iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41841

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 10 Issue IV Apr 2022- Available at www.ijraset.com

A Survey on Blockchain Based Digital Forensics Framework

H S Shrunga[5], Ashwini M[1], Deepthi U[3], Spandana R[2], Rakesh K R[4]
[1, 2, 3, 5]*Department of Computer Science and Engineering, Vidyavardhaka College of EngineeringMysuru*
[4]*Assistant professor, Department of computer science and engineering, Vidyavardhaka College of Engineering Mysuru*

Abstract: Blockchain is the best suited technology that well satisfies the purpose and needs of security and integrity of evidences or proof collected by the police department as digital forensics across the country. This paper potray a blockchain based digital forensics framework as the proposed system, enabling privacy preservation and proof of existence. The proposed system is achieved by using SHA algorithm, AES encryption technique (Rijndael) and blockchain methodology. SHA algorithm mainly consists of SHA functions which are a group of hashing algorithms used for hashing the input of variable size. The AES encryption technique makes the uploaded forensic data to be encrypted and the data storage very secure. This project comes out as the best application that the defence department can use. The nature of the blockchain being decentralized, establishes privacy and tamper-proof. It also easily detects any wrong happenings or modifications and alerts the concerned authority. The forensic investigation framework establishes authenticity, security, traceability, privacy, immutability and becomes a trustworthy system for the defence department.

I. INTRODUCTION

Blockchain is a highly secured system which records information such that it is difficult to change or hack its content or data by cheating the system. all blocks of the chain are made of numerous transactions, and for every incoming new transaction to the blocks, its transaction record is added to every participant's ledger. Blockchain's nature is decentralized which is accessed and managed by many users. Hence blockchain is known as a type of DLT in which the transactions have a cryptographic key called hash.

The properties of blockchain are as follows:

1) *Distributed:* All participants of the network have a copy of the ledger to achieve maximum transparency.
2) *Secure:* All records are encrypted separately.
3) *Immutable:* All validated records are irreversible and also unchangeable.
4) *Anonymous:* Participants' identity is either anonymous or sometimes pseudonymous.
5) *Time-stamped:* A timestamp is recorded for a transaction on a block
6) *Unanimous:* All network users consent or agree to the validity of every records.
7) *Programmable:* Blockchain is programmable (smart contracts).

From these features, it can be inferred that blockchain makes it tough for any hacker to get through a block in the chained system and tamer any data.

II. LITERATURE SURVEY

In this paper[1], they have tried to establish a linkage between forensic blockchain and artificial intelligence as it can help to filter and manage different crime cases.

The introduction part includes the working of the forensic blockchain in 5steps and its advantages over other conventional techniques.

A. *Blockchain-AI conversion*

1) Evidences are present in blockchain.
2) Blockchains undergo interchange and tokenization of the data
3) AI monitors this resource in an advanced way.
4) AI specifications and intelligence calculations will exchange sources across a tech stack.[1]

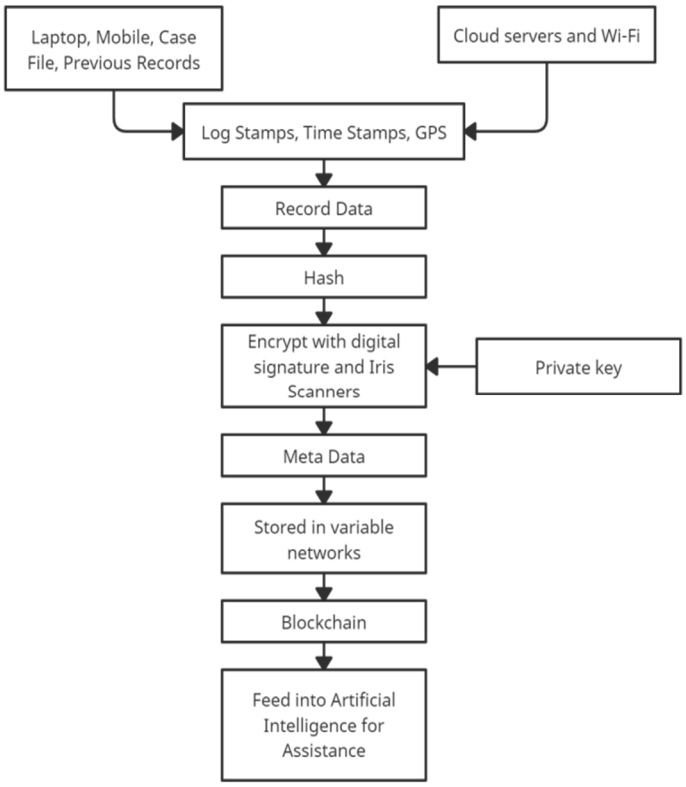


Figure 2.1-Flowchart of the link between AI-Blockchain [1]

This paper[2],shows various properties of soil like physical properties and chemical properties are examined for forensics. It has been caried out by performing few soil analysis experiments. One such important experiment is the PSDA. Soil samples and footprints are one of the important forensic data and evidence. This paper[2] gives bright insights about the soil analysis in an organized way.
PSDA considers soil texture and differentiate among soil samples by estimating proportions of sand, clay and silt using pipette method. After calculations, a triangular graph is plotted to determine the texture class and results are obtained analyzing it.

Sample ID	% Clay	% Silt	% Sand
1	1.58	2.38	96.04
2	0.27	2.15	97.58
3	20.59	20.8	58.61
4	1.91	0.6	97.49
5	19.51	20.68	59.81
6	16.77	21.9	61.33

Table 2.1- amount of clay, silt and sand in soil samples

From the table, the inference is that the texture of samples 4, 2 and 1 is sand as they have huge % of sand, whereas samples 6, 5 have a sandy loam texture and sample 3 has a sandy clay loam texture, as they have high content of clay and silt.[2]
In this paper[3],Network forensics deals with identifying how security is brought to stake or how the tampering is attempted. It is known as sub-branch of digital forensics which is concerned with supervising and analyzing traffic in the forensics system.
A proactive way of examining is taken up in this paper. A live data collection happens here making it easy and fast to solve the case.
The basic framework of investigation involves 3 stages:
Preparation, Investigation, Presentation
The proposed system uses encryption to provide integrity and it is maintained throughout with help of cryptography and decryption with use of a private key.

Proposed model of network forensics inculcates proactive investigation which undergoes below processes:

1) Function for event triggering
2) Collection of data
3) Data encryption
4) Preservation of data
5) Data decryption
6) Examination
7) Classification
8) Analysis of tested dat
9) Report of the investigation

In this paper[4], it presents the DNA forensic system architecture to the police center. It was discovered to help officers with work like collection, analysis and comparison of DNA. The design architecture is split into 2 parts→ networking and program. Networking deals with work as a distributed system and the program is developed to have a website for accessibility.

The methodology and design compresses of various stages like

a) Concept and architecture
b) Data input
c) Architecture design
d) System and service design

Finally, results are achieved better and in satisfactory terms with the proposed system. The proposed architecture takes 2 sec for sending request between centers, 10 sec to monitor status of work,2 min for data analysis, 2 sec sending results, 3 min is the total time spent on a case proving to be very efficient and reliable.[4]

In this paper[5],it presents a forensics framework in two layers which has multiple blockchain networks which is more secure. It verifies authenticity and integrity of collected data in case of possible tampering.

The proposed framework will be using MFI (Multi-Factor Integrity) system which is a multiple blockchains platforms at less cost. It is difficult to tamper or alter the data in aMFI. All of these systems are based on smart contracts, making communication between them simple. To decrease the amount of data posted on public block chains, hash algorithms and the Merkle tree are utilized. The method utilized to cut expenses is depicted below.

The IoT data hash is provided to a multi-level chain system's initial level from a boat IoT edge device in the first phase, based on some specified events or preconditions, and only interesting data is collected. As long as there is interesting data, it is sent to Stellar and EOS..

The confirmed transactions that were uploaded to initial level EOS and blockchain Stellar are collected from the rental company's data centre as part of the synchronization procedure. Another aspect that affects integrity is the Merkle root. As a result, it gets sent to Ethereum, a more efficient and safer blockchain.[5]

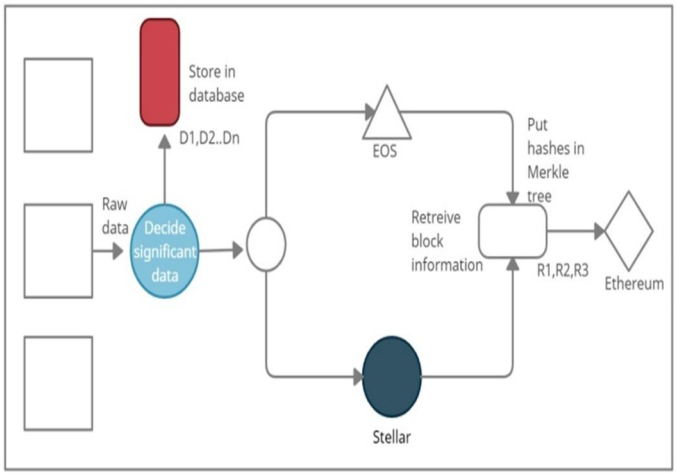


Figure 2.2: Proposed System Design

In this paper[6], Process provenance was established, which leverages block chain and cryptographic group signature technologies to provide effective evidence of existence and privacy preservation for process records. Process provenance offers evidence of existence and privacy protection for process records by integrating block chain and cryptographic group signature methods. The block chain-based process provenance architecture is depicted in the diagram below. For cloud forensics, the provenance system will enable auditing of process records. The following objectives will be achieved by the process provenance. A process record including the submission list and digital signatures of both interacting parties is delivered to the provenance auditor as soon as the acquired forensic data is submitted.

The important components of process provenance are:

- Submission list: The process record can be regarded the list file. As well as the sender and receiver's (group) signatures, included in this list
- Receiver: A receiver (typically an investigator) requests info from the cloud for forensics, and the sender fulfils the request.
- Sender: A sender (typically, a CSP or an investigator) gathers and distributes forensics data to the recipient. The sender sends the process record to the provenance auditor once the receiver validates the submission.
- Provenance auditor (PA): The PA receives process records from senders. If a sufficient number of documents have been gathered, PA embeds them in the block chain network and keep the related block chain receipt.
- CA (Certificate Authority): CA isn't mentioned in the diagram. The CA is in charge of the group signature system.[6]

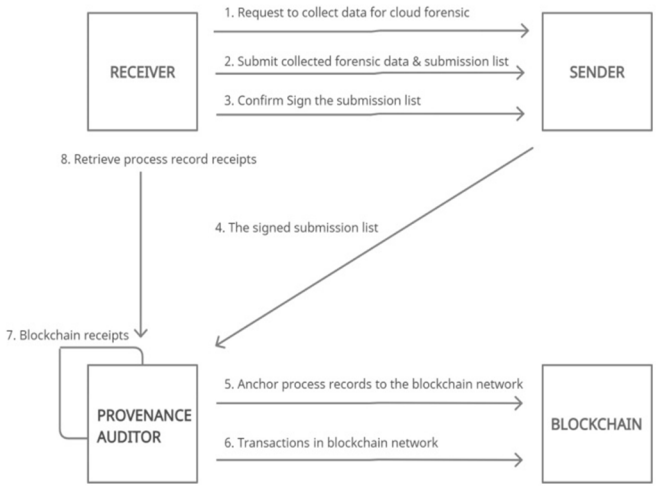


Figure 2.3: System Overview

In this paper[7],it has given that there are two technologies in cybercrime investigation –

- Theoretical digital forensic methodology
- Developing digital forensic tool through practically.

As a result, theoretical gives the steps to investigate the cybercrime, while the practical development gives the tools which systematically and sequentially study the digital devices where it helps in extracting the evidence to show beyond doubt of the crime.

Also, model uses past 25 forensic bodywork with more
cases along with history oriented, in order to generate an
algorithm that creates a brand new digital forensic model.
The history lookups will reduce the cost of investigation also gives the feedback which helps in the supply of information.

This paper includes some of the following sections:

- Provides an algorithm in order to generate a brand new model.
- Representation of all the research findings sequentially.
- Tabular representation for sequential logic.
- Future works to be done.

After proposing a model, it has some following advantages:

- Investigation through a method which is standardized.
- Theories are converted to tool.
- Facility in history lookup.
- Minimization of cost and time.
- Can be applied to various type of digital crime investigation. As a conclusion the proposed model is strengthened by 2 modules such as registration of case and evidence loader& history keeper. This provides practical hands-on for cases.[7]

In this paper[8],it gives us the insight of what to do when there is an attack in the internet. To detect any criminal activity where the forensic investigator is required to use some of the data recovering techniques. Decision tree is one technique which helps for file forensic investigation purpose.

What is digital forensic? It is nothing but collecting some of the information or evidence in digital devices and later, information is being examined to check whether there is any illegal activity like cyber-attack. Also, various types of attacks can happen such as:

- IP spoofing
- Salami of attack
- DOS of attack
- DDOS of attack
- Buffer flow attack

forensic analysis recovers data from digital devices, usually
general type of methodology is used for the analysis.

Preparation – data should be prepared by collecting them from log-files and browser history from web. It contains user session ID, session time, source ID, destination ID.

Detection – after gathering log files, next step is to detect an attack that has been occurred.

Generation – since log files gives us the detailed information about each file, This will create huge data which is difficult to maintain for forensic investigator.

Examine- this huge data is again examined to see whether
there is an exception.

Analysis – this step is very important because it helps in detecting a criminal activity and should take a decision according to that.

Investigation – this step is to understand what are the thoughts of an attacker behind her/his criminal activity.

Presentation – On getting the output it should be presented in tabular format/graphical format so that the investigator can easily understand the problem and give a decision on it. Data mining techniques are also used in identifying the crime records. To conclude log file is used as an input and stored in database as an evidence.

So usually this digital forensic is used to look out the behaviour of the attackers, to track them by gathering and examining log information in network.[8]

In this paper[9],Research has been done concerning the eGovernment frameworks.

To conduct a proper Digital Forensic Investigation (DFI) in eGovt frameworks, more importance on the use of Digital Forensics (DF) must be given.

The main intension of the author of this paper is that in future, DF tools will be developed thereby helps in facilitating the design of DFI tools in eGovt platforms more effectively or in an effective manner.

The figure represents the different DFI process classes. Proposed eGovernment Digital Forensic Investigation Framework:

- Definition of Scenario
- Identification source of evidence
- Detection of Plan incident
- Collection of potential digital evidence
- Preservation of Digital
- Storage process

The eGovernment forensics gives a clarity representation of all eGovernment related platforms which has to be investigated by the internationally recognized DFI methods.

Reactive Processes- it is a process which can be handled only when a security incident is detected. It consists of three phases:
Initialization phase
Acquisitive phase
Investigative phase
As a part of the duty for the future, the author plans to verify the findings of this study by designing a working prototype, otherwise they claim at this moment.[9]

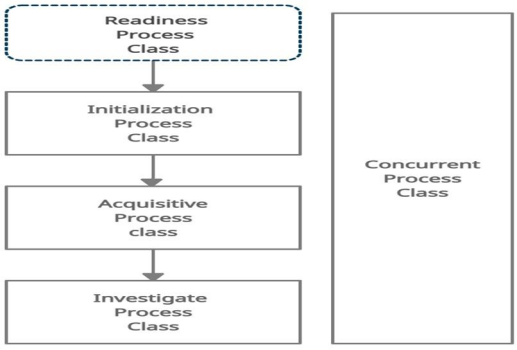


Figure 2.4: Digital Forensic Investigation Classes

In this paper[10],As the volume of data increases, there arises an option to build the case related knowledge and also to discover the evidence. A defined process of data reduction by the selective imaging and the quick analysis, it provides potential to undertake the analysis of the growing volume of data in a timely manner.
This paper gives a complete outline of the process of bulk
forensic data analysis that includes disparate device data.
Index terms that are used in this paper are: IoT Device
Forensics; Data Reduction; DF; Intelligence Analysis.
The contribution of this paper are:
a process of semi-automated scanning of disparate forensic
The data varies according to the devices,
and can be divided into: unstructured, structured, or a combination.
Specifically, the storage and processing power of many IoT
devices can be limited, and hence affect the ability to
undertake an investigation.
Digital forensic trainee will need to focus on relevant data, which may not necessarily be on a device.
The scope of Bulk Extractor can also be enlarged with
other device specific data included in the process of
identification and entity extraction.[10]

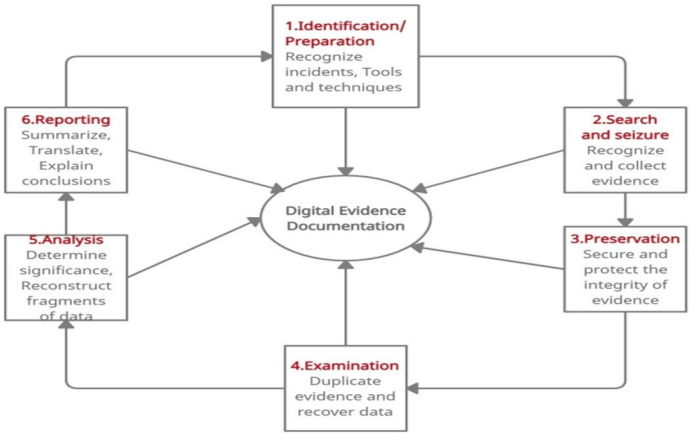


Figure 2.5: Digital Forensic Intelligence Analysis Cycle

III. METHODOLOGY

A. Application Manager

Application Manager have option to add areas because police stations are added based on area wise. Police Station login details generate a code using simple mail transfer protocol and login details are mailed to respective police station's email. Forensic staffs, Doctors & Higher Officers are added by application manager & login details are mailed to respective Email Id of the staffs.

B. Forensic Staff

Forensic Staff visit crime place, collect data which is needed by the lab to conduct test. Based on the collected data generate forensic report using Blockchain. Forensic report is a major part in crime investigation to collect evidence, so report need to be secure such a way that avoid manipulation or Blockchain tampering technique is adopted in forensic report to avoid any manipulation, and to recover it.

C. Doctor

Doctor generates medical report based on crime using Blockchain. Doctor report is also major part in crime investigation to collect evidence, so report need to be secure such a way that avoid manipulation or tampering. Blockchain technique is adopted in doctor's report in case if anybody try to access and alter the data.

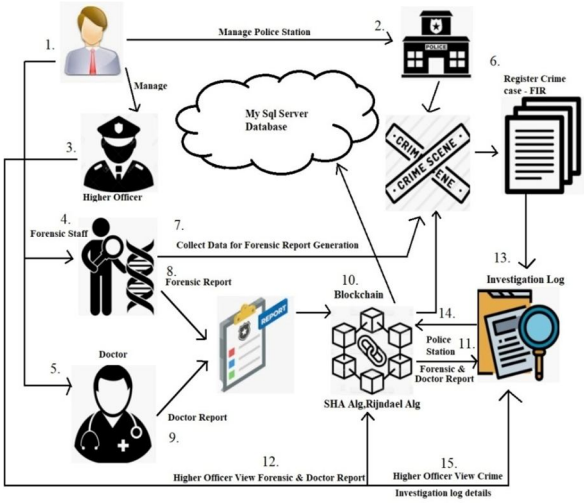
D. Police Station

Police Station Staff register FIR based on the crime. Based on the FIR copy, police station staff investigate crime using forensic report, doctor's report which is secured using blockchain. Police Station staff collect evidence from forensic report and doctor's report. Evidence plays a major role in crime investigation for
identification of criminals & punish them under law.

E. Higher Officer

Higher officers have an option to monitor crime details on police stations. Higher Officer have option to view crime investigation details, forensic report & doctor's report base on crime. Under higher officer's guidelines, police station staff investigate crime case, identify criminals & punish them on law.

1) Step 1: Data Collection by forensic staff at Crime Place
2) Step 2: Data Processing and conducting tests in forensic lab.
3) Step 3: Generate Forensic Report which includes results of fingerprint, type of Weapon, blood group and more.
4) Step 4: Forensic Report secured using SHA, AES Rijndael algorithm & Blockchain.
5) Step 5: Doctor Examination (Medical Examination) of dead body.
6) Step 6: Generate Medical Report (Calculate Death Hour, Toxic/poison inject or any kind of wounds)
7) Step 7: Medical Report secured using SHA, AES Rijndael algorithm & Blockchain.
8) Step 8: Police Station Staff investigate crime case based on Forensic & Medical Report.



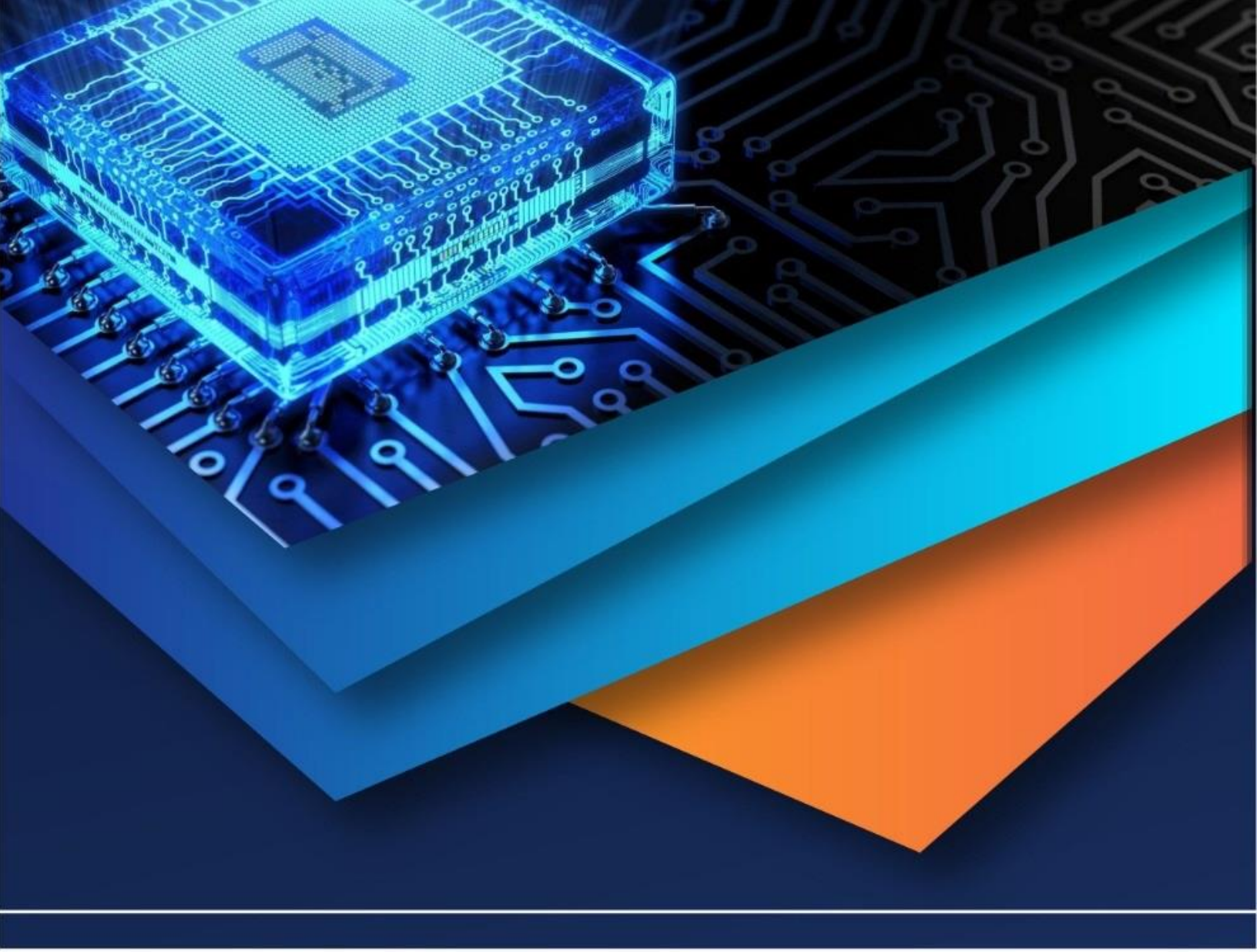
- The framework proposed can be incorporated to future digital forensics tools development, facilitating the design of effective digital forensics tools in e-Gov platforms.
- This framework can be used by private security agencies to provide data security.
- It displays the artifact that proves they once existed. And identifies the deleted files that still exists.
- It is used in civil cases such as forgeries, fraud or negligence.
- It is used by Police, Forensics, and Crime department.

IV. CONCLUSION

Forensic & Medical report is a major part in crime investigation & collecting evidence, so this project proposes to secure the forensic/Medical report using Rijndael algorithm with SHA algorithm and Blockchain technology. The crime forensic/medical report detail exchange to police department in a secure & authenticated way such that it is helpful in future crime investigation. This application is tamper proof, so that forensic/medical report is highly secured using blockchain technology.

REFERENCES

[1] Nikitha Mani, Soham Sanjay Parab, Srikuja Manaswini, Sharon Philip, Parli B Hari, Nrashant Singh, “Forensic Block Chain and it’s linkage with Artificial Intelligence: A new Approach”, 2021
[2] Mayssa Hachem, Bhoopesh Kumar Sharma, Ahmed El Naggar, Ishani Pilankar, Nashrah Anwar, “Systematic Approaches For Soil Analysis In Forensic Investigation”, 2020
[3] Abiram Sivaprasad, “Secured Proactive Network Forensic Framework”, 2017
[4] Amnart Rattanamuang, Sirapat Chiewchanwattana, Khamron Sunat, Boonsup Waikham, “DNA forensic system for police forensic science centre cooperation: Architectural design and implementation”, 2016
[5] Suat Mercan, Mumin Cebe, Ege Tekiner, Kemal Akkaya, Melissa Chang and Selcuk Uluagac, “A cost effiecient IoT forensics framework with blockchain”,2020
[6] Young Zhang, Songyang Wu*,BoJin, Jiaying Du, “A Blockchain- ased Process Provenance for Cloud Forensics”, 2017
[7] Nilakshi Jian, Dr. Dhananjay R Kalbande, “Digital Forensic Framework using feedback and case history keeper” 2015
[8] Ms. Priyanka Salunkhe, Mrs. Smita Bharne, Mrs. Puja Padiya, “Data analysis of file forensic investigation”,2016
[9] Ivan’s KIGWANA, Victor R. KEBANDE, H.S VENTER, University of Pretoria, Private Bag X20, Pretoria, 0028, South Africa, “A proposed digital forensic investigation framework for an eGovernment structure fro Uganda”, 2017
[10] Kwang Raymond Choo, Senior Member, IEEE, “Iot Device Forensics and Data Reduction” ,2017



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY