iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.48426

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 XII Dec 2022- Available at www.ijraset.com

Advanced Intuitive Model for Digital Forensics Collection Methods in the Context of Cloud Computing and IoT

Abhijith Kotasthane[1], Aparna Khare[2], Bapat Gaurav Sunil[3], Pradnya Kashikar[4], S Suhas[5], Subin Khullar[6]
[1]*DRDL Hyderabad*
[2]*National Informatics Centre, Government of India, Lucknow*
[3]*NTT Data, Tokyo*
[4]*BITS, Pilani*
[5]*Akamai Technologies Pvt. Ltd, Bengaluru*
[6]*Evalueserve, Gurgaon*

Abstract: ***With the wide scale adoption of cloud computing paradigms and Internet of Things implementations, the arena of service delivery has changed significantly for the world of technology-oriented services. While these new modes of service delivery have provided innovations that were not fathomable earlier, they not only create new non-traditional pathways for evidence generation, nevertheless, they have also been seen to carry a potential of creating and exposing a whole new set of security vulnerabilities that malicious actors can exploit. Traditional forensic investigation process falls short in many ways including the way it aims to identify and link crucial pieces of evidence in these scenarios due to a myriad of internal and external factors. Challenges and inadequacies have been identified in the community in relation to these specific sets of advancing technologies that hinder the efficient identification, extraction and processing of evidence generated in crimes involving them. In this paper we wish to surmise the current forensic collection methods, how they pose challenges when put together with the latest cloud and IoT technologies and then attempt to propose an advanced, more intuitive, and theoretically validated digital forensic collection process guided by zero trust principle and enforced with artificial intelligence and machine learning methodologies with the aim to fill the gaps and provide a more reliable, robust and intuitive model to perform digital evidence collection in the given context.***

Keywords: Digital Forensics, Digital Forensics Investigation Model, Zero Trust, Artificial Intelligence, Machine Learning, Internet of Things, Cloud Computing.

I. INTRODUCTION

Digital forensics has always been considered a science of being able to preserve, identify, acquire, extract, process, document, and present relevant evidence which can be used in a court of law. While this is very much a disciplined science, a very subtle undertone of innovation, creativity and promptness drives it. The validity of this statement relies on the fact that technology that fuels the modern-day cybercrimes is essentially changing every minute.

Cloud computing and Internet of Things (IoT) have together brought about a revolution in how the services are enhanced and delivered and how technology can be adapted for use in diverse use-case scenarios. The sheer variety of service delivery guarantees that there is no one fixed sequence of actions that cybercriminals may follow to attain their motives, even though a significant number may take up a common, well-known path that assures definite success in the malicious endeavors. Previous and recent surveys on digital forensics in the context of IoT and cloud computing demonstrate the close relationship between human-computer interaction. The daily activities of netizens generate a potential source of evidence that forensic experts can investigate in order to have a stand-alone digital forensics collection method in the available technological and physiological environment. [6]

The digital investigation process for a forensics expert has to be just as adaptive and intuitive as it is methodical of the ways in which the evidence is identified and collected, so that no essential evidence is lost due to technological or methodological barriers. In this regard, identification and collection form the basis of the digital forensic process and require to be malleable and instinctive to capture the adaptive nature of data being generated that may be of significant value.

The ability to connect the dots with one potential source of evidence to another and being able to relate what seems of no significance to the untrained eye is essentially the result of both discipline and flexibility. Such a collection model can effectively fill in for the inadequacies of the contemporary models of evidence collection and present a more effective approach towards the digital forensic process.

II. CONTEXT AND BACKGROUND

A. Early Digital Forensics

Digital Forensics, which was known as computer forensics up until late 1990s, evolved largely as a response to a demand for service from the law enforcement community [1]. The world of investigation saw an emergence of new problems when computing was made ubiquitous and available to the masses, malicious actors being an evident part of the same. The increasing volume of data, the ability to alter data without leaving any trace and the ability to mask or even delete data were new variables that forced the forensic fraternity to find better ways to handle evidence. Forensic Computer Investigation was born out of this understanding that there was a need for a higher level of specialist knowledge needed to investigate the new technology.

Approaches to forensic acquisition and sophisticated evidence collection techniques become increasingly important in shaping proposed models that may independently execute the discovery and accumulation of admissible evidence to perform an effective digital inquiry and additional forensic analysis. [10] By gathering evidence from a variety of sources, including cloud storage, Google drives, web browsing history and cookies, drop boxes, as well as through physical investigation and data acquisition processes, the Internet was eventually recognized to play a crucial role in identifying the sources of attacks, both active and passive. [7].

While the general objective of physical forensic sciences has been, through the application of rigorous scientific method, to be able to circumstantially reconstruct a series of events linking a suspect to a crime using the available trace evidence, the objective of computer forensics aims to provide the means whereby a series of events surrounding a crime with manifestations in a digital environment is reconstructed [2]. It is however important to map this distinction, that computer forensics, or now digital forensics must take into consideration numerous factors while performing the restructuring process, including the quantity of data, the mode of collection, and finding traces of evidence itself from the massive amount of digital information available at hand. What further complicates the process is the requirement that the application of the technology for the collection process must be carried out with due regard to the requirements of the law. The investigative procedure must be carried out in a way that is acceptable as part of the jurisdiction and permitted in the court of law if and only if the data gathering methods are deemed to be appropriate. Failure in such a case may result in the digital evidence being ruled tainted and inadmissible.

With the current cyber-crime scenarios in which physical and digital boundaries have essentially been diluted, resulting in a tremendous increase in cyber-attacks in recent years, the complexity, heterogeneous environments, and influential nature of IoT and cloud computing are driving the adoption of innovative and upcoming frameworks and models to deter and deal with. [9]

B. Digital Evidence Principles

For any digital evidence to be admissible in court of law, there are certain mandatory attributes that the evidence must have. These can be enumerated as below [2]:

1) *Admissible*: It must conform to certain set legal rules of admissibility before it may be presented in a court of law.
2) *Authentic*: The evidence must be positively linked with the incident.
3) *Complete*: The evidence must not be constrained by a singular perspective and should be able to relate completely.
4) *Reliable*: The evidence collection and handling process must be free of doubt as to its authenticity and veracity.
5) *Believable*: It must be promptly credible and understandable to the court.

C. Contemporary Digital Evidence Collection Challenges

The volatile and transitory nature of digital evidence requires extra consideration and significant challenges in general for anyone who is tasked with searching and seizing digital evidence. Securing and retrieving relevant information in such a manner that ensures that the digital evidence principles are met requires special knowledge and discipline. The hindrances in the collection process can essentially be identified in two categories [2]. These are mutability and interpretation. The mutability of computer-based evidence includes real time events that are transient in nature and are more sensitive to alteration and nonvolatile evidence that is persistently stored in a semi-permanent or permanent form of medium.

The interpretation aspect involves the degree to which the digital information itself needs to be processed so that it becomes understandable. This often involves careful reinterpretation of the information from its binary form ensuring that the digital evidence principles are met.

Given such a significant need for careful collection and interpretation, it is quite apparent that a model or a framework that efficiently weaves in the evidentiary requirements and the digital evidence principles alongside the legal considerations was deemed necessary to provide coherency and consistency to the digital forensic process. Several models have since been in practice that aim to handle the contemporary digital evidence collection process, each evolving one after the next giving consideration to the inadequacies left behind.

III.EXISTING MODELS

In this section, we will analyze some investigation models to infer the advantages and disadvantages of each of the existing models
.

A. Contemporary Digital Evidence Collection Challenges

This model was introduced in 1984. It comprised of four main phases: acquisition, identification, evaluation, and admission. Acquisition phase involves acquiring the evidence. Identification phase involves the collection of relevant data. In the evaluation phase, the collected data is subjected to estimation and hypothesis. In the final phase the collected data is presented to the court. Disadvantages of this model were firstly; this model was not focused on securing and preserving data from intrusion during the investigation process. Secondly, the model was linear with no relatable phases, which precludes updating of evidence. Thirdly, there was no provision for storing an investigation scenario.

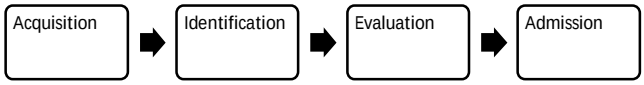


Fig.1 CFIP Flow Chart

B. Digital Framework Investigation Model (DFIM)

This model was introduced in 2001. It comprised of six phases namely: identification, preservation, collection, examination, analysis, and presentation. Identification phase was to plan the investigation process. Preservation phase was for maintaining data privacy and integrity. Collection phase involved the collection of data. The analysis and examination phase ensured that the consistency of the evidence is maintained. Presentation phase comprises the methodology of presentation of the evidence in the court. Disadvantages of this model include, first, there is no provision for going back to the previous phase in order to amend or modify tasks, second, the model does not mention about the preparation phase required before initiating the investigation procedure, which may result in increasing the investigation time, and third, the model does not lay emphasis on maintaining the sanctity of owner property.

