IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Enhancing Digital Forensic Inquiries with Data-Driven Decision Support

**[1]Saranya K, [1]Kavitha Bharathi M, [1]Madhumitha M, [2]Steffina Morin L**

[1]Student, Department of Information Technology, Anand Institute of Higher Technology, Chennai, India.

[2]Assistant Professor, Department of Information Technology, Anand Institute of Higher Technology, Chennai, India

***Abstract:*** The venture known as "Enhancing Digital Forensic Inquiries with Data-Driven Decision Support" is a web-based appeal. This software bestows a solution for confirming criminal felonies, problems", and mislay individuals to DIG. This software yields a facility for detailing online crimes, online protests, and mislaid persons appear criminal lists and points on the web page. Any number of the public can grumble online. Each user first makes their login to the server to share their openness. An effective way to start this task is to develop a mission statement that embodies the core functions of the unit, whether those functions are high-technology crime investigations, proof collection, or forensic analysis. However, Cyber forensics stifle steps to investigate or collect the data It is defined as the processes and devices used in investigations and gathering proof. Some of the decrees will be provided as a default such as category-wise. By analyzing the investigation report, the activity will be optimized to process the investigation process.

***Index Terms - AES Algorithm, Cyber Crime, Crime Data Management, Crime Investigation.***

## I. INTRODUCTION

Current science and automation technology have transformed the area of crime- resolving and have made the execution much more authentic and more rapid. The word "Forensic" mention all the science and automation technology used in resolving a crime.The motive of this complex is to direct and arrange the immense volumes of data that are assembled in the action of resolving crimes by the appeal of scientific procedure and current technology. When generating a new case binder, the complex will be able to retain specific data in a set.

## II. RELATED WORKS

Hossain and Sheikhi (2020) proposed the fast and accurate reconstruction of APT campaigns and presented two strategies, tag fading, and tag decay, to lessen the dependence eruption problem. It is extremely effective in the unmanned detection of covert APT-style effortsin real-time and fades over faulty alarms, relents, and compact precious graphs that seize most of the attacks.

Ul Hassan, et al. (2020) proposed the Omega Log: High-Fidelity Attack Investigation via Transparent Multi-layer Log Analysis where Omega Log an end-to-end origin-tracking complex uses the concept of universal fount to resolve the connotation gap and credit explosion issue that is now ongoing in source analysis frameworks. Gauging of real-world ambush scenarios appears Omega-Log grid is brief and ample with connotation information, similar to the state of the art.

Kiavash Satvat, et al. (2021) proposed the Extracting Attack Behavior from Threat Reports where the Threat Intelligence surveys are important to identify and rapidly respond to cyber threats. EXTRACTOR allows exact automatic extraction of crisp attacks and builds an origin graph from CTI reports in natural language. Gauging is done by various threat details andreal-world attack contexts, as it extracts graphs that match with those gaunt manually by securityexperts, and those graphs were used for threat detection.

Wei, et al. (2021) proposed the Insider Threat Prediction Based on Unsupervised Anomaly Detection Scheme for Proactive Forensic Investigation where BILSTM is a featured learning model able to contagious secular relations between efforts. BERT studying the model as the present centrifuge to see whether the showing can be embossed or not. AES has shownits robust ability in apart learning and extent reduction, and there are so many variances for reflex feature uprooting and dimension cutback for improving extend and urge the training pace in future work.

Umit Karabiyi and Karabiyik (2020) proposed A Game Theoretic Approach for Digital Forensics where this model suggests the most logical and optimum scheme for automated forensics investigators. These tools are tolerable in terms of the potency of a file chisel using either skewer or a Photo rec, which outcomes in a new plea regarding the changing of game-theoretic craving to various automated forensics-related areas.

Nieto (2020) proposed the Becoming JUDAS: Correlating Users and Devices during a Digital Investigation where this wrapper has preferred the JSON end users and tools audit (JUDAS) policy to agree with End users and tools, taking the edge of the JSON layout globally used by so many aid and technology, either to bole or to bestow outcomes of the act on

dataset through the probe of computer forensics. JUDAS spawns a merged study of the events of a digital(automated) perusal using the dataset.

Tong, et al. (2020) proposed the Finding Needles in a Moving Haystack: Prioritizing Alerts with Adversarial Reinforcement Learning a rife model of the alert sort offers a tome oracle and increases learning-based hail for discovering the finest sort policies deftly. An outcome of case cramming with a hand-root nexus invasion noting complex and machine swotting -hail deceit noting demonstrates that this scheme significantly hides non-prudent greetin nearly all cases.

Alghamdi (2021) proposed Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities where digital(automated) forensics has attained notable heed due to the enlarge in cyber felonies. Bitter software approaches and tools are being made and applied topose a threat to communal and private fireworks and use data storage. This hostage exposure and rift have inspired growth in the automated forensics area so that automated evidence can be uprooted from digital tools and can be used in the sinner and civil licit events.

Arshad, et al. (2020) proposed the semi-automated forensic investigation model for online social networks where these works group the basic concern of automatic forensic check on online social matrix, such as crime areas on deed framing, iteration fortify surmise trial, automated troupe and audit and data fount. This toil defines more chide aspects of a socialnetwork perusal that are not fairly framed by the subsites models.

Nisioti, et al. (2021) proposed the Game-Theoretic Decision Support for Cyber Forensic Investigations as rivals become new and sly, the use of anti-forensic manners for the smear of theodds of their sensing soar. Cyber perusal become more analytic and exigent, and analysts need brace systems that will grant them to expand their ability and ingenuity against prudent adversaries.

## III. EXISTING SYSTEM

Formerly they suggest DISCLOSE framework, whichever is the initial data-driven decision support chassis that supplies this skill to a moot examination. DISCLOSE agree theinvestigator steer along the pounce effort scope found on proofs unearth up to that point andthe expected aid obtain by each handy perusal act is more notable. Here anyone can undergo the data easily and it has a finite process to attain the result. Avail a repository of hostile plans, tools, and police, for each of which it collects menacing humint data to compute its odds link with the laze.

## IV. PROPOSED SYSTEM

By conferring our project, we point to establish more reliability for the document, sowe include AES Algorithm which encrypts and decrypts the data that will be inspected to optimize the action. From the report, the analysis action provides the decision-making solution. It will be coherent for data-driven processes.

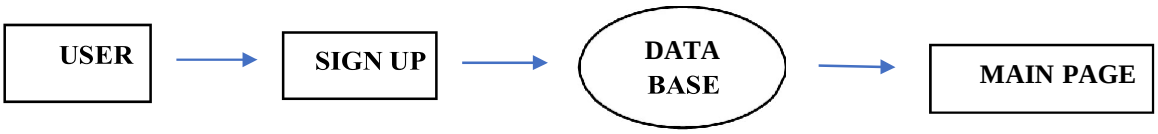
## MODULES

### REGISTER :

The register module supplies a theoretical framework for seizing data on that department in a way that: eases data entry and accuracy by corresponding the department ingress to a data root (usually note deed generated at a tip of care) such as local police andlawyer, ties simply back to individual subsection evidence to join registers to department data and amass data portion to allow superior operation of airy programs.


### LOGIN:

This arm in our gauge here embodies a part of work executed within an index oversight system (or similar system) in the case of a database and serves in a logical and reliable data way free of other agreements. Annals mostly act for any swap in the index each arm login appears on its own pages.




### CID:

In this module of our project, here describe the CID work and techniques,

- **ADD CRIMINAL DATA:**

In this arm of our project, CID can add data about former criminals data such as kidnapping, chain snatching, murder, and other cases of clear details to the database.


- **VIEW LAWYER REQUEST:**

In this module in our project, CID views the lawyer's appeal such as the lawyer required to know the criminal details for his investigations. If the lawyer is a sanctioned person to view the criminal details the CID sends it to the DIG.

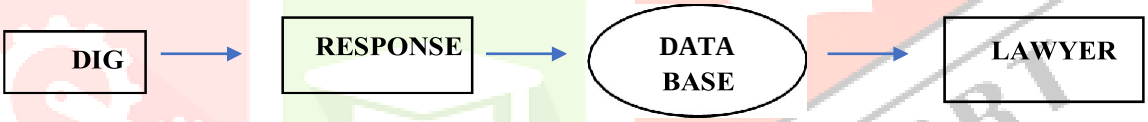

**DIG:**

1. **MAINTAIN CRIMINAL DATA:**

In this module of our project, DIG must maintain all criminal details in his database,such as CID-added data and local police-added data.


2. **RESPONSE TO LAWYER:**

In this arm of our project, DIG has to replay to prolong the data. Here the DIG view the request from the lawyer. If the lawyer is a sanctioned user, then the DIG responds to the request to the lawyer for the name of the secret key.

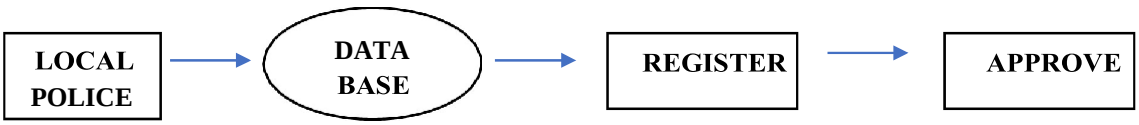



**STATE POLICE:**

In this module of our project, here describe the State police work and techniques,

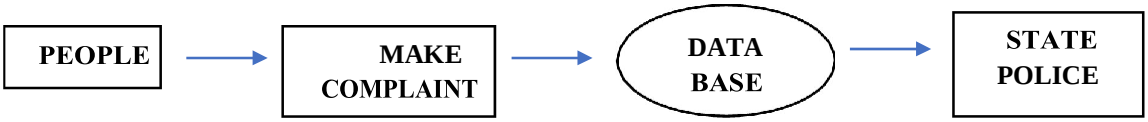
1. **APPROVE REGISTRATION:**

In this module in our project, state police need to accept the local police registration for their instance. Here the registration is not received by the state police the local policecannot be login. So, state police need to accept the registration.



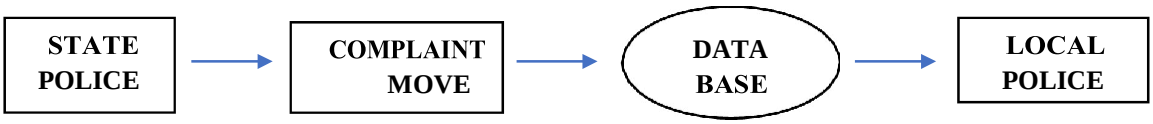

2. **VIEW PUBLIC COMPLAINTS:**

In this module in our project, here the state police view the public complaint.



### 3. MOVE TO THE LOCAL STATION:

In this arm in our project, here the state police are going to the people cavil to the local policestation is in the same zone area as people complain.

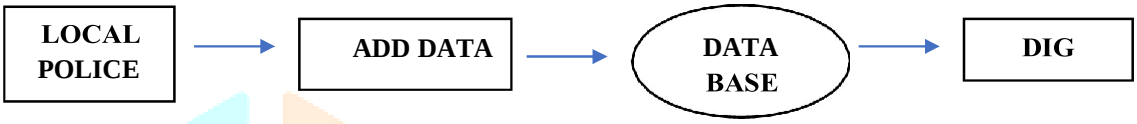



## LOCAL POLICE:

In this module of our project, here describe the Local police work and techniques,

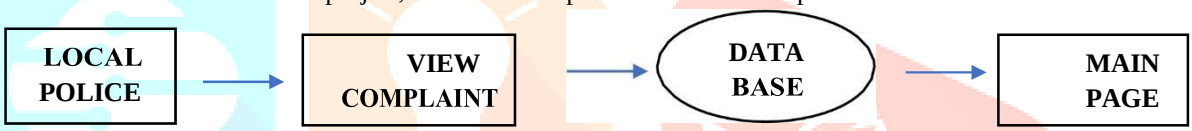
### 1. ADD CRIMINAL DATA:

In this module of our project, here the local police also need to add criminalrecords to the database. It will be viewed by DIG.



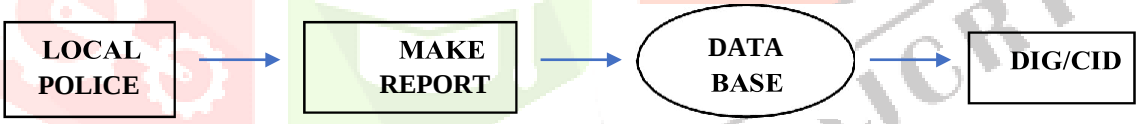

### 2. VIEW THE STATE POLICE FILE:

In this module in our project, here the local police view the state police forwardedfile for the new investigation.



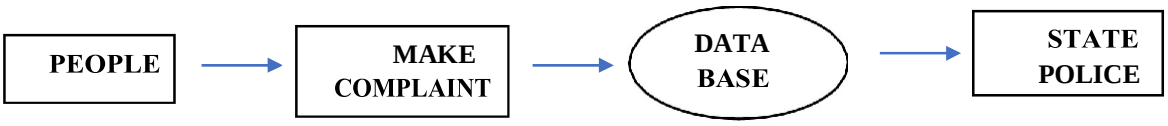

### 3. MAKE REPORT:

In this module in our project, here local police make the report for everyinvestigation.




## PUBLIC ADD COMPLAINT

In this arm of our project, usually people make complaints online. The complaint directlyviewed by the state police.



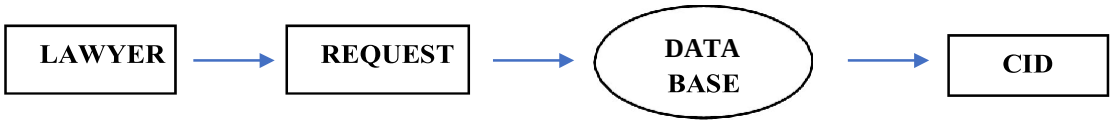

## LAWYER

### 1. VIEW THE LOCAL POLICE DATA:

In this module in our project, here the Lawyer views some records from the local police station. But cannot view all records. Some confidential files will secretly maintain by the DIG office.

**2. REQUEST CRIMINAL DATA:**

In this module of our project, the particular lawyer needs some criminal datafor his investigation. So, the lawyer requests criminal data from the DIG.




**3. DOWNLOAD:**

In this module in our project, After DIG responds to the request with thesecret key. Then enter the key to download the records.


## V. CONCLUSION

Digital rhetoric involves the act of identifying, obtaining, and protecting the document by scan, and hand over digital proofs. Automated proofs must be validated to verify their bearing in a field of law. Finally, the forensic relic and moot system used for fixed or live acquisition rely on the cases and their division. Real proofs must be authenticated, and material. This software is evolving with a portable detain. All modules in this complex have been trailed with valid facts and all worked auspiciously.

## REFERENCES

**[1]** K. Finnerty, S. Fullick, H. Motha, J. N. Shah, M. Button, and V. Wang, 2019. "Cyber securitybreaches survey 2019," Dept. Digit., Culture, Media Sport, London, U.K., Tech. Rep., Apr.

**[2]** Cost of a Data Breach Report 2019, IBM Security, New York, NY, USA,2019.

**[3]** A. Brinson, A. Robinson, and M. Rogers, 2006. "A cyber forensics ontology: Creating a newapproach to studying cyber forensics," Digit. Invest., vol. 3, pp. 37–43, Sep.

**[4]**L.Martin . Cyber Kill Chain. [Online]. Available: http://cyber.lockheedmartin.com/hubfs/GainingAdvantageCyberKillChain.pdf, 2014.

**[5]** V. Diaz, D. Emm, and C. Raiu, "Kaspersky security bulletin 2019: Advanced threatpredictions for2020," Kaspersky Lab., Moscow, Russia, Tech. Rep.,

**[6]** K. Kent, S. Chevalier, T. Grance, and H. Dang, 2006. "Guide to integrating forensic techniques into incident response," NIST Special Publication, vol. 10, no. 14, pp. 800–886.

**[7]** J. Williams, 2012. "Acpo good practice guide for digital evidence," Metrop. Police Service,Assoc. Chief Police Officers, GB, London, U.K., Tech. Rep., Mar.

**[8]** V. S. Harichandran, F. Breitinger, I. Baggili, and A. Marrington,, Mar. 2016. "A cyber forensics needs analysis survey: Revisiting the domain needs a decade later," Comput. Secure., vol. 57, pp. 1– 13.

**[9]** S. Barnum, Jan.2012. "Standardizing cyber threat intelligence information with the structured threat information expression (STIX)," Mitre Corp., vol. 11, pp. 1–22.

**[10]** J. Navarro, A. Deruyver, and P. Parrend, Jan.2012. "A systematic survey on multistep attackdetection,"Comput. Secur., vol. 76, pp. 214–249.