KeAi
CHINESE ROOTS
GLOBAL IMPACT

Journal of Digital Economy

AI-BASED FORENSIC ANALYSIS OF DIGITAL IMAGES: TECHNIQUES AND APPLICATIONS IN CYBERSECURITY

Hitesh Premshankar Rai
Independent Researcher, USA.

Pavan Ogeti
Independent Researcher, USA.

Narendra Sharad Fadnavis
Independent Researcher, USA.

Gireesh Bhaulal Patil
Independent Researcher, USA.

Uday Krishna Padyana
Independent Researcher, USA.

Abstract

In order to find uncommon genetic disorders early on, this Narrative Study examines the possibilities, difficulties, and outcomes of applying Artificial Intelligence (AI) to scan massive government-held face imagine datasets. Artificial intelligence and government-owned face picture databases have the ability to completely change the early detection of uncommon genetic illnesses. Within the ever-changing field of digital forensics, the combination of AI and ML represents a game-changing technological advancement that has the potential to significantly increase the effectiveness and accuracy of digital forensics inquiries. In the law enforcement agencies throughout the world, multi-year digital forensic shortages are becoming the norm. Due to the sheer number of cases needing their skills and the volume of data that has to be processed, digital forensic investigators are overworked. Artificial intelligence is frequently considered the answer to a wide range of big data issues. The techniques and methods for digital forensics that are currently based on artificial intelligence are summarised in this article. Digital forensic analysis may be completed more quickly and with more case processing capacity if automated evidence processing using AI-based methods is used. Every artificial intelligence application that is mentioned has a number of current obstacles and potential future effects that are examined.

Keywords: - Artificial Intelligence (AI), Dynamic Landscape, Digital Forensic, Leveraging Artificial Intelligence, Genetic Diseases, Transformative Technology, Machine Learning (ML).

I. INTRODUCTION

According to [1], the discipline of digital forensics has grown significantly in recent years and now uses technology to gather and examine digital proof during criminal investigations. Successful and effective crime investigation methods are more important than ever as the use of digital proof in the investigation of crimes grows [1, 2]. Digital forensics could go through a revolution because to the potent innovations of Machine Learning (ML) and Artificial Intelligence (AI), which allow analysts to analyse large volumes of data quickly and accurately and find important evidence [2, 3].

The subject of electronic forensics and the difficulties faced by digital forensic analysts—such as the vast amount of data, the wide range of digital devices, and the constantly changing nature of the digital world—will be briefly discussed at the outset of this research study [2, 3]. Next, the article will look at how AI and ML are currently used in forensic computing and the challenges that it faces, such a lack of standards and interpretability problems. This research aims to investigate several approaches that AI and ML may employ to enhance the efficacy and precision of digital forensic investigation. These approaches include picture and text analysis, analysis of networks, and machine-assisted making choices. Finally, possible future research paths, debates, and discoveries will be covered, along with the difficulties and restrictions of applying AI and ML in digital forensics [3, 4].

An increasingly popular application of digital forensics in investigating crimes has surfaced. The vast amounts of data that need to be gathered, processed, and analysed in this new sector demand significant computers, which makes the procedure tedious and time-consuming [4]. A range of applications including the use of Artificial Intelligence (AI) are being considered as a solution to this problem. Examples of these include the application of AI methods in the context of incident response in a limited environment and the area of Disaster Response (DF). Notably, [3]—especially in light of the growing [4]—AI application in investigations into crimes is crucial.

The subject of digital forensics and the difficulties faced by digital forensic analysts, such as the vast amount of data, the wide variety of electronic devices, and the ever-changing character of the digital world, will be briefly discussed at the outset of this research study [4]. After that, the study will look at how AI and ML are currently used in digital forensics and the challenges that it faces, such a lack of standards and interpretability problems [5]. Additionally, this article will examine many approaches that leverage AI and ML to enhance the efficacy and precision of digital forensic investigation, which relies on analysis of networks, machine-assisted decision-making, and picture and text analysis. Finally, possible future research paths, debates, and conclusions will be covered, along with the difficulties and restrictions of applying AI and ML in digital forensic science [5].

An increasingly popular application of digital forensics in criminal investigations has surfaced. Large amounts of data must be gathered, processed, and analysed in this new discipline, which means extensive computing and lengthy processes. A range of applications including the use of Artificial Intelligence (AI) are being used to solve this problem [5, 6]. Examples of these include the application of AI methods in the context of responding to incidents in a limited environment

and in the field of Disaster Response (DF) [6, 7]. Notably, considering the growing prevalence of technology and cybercrime, AI applications in criminal investigations are crucial [6, 7]. Several studies have demonstrated that the great majority of cybercrimes are electronic in nature, underscoring the need of the suggested digital remedy. The amount of data kept on closed, open, and pending cases is increasing, yet for security and accessibility reasons, it must remain available online. Because of this, it makes sense to train datasets for use by digital forensics investigators using artificial intelligence (AI) and machine learning (ML) tools [7, 8].

1.1 Artificial Intelligence Background

The study of intelligent agents, or agents that respond to their surroundings to find the best route to their objective, is known as artificial intelligence, or machine intelligence [7, 8]. AI in computer science may be divided into two main categories: deep learning (DL) and machine learning (ML). Insofar as the precise output is not controlled by explicit code, the success of AI is data-driven [7, 8]. Data pre-processing is a crucial stage in machine learning, and the datasets used to train the models are essential [8]. A summary of the dataset in Digital Forensics that may be used to train AI models is given [9].

1.2 The Machine Learning

The application of Machine Learning (ML) has been extensively used in digital forensic investigations for network forensics, data discovery, and device triage. The components of machine learning include tasks—problems that can be solved—models—ML's output—and features—[9, 10]—the ML workhorses. For ML programmes, there are 3 stages:

- Task definition;
- Feature construction;
- Evaluation and optimisation.

An abstract representation of the issue is called an ML task. Depending on the kind of objective labels, a prediction issue can be classified as either a regression problem or a classification/clustering challenge. Consider the assessment of age [10]. It may be classified as a task for classification if the age is categorical, and as a regression task if it is numerical.

1.3 Deep Learning Introduction

The primary distinction between DL and ML is that the former's characteristics are not created by human engineers. Rather, a general-purpose learning process is used to learn them from data. Analysis of the input must be computationally convenient for ML jobs. But engineering aspects of real-world data, such pictures, videos, [5, 10], and sensor data, is frequently challenging. Artificial Neural Networks (ANNs) use representation (feature) learning techniques to enable a system to automatically find the mathematical models needed for feature detection or classification from unprocessed data. The two phases of a DL model are inference and optimisation. The weights linking the layers of neurons described in the model are updated during the optimisation process, sometimes referred to as training. The backpropagation algorithm is responsible for achieving the weight updating process. A loss goal is created to quantify the difference or inaccuracy between the expected outputs and the desired outcomes prior to training a deep learning model [5, 6].

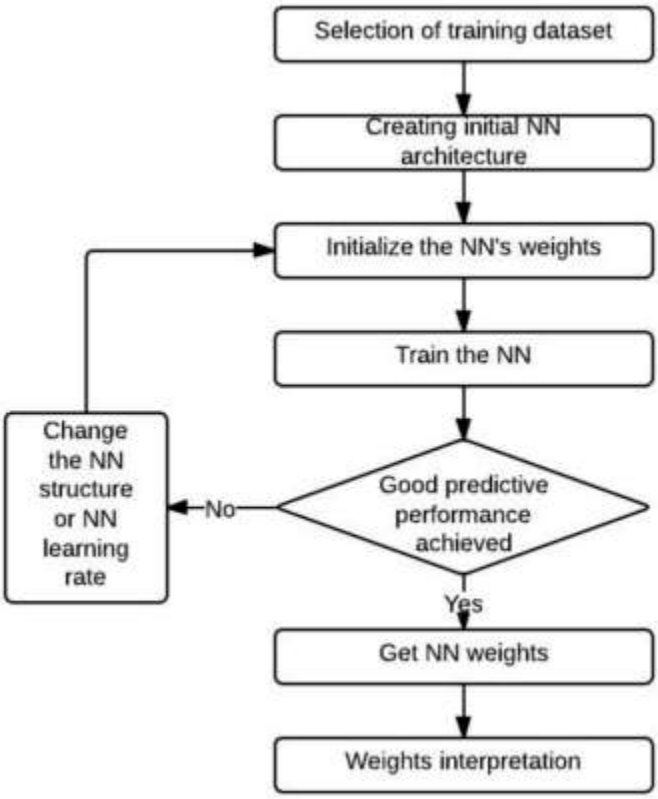

Fig. 1.1 Digital Forensic Classification Model. [7, 10].

II. APPLICATIONS OF AI IN DF

- **Identifying and Recovering Data:** Making the digital proof that has been gathered available in a form that can be read by humans is one of the first steps in a digital investigation (extraction). This might involve retrieving deleted data in addition to data extraction from well-known file systems and types of data [10, 11].
- **Data Discovery: The State of the Art with AI:** If certain metadata is still there, deleted files inside a file system could be recoverable deterministically [11]. The file content, however, may occasionally exist in the unallocated portions of a disc and this information may be missing. The method of retrieving such files without their metadata is called file carving. These files might, nonetheless, also end up partially erased and scattered around the disc. Based on fragment information gathered from more than 350 discs with the file systems FAT, NTFS, and UFS [11]. A usual disc fragmentation rate is minimal, but for data that are significant for forensic analysis, such Word documents, JPGs, and emails, fragmentation rate is rather high. Finding the file type of a fragment helps speed up the search process since the search space for pieces that belong to a certain file is so big [11]. NLP was one method suggested for classifying file fragments. This study uses a supervised learning methodology that combines the bag-of-words model with support vector machines (SVM). File fragments are shown as "bags of bytes" containing feature vectors made up of bigram and a unigram counts together with additional statistical metrics (such as entropy). [12, 13].

- **Device Triage:** The amount of data that Law Enforcement Agencies (LEAs) must deal with during investigations has increased significantly due to the widespread use of digital evidence. For the prompt detection, evaluation, and interpretation of digital evidence, a method model called "digital evidence triage" was put out. At the moment, the investigating officer determines which devices to acquire and process first at a crime scene [13]. On-scene preliminary inspection might swiftly direct the analysis towards equipment that is most likely to have case-progressing information initially as more AI-based approaches are created.
- **AI's Current Status in Device Triage:** The growing importance of mobile device forensics has led to the development of a data mining and Machine Learning (ML) technique for device prioritising. The study's findings about the categorization of mobile phones in a genuine child abuse investigation case are presented in this paper. The phone model, contacts, calls made, text messages sent, received, and read, quantity of video, audio, and photo files, URL, email, and memoranda were among the features that were used [13, 14]. Performance on the feature value expressed as a numeric (a number) and category (the number is low, medium, or high) was examined in the experiment.
- **Present Difficulties and Future Prospects:** One obstacle in the development of AI triage models is the absence of a sufficiently big, shared dataset. To assist investigators in reducing noise and swiftly identifying pertinent material, the triage work involves a quick, straightforward review and analysis. Therefore, creating an imitated, realistic dataset is a significant challenge. Effective device triage may play a major role in future digital inquiry. According to the research, there are significant backlogs in digital forensics, making it nearly difficult to thoroughly examine every digital device. Reducing the amount of resources wasted on processing irrelevant data would come from improving triage accuracy. Furthermore, as is the case with other machine learning techniques, the model's performance is dictated by the training dataset [14, 15].

III. NETWORK TRAFFIC ANALYSIS

Due to the volume of data related to Network Traffic Analysis (NTA), artificial intelligence (AI) techniques may be applied to effectively filter out unnecessary information and automate the identification of criminal activity and other types of misbehaviour [15].

- **AI's Current State of Knowledge in Network Traffic Analysing:** A larger investigation encompassing response to incidents, cloud, IoT, cell phones, wearable technology, and illicit financial activity sometimes includes network probes [15, 16]. Usually, a number of interconnected equipment or technologies are involved in these studies. Investigators may find a plethora of research on using Intrusion Detection methods to process network information offline in a batch fashion after the fact [16]. Surveys on AI's application in IDS.
- **Present Difficulties and Future Prospects:** With the increased hierarchical nature of internet traffic analysis, there is more opportunity to correlate user data across many networks and devices. The behaviours and individual suspicious users may be more thoroughly profiled thanks to modern networks and gadgets. Additionally, device dependence should be considered when correlating occurrences in novel and developing

situations. This is especially crucial in situations like those involving contemporary vehicle accidents [16, 17]. Inter-user correlation, such as the correlation of mobile phone communication through data network apps to determine who a suspect is in touch with frequently or most recently in connection to a specific time period, will also rise in network activity analysis.

- **Data Encryption and Forensics:** Encrypted data is one of the biggest problems that digital forensics investigators worldwide have to deal with. The increasing amount of data and devices that are cryptographically secured makes digital forensic investigation unavoidably vulnerable. The forensic disc image is rendered useless if the device being investigated has disc encryption enabled. At the moment, a lot of nations have laws requiring the device's owner to turn over their keys or passwords to police enforcement upon request [17]. Nevertheless, the encryption device examination frequently comes to an end due to non-compliance or unavailability. Modern cryptographic algorithms employ high bit lengths, making a successful brute-force assault practically impossible.
- **AI's Current State for Handling Encrypted Data:** AI approaches can help with two possible EM-SCA avenues: executing cryptographic key retrieval assaults and getting important insights without accessing the encrypted information. A variety of AI techniques have been used using power and electronic side-channel observational information to work towards the first objective. An investigator may find it helpful to know if a target device utilises the anticipated software or firmware [17, 18]. This is because a rogue person may have altered the firmware. Through power consumption side-channels, DL algorithms like Multilayer Perceptron (MLP) and Long Short-Term Memory (LSTM) have been utilised to recognise abnormalities in IoT devices. Moreover, a number of insights are demonstrated to be detectable with DL approaches, including the identification of the particular hardware device or software programme and the software's activity [18].
- **Present Difficulties and Future Prospects:** It is realistic to assume that in the future, a significant portion of the computer equipment used in digital forensic investigations will be encrypted. As a result, cryptography is becoming a very significant problem in digital forensics. The growing use of Software Defined Radio (SDR) devices makes the process of acquiring electromagnetic traces simpler and more economical.

IV. RECONSTRUCTION OF THE TIMELINE AND EVENT

Finite state machines have been used in digital forensics to specify event reconstructions. Less technically, nevertheless, it describes a procedure that can,

> *"Transform the [digital] objects' status into the circumstances that led to it".*

This may involve only being able to ascertain that something took place, or more specifically, that an event took place at a specific moment. The timestamps that can be recovered from digital forensic artefacts would be examined in order to accomplish this second's more thorough event reconstructions. Time stamps can come from more complicated file formats, such as Windows Registry, SQLite databases, logs of events, etc., but they can also come from time stamps from

the file system, such as [18, 19], file changed, accessed, created, entry edited, etc. With a large number of plugins and parsing tools, Plaso (log2timeline) represents the current state of the art in timestamp extraction. The problem, though, is that millions of these timestamps would be produced throughout a system study, even in the case of very little user activity [19]. An automated investigation into this large amount of records the timestamp has been attempted in an attempt to extract a useful activity history from the data.

- **AI's current state of play for event reconstruction:** The use of machine learning techniques for pattern matching in temporal data is not well documented, despite the potential of these approaches. A neural network-based method for reconstructing events utilising file system timings and explain how the parallelism and generalisation properties of neural networks make them suitable for handling massive amounts of data [19, 20]. Both feedforward and recurring neural network designs were put to the test.
- **Present Difficulties and Future Prospects:** Numerous difficulties exist in this field. The use of timestamps for event reconstruction entails an implicit assumption on their accuracy [20]. This might not be the case for a variety of reasons, such as clock drift, manual system clock changes, rewritten timestamps from regular system operations, or anti-forensic methods [20]. While some of them have been mitigated, such as by developing a rule-based method for identifying timestamp discrepancies, there could also be value in trying an ML-based solution for this issue.

V. MULTIMEDIA FORENSICS

A kind of digital forensics known as "Multimedia Forensics" examines data from digital forensics investigations, including CCTV analysis in addition to computers and mobile devices. This data includes photographs, videos, and sounds. There are several facets of this subject to investigate. This particular issue is the first [19, 20]. Thousands of media files may be found on typical devices, and it might be difficult to find the important ones because they cannot be found with a simple keyword search. The second category involves analysis to ascertain the source of the media, which may offer a connection to a suspect [19, 20]. Since it is easy to tamper with digital photographs, the third category is forgery detection [20].

- **Current AI State of the Art for Computer Vision:** Because there are so many confiscated devices, it is difficult to find things of interest in digital photographs while trying to identify relevant images from a huge group [21, 22]. The requirement for automatic object detection [21], particularly in low-quality photos, has led to the development of efficient image mining methods to digital forensics application [22].
- **AI's Current Status in Forgery Detection:** Lastly, as was already indicated, it might be difficult to identify picture forgeries [22, 23]. Since a digital image is now recognised as "proof of occurrence" for an event, it is critical to provide evidence of its authenticity. Five types of categorised tools are used to identify image forgeries:

— Techniques using pixels to identify statistical irregularities introduced at the level of the pixel.

— Statistical correlations created by a particular loss compression approach can be utilised using format-based strategies [23, 24].
— Methods using cameras that take use of artefacts caused by the sensor, lens, or on-chip the post-processing.
— Methods rooted in reality that specifically simulate and identify irregularities in the three-dimensional interplay of real-world objects, light, and the camera [24].
— Approaches based on geometry that measure real-world objects and their distances from a camera.

- **Present Difficulties and Future Prospects:** Skin tone detection algorithms and hash comparisons have been employed in the past as automated methods to identify CSEM. However, the performance has been insufficient or the method has been insignificant. Impressive and promising findings have been made possible by the emergence of CNNs [24]. Numerous applications have to be investigated in order to enhance the efficacy of algorithms designed to identify CSEM. Certain models trained on poor-quality data might be used to images that are clearly difficult for the human eye to see due to their low resolution capabilities. Low-quality objects discovered on CSEM may benefit from the formation of ensembles for various kinds of objects that adhere to certain quality requirements [24, 25].
- **One expanding field in digital forensics is fingerprinting devices:** It includes malware behavioural assessment and classification based on programme execution structures, camera sensor the identification (based on minute flaws in camera detectors), server-side fingerprinting of websites (based on the distinct set of browser and expansion metadata/configuration provided by a web server), and more [26].
- **The state of AI fingerprinting technology:** AI classification approaches work well for tasks like fingerprinting. Malware categorization, for instance, has been a widely used application area, with a substantial body of work in this field already completed in both static and dynamic analysis [26]. Concerning the previously discussed question of media provenance [28].
- **Further Action:** Anomaly detection may benefit substantially from fingerprinting of devices and user activity. This can lead to more effective host-based and network-based detection of intrusion for networked devices [28, 29]. Analysing each user's use and behavioural patterns on a system may also be utilised to predict account breach.

VI. CONCLUSION

A robust proposal for the use of Artificial Intelligence (AI) and Machine Learning (ML) approaches in current and future digital forensics research is derived from the thorough survey carried out in this work. These methods have great potential to improve both the precision and efficacy of investigations, especially when it comes to dealing with the growing incidence of cybercrime. However, data validity is a problem that needs to be carefully considered, particularly when working with a variety of data from different people, devices, platforms, and cultural settings.

This study has demonstrated how various AI algorithms are now applied in various digital forensics domains. Additionally, it has brought to light common obstacles such being the unavailability of data sets in some regions, particular difficulty in elucidating the outcomes when particular methodologies are employed, and even difficulties in releasing models when the models may be able to infer constrained training data. Nevertheless, there is a tonne of untapped potential for further research despite these obstacles. As was previously said, this relates to both enhancing the effectiveness of some of the existing methods and the fact that certain strategies have not yet been put to the test in particular domains. Because of the systematisation of information, these gaps should now be easier to identify, which will speed up advancements in this subject.

Future research

As earlier sections have demonstrated, a substantial amount of work has already been done in applying AI to certain digital forensics applications. This section covers general issues as well as possible prospects, such as uncharted territory where new and developing AI approaches have not yet been used. One apparent area of concentration for general issues is increasing technique precision. In the context of digital forensics, it can be difficult to train models and assess their accuracy due to the absence of big, clear, labelled datasets in certain places or the private nature of the datasets that do exist.

Furthermore, it's important to think about whether sharing models is suitable in some situations. Model inversion and membership inference are two examples of threats that are summarised in relation to GDPR and AI-trained models. Because of this, it's important to take this into account when creating digital forensic solutions using AI and possibly sensitive training data. Notwithstanding these difficulties, there are plenty of chances to improve AI applications and use AI in other digital forensics domains. Among these are the inferences about conduct made from data gathered from innovative sources, such as IoT sensors, smart homes, car forensics, and their combinations. Artificial intelligence approaches have the potential to be helpful in situations when it's necessary to correlate data from several sources, such as different suspects, gadgets, or cases. For such efforts, non-AI-based initiatives like standard representation formats, like CASE, would be essential.

VII. REFERENCES

1. Brkan, M., Bonnet, G., 2020. Legal and technical feasibility of the GDPR’s quest for explanation of algorithmic decisions: of black boxes, white boxes and fata morganas. European Journal of Risk Regulation 11, 18–50.
2. Cabitza, F., Campagner, A., Basile, V., 2023. Toward a perspectivist turn in ground truthing for predictive computing. In: Proceedings of the AAAI Conference on Artificial Intelligence, vol. 37, pp. 6860–6868.
3. Chabot, Y., Bertaux, A., Nicolle, C., Kechadi, M.-T., 2014. A complete formalized knowledge representation model for advanced digital forensics timeline analysis. Digit. Invest. 11, S95–S105.

4. Decelle, A., 2022. An introduction to machine learning: a perspective from statistical physics. Physica A: Statistical Mechanics and its Applications, 128154.
5. Dimitriadis, A., Lontzetidis, E., Kulvatunyou, B., Ivezic, N., Gritzalis, D., Mavridis, I., 2023. Fronesis: digital forensics-based early detection of ongoing cyber-attacks. IEEE Access 11, 728–743.
6. Haendel, M.; Vasilevsky, N.; Unni, D.; Bologa, C.; Harris, N.; Rehm, H.; Hamosh, A.; Baynam, G.; Groza, T.; McMurry, J.; et al. How many rare diseases are there? Nat. Rev. Drug Discov. 2020, 19, 77–78.
7. Dawkins, H.J.; Molster, C.M.; Youngs, L.M.; O'Leary, P.C.; Noc, T.N.O.C. Awakening Australia to Rare Diseases: Symposium report and preliminary outcomes. Orphanet J. Rare Dis. 2011, 6, 57.
8. Knight, A.W.; Senior, T.P. The common problem of rare disease in general practice. Med. J. Aust. 2006, 185, 82–83.
9. Cox-Brinkman, J.; Vedder, A.; Hollak, C.; Richfield, L.; Mehta, A.; Orteu, K.; Wijburg, F.; Hammond, P. Three-dimensional face shape in Fabry disease. Eur. J. Hum. Genet. 2007, 15, 535–542.
10. Hammond, P.; Suttie, M. Large-scale objective phenotyping of 3D facial morphology. Hum. Mutat. 2012, 33, 817–825.
11. Hong, D.; Zheng, Y.-Y.; Xin, Y.; Sun, L.; Yang, H.; Lin, M.-Y.; Liu, C.; Li, B.-N.; Zhang, Z.-W.; Zhuang, J.; et al. Genetic syndromes screening by facial recognition technology: VGG-16 screening model construction and evaluation. Orphanet J. Rare Dis. 2021, 16, 344.
12. Matthews, H.; De Jong, G.; Maal, T.; Claes, P. Static and Motion Facial Analysis for Craniofacial Assessment and Diagnosing Diseases. Annu. Rev. Biomed. Data Sci. 2022, 5, 19–42.
13. Roosenboom, J.; Hens, G.; Mattern, B.C.; Shriver, M.D.; Claes, P. Exploring the Underlying Genetics of Craniofacial Morphology through Various Sources of Knowledge. BioMed Res. Int. 2016, 2016, 1–9.
14. Dudding-Byth, T.; Baxter, A.; Holliday, E.G.; Hackett, A.; O'Donnell, S.; White, S.M.; Attia, J.; Brunner, H.; De Vries, B.; Koolen, D.; et al. Computer face-matching technology using two-dimensional photographs accurately matches the facial gestalt of unrelated individuals with the same syndromic form of intellectual disability. BMC Biotechnol. 2017, 17, 90.
15. Stoney, D.A., Stoney, P.L., 2015. Critical review of forensic trace evidence analysis and the need for a new approach. Forensic Sci. Int. 251, 159–170.
16. Su, Z., Li, Mengke, Zhang, G., Wu, Q., Li, Miqing, Zhang, W., Yao, X., 2023. Robust audio copy-move forgery detection using constant Q spectral Sketches and GA-SVM. IEEE Trans. Dependable Secure Comput. 20, 4016–4031.
17. Tallon-Ballesteros, ´ A.J., Riquelme, J.C., 2014. Data mining methods applied to a digital forensics task for supervised machine learning. Computational intelligence in digital forensics: forensic investigation and applications 413–428.

18. Tankard, C., 2011. Advanced Persistent threats and how to monitor and deter them. Netw. Secur. 2011, 16–19.
19. Tanner, A., Bruno, J., 2019. Timely: a chain of custody data visualizer. In: 2019 SoutheastCon. IEEE, pp. 1–5.
20. Teimouri, M., Seyedghorban, Z., Amirjani, F., 2020. Fragments-Expert: a graphical user interface MATLAB toolbox for classification of file fragments. Concurrency Compute. Pract. Ex. 33.
21. Thagard, P., 1990. Philosophy and machine learning. Can. J. Philos. 20, 261–276.
22. Simran Fitzgerald, George Mathews, Colin Morris, and Oles Zhulyn. 2012. Using NLP techniques for file fragment classification. Digital Investigation 9 (2012), S44–S49.
23. David Freire-Obregon, Fabio Narducci, Silvio Barra, and Modesto Castrillon Santana. 2018. Deep learning for source camera identification on mobile devices. Pattern Recognition Letters (2018).
24. Takeshi Fujino, Takaya Kubota, and Mitsuru Shiozaki. 2017. Tamper-resistant cryptographic hardware. IEICE Electronics Express 14, 2 (2017), 20162004– 20162004.
25. Ekta Gandotra, Divya Bansal, and Sanjeev Sofat. 2014. Malware analysis and classification: A survey. Journal of Information Security 2014 (2014).
26. Simson Garfinkel, Paul Farrell, Vassil Roussev, and George Dinolt. 2009. Bringing science to digital forensics with standardized forensic corpora. Digital investigation 6 (2009), S2–S11.
27. Christopher Hargreaves and Angus Marshall. 2019. SyncTriage: Using synchronisation artefacts to optimise acquisition order. Digital Investigation 28 (2019), S134–S140.
28. Gabriel Hospodar, Benedikt Gierlichs, Elke De Mulder, Ingrid Verbauwhede, and Joos Vandewalle. 2011. Machine learning in side-channel analysis: a first study. Journal of Cryptographic Engineering 1, 4 (2011), 293.
29. Wenyi Huang and Jack W Stokes. 2016. MtNet: a multi-task neural network for dynamic malware classification. In International conference on detection of intrusions and malware, and vulnerability assessment. Springer, 399–418.
30. J. Jasmine and S. Annadurai. 2019. Real time video image enhancement approach using particle swarm optimisation technique with adaptive cumulative distribution function based histogram equalisation. Measurement 145 (2019), 833 – 840.
31. Varun Nakra, Pandi Kirupa Gopalakrishna Pandian, 2021. "Anomaly Detection in Cybersecurity: Leveraging Machine Learning Algorithms" ESP Journal of Engineering & Technology Advancements 1(2): 34-41.")
32. Kaur, J. (2021). Big Data Visualization Techniques for Decision Support Systems. Jishu/Journal of Propulsion Technology, 42(4). https://propulsiontechjournal.com/index.php/journal/article/view/5701
33. Ashok : "Choppadandi, A., Kaur, J.,Chenchala, P. K., Nakra, V., & Pandian, P. K. K. G. (2020). Automating ERP Applications for Taxation Compliance using Machine Learning at

SAP Labs. International Journal of Computer Science and Mobile Computing, 9(12), 103-112. https://doi.org/10.47760/ijcsmc.2020.v09i12.014

34. Chenchala, P. K., Choppadandi, A., Kaur, J., Nakra, V., & Pandian, P. K. G. (2020). Predictive Maintenance and Resource Optimization in Inventory Identification Tool Using ML. International Journal of Open Publication and Exploration, 8(2), 43-50. https://ijope.com/index.php/home/article/view/127
35. Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). AI Applications in Smart Cities: Experiences from Deploying ML Algorithms for Urban Planning and Resource Optimization. Tuijin Jishu/Journal of Propulsion Technology, 40(4), 50-56.
36. Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service . (2019). International Journal of Transcontinental Discoveries, ISSN: 3006-628X, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98
37. Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service. International Journal
38. of Transcontinental Discoveries, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98
39. Choppadandi, A., Kaur, J., Chenchala, P. K., Kanungo, S., & Pandian, P. K. K. G. (2019). AI-Driven Customer Relationship Management in PK Salon Management System. International Journal of Open Publication and Exploration, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128
40. Ashok Choppadandi, Jagbir Kaur, Pradeep Kumar Chenchala, Akshay Agarwal, Varun Nakra, Pandi Kirupa Gopalakrishna Pandian, 2021. "Anomaly Detection in Cybersecurity: Leveraging Machine Learning Algorithms" ESP Journal of Engineering & Technology Advancements 1(2): 34-41.
41. Ashok Choppadandi et al, International Journal of Computer Science and Mobile Computing, Vol.9 Issue.12, December- 2020, pg. 103-112. (Google scholar indexed)
42. Choppadandi, A., Kaur, J., Chenchala, P. K., Nakra, V., & Pandian, P. K. K. G. (2020). Automating ERP Applications for Taxation Compliance using Machine Learning at SAP Labs. International Journal of Computer Science and Mobile Computing, 9(12), 103-112. https://doi.org/10.47760/ijcsmc.2020.v09i12.014
43. Chenchala, P. K., Choppadandi, A., Kaur, J., Nakra, V., & Pandian, P. K. G. (2020). Predictive Maintenance and Resource Optimization in Inventory Identification Tool Using ML. International Journal of Open Publication and Exploration, 8(2), 43-50. https://ijope.com/index.php/home/article/view/127
44. AI-Driven Customer Relationship Management in PK Salon Management System. (2019). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128

45. Mitul Tilala, Abhip Dilip Chawda, Abhishek Pandurang Benke, Akshay Agarwal. (2022). Regulatory Intelligence: Leveraging Data Analytics for Regulatory Decision-Making. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 1(1), 78–83. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/77
46. Tilala, Mitul, and Abhip Dilip Chawda. "Evaluation of Compliance Requirements for Annual Reports in Pharmaceutical Industries." NeuroQuantology 18, no. 11 (November 2020): 138-145. https://doi.org/10.48047/nq.2020.18.11.NQ20244.
47. Kamuni, Navin, Suresh Dodda, Venkata Sai Mahesh Vuppalapati, Jyothi Swaroop Arlagadda, and Preetham Vemasani. "Advancements in Reinforcement Learning Techniques for Robotics." Journal of Basic Science and Engineering 19, no. 1 (2022): 101-111. ISSN: 1005-0930.
48. Narukulla, Narendra, Joel Lopes, Venudhar Rao Hajari, Nitin Prasad, and Hemanth Swamy. "Real-Time Data Processing and Predictive Analytics Using Cloud-Based Machine Learning." Tuijin Jishu/Journal of Propulsion Technology 42, no. 4 (2021): 91-102.
49. Nitin Prasad. (2022). Security Challenges and Solutions in Cloud-Based Artificial Intelligence and Machine Learning Systems. International Journal on Recent and Innovation Trends in Computing and Communication, 10(12), 286–292. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10750
50. Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
51. Shah, J., Prasad, N., Narukulla, N., Hajari, V. R., & Paripati, L. (2019). Big Data Analytics using Machine Learning Techniques on Cloud Platforms. International Journal of Business Management and Visuals, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
52. Cygan, Kamil J., Ehdieh Khaledian, Lili Blumenberg, Robert R. Salzler, Darshit Shah, William Olson, Lynn E. Macdonald, Andrew J. Murphy, and Ankur Dhanik. "Rigorous Estimation of Post-Translational Proteasomal Splicing in the Immunopeptidome." bioRxiv (2021): 1-24. https://doi.org/10.1101/2021.05.26.445792
53. Shah, Darshit, Ankur Dhanik, Kamil Cygan, Olav Olsen, William Olson, and Robert Salzler. "Proteogenomics and de novo Sequencing Based Approach for Neoantigen Discovery from the Immunopeptidomes of Patient CRC Liver Metastases Using Mass Spectrometry." The Journal of Immunology 204, no. 1_Supplement (2020): 217.16-217.16. American Association of Immunologists.
54. Mahesula, Swetha, Itay Raphael, Rekha Raghunathan, Karan Kalsaria, Venkat Kotagiri, Anjali B. Purkar, Manjushree Anjanappa, Darshit Shah, Vidya Pericherla, Yeshwant Lal Avinash Jadhav, Jonathan A.L. Gelfond, Thomas G. Forsthuber, and William E. Haskins. "Immunoenrichment Microwave & Magnetic (IM2) Proteomics for Quantifying CD47 in the EAE Model of Multiple Sclerosis." Electrophoresis 33, no. 24 (2012): 3820-3829. https://doi.org/10.1002/elps.201200515.

55. Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
56. Cygan, K. J., Khaledian, E., Blumenberg, L., Salzler, R. R., Shah, D., Olson, W., & ... (2021). Rigorous estimation of post-translational proteasomal splicing in the immunopeptidome. bioRxiv, 2021.05.26.445792.
57. Mahesula, S., Raphael, I., Raghunathan, R., Kalsaria, K., Kotagiri, V., Purkar, A. B., & ... (2012). Immunoenrichment microwave and magnetic proteomics for quantifying CD 47 in the experimental autoimmune encephalomyelitis model of multiple sclerosis. Electrophoresis, 33(24), 3820-3829.
58. Mahesula, S., Raphael, I., Raghunathan, R., Kalsaria, K., Kotagiri, V., Purkar, A. B., & ... (2012). Immunoenrichment Microwave & Magnetic (IM2) Proteomics for Quantifying CD47 in the EAE Model of Multiple Sclerosis. Electrophoresis, 33(24), 3820.
59. Raphael, I., Mahesula, S., Kalsaria, K., Kotagiri, V., Purkar, A. B., Anjanappa, M., & ... (2012). Microwave and magnetic (M2) proteomics of the experimental autoimmune encephalomyelitis animal model of multiple sclerosis. Electrophoresis, 33(24), 3810-3819.
60. Salzler, R. R., Shah, D., Doré, A., Bauerlein, R., Miloscio, L., Latres, E., & ... (2016). Myostatin deficiency but not anti-myostatin blockade induces marked proteomic changes in mouse skeletal muscle. Proteomics, 16(14), 2019-2027.
61. Shah, D., Anjanappa, M., Kumara, B. S., & Indiresh, K. M. (2012). Effect of post-harvest treatments and packaging on shelf life of cherry tomato cv. Marilee Cherry Red. Mysore Journal of Agricultural Sciences.
62. Shah, D., Dhanik, A., Cygan, K., Olsen, O., Olson, W., & Salzler, R. (2020). Proteogenomics and de novo sequencing based approach for neoantigen discovery from the immunopeptidomes of patient CRC liver metastases using Mass Spectrometry. The Journal of Immunology, 204(1_Supplement), 217.16-217.16.
63. Shah, D., Salzler, R., Chen, L., Olsen, O., & Olson, W. (2019). High-Throughput Discovery of Tumor-Specific HLA-Presented Peptides with Post-Translational Modifications. MSACL 2019 US.
64. Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
65. Pavan Ogeti, Narendra Sharad Fadnavis, Gireesh Bhaulal Patil, Uday Krishna Padyana, Hitesh Premshankar Rai. (2022). Blockchain Technology for Secure and Transparent Financial Transactions. European Economic Letters (EEL), 12(2), 180–188. Retrieved from https://www.eelet.org.uk/index.php/journal/article/view/1283
66. Fadnavis, N. S., Patil, G. B., Padyana, U. K., Rai, H. P., & Ogeti, P. (2021). Optimizing scalability and performance in cloud services: Strategies and solutions. International Journal on Recent and Innovation Trends in Computing and Communication, 9(2), 14-23. Retrieved from http://www.ijritcc.org

67. Challa, S. S. S., Tilala, M., Chawda, A. D., & Benke, A. P. (2021). Navigating regulatory requirements for complex dosage forms: Insights from topical, parenteral, and ophthalmic products. NeuroQuantology, 19(12), 971-994. https://doi.org/10.48047/nq.2021.19.12.NQ21307
68. Fadnavis, N. S., Patil, G. B., Padyana, U. K., Rai, H. P., & Ogeti, P. (2020). Machine learning applications in climate modeling and weather forecasting. NeuroQuantology, 18(6), 135-145. https://doi.org/10.48047/nq.2020.18.6.NQ20194