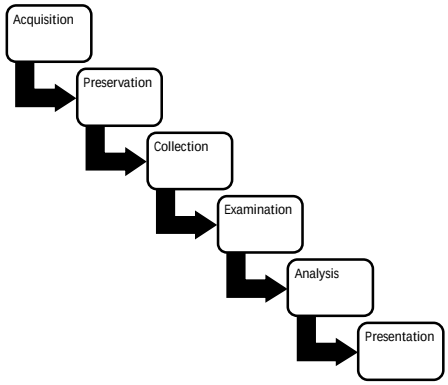


Fig. 2. DFIM Flow Chart

C. Abstract Digital Forensics Model (ADFM)

This model was introduced in 2002. It comprised of nine main phases. This model introduced preparation phase, approach strategy and returning evidence phases to the previous model. The additional phases were added to minimize the investigation time, preservation of data, possibility of error correction at later stages and returning of evidence to the owner. The disadvantage of this model includes less emphasis on maintaining the data confidentiality and integrity and no phase for storage and reporting investigation events.

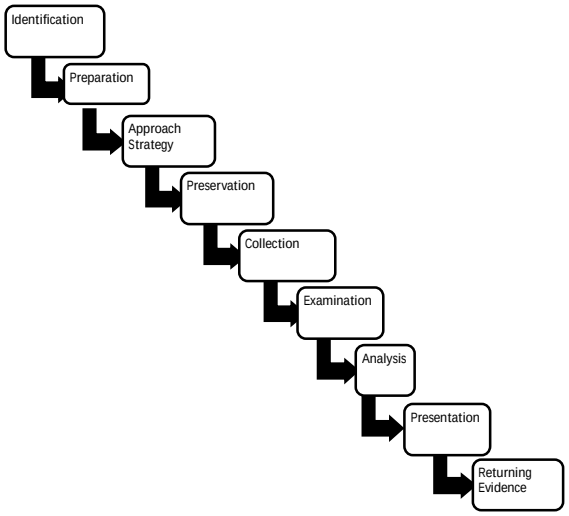


Fig. 3 ADFM Flow Chart

D. Integrated Digital Investigation Process (IDIP)

This model was introduced in 2003. It comprises of five phases: Readiness phase, Deployment phase, Physical Crime Scene Investigation phase, Digital Crime Scene investigation and Review phase. The advantages of this model include minimization of investigation time, segregation of physical crime scene investigation phase and digital crime scene investigation phase, ensuring integrity and confidentiality of evidence. The disadvantage of this model is that there is no reference to ensuring the sanctity of owner property.

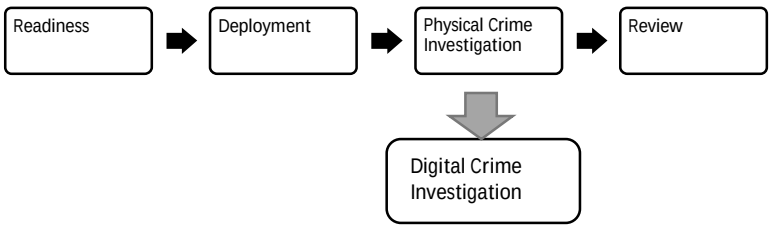


Fig. 4. IDIP Flow Chart

E. Enhanced Digital Investigation Model (EDIP)

This model was introduced in 2004. It includes all the phases of IDIP and amalgamates Digital and Physical Crime Investigation Crime phases into one phase named Submission phase. The advantage of this model is that the concept of chronological evidence collection was introduced which reduced the investigation time and enhanced the reliability of evidence. However, like IDIP this model also gives no reference to confidentiality, integrity of evidence and does not ensure the sanctity of owner property.

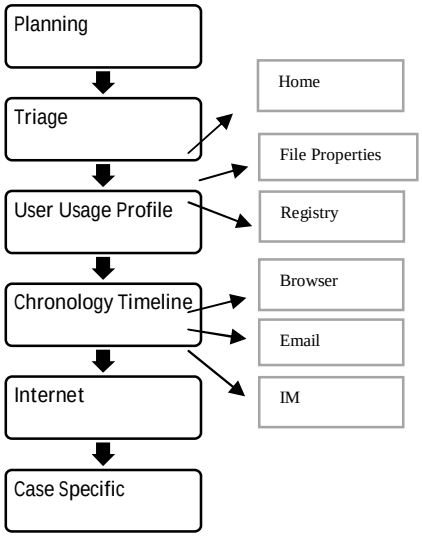


Fig. 5 EDIP Flow Chart

F. Computer Forensics Field Triage Process Model (CFFTPM)

It was introduced in 2006. This model proposes six steps namely: planning, triage, user usage profile, chronology timeline, internet, case specific. Advantages of this model are it reduces the investigation time; user profile adds user features (helps in understanding the case better) and increase in clarity due to case specific phase. The disadvantage includes no reference of confidentiality and integrity of collected information, sanctity of owner property not maintained.

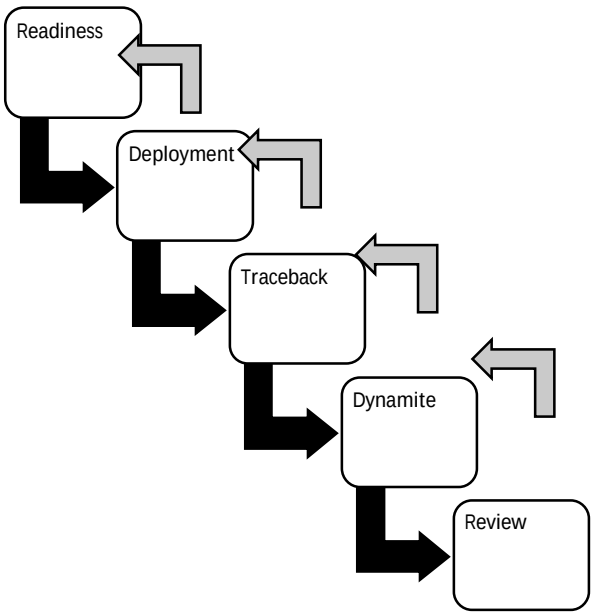


Fig. 6. CFFTPM Flow Chart

G. Digital Forensics Model Based on Malaysian Investigation Process

This model was introduced in 2009. It comprises of seven phases. It introduced a new phase called Archive Storage. The advantages include reduction in investigation time, ensuring the confidentiality and integrity of evidence data and the process can be reused in future investigation. Disadvantages of this model include no reference to ensuring the sanctity of owner property and no provision for correction of steps at a later time frame.

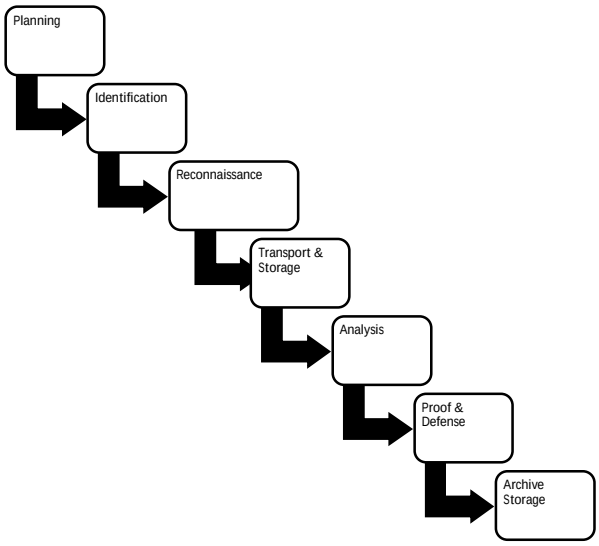


Fig. 7. DFMMIP Flow Chart

H. Other Models

Many other models have been proposed to address the issue of evidence collection, some of which are listed below:

1) Scientific Crime Scene Investigation Model (2001)
2) End to End Digital Investigation (2003)
3) Extended Model of Cybercrime Investigation (2004)
4) A Hierarchical, Objective-Based Framework for the Digital Investigations Process (2004)
5) Framework for a Digital Forensic Investigation (2006)
6) Common Process Model for Incident and Computer Forensics (2007)
7) Dual Data Analysis Process (2007)
8) Network Forensic Generic Process Model (2010)

IV. ASSESSMENT OF EXISTING MODELS

On assessing the existing models and comparing them following can be inferred

1) *Phase one: Preparation phase* – This phase deals with the steps wherein the investigators decide on approach methodology, Planning, Pre-Analysis and Preparation for collection of evidence.
2) *Phase two: Acquisition phase* – The major steps that have been defined by the existing models cover aspects of identification, & Storage.
3) *Phase three: Analysis* – This phase deals with the steps to be taken after the collection of the evidence. It mainly covers the process of analyzing the evidence, Timelining, Evaluation, and reconstruction.
4) *Phase four: Presentation* – In this phase the evidence collected is presented in the format along with proofs and analysis.
5) *Phase five: Post Process* – In this phase the entire process of evidence collection culminates wherein the closure report is prepared and the information is disseminated to the concerned and review report is prepared.

V. CHALLENGES AND IDENTIFYING THE GAPS

Based on the study of the contemporary models, it is apparent that with the emergence of upcoming technologies such as IoT and Cloud Computing, digital forensics is now having to deal with unprecedented amounts of data in the form of evidence from myriad sources. The processing of such a large amount of data (often termed now as Big Data) poses various challenges in digital forensics in acquisition, handling, and processing. For example, data may be distributed across locations/sources and may be present on various online social media platforms, cloud networks, and personal/institutional storage units. Forensic experts may be required to collate such data spread across all such locations/sources. Also, privacy laws and law-enforcement agencies may require that the private and confidential data of individuals and firms may not be disclosed or accessed for forensic examinations or otherwise without prior permissions and legal hassles. Further, now-a-days, techniques, such as, information masking, encryption, and cloaking may prevent forensic experts from easily gathering and analyzing digital evidence.

Broadly, there are three prime challenges that have been identified.

1) First, is the need to be able to validate and verify data that is being received from such vast sources. Data can easily be altered unless proven untainted and that is where the idea of zero trust comes in. It is imperative to be able to present reliable results to ensure the evidence can serve its purpose. While some sources of evidence can be reliably trusted, most of the time the source and the validity of the evidence requires critical evaluation. Implementing zero trust as a set of guiding principles in a digital forensic investigation model can bring in the critical "do not trust, until verified" evaluation that is a necessity with the myriad sources of information at disposal for evidence collection.

2) Second, there is a need to consistently handle the volume, velocity and variety in a standardized manner for acquisition and processing. This can be handled using artificial intelligence and machine learning methodologies. There are various AI/ML techniques, such as neural network models (e.g., Generative Adversarial Network models), that may be useful in extracting and analyzing incriminating digital evidence. For example, GAN models may be useful for identifying fake videos and images (also called deepfakes), which may seem like legitimate ones to the human eye [3].

3) Third, there is a need to provide a mechanism for storing this voluminous evidential data in such a manner that it stays untampered with adequate redundancy. The problem with existing digital evidence storage is, some central server/ cloud storage methods are used which can be tampered with at any time. Even though hacking scenarios can be proved later, once critical evidence is lost or if chain of custody cannot be explained because of some reason, integrity issues may add up the problems in investigation. Centralization of data also results in serious issues regarding lack of control and potential single point of failure if this centralized data store is not available etc.

An approach to handling such challenges is being proposed in a new model that has been built upon the learnings of existing models and utilizing methodologies built upon zero trust, artificial intelligence, machine learning and blockchain technology.

VI. PROPOSING A NEW MODEL

A new model for digital forensic investigation is being proposed with the aim to overcome the lacunas existing in the previous models and ensure confidentiality, integrity and availability of the evidence, its collection and presentation keeping in view the futuristic cyber domain.

A. Building A New Comprehensive Model

The previous models concentrated more on collection of evidence and were suffering from one or more of following features namely: preparation for collection of evidence, securing of evidence, ensuring the confidentiality and integrity of evidence, maintaining the sanctity of owner property and coverage of all types of crime.

B. Discussion on Proposed Model

The cyber domain is expanding itself at a very fast pace and with the introduction of IoT, Cloud and AI enabled features the complexity has increased manifold. The model proposed in this paper has been named Advanced Intuitive Cyber-Crime Investigation Model (AICCIM). It is a seven-phase model.

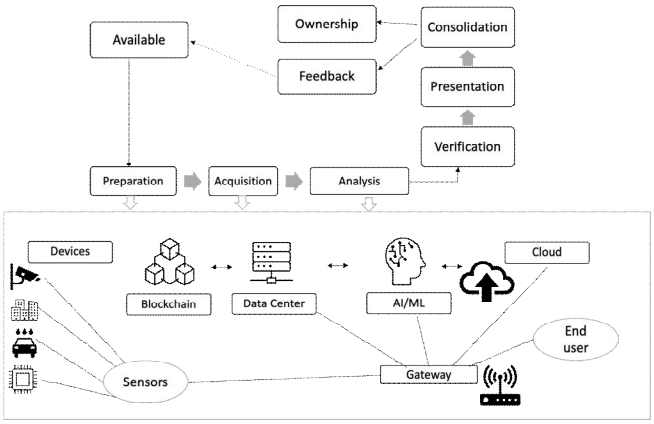


Fig. 8 Proposed Model

1) Phase One: Available Phase

The everchanging cyber arena entails that the investigators and the investigation labs are ever prepared to investigate the crime scene. This will involve all the steps required to be done prior to the actual investigation and collection of data. The major tasks will include availability of accredited investigators, availability of hardware and software tools (duly upgraded to latest standards), formats for recording of evidence, Standard operating procedures to be followed.

2) Phase Two: Preparation Phase

This phase initiates reporting of the incident. Since every incident is unique and hence a dedicated and concentrated preparation is required as per the incident. Major activities involved in this phase are pre analysis, composition of the team (including hardware and software tools), collection of formats and requisite permissions for the authorities. The preparation techniques will entail an individualistic approach for cloud/ IoT/ blockchain /AI/ML domains.

3) Phase Three: Acquisition Phase

This phase is the most important phase, as it deals with the actual collection of evidence which will form a basis for future phases. The major steps involved are crime scene investigation, user investigation, reconnaissance, identifying, acquiring, collecting, storing, transporting and preserving of data. The steps missed in this phase are irreversible. Acquiring the evidence in a blockchain will be at a fast pace as the data will be available at more than one place and will be untampered. On the similar lines the evidence acquisition from IoT devices, cloud platforms (SAAS/PAAS) or AI/ML platforms will involve tracing of data flow from the devices on these platforms and their interaction with each other. This phase may also utilize blockchain technology for the purpose of evidence storage and handling across distributed nodes to provide security and redundancy.

Addition of blockchain technology in criminal investigation will not add a new layer in model, but it will try to strengthen the acquisition phase. As the acquisition phase involves evidence storage and chain of custody plays an important role in criminal investigation for proving the crime, we think that the blockchain will add significant benefit and speedup the current investigation process. Blockchain has revolutionized the way distributed ledgers are managed on peer-to-peer networks and allowing all network nodes to participate in consensus to validate transactions on blockchain, we can use this to save and share critical evidences to governing body along with chain of custody data maintained by blockchain, removing explicit handling of it. With simple blockchain we can implement the whole network, but it will have some problems like an infinitely growing evidence chain, so once a case is over if you want to delete details from blockchain, it cannot be done. Or it can even hamper the network performance of the investigation office for long hours if continuous transactions on blockchain are happening because everything (log, hard drive copies etc.) is stored on the blockchain.

A couple of solutions were surveyed to tackle this problem mainly under the domain of off chain data storage. It is essentially non-transactional data at scale. As for some of the evidences it will be inconvenient to store them on blockchain due to size (Disk images), frequent updates, deletion requirements (Logs, IoT data) we save such data on off-chain shared only with authorized parties of network (investigating officers, governing bodies) while storing metadata on blockchain. With distributed data storage, all nodes in the datastore network maintain a shared copy of the data. This solves the single point of failure problem of data availability. It also supports more complex peer-to-peer sharing models where data can only be sent between parties. Blockchain supports various off-chain data management mechanisms such as Interplanetary File System (IPFS), Ethereum Swarm, StorJ, MaidSafe, Sia (HLF, Corda also provides functionality).

4) Phase Four: Analysis Phase

This phase involves analysis of the evidence collected, segregation of evidence collected (physical and digital), reconstruction of the events, Chronological event analysis. This phase deals with organizing the evidence collected and recording of events and evidence collection to act as a basis of the next phase. A detailed analysis will help in establishing the interrelationship between domains (AI/ML, Cloud Computing, IoT, Blockchain) and evolving a firm evidence data. AI/ML models may be used for live forensics, data recovery, password recovery, file filtering, and timeline analysis. Following use cases have been identified with regards to utilization of artificial intelligence and machine learning (AI/ML) technologies in this phase of the model [4] [5]:

a) *Knowledge representation for digital forensics:* AI/ML models may be used to create ontologies or taxonomies from digital evidence (e.g., images, videos, text, logs) to share digital forensics data in a structured format, such as, an XML or an RDF format. Such knowledge representation in the form of ontologies or taxonomies may help to organize case information as a reusable case repository.

b) Reasoning process for digital forensics: AI/ML models may be used to explain a reasoning process of a case. AI/ML models for reasoning process are divided into two types, namely, symbolic, and non-symbolic. In the case of symbolic, the reasoning process is based on a discrete entity from a knowledge base. As an example, the symbolic type includes an expert system. Further, a case-based reasoner (CBR) is a symbolic type of AI/ML model, which works on principles of psychology as the domain knowledge. On the other hand, the non-symbolic reasoning process is based on knowledge extracted from a representation structure.

c) Pattern recognition for digital Forensics: Various classifiers (such as, neural network models and decision trees) and clustering models (such as, unsupervised learning models, for example, K-means model) may be used to recognize patterns in data, identify categories/clusters, detect anomalies, and predict outcomes. Classifiers and clustering techniques may be very useful in sifting through mounds of data and detecting suspicious events, predicting suspects, and flagging security loopholes.

d) Knowledge discovery for Digital Forensics: Data mining is a field that encompasses AI and statistics and can be used for pattern analysis. Data mining techniques such as exploratory data analysis (or EDA) can be used to find meaningful relationships between data variables. EDA can also be used to establish dependency between data variables to achieve better feature engineering and thereby improve the accuracy of other AI/ML tools applied on the data.

e) Adaptation of AI/ML models for digital forensics: AI/ML models may be dynamic learning models that may adapt to instances of new data items fed to the model. Thus, based on new progresses in the field of digital forensics, and discovery of new facts in forensic cases, the AI/ML models may be re-trained or fine-tuned. This adaptation of the AI/ML models may ensure that their accuracy increases with time and each case.

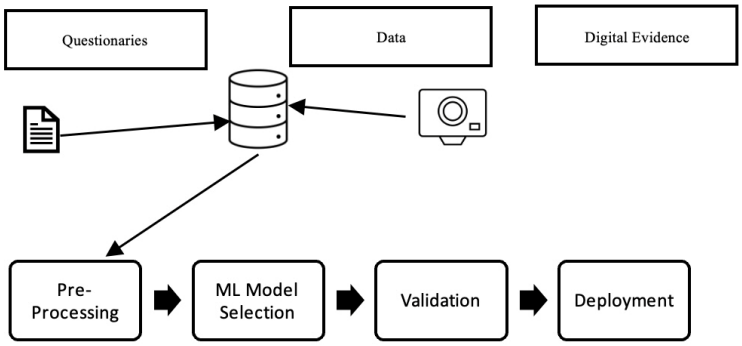


Figure 9. AI/ML Influence Model

5) Phase Five: Verification Phase

This phase is furtherance to Analysis phase as the evidence collected is analyzed in depth to form a logical event flow chart, responses of users at every step is assessed, the source of crime and criminal is identified. For the assessment statistical tools, estimation techniques are used with an aim to understand the incident. Verification will enable the team in reviewing and correcting the analysis as reverting back to the analysis step is possible. This phase ensures flexibility in the model.

6) Phase Six: Presentation Phase

This phase involves admission of evidence and submission of reports. The assessment phase forms the basis for documenting and presenting the evidence to the authorities. It is pertinent to mention that the case must be presented so that it is easily grasped by the authorities and is supported with evidence in acceptable format. The presentation phase will indict or acquit the alleged party or criminal.

7) Phase Seven: Consolidation Phase

This phase involves proper closing of the investigation. The sub phase of this phase is Owner wherein the evidence collected is returned to the actual owner. Preparation of closure report, docketing of investigation process, Preparation of lesson learnt for evolving the evidence collection process in future cases, dissemination of relevant steps to other forensics labs so that the lesson can be used for updating investigation techniques.

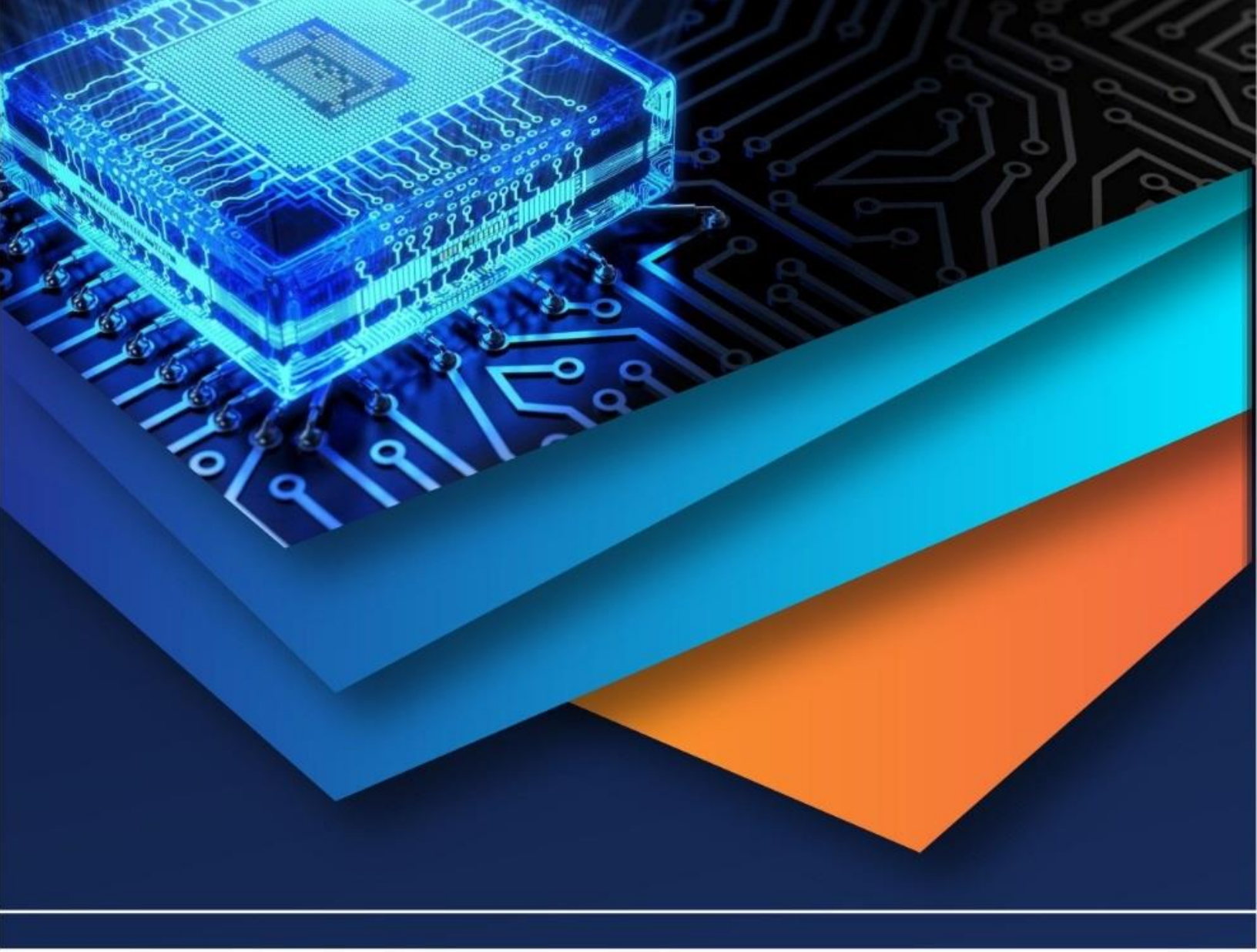
VII. CONCLUSION

The traditional frameworks, models, and tools used for evidence collection have evolved dramatically as a result of ever-changing exponential and transformational technologies to meet evidentiary requirements and the fundamental principles of evidence acquisition, as well as provisions for the preservation of the evidence's integrity. The models proposed in this paper are appropriate for data collection in the context of cutting-edge technologies and numerous multidisciplinary applications utilizing cloud computing and IoT. [8] With the rate at which internet usage and technology are growing, improvements to the models mentioned are both necessary and unavoidable.

Technological advancements in the cyber domain have increased by leaps and bounds, often blurring the boundary of legitimate and illegitimate use of the technology. Forensic evidence collection has always been challenging and has been more pronounced in recent times. This paper investigated the difficulties that forensic experts face when collecting digital evidence. The reliance on cloud service providers, openly accessible lines, and unprotected networks are creating more gaps in gathering evidence admissible in court. The realistic and achievable technical solutions enable investigators to collect evidence in a timely and intellectually valuable manner, taking into account the tangible and intangible value of the evidence; the integrity and storage of the collected evidence becomes the primary task to justify the technical, legal, and organizational readiness to handle cyber forensics and digital evidence collection methods in a more disciplined manner. The Advanced Intuitive Cybercrime Investigation Model (AICCIM) proposed in this paper presents an intuitive approach which can serve as an advanced investigation model so that the evidence gathering process remains immune to the latest technological advancements. The confidentiality, integrity, and authenticity of the evidence and data collected with the help of the model and flow discussed in the proposed model springs unique ways in building stronger evidence records to combat electronic crimes in the context of technologies such as cloud computing and IoT.

REFERENCES

[1] M. M. P. L. A. P. Michael G. Noblett, "Recovering and Examining Computer Forensic Evidence," [Online]. Available: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm.
[2] A. A. B. C. O. d. V. a. R. M. G. Mohay, Computer and Intrusion Forensics, Artech House, Boston, Massachusetts, 2003
[3] B. Hartwig (2022) [Online]. Available: https://itsupplychain.com/ai-cyber-forensics-how-does-ai-contribute-to-digital-forensics/.
[4] H. C. Jadhav (2022) "Artificial Intelligence in Digital Forensics" [Online]. Available: https://community.nasscom.in/communities/emerging-tech/ai/artificial-intelligence-in-digital-forensics.html.
[5] D. F. Mitchell (2022) "The Use of Artificial Intelligence in Digital Forensics: An Introduction," [Online]. Available: https://sas-space.sas.ac.uk/5533/1/1922-2707-1-SM.pdf.
[6] Hou, Jianwei & Li, Yuewei & Yu, Jingyang & Shi, Wenchang, "A Survey on Digital Forensics in Internet of Things," IEEE Internet of Things Journal, vol. 22, Sept. 2019.
[7] T. R. Sree, and S. M. S. Bhanu, "Data Collection Techniques for Forensic Investigation in Cloud", *Digital Forensic Science. London, United Kingdom: IntechOpen*, 2020.
[8] Kirmani, Mariya & Banday, M. Tariq. (2020). *Digital Forensics in the Context of the Internet of Things*, Cyber Warfare and Terrorism, pp.1178-1200, Jan. 2020.
[9] Bhagat, S.P., Meshram, B.B. (2022). "Digital Forensic Tools for Cloud Computing Environment," in *ICT with Intelligent Applications. Smart Innovation, Systems and Technologies*, vol 248. Springer, Singapore, Dec. 2021.
[10] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich, "A forensic acquisition and analysis system for IaaS," *Cluster Compute.*, vol. 19, no. 1, pp. 439 - 453, Mar. 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY