iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70702

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

AI-Powered Cybercrime Reporting System

Sabitha K[1], Jeyaprabakaran S[2], Vishwanatha Sriram M[3], Albin Tenny[4], Sasidharan S[5]
[1]*Assistant Professor,* [2, 3, 4, 5]*Student, Department of Cyber Security, Sri Shakthi Institute of Engineering And Technology, Coimbatore, India*

Abstract:With the exponential increase in digital threats, the traditional cybercrime reporting process remains largely unstructured and inaccessible to common users.This article proposes an AI-powered cybercrime reporting system that takes advantage of natural language processing and machine learning to offer an intelligent, guided interface for victims to report incidents.The system employs a fine-tuned RoBERTa-base model to classify cybercrimes into 23 predefined categories based on user descriptions and dynamically adjusts the reporting flow to collect appropriate data. Additionally, it enables secure digital evidence handling and automated PDF report generation for law enforcement. The proposed system improves reporting accuracy, user confidence, and evidence completeness, representing a transformative change in digital law enforcement support tools.

Keywords: Cybercrime, Artificial Intelligence, NLP, Evidence handling, Fine-tuned RoBERTa, Crime reporting, PDF generation, law enforcement support

I. INTRODUCTION

Cybercrime is a growing issue, and it presents significant challenges when it comes to reporting and law enforcement. This is especially true for people who aren't familiar with technology. Traditional systems are often unclear and inconsistent, making it difficult for people to report cybercrimes and for authorities to respond effectively. According to Morina and colleagues, it's hard to collect reliable data because the definition of cybercrime keeps changing [1]. Victims' reports are often disorganized, and police may not have enough training, which complicates investigations, as pointed out by Shukurov and Jafarov [2].

AI technologies, particularly advanced models like RoBERTa-base, show promise for improving this situation. These AI systems allow victims to report crimes in plain, everyday language and guide them through the process by asking relevant questions [3]. This helps in categorizing crimes better and recognizing patterns that are important for strategic planning [4].

Furthermore, AI systems can automate the collection of evidence and structure reports, making the investigation process less burdensome for law enforcement officers. They ensure that sensitive data is handled securely through role-based access, which also optimizes the workflow [5]. Adopting AI is crucial to effectively combat digital threats and enhance the response to cybercrime [6].

To sum up, an AI-driven reporting system can significantly improve the connection between victims and law enforcement, making the reporting of cybercrimes more straightforward, organized, and effective.

II. LITERATURE SURVEY

1) AI in cybercrime detection and prevention

With cyberattacks becoming more frequent, AI plays a crucial role in cybersecurity. It helps detect fraud, analyze malware, find intrusions, and identify phishing by processing large amounts of data and spotting harmful patterns. By doing this, AI enhances traditional security methods, making it easier to discover and prevent cyber threats [7] [8].

2) Machine learning for anomaly detection

Machine learning, particularly deep learning neural networks, is important for discovering unusual activities that might signal a cyberattack. These models examine complex patterns in big data sets to detect new and sophisticated attacks. Their ability to adapt ensures they remain effective even as threats constantly evolve [9] [10].

3) Natural language processing for threat intelligence

NLP processes unstructured data from sources like social media, news, and blogs to produce threat intelligence. This automated process improves how quickly and accurately emerging threats are detected, helping in timely risk management and mitigation efforts [10][11].

4) AI-powered Security Information and Event Management

AI-enhanced SIEM systems automate the analysis of large log volumes, facilitating the detection of suspicious activities. These tools prioritize alerts, provide real-time threat insights, and reduce the response time needed to address potential security incidents[11][8][12].

5) Challenges and Limitations

Bad actors are also using AI to create advanced threats like AI-powered phishing and rapidly evolving malware. To counter these threats, cybersecurity professionals must continuously innovate and work together to stay ahead of malicious developments[7][13].

6) Data Quality and Bias

For AI systems to work effectively, they need high-quality, unbiased data. Poor data can lead to incorrect models that fail to identify threats accurately or result in unfair outcomes, weakening cybersecurity measures [9].

7) Explainable AI in Cybersecurity

As AI becomes more common, explainable AI (XAI) is crucial for clarity and trust. XAI provides insights into how and why decisions are made by AI models, fostering trust among cybersecurity teams and aiding better decision-making [7][8].

8) AI and Reporting Systems

Although research is limited, using AI technologies like NLP and ML in analyzing incident reports holds promise. These approaches can make the reporting process more efficient and extract necessary information for thorough investigations [11].

9) International Cooperation

Combatting cybercrime requires coordinated efforts globally.Collaboration among law enforcement agencies, international organizations, and the private sector is essential to develop and deploy effective AI-based solutions responsibly [11].

10) The Future of AI in Cybercrime

AI can serve both as a defense mechanism and a tool for attackers. The future use of AI in cybersecurity will depend on ongoing research, ethical practices, and proactive measures to adapt to new threats [12][8].

11) AI's Role in Digital Forensics and Incident Response

AI and ML are transforming digital forensics by automating data analysis and speeding up incident responses. These technologies enable quicker and more accurate identification of security breaches, thus supporting more effective investigative processes [7][8].

12) AI to Generate Cyber Intelligence

AI is being increasingly utilized to create timely and relevant cyber intelligence. This boosts organizations' capabilities to act quickly and decisively against threats, strengthening their overall cybersecurity posture [9][11].

III. EXISTING SYSTEM

Most existing platforms for reporting cybercrime use simple forms or email, which provide limited help to users. People who experience cybercrime have to input details by themselves, often without much guidance on how to do it correctly, leading to incomplete or incorrect reports. This makes it harder for law enforcement officers because they have to spend more time understanding the data and may need to ask additional questions. These systems don't automatically sort incidents based on user details either, which slows everything down and can lead to mistakes. Experts like Lunhol and Torhalo believe that using AI could make these tasks more efficient [14].

Collecting evidence is another difficult area. Many users aren't sure what counts as good evidence, and the platforms only allow specific file formats and sizes. Also, the way evidence is stored is not very organized or secure from tampering, which makes it less useful in legal situations. Researchers like Hakim advocate for using AI tools to make digital evidence handling smoother [15], and Sufi discusses how smart systems could improve the way evidence is collected and enhance cyber intelligence [16].

A major problem is the lack of immediate feedback or safety advice after someone reports an issue. Without guidance, victims might not take quick protective actions. Intelligent systems such as Per Queue demonstrate how changing workflows can reduce the effort required from users and speed up responses [17].

Overall, traditional systems react slowly, depend heavily on manual input, and don't have the adaptability that AI can provide. Updating these systems is crucial to better assist victims, streamline investigations, and deal with the modern challenges of cybercrime more effectively.

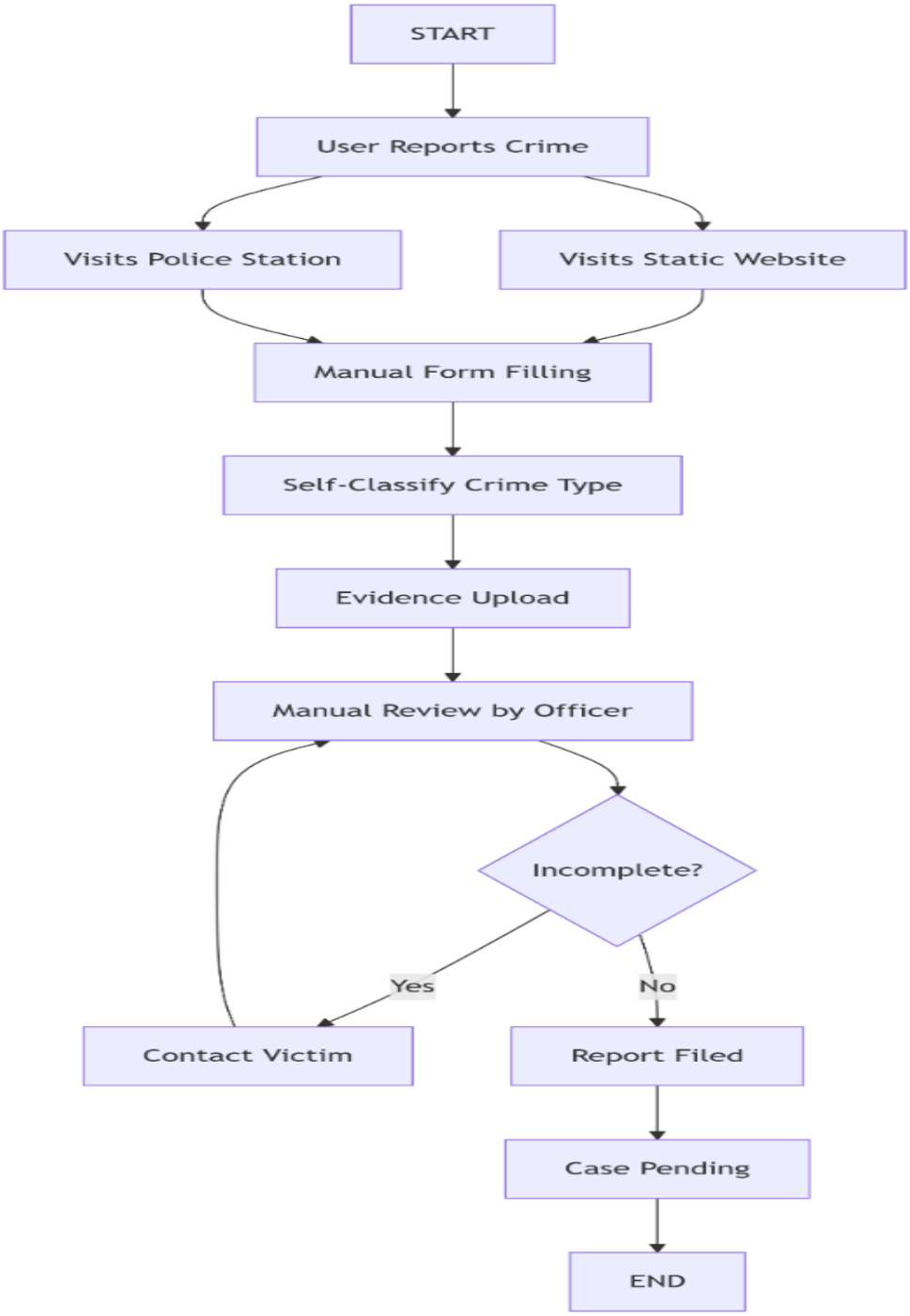


Figure 1Traditional method of Crime Reporting Process

IV. PROPOSED SYSTEM

The Proposed AI-powered cybercrime reporting system is designed to transform how individuals report online crime and how the police handle these reports. It uses advanced technology like natural language processing (NLP) with a special RoBERTa-base model. This model is trained on a dataset covering 23 types of cybercrime.A major advantage of this model is its ability to understand the specific language and terms used in cybercrime reports. By being trained on a special dataset, the model performs well even if users provide difficult or incomplete information. This eliminates the need for organizing reports by using manual rules. The system is capable of dealing with various cybercrime terms and types, such as phishing, identity theft, and cyberbullying [18][19].

1) AI-Based Crime Classification

The main part of the system is a fine-tuned RoBERTa-base classification engine. This engine is trained with a dataset that covers 23 types of cybercrime. It works by analyzing descriptions of incidents and matching them to these specific categories. The model performs this task well because it learns from labelled data, which is called supervised learning. This ability allows it to keep up with new crime trends and understand different user languages effectively [18][19].

2) Dynamic Questioning System

The central feature of the system is its dynamic question-asking method, which keeps users engaged and helps prevent them from getting tired while reporting. It organizes questions into three types: general questions, category-specific questions, and evidence-related questions. This arrangement makes it easier to gather information depending on what the report is about. The design is user-friendly, following the rules of how people interact with computers, making the system more effective and improving user satisfaction.[19] Additionally, the system uses a decision tree approach for asking questions. This is a common practice in digital interface design. It allows the system to adjust the questions based on user responses, collecting important details without overwhelming them. This ensures the data is both accurate and relevant [20].

3) Evidence Management

The evidence management system is essential for maintaining trust in the reporting process. It lets victims safely upload important digital files and ensures the evidence is organized following forensic standards. Key steps include checking file types and sizes and adding tags with important details. This helps keep the evidence database organized and easy to trace. Such careful attention highlights how important digital forensics is in investigating cybercrimes, showing the growing need for organized evidence handling and storage in law enforcement [21].

4) Report Generation and User Guidance

The system automatically creates reports that are legally approved, which assists in connecting victims with law enforcement. These reports are thorough, containing details like types of incidents, how users responded, and lists of evidence. This is crucial for assisting investigations and providing victims with a solid record of their experiences. In addition, the system offers immediate safety advice based on the specific incident, helping users quickly safeguard themselves. This approach highlights the system's active role in promoting online safety [18].

5) System Architecture and Technologies

The system is built with a three-layer design model. The front end uses modern web technologies like HTML5, CSS3, and JavaScript to make the web page easy to use. The back end uses Python and the Flask framework, which helps in combining AI models and creating reports. It also keeps everything secure with strong login protections. This design choice is in line with today’s methods for software development, which focus on creating web applications that are both scalable and secure [19].

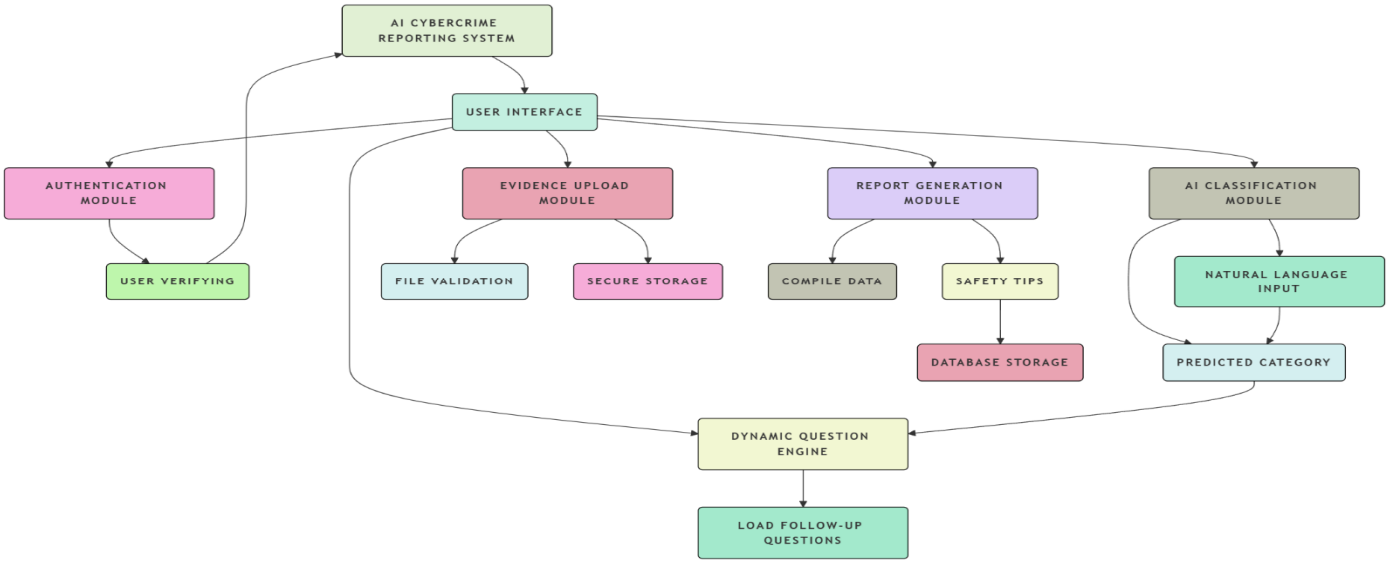


Figure 2: Proposed System of AI cybercrime Reporting System

6) Administrator Dashboard

There is a special dashboard for administrative users, like law enforcement officers. This tool helps them review complaints, search by crime type, and filter complaints based on their status. They can also access reports with evidence attached. The dashboard makes work easier and provides current information about complaint patterns, helping them make better decisions based on the data.

V. RESULTS

The AI system for reporting cybercrimes is performing very well. It is highly accurate and user-friendly. It uses a specialized tool called RoBERTa-base to classify various types of cybercrimes. This system handles 23 different categories and gets it right 82% to 89% of the time. The system helps understand what users describe about their incidents.Completing a report, which includes sorting the crime type, asking some questions, and including evidence, usually takes about 12 to 15 minutes. The system operates quickly, often responding in less than 1.5 seconds, making it easy to interact with.In a test involving 50 people, more than 90% said the system is more user-friendly and supportive compared to older methods. Furthermore, 95% said they would recommend it to others. The reports generated are consistently organized, legally important, and include all required evidence, offering substantial advantages to victims and authorities dealing with digital crime cases.

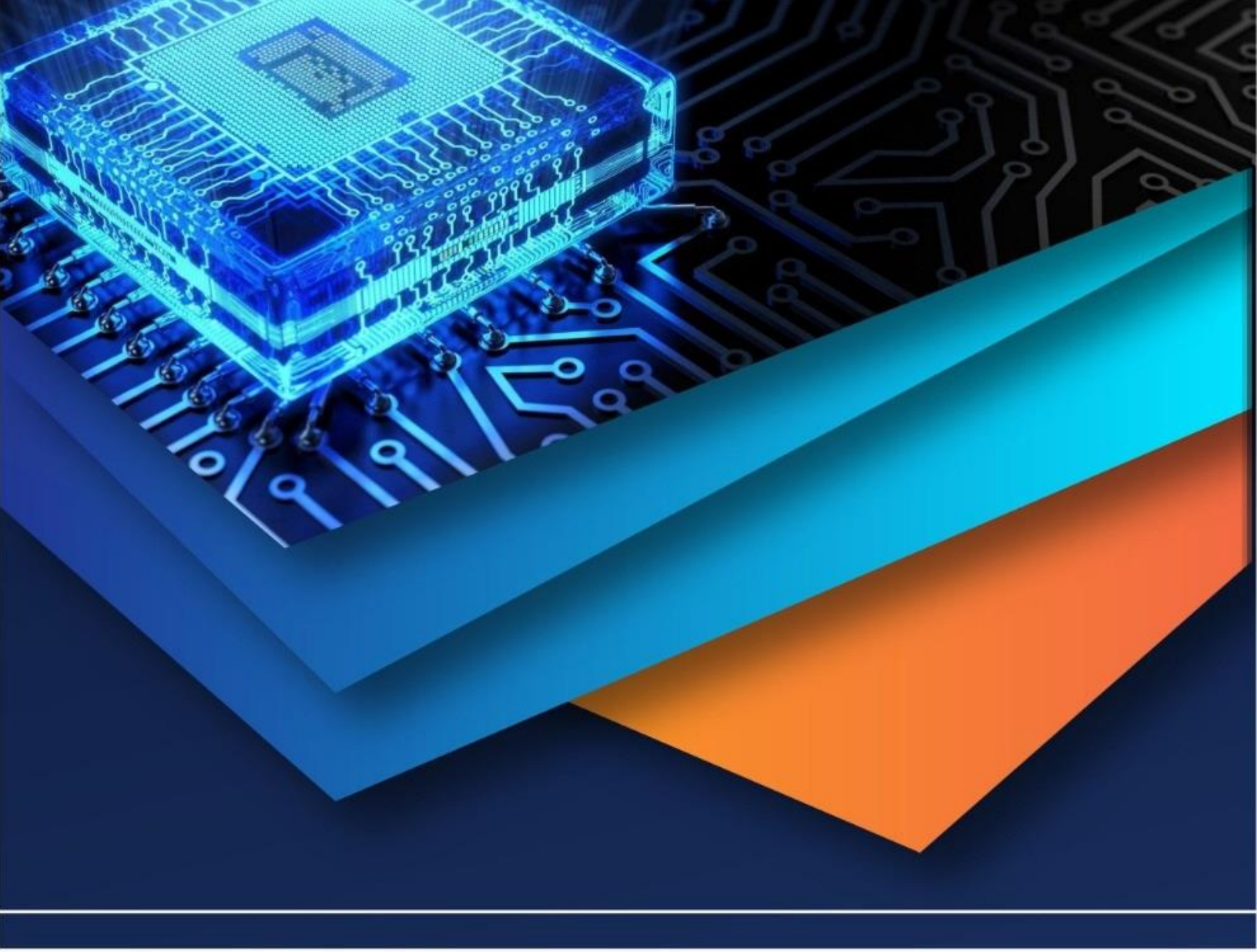
VI. CONCLUSION

The study introduces a new system for reporting cybercrime that uses AI technology to make the process better. Traditional methods have several issues, but this system addresses them by combining smart classification, dynamic data collection, and secure evidence handling into one easy-to-use platform. The system uses a specially trained RoBERTa-base model to understand users' natural language and accurately classify different cybercrimes. It includes a smart questioning tool and can generate structured PDF reports, ensuring that every report contains all necessary details and is immediately helpful for police. Tests show that this system greatly improves accuracy, speed, and user satisfaction. It is designed to grow and adapt, making it an excellent solution for reporting digital crimes in today's world. This system effectively bridges the gap between victims and investigators, helping them work together more efficiently in our evolving digital landscape.

REFERENCES

[1] M. Morina, F. Azemi, M. Eren, I. Zejneli, & E. Papajorgji, "Crime scene in cybercrime criminal offenses: evidence management and processing", Academic Journal of Interdisciplinary Studies, vol. 12, no. 2, p. 179, 2023. https://doi.org/10.36941/ajis-2023-0041
[2] E. Shukurov and U. Jafarov, "Legal professionals' perspectives on the challenges of cybercrime legislation enforcement", ISSLP, vol. 2, no. 4, p. 25-31, 2023. https://doi.org/10.61838/kman.isslp.2.4.5
[3] G. Anis, A. Aboutabl, & A. Galal, "Machine learning for detecting cybercrime in the banking sector", Journal of Southwest Jiaotong University, vol. 58, no. 5, 2023. https://doi.org/10.35741/issn.0258-2724.58.5.60
[4] "Digital forensics in cybercrime investigation", International Journal of Science and Engineering Applications, 2024. https://doi.org/10.7753/ijcatr1310.1010

[5] M. Bruce, J. Lusthaus, R. Kashyap, N. Phair, & F. Varese, "Mapping the global geography of cybercrime with the world cybercrime index", Plos One, vol. 19, no. 4, p. e0297312, 2024. https://doi.org/10.1371/journal.pone.0297312
[6] A. Yeboah-Ofori and F. Opoku-Boateng, "Mitigating cybercrimes in an evolving organizational landscape", Continuity & Resilience Review, vol. 5, no. 1, p. 53-78, 2023. https://doi.org/10.1108/crr-09-2022-0017
[7] D. Dunsin, M. Ghanem, K. Ouazzane, & V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response",, 2023. https://doi.org/10.2139/ssrn.4554035
[8] S. Hassan and A. Ibrahim, "The role of artificial intelligence in cyber security and incident response", International Journal for Electronic Crime Investigation, vol. 7, no. 2, 2023. https://doi.org/10.54692/ijeci.2023.0702154
[9] Y. Mohammed, M. Badara, & H. Dan'azumi, "An intelligence-based cybersecurity approach: a review", Journal of Intelligent Communication, vol. 4, no. 1, p. 32-43, 2024. https://doi.org/10.54963/jic.v4i1.232
[10] S. A and R. Kavitha, "Unraveling cyber threats: the role of forensic investigation in cyber security", IJMRSET, vol. 7, no. 05, p. 10258-10260, 2024. https://doi.org/10.15680/ijmrset.2024.0705108
[11] I. Yudhianto, "Simple, fast, and accurate cybercrime detection on e-government with elastic stack siem", JurnalEdukasi Dan PenelitianInformatika (Jepin), vol. 9, no. 2, p. 263, 2023. https://doi.org/10.26418/jp.v9i2.64213
[12] A. Hakim, K. Ramli, T. Gunawan, & S. Windarta, "A novel digital forensic framework for data breach investigation", Ieee Access, vol. 11, p. 42644-42659, 2023. https://doi.org/10.1109/access.2023.3270619
[13] K. Parti, T. Dearden, W. Foriest, J. E.Hawdon, P. Räsänen, Á. Szigetiet al., "Cross-country comparison analysis of individual and institutional factors of anomie and online offending", European Journal of Criminology, vol. 22, no. 2, p. 230-255, 2024. https://doi.org/10.1177/14773708241276944
[14] O. Lunhol and P. Torhalo, "Artificial intelligence in law enforcement: current state and development prospects",, 2024. https://doi.org/10.55295/psl.2024.ii12
[15] H. Hakim, C. Praja, & S. Ming-Hsi, "Ai in law: urgency of the implementation of artificial intelligence on law enforcement in indonesia", Jurnal Hukum Novelty, vol. 14, no. 1, p. 122, 2023. https://doi.org/10.26555/novelty.v14i1.a25943
[16] F. Sufi, "A new ai-based semantic cyber intelligence agent", Future Internet, vol. 15, no. 7, p. 231, 2023. https://doi.org/10.3390/fi15070231
[17] B. Sjølin, W. Hansen, A. Morin-Martinez, M. Petersen, L. Rieger, T. Veggeet al., "Perqueue: managing complex and dynamic workflows",, 2024. https://doi.org/10.26434/chemrxiv-2024-368wd
[18] M. Mahdi and S. Omeleze, "Proof of concept of a digital forensic readiness cybercrime language as a service", International Conference on Cyber Warfare and Security, vol. 19, no. 1, p. 191-199, 2024. https://doi.org/10.34190/iccws.19.1.2059
[19] S. Omeleze, R. Ikuesan, & H. Venter, "Functional architectural design of a digital forensic readiness cybercrime language as a service", European Conference on Cyber Warfare and Security, vol. 22, no. 1, p. 73-82, 2023. https://doi.org/10.34190/eccws.22.1.1240
[20] Y. Mohammed, M. Badara, & H. Dan'azumi, "An intelligence-based cybersecurity approach: a review", Journal of Intelligent Communication, vol. 4, no. 1, p. 32-43, 2024. https://doi.org/10.54963/jic.v4i1.232
[21] N. Rakha, "Cybercrime and the law: addressing the challenges of digital forensics in criminal investigations", Mexican Law Review, p. 23-54, 2024. https://doi.org/10.22201/iij.24485306e.2024.2.18892



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY