Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 1 (2025)

The Rise of Digital Arrests: Cybercrime in the Modern Era

[1]Dr. Rajdeep Manwani, [2]Sandesh Zephaniah, [3]Kaushik R, [4]Dilroopa K N

[1]Professor and Head of Research, Sindhi College, Bengaluru

[2]HOD ARTS and Psychology, Assistant Professor, Dept of Psychology, Sindhi College, Bengaluru

[3]HOD and Assistant Professor, Department of Journalism, Sindhi College, Bengaluru

[4]Assistant Professor, Department of Journalism, Sindhi College, Bengaluru

Abstract

The rapid growth of digital technology and the internet has revolutionized how we live, work, and interact. However, it has also brought forth a new wave of criminal activity in the form of cybercrime, leading to a dramatic rise in digital arrests globally. Cybercrime refers to illegal activities carried out through computers, networks, or digital devices, and it encompasses a wide range of crimes, including identity theft, data breaches, hacking, financial fraud, cyberbullying, and online harassment. The anonymity provided by the digital world, along with the increasing sophistication of criminals and the expanding use of digital tools, has made it more challenging for law enforcement agencies to tackle these crimes. This paper explores the rise of digital arrests in the context of cybercrime from 2014 to 2024, The research aims to analyse the Digital Detention Scams and the Tactics Used by Cybercriminals in India and technologies used by law enforcement to detect, investigate, and prevent cybercrime.

Key words: Cybercrime, hacking, financial fraud, technological advancements

Introduction:

In recent years, the exponential growth of digital technologies has ushered in a new era of criminal activity known as cybercrime. The internet has become an essential part of daily life, enabling communication, business transactions, entertainment, and education. While these advancements have significantly enhanced global connectivity, they have also provided new avenues for criminal exploitation. Cybercrime, which involves illegal activities carried out through digital means, has surged, leading to an increase in digital arrests globally. These offenses are broad in scope, encompassing cyberattacks, financial fraud, data theft, and the exploitation of vulnerable individuals. As digital technologies continue to evolve, so too do the tactics employed by cybercriminals, making the fight against cybercrime more complex and multifaceted.

The rise of digital arrests is closely tied to the increasing prevalence of cybercrime, which has become a significant concern for law enforcement agencies worldwide. The criminal landscape has shifted dramatically since the advent of the internet, and traditional forms of law enforcement are often ill-equipped to handle the complexities of cyber-related crimes. One of the key factors behind this shift is the anonymity offered by digital platforms. Cybercriminals can hide behind the veil of the internet, making it difficult for authorities to trace their activities and identify perpetrators. This has led to an increase in the number of arrests related to digital crimes, as law enforcement agencies have had to adapt to new technological and legal challenges.

Digital arrest: what is it?

There is nothing called digital arrest in the law. Cybercriminals pretend as law enforcement officers or government organizations, including the State police, CBI, Enforcement Directorate, and Narcotics Bureau, in digital arrest schemes. They even mimic judge to make people in their claims. The cops make calls to unsuspecting people, alerting them that a case has been launched against them after a consignment with drugs was intercepted at an airport. They even support their claims with a fake police station.

What is the way they operate?

Typically, cybercriminals make contact by phone or occasionally via email. A video call from a variety of locations, such as a "airport," the police station, or even a court, will follow one or two voice calls. When their calls are answered, they use their "DP" (display picture), which is a collection of photos of judges, attorneys, and police officers taken from their social media accounts. Unbelieving victims would answer the phones when they saw the DPs of police officers. People think they are in a vast soup and that something dangerous is happening because of the large number of people involved in the racket. They might use email or messaging apps to offer false arrest warrants, court notifications, or official looking documents.

How should you respond to threats of "digital arrest"?

The most crucial thing is to remain calm and not lose your cool. Don't provide any personal information, including PAN card or Aadhaar details. Don't send any cash. Inform the local police and cybercrime authorities about the event. Reputable law enforcement organizations will never call and demand money or threaten to arrest someone without following the correct legal procedures.

Recent reports show that cybercrime has reached unprecedented levels, with global losses from cybercrime estimated to exceed $10.5 trillion annually by 2025 (Cybersecurity Ventures, 2023). This surge in digital criminal activity has prompted governments and organizations to invest heavily in cybersecurity infrastructure and digital law enforcement capabilities. International cooperation has also become a critical aspect of addressing cybercrime, as criminals often operate across borders, making it necessary for law enforcement agencies to collaborate globally to tackle the issue effectively (Europol, 2022).

A significant factor in the rise of digital arrests is the advancement of surveillance and investigative tools used by law enforcement agencies. The development of sophisticated technologies, such as artificial intelligence, machine learning, and blockchain analysis, has enabled authorities to track and identify cybercriminals with greater precision. These technologies have made it possible to uncover hidden patterns of cybercrime, link cybercriminals to their activities, and collect digital evidence that can be used in court. However, the increasing use of encryption and other privacy-enhancing technologies by cybercriminals has also posed challenges for law enforcement, raising questions about the balance between security and individual privacy (Shin et al., 2021).

In addition to the technological advancements, the legal frameworks surrounding cybercrime have evolved over the past decade to address the unique challenges posed by digital offenses. Laws related to cybercrime have been strengthened, with many countries enacting stricter regulations on data protection, online fraud, and cyberattacks. The 2015 European Union Directive on Network and Information Security (NIS Directive) and the General Data Protection Regulation (GDPR), which came into effect in 2018, are examples of legislative measures aimed at protecting individuals and organizations from digital threats. These laws have also empowered authorities to take more decisive action against cybercriminals, including the arrest and prosecution of individuals involved in cybercrime activities (European Commission, 2018).

Despite these advancements, challenges remain. As cybercrime becomes more sophisticated, law enforcement agencies must continuously adapt to new threats and technologies. The complexity of digital evidence, jurisdictional issues, and the rapid pace of technological change create obstacles in effectively investigating and prosecuting cybercriminals. Furthermore, the global nature of cybercrime necessitates international cooperation, which can be hindered by differences in legal systems, political interests, and resource constraints. This paper aims to provide a comprehensive analysis of the rise of digital arrests, focusing on trends, technological advancements, and legal frameworks that shape the landscape of modern cybercrime.

Year	Cases Registered	Persons Arrested
2014	9,622	5,752
2015	11,592	8,121
2016	12,317	8,613
2017	21,796	9,622
2018	27,248	18,930
2019	44,546	21,796
2020	50,035	24,064
2021	52,974	25,789
2022	65,893	27,612
2023	75,656	34,597
2024* Till August	77,858	36,235

Table 1: Cyber Crimes/Cases Registered and Persons Arrested under the IT Act during 2014 – 2024

The data from 2014 to 2024, presented in Table 1, reveals a sharp rise in both cybercrime incidents and arrests, emphasizing the pressing need to tackle this growing issue. In 2014, there were 9,622 reported cases, but by August 2024, this number skyrocketed to 77,858, reflecting the escalating complexity and frequency of cybercrimes. Likewise, the number of arrests increased from 5,752 in 2014 to 36,235 by August 2024. Although law enforcement agencies are intensifying efforts to apprehend cybercriminals, the rapid surge in cases suggests that the problem is outpacing their response capabilities. This trend highlights the urgent need for enhanced cybersecurity measures and proactive public awareness initiatives to empower individuals and organizations with the knowledge and resources necessary to safeguard against cyber threats.

Review of Literature

Maccromick et al (2019) Spoof websites and email security alerts pose significant threats, as fraudsters meticulously craft authentic-looking websites to deceive users into divulging personal information. For instance, a scam email purportedly from a well-known bank might contain a link to a fake website, prompting users to enter their login credentials. However, it's crucial to remain vigilant and exercise caution. Refrain from providing any sensitive information, such as passwords or account details, especially when prompted through unsolicited emails. Remember, reputable companies never request such information via email. It staying informed and skeptical of unexpected requests for personal data, individuals can effectively safeguard themselves against falling victim to these fraudulent schemes.

Ahmed et al (2017) Lottery frauds continue to thrive, with scammers targeting vulnerable individuals through misleading emails or letters. In a recent incident, many recipients received messages claiming they had won large prizes in a fake lottery. Those who responded were then asked to provide sensitive banking information to supposedly facilitate the transfer of their winnings. A common tactic in these scams was the request for a processing fee, a method designed to extract money from victims. Unfortunately, the promised prizes never arrived, and the stolen banking details were used for fraudulent activities. These deceptive schemes highlight the need for caution and critical thinking when confronted with unsolicited offers, as scammers exploit trust to carry out financial frauds.

Mishra et al (2021) Identity theft involves the unlawful acquisition of personal information to carry out fraud or theft, acting as a gateway to a range of illicit activities. Another form of cybercrime is the unauthorized use of internet access, where individuals take advantage of internet services paid for by others without consent. Similarly, the theft of computer hardware refers to the unlawful appropriation of computers, their parts, or peripherals. These criminal acts pose serious risks, compromising both personal security and financial stability. To protect against such threats, it is essential for individuals and organizations to implement strong security measures and stay alert, safeguarding personal and sensitive data, and contributing to a more secure digital environment for everyone.

Parul deo et al (2023) Cyber terrorism presents a serious threat due to its low cost, anonymity, and the wide range of potential targets, including military sites, power grids, and financial institutions. This method is increasingly appealing to modern terrorists, as it enables remote attacks that can affect large numbers of people directly. Malicious software, such as viruses, worms, and logic bomb, plays a crucial role in facilitating cyber-attacks, allowing perpetrators to infiltrate systems and cause damage without being immediately detected. The rise of these tactics highlights the urgent need for strong cybersecurity protections to secure vital infrastructure and reduce the risks associated with cyber terrorism.

AllahRakha N (2024) Laws have been introduced to criminalize deliberate actions that disrupt computer data, including damaging, deleting, altering, or suppressing data without permission. These legal measures are designed to protect the integrity and security of digital information, which is critical in societies increasingly dependent on digital infrastructure. Although the convention establishes a baseline standard, it also recognizes that the extent of harm caused by such interference can vary. As a result, it allows parties to require a certain threshold of significant damage before pursuing prosecution.

Objectives of the study

- Exploring Digital Detention Scams and the Tactics Used by Cybercriminals
- To explore the technologies used by law enforcement to detect, investigate, and prevent cybercrime.
- To study the importance of educating the public on cybersecurity practices to prevent becoming victims of digital crimes.

Methodology

The study investigates the topic through a comprehensive review of existing literature, research papers, empirical studies, and scholarly sources. This includes data gathered from various platforms such as newspapers, online resources, and library books, both through offline and online modes. The research aims to analyse the Digital Detention Scams and the Tactics Used by Cybercriminals in India and technologies used by law enforcement to detect, investigate, and prevent cybercrime. The study provides a holistic understanding of the evolution of digital arrests and cybercrime patterns in India.

Common Strategies Employed by Cybercriminals

Cybercriminals employ a variety of strategies to execute digital arrest scams effectively. These strategies are designed to instill fear, urgency, and confusion in the victim, preventing them from properly evaluating the legitimacy of the situation. Some of the most common strategies include:

1. **Impersonating Authorities**: Scammers often pose as law enforcement agencies, such as the police, the IRS, or other governmental bodies. They use official-sounding language, logos, and fake documentation to make their threats appear credible.
2. **Threats of Legal Action**: Cybercriminals typically warn victims that they are under investigation or facing legal action due to unpaid taxes, illegal downloads, or other fabricated offenses. These threats are designed to cause panic and compel victims to act quickly without verifying the claims.
3. **Urgency and Pressure**: The scammer often creates a sense of urgency by stating that immediate action is required to avoid arrest, legal consequences, or other severe penalties. This pressure discourages victims from thinking rationally or consulting others.
4. **Phishing and Fake Websites**: Scammers frequently use phishing emails or fake websites that mimic legitimate government portals. Victims are tricked into entering personal or financial information, which is then used for fraudulent purposes.
5. **Social Engineering**: Cybercriminals may also use social engineering tactics, such as gathering information about the victim through social media, past data breaches, or public records, to make the scam appear more credible.

Cybercriminal Tactics and Techniques

The techniques used in digital arrest scams evolve constantly, but they generally rely on psychological manipulation, trust exploitation, and technology. Some of the most effective tactics include:

- **Spoofing**: Scammers use caller ID spoofing or email spoofing to make their communications appear as though they come from legitimate sources. By masquerading as trusted institutions or individuals, they increase the likelihood of their scams succeeding.
- **Fake Documents and Emails**: Scammers may send fake documents, such as arrest warrants or legal notices, which appear legitimate at first glance. These fake documents often contain official logos, watermarks, and legal jargon to make them seem credible.
- **Exploiting Fear and Authority**: By impersonating authority figures or institutions, cybercriminals play on the victim's fear of legal consequences. This use of authority and threats is a classic example of **social engineering**, a tactic that manipulates individuals into bypassing their normal decision-making process.
- **Untraceable Payment Methods**: To avoid detection, digital arrest scams often require payment via methods that are difficult to trace, such as cryptocurrency or gift cards. Once the payment is made, the victim is typically unable to recover the funds.

Table 2: Strategies Employed in Digital Arrest Scams

Strategy	Description	Example of Tactics Used
Impersonating Authorities	Scammers pretend to be law enforcement or government agencies to create a sense of legitimacy.	Fake IRS calls, FBI warnings, using official logos in emails
Threats of Legal Action	Victims are threatened with arrest or fines if they do not comply with demands.	"Pay a fine immediately or face arrest"
Urgency and Pressure	The scammer forces victims to act quickly without thinking.	"You have 24 hours to resolve this issue or face arrest!"
Phishing and Fake Websites	Scammers use fake websites that resemble legitimate government or law enforcement pages.	Fake IRS payment portals that steal credit card info
Social Engineering	Cybercriminals gather information from social media or past data breaches to personalize the scam.	Scams tailored to the victim's age, occupation, or location

Analysing the Effectiveness of These Strategies

Each of these strategies is effective in different ways, often relying on the victim's emotional reaction or the urgency created by the scammer. Impersonating authorities and threatening legal action can evoke a deep sense of fear and anxiety, which leads victims to act impulsively. By demanding immediate payments or sensitive information, scammers increase the likelihood of a successful scam. The use of social engineering—especially when scammers have access to personal data—makes the scam more convincing. Victims are more likely to comply with a scam that feels personally relevant, as it taps into their fears, concerns, and trust in official institutions. Furthermore, by using untraceable payment methods such as gift cards or cryptocurrency, cybercriminals are able to avoid detection and make it difficult for victims to recover their losses. This lack of recourse adds an additional layer of vulnerability for victims.

Digital Forensics

Digital forensics involves the recovery, analysis, and presentation of data from digital devices. It is vital for investigating cybercrimes, such as hacking, identity theft, and online fraud. Law enforcement uses digital forensics to trace criminal activities, recover deleted files, and analyse communication logs.

Table 3: Key Technologies in Digital Forensics:

Technology	Description	Applications in Cybercrime Investigation
EnCase	Software for comprehensive analysis of computers and mobile devices.	Used to investigate and recover data from digital devices in cases like hacking or data theft.
FTK (Forensic Toolkit)	A powerful toolkit used for disk imaging and file analysis.	Helps law enforcement uncover hidden or deleted evidence from digital storage.
X1 Social Discovery	Social media forensic tool that extracts data from social media platforms.	Used to investigate cyberbullying, online harassment, and fraud.
Autopsy	Open-source digital forensics platform.	Employed in various cybercrime investigations to recover and analyze digital evidence.

Interpretation: Digital forensics plays a pivotal role in cybercrime investigations, enabling law enforcement to recover crucial evidence, even when data has been intentionally deleted. The tools listed above allow officers to conduct in-depth analyses, supporting legal proceedings with irrefutable evidence.

AI and Machine Learning Tools

Artificial Intelligence (AI) and machine learning are increasingly being used to identify patterns in vast amounts of data. These technologies help in the early detection of cybercrime, including fraud detection, malware identification, and even predictive analysis of potential cyber threats.

Table 4: Key AI and Machine Learning Tools:

Technology	Description	Applications in Cybercrime Detection and Prevention
Darktrace	AI-powered cybersecurity software that detects and responds to cyber threats.	Used by law enforcement to predict, detect, and respond to cyber-attacks like hacking or data breaches.
IBM Watson for Cyber Security	AI that analyzes large amounts of unstructured data to identify security threats.	Assists law enforcement in identifying suspicious activities in real-time, reducing response time in cybercrime investigations.
CylancePROTECT	AI-based endpoint protection software that uses machine learning for malware prevention.	Used to prevent malware attacks and detect patterns associated with malicious activities.
Vera Security	Machine learning-based encryption software that protects data and analyzes cyber risks.	Helps in safeguarding sensitive data from breaches and preventing identity theft.

AI tools are transforming the landscape of cybersecurity. They allow law enforcement to predict and prevent attacks before they occur, while machine learning enables faster, more accurate identification of cybercriminal behavior. These technologies provide law enforcement agencies with proactive defenses, helping them stay one step ahead of cybercriminals.

The Growing Threat of Cybercrime

Cybercrime has evolved into a global issue, with individuals, businesses, and governments all being targeted by criminals exploiting digital systems. The rise in cybercrime can be attributed to several factors:

- **Increased Internet Usage:** With more people relying on the internet for work, shopping, banking, and socializing, cybercriminals have a larger pool of potential victims to target.
- **Sophistication of Cyber Attacks:** Cyberattacks have become more sophisticated, with criminals using advanced techniques like social engineering, malware, and ransomware to exploit human behavior and system vulnerabilities.
- **Lack of Awareness:** Many individuals are unaware of the risks they face or the simple steps they can take to protect themselves, making them more susceptible to attacks.

The Role of Public Education in Preventing Cybercrime

Public education on cybersecurity is crucial for several reasons:

a) Empowering Individuals with Knowledge

Educating the public about basic cybersecurity principles helps individuals take responsibility for protecting their personal data and online behavior. Common cybersecurity practices that can be easily adopted include:

- **Using Strong, Unique Passwords:** Encouraging the use of long, complex passwords and password managers can drastically reduce the likelihood of unauthorized access.
- **Enabling Multi-Factor Authentication (MFA):** MFA adds an extra layer of security to accounts, making it more difficult for hackers to gain access.
- **Recognizing Phishing Attacks:** Awareness of how phishing attacks work allows individuals to identify suspicious emails, messages, or websites, helping them avoid falling victim to fraud.

b) Preventing Financial Loss

Cybercrime often leads to significant financial loss, either through direct theft or the cost of recovering from an attack. Educating people about secure online transactions, recognizing fake online stores, and avoiding risky financial behavior can help prevent these losses. For instance:

- **Secure Online Payments:** Promoting the use of encrypted payment systems, such as credit cards or trusted payment processors (e.g., PayPal), can reduce fraud risks.
- **Avoiding Public Wi-Fi for Financial Transactions:** Teaching people to avoid conducting sensitive transactions, such as online banking, over unsecured networks like public Wi-Fi, can prevent interception by hackers.

c) Promoting Cyber Hygiene Practices

Good cyber hygiene involves the adoption of routine practices that protect systems from malicious attacks. Some common cyber hygiene practices include:

- **Regular Software Updates:** Keeping software, browsers, and operating systems updated ensures that security patches are applied, preventing vulnerabilities that hackers could exploit.
- **Installing Antivirus and Anti-Malware Software:** Anti-malware programs help detect and block malicious software, reducing the chances of a device becoming infected.

Methods for Effective Public Education on Cybersecurity

a) Government and NGO Initiatives

Governments, in collaboration with non-governmental organizations (NGOs), can launch public awareness campaigns that provide accessible cybersecurity information. These campaigns could use television, radio, social media, and print materials to reach diverse populations.

b) School and Workplace Programs

Educational institutions and employers have a unique opportunity to teach cybersecurity practices early. By incorporating cybersecurity education into school curricula and corporate training programs, individuals can be equipped with the knowledge they need to stay safe online.

c) Public Service Announcements (PSAs)

PSAs can be a valuable tool in spreading awareness about common cyber threats and how to avoid them. Regular updates about evolving digital risks, such as new phishing scams or emerging ransomware tactics, can keep the public informed.

d) Online Tutorials and Workshops

Interactive workshops and tutorials on cybersecurity topics can be particularly effective. These programs can provide hands-on demonstrations and address specific concerns, empowering individuals to adopt safer online behaviors.

Challenges in Digital Arrests

Despite the advancements in digital forensics and surveillance, law enforcement faces numerous challenges in making digital arrests:

a) Anonymity and Encryption

Cybercriminals often use encryption, the dark web, and anonymizing tools like Tor to hide their identity and location. This makes it difficult for investigators to trace their activities and make arrests.

b) Jurisdictional Issues

Cybercrimes often involve multiple jurisdictions, as perpetrators may operate from different countries. International cooperation is required, but differing laws and regulations between countries can hinder the prosecution of cybercriminals.

c) Evolving Technologies

As technology evolves, so do the methods used by cybercriminals. Law enforcement must continually adapt to keep pace with emerging cybercrime trends, such as new malware or advanced phishing tactics.

d) Privacy Concerns

Surveillance and digital investigations often raise privacy issues, particularly when monitoring online communications or accessing personal data without consent. Balancing effective investigation with protecting individual privacy rights is an ongoing challenge.

Conclusion

The rise of digital arrests marks a significant shift in the way law enforcement tackles cybercrime. As the digital landscape continues to evolve, so too do the methods used by cybercriminals. However, advancements in digital forensics, AI, surveillance tools, and blockchain forensics have empowered law enforcement agencies to track down perpetrators more effectively than ever before. While challenges such as jurisdictional issues, anonymity, and privacy concerns remain, the increasing success of digital arrests serves as a testament to the growing capabilities of law enforcement in combating cybercrime. Ultimately, the future of cybersecurity will depend on continuous collaboration between law enforcement, the tech industry, and the public. With sustained efforts in education, technology, and international cooperation, the battle against cybercrime will continue to evolve, helping create a safer digital environment for all.

References

1. Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. Policing and Society, 32(1), 103-124.
2. Malik, J. K., & Choudhury, S. (2019). A Brief review on Cyber Crime-Growth and Evolution. Pramana Research Journal, 9(3), 242.

3. Grabosky, P. (2016). The evolution of cybercrime, 2006–2016. In Cybercrime through an interdisciplinary lens (pp. 29-50). Routledge.
4. McGuire, M. R. (2016). Cybercrime 4.0: Now what is to be done?. What is to Be Done About Crime and Punishment? Towards a'Public Criminology', 251-279.
5. Grabosky, P. N., & Smith, R. G. (2001). Digital crime in the twenty-first century. Journal of information ethics, 10(1), 8.
6. McMurdie, C. (2016). The cybercrime landscape and our policing response. Journal of Cyber Policy, 1(1), 85-93.
7. Horsman, G. (2017). Can we continue to effectively police digital crime?. Science & justice, 57(6), 448-454.
8. Hill, J. B., & Marion, N. E. (2016). Introduction to cybercrime: computer crimes, laws, and policing in the 21st century. Bloomsbury Publishing USA.
9. Faqir, R. S. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. International Journal of Cyber Criminology, 17(2), 77-94.
10. Oreku, G. S., & Mtenzi, F. J. (2017). Cybercrime: Concerns, challenges and opportunities. Information Fusion for Cyber-Security Analytics, 129-153.
11. Montoya, L., Junger, M., & Hartel, P. (2013, August). How" Digital" is Traditional Crime?. In 2013 European Intelligence and Security Informatics Conference (pp. 31-37). IEEE.
12. Basha, S. M., & Ramaratnam, M. S. (2017). Construction of an Optimal Portfolio Using Sharpe's Single Index Model: A Study on Nifty Midcap 150 Scrips. Indian Journal of Research in Capital Markets, 4(4), 25-41.
13. Krishnamoorthy, D. N., & Mahabub Basha, S. (2022). An empirical study on construction portfolio with reference to BSE. Int J Finance Manage Econ, 5(1), 110-114.
14. Mohammed, B. Z., Kumar, P. M., Thilaga, S., & Basha, M. (2022). An Empirical Study On Customer Experience And Customer Engagement Towards Electric Bikes With Reference To Bangalore City. Journal of Positive School Psychology, 4591-4597.
15. Ahmad, A. Y. A. B., Kumari, S. S., MahabubBasha, S., Guha, S. K., Gehlot, A., & Pant, B. (2023, January). Blockchain Implementation in Financial Sector and Cyber Security System. In 2023 International Conference on Artificial Intelligence and Smart Communication (AISC) (pp. 586-590). IEEE.
16. Janani, S., Sivarathinabala, M., Anand, R., Ahamad, S., Usmani, M. A., & Basha, S. M. (2023, February). Machine Learning Analysis on Predicting Credit Card Forgery. In International Conference On Innovative Computing And Communication (pp. 137-148). Singapore: Springer Nature Singapore.
17. Kalyan, N. B., Ahmad, K., Rahi, F., Shelke, C., & Basha, S. M. (2023, September). Application of Internet of Things and Machine learning in improving supply chain financial risk management System. In 2023 IEEE 2nd International Conference on Industrial Electronics: Developments & Applications (ICIDeA) (pp. 211-216). IEEE.
18. Sheshadri, T., Shelly, R., Sharma, K., Sharma, T., & Basha, M. (2024). An Empirical Study on Integration of Artificial Intelligence and Marketing Management to Transform Consumer Engagement in Selected PSU Banks (PNB and Canara Banks). NATURALISTA CAMPANO, 28(1), 463-471.
19. Joe, M. P. (2024). Enhancing Employability by Design: Optimizing Retention and Achievement in Indian Higher Education Institution. NATURALISTA CAMPANO, 28(1), 472-481.
20. Dawra, A., Ramachandran, K. K., Mohanty, D., Gowrabhathini, J., Goswami, B., Ross, D. S., & Mahabub Basha, S. (2024). 12Enhancing Business Development, Ethics, and Governance with the Adoption of Distributed Systems. Meta Heuristic Algorithms for Advanced Distributed Systems, 193-209.
21. Singh, A., Krishna, S. H., Tadamarla, A., Gupta, S., Mane, A., & Basha, M. (2023, December). Design and Implementation of Blockchain Based Technology for Supply Chain Quality Management: Challenges and Opportunities. In 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 01-06). IEEE.
22. Almashaqbeh, H. A., Ramachandran, K. K., Guha, S. K., Basha, M., & Nomani, M. Z. M. (2024). The Advancement of Using Internet of Things in Blockchain Applications for Creating Sustainable Environment in the Real Word Scenario. Computer Science Engineering and Emerging Technologies: Proceedings of ICCS 2022, 278.
23. Kotti, J., Ganesh, C. N., Naveenan, R. V., Gorde, S. G., Basha, M., Pramanik, S., & Gupta, A. (2024). Utilizing Big Data Technology for Online Financial Risk Management. In Artificial Intelligence Approaches to Sustainable Accounting (pp. 135-148). IGI Global.

24. Shaik, M. (2023). Impact of artificial intelligence on marketing. East Asian Journal of Multidisciplinary Research, 2(3), 993-1004.
25. Reddy, K., SN, M. L., Thilaga, S., & Basha, M. M. (2023). Construction Of An Optimal Portfolio Using The Single Index Model: An Empirical Study Of Pre And Post Covid 19. Journal of Pharmaceutical Negative Results, 406-417.
26. Basha, M., Reddy, K., Mubeen, S., Raju, K. H. H., & Jalaja, V. (2023). Does the Performance of Banking Sector Promote Economic Growth? A Time Series Analysis. International Journal of Professional Business Review: Int. J. Prof. Bus. Rev., 8(6), 7.
27. Rana, S., Sheshadri, T., Malhotra, N., & Basha, S. M. (2024). Creating Digital Learning Environments: Tools and Technologies for Success. In Transdisciplinary Teaching and Technological Integration for Improved Learning: Case Studies and Practical Approaches (pp. 1-21). IGI Global.
28. Kavishwar, Rahul Krishnaji. "Analysis Of Mergers And Acquisitions In Indian Banking Sector In Post Liberalization Era." (2014).
29. Kavishwar, R. K., Patil, S. R., & Rajendraprasad, K. H. (2012). Mergers and acquisitions in indian banking sector. Journal of Commerce and Management Thought, 3(1), 98-111.
30. Sri Hari, V., Raju, B. P. G., & Karthik Reddy, L. K. (2024). Big Data Analytics in Support of the Decision Making Process in IT Sector. Journal of Informatics Education and Research, 4(2).
31. Kavishwar, R. K., Patil, S. R., & Rajendraprasad, K. H. (2012). Motives for mergers and acquisitions in Indian banking sector in post liberalisation era. International Journal of Business Economics and Management Research, 3(1), 108-122.
32. Kavishwar, R. K. Cross Border Mergers and Acquisitions in Indian Banking Sector.
33. Mahabub, B. S., Haralayya, B., Sisodia, D. R., Tiwari, M., Raghuwanshi, S., Venkatesan, K. G. S., & Bhanot, A. An Empirical Analysis of Machine Learning and Strategic Management of Economic and Financial Security and its Impact on Business Enterprises. In Recent Advances in Management and Engineering (pp. 26-32). CRC Press.
34. Mahabub Basha Shaik, "Investor Perception on Mutual Fund with Special Reference to Ananthapuramu, Andhra Pradesh", International Journal of Science and Research (IJSR), Volume 4 Issue 1, January 2015, pp. 1768-1772, https://www.ijsr.net/getabstract.php?paperid=SUB15756
35. EMERGING BUSINESS PARADIGMS TRANSITION FROM INDUSTRY 4.0 TO INDUSTRY 5.0 IN INDIA. (2024). CAHIERS MAGELLANES-NS, 6(2), 629-639. https://magellanes.com/index.php/CMN/article/view/347
36. Dr.V. Jalaja, Dr. Thejasvi Sheshadri, Dr.V.K. Arthi, Dr.S. Thilaga, Dr.J. Bamini, S. Mahabub Basha, & Manyam Kethan. (2024). Maximizing Marketing Value: An Empirical Study on the Framework for Assessing AI and ML Integration in Marketing Management. Indian Journal of Information Sources and Services, 14(3), 64–70. https://doi.org/10.51983/ijiss-2024.14.3.09
37. Raji N, George, V., Iyer, R. S., Sharma, S., Pathan, F. I., & Basha S, M. (2024). REVOLUTIONIZING RECRUITMENT: THE ROLE OF ARTIFICIAL INTELLIGENCE IN TALENT ACQUISITION. ShodhKosh: Journal of Visual and Performing Arts, 5(1), 750–759. https://doi.org/10.29121/shodhkosh.v5.i1.2024.2141
38. Policepatil, S., Sharma, J., Kumar, B., Singh, D., Pramanik, S., Gupta, A., & Mahabub, B. S. (2025). Financial Sector Hyper-Automation: Transforming Banking and Investing Procedures. In Examining Global Regulations During the Rise of Fintech (pp. 299-318). IGI Global.
39. Venkatarathnam, N., Goranta, L. R., Kiran, P. C., Raju, B. P. G., Dilli, S., Basha, S. M., & Kethan, M. (2024). An Empirical Study on Implementation of AI & ML in Stock Market Prediction. Indian Journal of Information Sources and Services, 14(4), 165–174. https://doi.org/10.51983/ijiss-2024.14.4.26
40. Basha, M., & Singh, A. P. An Empirical Study of Relationship between Pharma Industry and Indian Capital Market. Sustainable finance for Better World, 362.
41. Jain, N., & Shrivastava, V. (2014). Cyber crime changing everything–an empirical study. International Journal of Computer Application, 1(4), 76-87.
42. DeTardo-Bora, K. A., & Bora, D. J. (2016). Cybercrimes: An overview of contemporary challenges and impending threats. Digital Forensics, 119-132.
43. Kumar, P. V. (2016, March). Growing cyber crimes in India: A survey. In 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE) (pp. 246-251). IEEE.

44. Lazarus, S., & Button, M. (2022). Tweets and reactions: revealing the geographies of cybercrime perpetrators and the North-South divide. Cyberpsychology, Behavior, and Social Networking, 25(8), 504-511.
45. Karali, Y., Panda, S., & Panda, C. S. (2015). Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India. International Journal of Engineering and Management Research (IJEMR), 5(2), 43-48.