BRIHASPATI: A cyber forensic web application designed to assist investigators in detecting and analyzing illegal content present on mobile devices.

Mr. Bhaumik Machhi[1] , Mr. Vikas Singh[2], Ms.Sharline Job[3], Mr.Jainam Soni[4], Mr. Narendra Chaudary[5]

[1]Assistant Professor , CSE , SOT, GSFC University , Vadodara, Gujarat , India
2B.Tech CSE, SOT, GSFC UNIVERSITY, Vadodara, Gujarat, India.
3B.Tech CSE, SOT, GSFC UNIVERSITY, Vadodara, Gujarat, India.
4B.Tech CSE, SOT, GSFC UNIVERSITY, Vadodara, Gujarat, India.
5B.Tech CSE, SOT, GSFC UNIVERSITY, Vadodara, Gujarat, India.

ARTICLE INFO

Received: dd Month 20--

Accepted: dd Month 20--

ABSTRACT

Brihaspati is a forensic analysis platform powered by AI that has been developed to help investigators identify illegal content on mobile phones. The platform utilizes ADB (Android Debug Bridge) and Autopsy, two popular forensic tools, to recover multimedia information like images, videos, audio, and text from Android phones. The recovered data is processed thereafter with a specially developed AI model that can identify banned products such as drugs, weapons, and adult content. The backend of the app is completed with Node.js and Express, along with MongoDB for effective data storage, and the frontend completed with Angular, for effective and responsive user experience. Brihaspati aims to accelerate the digital forensic process by automating content recognition, thereby reducing human efforts and speeding up investigations. The platform was examined for accuracy, performance, and scalability and achieved promising findings in real-time analysis and detection. This research validates the feasibility and effectiveness of integrating AI with forensic tools to boost the speed and precision of digital investigation

Keywords: Smartphone Forensics, AI Content Detection, ADB, Autopsy Tool , Digital Forensic Analysis, Illegal Content Detection, Multimedia Analysis

INTRODUCTION

The rapid proliferation of smartphone usage has resulted in an Increase in digital crimes associated with mobile phones. Smartphones typically hold vital evidence in the form of pictures. Conventional forensic examination of all this data is time-consuming and labor - intensive to detect criminal or suspicious material. Here, the convergence of Artificial Intelligence (AI) and digital forensics offers a strong solution to automate and expedite the investigation process[1].

This paper introduces Brihaspati, an AI- powered forensic platform that is meant to extract and analyze data from Android mobile phones. The platform employs Android Debug Bridge (ADB) to fetch data and Autopsy, a forensic tool, to analyze the data. The platform's core is a custom developed AI -model that can identify illegal content— such as drugs, weapons, and explicit content— within multimedia files. With this process being automated, Brihaspati will assist investigators in quickly identifying important evidence[2].

The framework is developed with a full-stack methodology: Node.js and Express comprise the backend, MongoDB ensures data management, and Angular drives an interactive, responsive

frontend interface[3]. This paper outlines the design, development, and testing of Brihaspati and its ability to speed up and enhance the accuracy of digital forensic investigations.

Figure. 1. Data Flow Diagram

OBJECTIVES

The Brihaspati project is built around the idea of using artificial intelligence to make digital investigations on smartphones faster, smarter, and more efficient. The main objective is to create a tool that can help investigators automatically detect illegal or suspicious content—like drugs, weapons, or explicit material—stored on Android devices. To do this, we first had to find a method of accessing and pulling data from smartphones, which we accomplished with ADB (Android Debug Bridge). This is a tool that enables us to pull valuable data such as images, videos, audio recordings, and messages from the internal storage of the device[4]. After the data is extracted, it is analysed with the help of Autopsy, a forensic tool that helps organize and view digital evidence in a structured way.

One of the most noteworthy aspects of the project is the development of a trustworthy AI model that has been trained to identify different kinds of prohibited content[5]. In order to speed up the investigation and eliminate human error, the AI scans the extracted data and flags dubious files in place of human verification. To integrate everything, we developed a full-stack web application. The frontend was constructed using Angular to make it responsive and user-friendly, while the backend uses Node.js and Express to manage all the logic and data manipulations[6]. MongoDB is our database of choice because it is easy to use and has the capacity to efficiently handle large volumes of data.

In addition to writing, we also ensured that we ran each component of the system to ensure proper functionality[7]. This involved verifying the correctness of the AI model, verifying that the data extraction and analysis features were functional as desired, and

that the web application was responsive and user-friendly on any device[8]. Overall, the goal of Brihaspati is to streamline and accelerate the digital forensic process through the virtue of AI and to give investigators a functional and useful tool for use in the real world[9].

METHODS

In order to build the Brihaspati platform, we adopted a step-by-step process, which involved data extraction from Android devices, AI-based content identification, and the design of an intuitive web application. The following is a summary of the processes that were employed in order to realize project:

Data Extraction: Extracting data from Android phones was the initial step in the process. We employed Android Debug Bridge (ADB), which is a versatile tool used for communication between an Android device and a computer. By turning ADB debugging on the target phone, we were able to browse the file system of the device and pull relevant data like pictures, videos, audio files, and SMS[10].

AI Model Development: Brihaspati's greatest strength lies in its AI model for detecting prohibited content. We developed the model by gathering a dataset of images, videos, and audio content having various types of prohibited material, such as weapons, narcotics, and adult content[11]. We used deep learning-based methods to train the AI model, including CNNs for images and RNNs for sound. The trained model was further implemented in the backend system for real-time detection and flagging of suspicious content a fresh data is being pulled from Android devices[1], [12].

Web Application Development: Angular, the most widely used responsive and dynamic web application development framework, was employed to develop the frontend of the platform. The web interface was designed interactive and user-friendly so that the investigators can directly interact with the system. It contains a login facility, an output dashboard to display the output of the AI processing, and very minimalist navigation widgets to navigate through different sections of the platform. On the server side, Express and Node.js were used to create a well-established server infrastructure that allowed seamless communication between frontend and database. MongoDB as a database to store the pulled content and result of analysis was also used easily to store and retrieve results.

System Testing and Validation: After the platform was completely developed, we put it through rigorous testing to make sure the system was precise, effective, and ready to use in practical situations. We tested the AI model for its effectiveness in properly detecting illegal content, ensured that the data extraction process was seamless and trustworthy, and tested the overall functionality of the web application on various devices. We also conducted stress tests to see how the system performs under data volumes typical of forensic analysis.

OUTCOMES

The creation of the Brihaspati platform brought with it numerous successful outcomes that attest to the real-world application of AI in digital forensics. Among the most significant achievements was the creation of a system that could extract and process smartphone data effectively using ADB and Autopsy. We were able to extract different kinds of data—images, videos, audio files, and text—from

Android devices in a structured and usable form, setting the stage for automatic analysis.

A key achievement of the project was the effective integration of a custom AI model to identify illicit or objectionable content within media files. The model worked efficiently to identify substances such as drugs, weapons, and objectionable material from images and videos of files with fair accuracy. Though the system is immature and long from being perfect, the efficacy of the AI proved the potential of machine learning to aid digital investigation and reduce time spent on content review by humans.

We also created a completely functional web-based interface that makes it easy for users to interact with the platform. The frontend was interactive and responsive, while the backend handled data processing and storage using Node.js, Express, and MongoDB. The user interface tested on devices proved to be stable and efficient and easily accessible for results of analysis.

In total, Brihaspati achieved its fundamental goals through the integration of AI and forensic tools into a single system. It was able to effectively show the world how technology can be utilized to aid police or forensic teams in the identification of dangerous content more efficiently and effectively. The project provides a solid platform for further improvements, such as enhanced AI accuracy, more data types, and more automation in forensic processes.

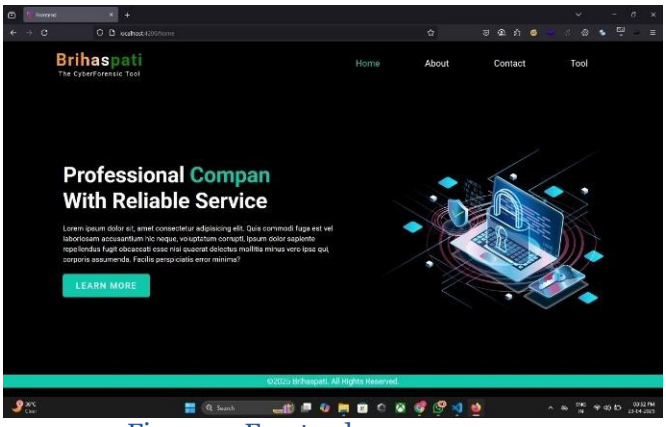

Figure. 2. Frontend

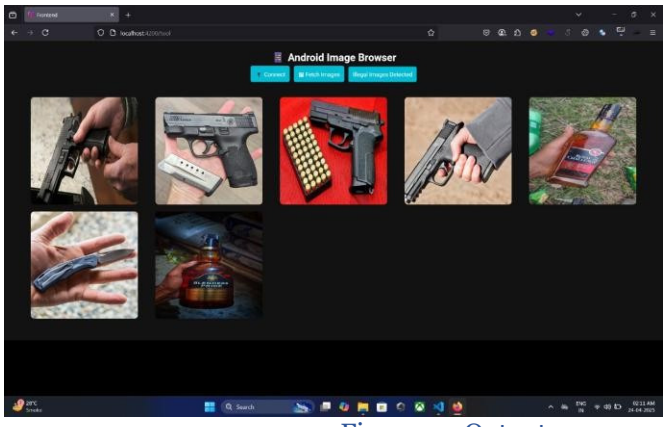

Figure. 3. Output

CONCLUSION

The Brihaspati project was developed with the goal of making smartphone forensic investigations faster, smarter, and more efficient by using AI and digital forensic tools. Through this project, we were able to successfully extract data from Android devices using ADB, it using Autopsy, and apply an AI model to automatically detect illegal or suspicious content in various media files.

This integration of tools and technologies assisted us in developing a system that is capable of assisting investigators in saving time and effort in performing manual analysis.

The easy and intuitive web interface of the platform, developed with Angular and supported by

Node.js and MongoDB, enabled us to integrate all the technical pieces into one viable solution. The AI model worked well and demonstrated its capability to identify drug-related content, weapons, and obscene material with reasonable accuracy. Although there remains much scope for improvement, particularly in improving the detection model and adding more features to the platform's functionality, the foundation we established is sound and has scope for application in digital forensic cases.

Lastly, Brihaspati shows the possibility of utilizing AI for providing valuable inputs to modern forensic investigations. Not only did this project help us familiarize ourselves with the technicality of making such a device, but also illustrated the magnitude of good and great work this technology can do in real-life applications. We look forward to improvements such that Brihaspati could prove an efficient tool for forensic experts and law enforcement agencies.

REFERENCES

[1] B. Machhi, P. Kotak, D. Parikh, and T. Patalia, “Advancing S-LEACH Protocol for Real-Time Underwater Observation in Freshwater Ecosystems (Rivers/Lakes),” Feb. 2025. [Online]. Available: https://www.jisem-journal.com/

[2] M. B. Machhi, P. Kotak, D. Parikh, and T. Patalia, “Implementation and Iterative Analysis of LEACH and Its Variants in UWSN Protocols,” Feb. 2025. [Online]. Available: https://www.jisem-journal.com/

[3] Mr. Bhaumik Machhi and Dr. Paresh P kotak, “An Implementation & Iterative study on LEACH and Its Different Versions of Protocol of UWSN,” 2023. Accessed: Sep. 05, 2024. [Online]. Available: https://www.eurchembull.com/archives/volume-12/issue-5/6169

[4] Mr. Bhaumik Machhi and Dr. Paresh P Kotak, “UWSN for Real-time Underwater Observation Technique for Freshwater (River/Lake) Section A-Research paper Eur,” 2023. Accessed: Sep. 05, 2024. [Online]. Available: https://www.eurchembull.com/archives/volume-12/issue-7/6650

[5] “Chapter_20_Final”.

[6] P. Saurabh and A. Jay Kumar Roy, “INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES Role of Cyber Forensics in Investigation of Cyber Crimes,” *International Journal of Law Management & Humanities*, vol. 4, 2021, doi: 10.10000/IJLMH.11543.

[7] “Digital Forensics in Cybercrime Investigation,” *International Journal of Science and Engineering Applications*, Oct. 2024, doi: 10.7753/IJCATR1310.1010.

[8] A. ALJAHDALI, N. ALSAIDI, M. ALSAFRI, A. ALSULAMI, and T. ALMUTAIRI, “Mobile device forensics,” *Revista Română de Informatică şi Automatică*, vol. 31, no. 3, pp. 81–96, Sep. 2021, doi: 10.33436/v31i3y202107.

[9] M. Kaur, N. Kaur, and S. Khurana, “A Literature review on Cyber Forensic and its Analysis tools,” *IJARCCE*, vol. 5, no. 1, pp. 23–28, Jan. 2016, doi: 10.17148/ijarcce.2016.5106.

[10] A. Almuqren, H. Alsuwaelim, M. M. Hafizur Rahman, and A. A. Ibrahim, “A Systematic Literature Review on Digital Forensic Investigation on Android Devices,” in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 1332–1352. doi: 10.1016/j.procs.2024.04.126.

[11] C. Forensics Page, “Fourth year-Eight Semester 09OE801-Open Elective-III (CYBER FORENSICS).”

[12] J. B. Vala and V. M. Vekariya, “The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection,” *Int J Life Sci Biotechnol Pharma Res*, vol. 13, no. 6, pp. 413–420, Jul. 2024, doi: 10.69605/ijlbpr_13.6.2024.80.