the court room experts.

The techniques used in digital forensic investigations strictly enforce the integrity of the evidence and its admissibility. The very process involves multiple steps to ensure the correct data recovery and minimal or no tampering of the evidence. Though collecting the digital evidence is not a simple process and may require expertise for proper management. If by any chance the method of interpreting the digital evidence is inaccurate, it may lead to false data being presented for the examination because of which any important subsequent investigation can be compromised even without the knowledge of the practitioner[4]. Another important part of computer related criminal investigations is the digital documentation. As the data is stored electronically on multiple electronic devices, it is collected using well-defined methods that will be helpful and can provide substantial proof for any digital forensic investigation[5]. The common forms of digital evidences include e-mails, audio/video recordings; software-based data, cloud data, Meta data, etc. Figure 1 includes some of keywords from digital forensic.

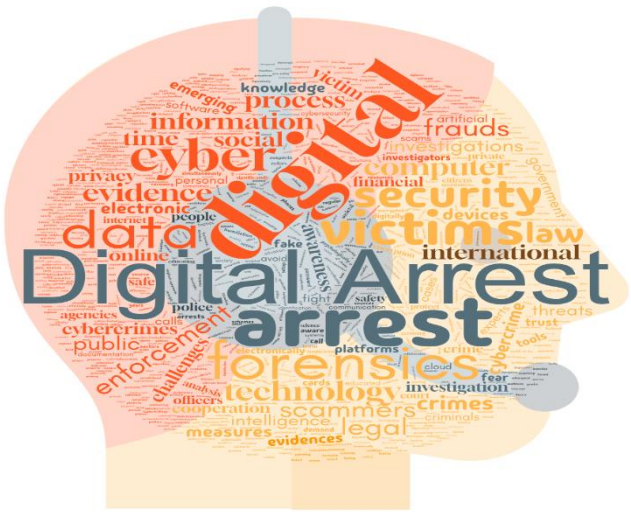

Figure 1: Words Cloud of Digital Forensic

Artificial Intelligence (AI) and Machine Learning are currently the most important emerging technologies that can be used as digital assets for any digital investigation purposes. They have revolutionized the domain of digital forensics by automating complex assignments and enhancing the examination of enormous amounts of data[6][7][8]. With advanced encryption and security features, decoding electronic devices has become a significant challenge for the investigators. Newer technology, such as block chain technology is known for its secure and immutable ledger which is gaining a lot of popularity in digital investigations. The investigators and experts today are looking for more potent tools to deal with the challenges arising due to advanced technologies such as crypto currencies and block chain technologies. Another threat that is the Internet of Things (IoT) has elevated which links billions of devices and generated enormous amount of data which may be valuable in forensic investigations. The emergences of these new technologies undoubtedly possess many advantages and innovations but they equally pose new cyber security threats [9], which have a lot of impact on various agencies such as government setup, banks, enterprises, e-commerce, online transactions, net-banking, etc.[10].Amongst all the existing tools and techniques, emerging methods and challenges what is most significant in most common financial frauds is the social engineering-enabled fraud commonly known as digital arrest. There is an alarming situation as no recovery is generally ensured due to the nature of crime itself. This review article adheres on the emerging trends in digital forensics with the special emphasis on the common digital frauds such as digital arrest.

IV. DIGITAL ARREST

Digital Arrest has been the most practiced cyber-scam in which the attacker/scammer influences online data and communication system under the impression of law enforcement operations[11][12].Victims are compelled to remain on video calls with the scammers, who pose as officials, until their financial or other demands are met. The fraudsters exploit victims' fear and lack of awareness by threatening to expose them with fabricated legal charges and extort money. Although such schemes are presented as measures to check and curb cybercriminal activities, they are, in reality, sophisticated forms of cyber extortion. Traditionally, "arrest" refers to the physical detention of an individual by law enforcement officers. However, while dealing with cybercrimes like; identity theft, hacking and other online fraud, "digital arrest" could metaphorically be described as the process of recognizing and detaining the persons who commit the crime over digital platforms. Advanced investigation techniques are needed to perform such operations of finding, recognizing and apprehending the suspects engaged in such illegal activities on digital platform.

 [ISSN 2581-5369]

A. Process of Digital Arrest

Potential victims are initially contacted through video call or phone call by the scammers. These scammers improve their authority by making apparently reasonable declarations, often pretending as police officers, custom officers or some other law enforcement personnel. The scammers claim that the victim have sent or are the intended receiver of a parcel allegedly enclosing illegal things like smuggled goods, drugs or fake passports. In some cases, fraudsters also make them believe that some relatives or close friends are part of a crime or involved in accident and currently detained by the officials. The scammers claim that the person is in immediate danger prompting instant action.

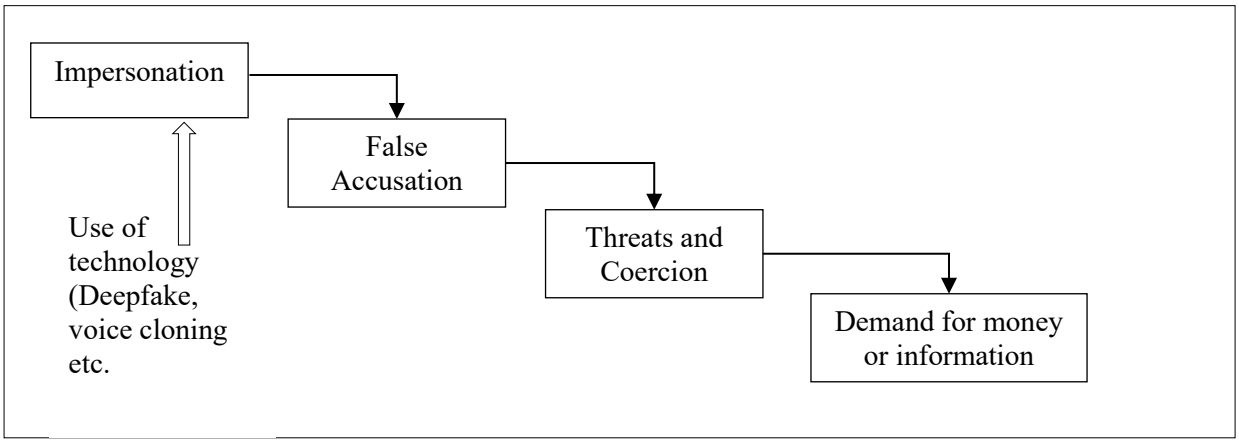

Figure 2: Modus Operandi of Digital Arrest

In fact, some criminals influence the victim psychologically to maintain their control over the victims. These victims may find themselves figuratively digitally arrested for long periods, additionally increasing their vulnerability to corruption. These fake government officials or scammers impart fear or sense of urgency to force victims into agreement. It is very common that the scammers put monetary demand before the victim as the scammers insist on settling pretended legal issues. They pressurize the victim to take the decision immediately by creating panic and urgency. These real-time, immersive interactions make the deception even more compelling. They use threatening language, show fake evidences and demand huge amounts, which leaves the victim financially and emotionally distressed. In most of the cases of digital arrest, the aim is monetary extortion (Fig. 2 depicts this process of Digital Arrest).

B. Real Cases of Digital Arrest

Mohammed Zubair Ahmed, the main accused in a large-scale FedEx digital arrest scam, was arrested by Hyderabad Cyber Crime Police upon arrival from Dubai, based on a Lookout Circular. The case began with a Hyderabad resident being duped into transferring ₹55 lakh after a fake Skype call with impersonators posing as Mumbai police. The fraud involved 52 bank

 [ISSN 2581-5369]

accounts operated by Zubair and his associates to launder money.

An 86-year-old woman from South Mumbai was duped of over ₹20 crore in a 'digital arrest' scam by fraudsters posing as CBI officials. She was coerced into isolation for two months and intimidated through frequent video calls, claiming her Aadhaar-linked account was involved in money laundering. The scammers extorted money under the pretext of clearing her name and court formalities. Three suspects have been arrested, and police have managed to freeze ₹77 lakh. Authorities believe the accused are part of a larger cyber fraud network.

In one more case, a victim was digitally detained for over three months by cybercriminals impersonating law enforcement officers and extorted 42 times, losing ₹7.67 crore. The CBI took over the case and used advanced investigative methods to track the culprits. Raids were conducted at 12 locations across five cities, resulting in the arrest of four individuals. Investigators seized key evidence, including bank documents and digital devices. The accused were remanded to five days of police custody.

In a digital arrest scam, a 75-year-old retired engineer was coerced by fraudsters posing as CBI and ED officials into paying ₹4.7 crore. The South-East Cyber Crime Police arrested two individuals, including a Hyderabad-based industrialist, whose accounts were used to receive the funds. The case also revealed links to a Sri Lankan casino, where part of the money was gambled. The victim, unaware of the fraud, had been transferring funds under pressure. The police have seized and returned a portion of the money and continue investigating the broader cyber fraud network.

C. Checklist to Identify Digital Arrest

After going through the cases of digital arrest, a checklist of some questions has been formed.

- Was the victim contacted by someone posing as a government/law enforcement officer?
- Was the victim told that their Aadhaar/bank account was involved in criminal activity?
- Did the contact involve a video or audio call to intimidate or issue threats?
- Was the victim instructed not to leave their home or talk to others?
- Were multiple payments/extortions made over time to “clear their name”?
- Did the victim isolate themselves, act under pressure, or hand over personal documents?

If most of the answers are “yes” then it is likely a digital arrest case not a general cyber fraud.

 [ISSN 2581-5369]

D. Implications of Digital Arrest

The victims pay the cost of being digitally arrested/ detained in various ways. Digital arrest victims are financially, socially, psychologically and legally impacted. Psychological costs of these victims are profound, which often leaves them with long-term emotional scars. Fear and anxiety are the primary impacts as victims deal with the forthcoming threat of lawful repercussions and societal humiliation. These states of mind are intensified by fears about likely harm to their repute, profession, and their private lives for sure. Furthermore, victims generally experience extreme embarrassment, self-blame and guilt, particularly if they have been openly exposed in public or mocked. This situation develops their emotional suffering. Such type of emotional sufferings sometimes may lead to serious conditions like depression or low self-worth. The scam may cause the turmoil of social-exclusion and financial difficulties, which may leave the victims feeling helpless, worthless and desperate. Even, the victims may develop Post-Traumatic Stress Disorder (PTSD)[13]. PTSD is a mental health condition developed after a traumatic event. Some of the characteristics of PTSD are disturbing thoughts, flashbacks, sleep disorders and escaping behaviours. Sometimes the victims are affected by the loss of trust in others as they have been betrayed by cybercriminals which makes it difficult for victims to trust someone [14].

Another implication of digital arrest is social isolation. Due to embarrassment or fear of being victimized again the victims may avoid social situations. This social isolation can lead to loneliness, intense anxiety, mistrust, added delaying social interconnection [15]. Additionally, we can't ignore the economic implication of this scam. It may affect not only individuals but also the businesses and the broader economy. The exhaustion of resources caused by such scams weakens financial productivity and wears away consumer confidence. Legal and Societal challenges are increasing with the growing number of digital arrest cases which in turn poses threat to public safety. Therefore, authorities and civilians need to be more aware and use pre-emptive measures to stay safe from this type of scam. The surprising thing is that educated people are getting more involved or targeted. Every day, we see on TV that IT professionals, police official or the educated class have been digitally arrested and defrauded of money. In view of all this, we can say that the cybercrime policies should be revised. The growing incidence of digital arrest underlines the necessity for streamlining the laws and global cooperation to fight global threats effectively. Figure 3 show money lost in cybercrime from 2019 in billion U.S.dollars.

 [ISSN 2581-5369]

Figure 3: Money lost in Cybercrimes [https://www.statista.com/chart/32341/worldwide-reported-losses-connected-to-cybercrime/]

D. Protecting Oneself from Digital Arrest

To avoid being victimized by such digital frauds one has to be proactive and must have a watchful attitude towards cyber security. To stay safe against digital arrest, it is essential to take hands-on measures. Sustaining good cyber sanitation is a crucial step and this includes keeping software, security and password updated. Two-factor authentication (2FA) should be enabled for reducing the risk of unauthorized access of personal accounts. One should not download files from unidentified sources or click on suspicious links. One has to always verify the legitimacy of emails, phone calls or text messages.

Another way to stay safe is by using protected equipment like; antivirus and anti-malware software. We should also ensure the operating system and other application or system software need to be updated time to time with latest security patches. One should avoid sharing personal data on social platforms and adjust privacy settings to strengthen the protection. Internet connection should be encrypted by the use of Virtual Private Network (VPN) to enhance privacy and security. It is also important for oneself to be aware about the recent trends of cybercrimes happening in the world. There is a program run by the Government of INDIA i.e. Cyberdost by I4C. I4C also launches newsletter for spreading awareness in general public. There are other programs also run by the Government. Such platforms help individuals in staying ahead of potential threats.

Using encrypted secure communication techniques also protects sensitive communications. It is important to use caution while sharing passwords and private information over unsecured channels. To deal with the scams like digital arrest, people should be aware by identifying and blocking fake or questionable calls or any kind of contact the scammers want to create. Even the law enforcement agencies and the telecom sector should shake hands to limit the entry point used by the scammers. People may greatly improve their internet security and reduce the

likelihood of scams by taking these thorough safeguards.

V. CAUTIONS IN DIGITAL DETENTION

The crime of digital detention necessitates careful management to uphold those standards that are set forth in government laws as well as ethical standards, which are based on the human principles of right or wrong. It is essential to use technology ethically, ensuring that digital tools such as electronic devices, software applications, or other resources that use digital technology to perform a task, improve a function or facilitate process for apprehension are only used for legitimate purposes and not for illicit purposes. Information privacy should be prioritized through the implementation of strict regulations aimed at protecting the privacy of those who are not involved and limiting access to sensitive data. Advanced algorithms and cross-verification techniques must be used to reduce errors and avoid false positives when identifying suspects. To maintain the integrity of the tests and ensure their admissibility in legal proceedings, it is essential to maintain the series of documentation and procedures that ensure the evidence is not contaminated or tempered with. It refers to the order in which items of evidence have been handled during the investigations of case. Proving that an item has been properly handled through an unbroken chain of custody, which is required for it to be legally accepted as evidence in court. Additionally, it is essential to protect digital arrest infrastructures from cyber attacks by implementing regular updates and isolated encryption mechanisms to maintain the integrity of the entire process.

VI. AWARENESS FOR EFFECTIVE IMPLEMENTATION OF DIGITAL ARRESTS

Effective digital arrest implementation also demands exhausting acquaintance with strategies to ensure that all stakeholders are conscious of and equipped to handle digital arrest tools. Robust cyber security frame work including hardware and software security, constant cyber patrolling will ensure the safety of common mass from cyber criminals. Law and justice professionals should be trained in the limitations and functions of digital arrest techniques, with ongoing programs designed to improve their technical skills. Initiatives to raise public awareness campaigns through short films, jingles, nukkad nataks, print and social media, sharing vital information on avoiding digital frauds such as OTP frauds, fake websites, and investment frauds etc can play a vital role in educating the public about the importance of cybersecurity and the role of digital forensics in the fight against cybercrime. In addition to fostering a relationship between the police and the public, operational transparency through clear and public protocols can help prevent the misuse of digital arrest technologies. The use of latest technology and support from cybercrime experts ensures pro-active protection against

 [ISSN 2581-5369]

potential threats. Encouraging normative measures that protect individual rights while simultaneously addressing the need for effective legal implementation is necessary to strike a balance between surveillance and privacy. The efforts also include security audits and continuous monitoring of social media and other platforms as well as legal action on cyber fraud-related complaints. Lastly, encouraging collaboration between legal bodies, business leaders, and academic institutions may result in the development of more advanced tools and tactics, strengthening the global fight against cybercrime even more. This integrated strategy, which includes advancements in digital forensics, awareness campaigns, and coordinated international efforts, ensures that digital detentions remain an effective tool in the fight against cybercrime while also protecting individual rights and fostering trust in digital justice.

VII. CHALLENGES AND FUTURE DIRECTIONS

Despite the significant advancements in the equitable treatment of all people in technology and information regardless of race, abilities, gender, age, personal circumstances or social context, the arrest process is still difficult and complex. Certain behaviour's by victims or guards lead to such crimes. False accusations intimidate those impacted by identity fraud, and false notices and racial remarks directed at them further enrage them. The guards keep an eye on the victims in line for these crimes [16].The cutting-edge technology of forensic science and AI is leading to efficiencies and benefits at the same time posing challenges. Numerous key strategies are proposed to address the challenges posed by digital investigations and digital detentions. The uniformed international agreements that strengthen the legal framework may speed up the process of addressing jurisdictional issues. It's a time of rapid change and innovation across many fields, with AI impacting sectors like cyber security.

The government must frame a common set of guidelines for the seizure and handling off documents in digital or paper form, by investigative agencies in connection with their probes, amid indications that the focus is on devising ways to exclude personal chats and documents unrelated to alleged offences from the purview of probes. In order to improve their skills and stay up to date with the latest cybercrime tactics, both governments and businesses must also invest in forensic technologies, particularly in automation solutions based on AI.

Implementing public information programs is essential for educating the public on the best practices for information security, minimizing vulnerabilities, and cyber-attacks. It is essential to start cyber security training as quickly as possible. The need to initiate cyber security education at the earliest possible stages is also suggested by [17] [18]. Additionally, encouraging cooperation between the business, academic, and law enforcement sectors may

 [ISSN 2581-5369]

spur innovation and improve cybercrime prevention measures. In this regard Microsoft plans to invest $3 billion in India in cloud and AI infrastructure, including setting up new data centres over the next two years for training 10 million technocrats with AI skills by 2030. As the diffusion rate of AI is exciting, therefore this is the golden time for system when it comes to innovation. In conclusion, it is essential to adjust to technological advancements like AI, block chain [19], and quantum computing.

VIII. CONCLUSION

The growing prevalence of "Digital Arrest" crime possess a huge risk to the principle that data is complete, trustworthy and has not been modified or accidently altered by an unauthorized user. The use fear as a powerful tool to influence and deceive victims is the key factor. By inculcating an imaginary sense of exposure to the risk, the criminals are able to compel by force for enormous sums of money out of their victims, hence underscoring the urgent requirement for comprehensive measures to combat this crime. Individuals who have successfully resisted such schemes serve as a role model and source of motivation for society, which is a very encouraging development. It is advised not to disclose the confidential personal information and not get affected psychologically which considerably reduces the risk. At the same time, it is essential for citizens to remain informed about changing cyber risks, adopt educated practices, and harness collective knowledge. The laws governing cyber security need to be strengthened by legislative authorities, and international cooperation is necessary in order to combat the transnational nature of these syndicates that are registered in different jurisdictions.

*****

 [ISSN 2581-5369]

IX. REFERENCES

[1] G. Horsman and A. Dodd, "Competence in digital forensics," *Forensic Science International: Digital Investigation,* vol. 51, p. 301840, 2024.

[2] M. Pollitt, "A history of digital forensics," in *Advances in Digital Forensics VI: Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, January 4-6, 2010, Revised Selected Papers 6*, 2010.

[3] H. Arshad, A. B. Jantan and O. I. Abiodun, "Digital forensics: review of issues in scientific validation of digital evidence," *Journal of Information Processing Systems,* vol. 14, p. 346–376, 2018.

[4] G. Horsman, "Tool testing and reliability issues in the field of digital forensics," *Digital Investigation,* vol. 28, p. 163–175, 2019.

[5] P. M. Wanjohi, "Curbing mobile phone terrorism and financial fraud: A Kenyan perspective," *Journal of ICT Standardization,* vol. 4, p. 237–246, 2016.

[6] S. Sai, U. Yashvardhan, V. Chamola and B. Sikdar, "Generative ai for cyber security: Analyzing the potential of chatgpt, dall-e and other models for enhancing the security space," *IEEE Access,* 2024.

[7] A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," *IEEE Access,* vol. 11, p. 137188–137203, 2023.

[8] T. Awosika, R. M. Shukla and B. Pranggono, "Transparency and privacy: the role of explainable ai and federated learning in financial fraud detection," *IEEE Access,* 2024.

[9] R. Montasari, R. Hill, S. Parkinson, P. Peltola, A. Hosseinian-Far and A. Daneshkhah, "Digital forensics: challenges and opportunities for future studies," *International Journal of Organizational and Collective Intelligence (IJOCI),* vol. 10, p. 37–53, 2020.

[10] A. Hosseinian-Far, M. Ramachandran and D. Sarwar, Strategic engineering for cloud computing and big data analytics, Springer, 2017.

[11] A. Mallick and P. Ganguli, "Understanding Of Digital Arrest: Definition, Methods And Implications," *Methods And Implications (September 27, 2024),* 2024.

 [ISSN 2581-5369]

[12] N. s. Pooja Yadav, "Digital Arrest: Exploring Disruptions In The Digital Ecosystem With An Indian Perspective," *International Journal of Research Publication and Reviews,* vol. 5, pp. 3398-3400, December 2024.

[13] R. Pant and U. Chaubey, "Protecting Minds in the Digital Age: A Review Based Study on Psychological Impact of Cybercrime," *International Journal of Indian Psychology,* vol. 12, 2024.

[14] L. Ahe, "Mental Wellbeing and Cybercrime (The Psychological Impact of Cybercrime on the Victim)," 2022.

[15] T. Begotti, M. Bollo and D. Acquadro Maran, "Coping strategies and anxiety and depressive symptoms in young adult victims of cyberstalking: A questionnaire survey in an Italian sample," *Future Internet,* vol. 12, p. 136, 2020.

[16] J. Chauhan, "Digital Arrest: An Emerging Cybercrime in India," *International Jounral of Law Management & Humanities,* vol. 7, pp. 1632-1646, 2024.

[17] M. Ayyash, T. Alsboui, O. Alshaikh, I. Inuwa-Dute, S. Khan and S. Parkinson, "Cybersecurity Education and Awareness Among Parents and Teachers: A Survey of Bahrain," *IEEE Access,* 2024.

[18] A. Sareen and S. Jasaiwal, "Need of cyber security education in modern times".

[19] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*, 2017.

*****

 [ISSN 2581-5369]