INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN(O): 2455-0620 [ Impact Factor: 7.581 ]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 9, Issue - 5, May - 2023 Publication Date: 10/05/2023

DOIs:10.2015/IJIRMF/202305011 --:-- Research Paper / Article / Review

# Corollary of digital forensics in e-governance

**Kritika**
Government of India, Delhi, India
Email – kritikaa2297@yahoo.com

***Abstract:*** *The augmenting rate of digital crimes in the contemporary era has coerced the desideratum of new fangled cyber forensic technologies. With the upgradation of technological resources from web 1.0 to web 3.0, from traditional cashing methods to manoeuvre of cryptocurrencies for transactions and the perception of e-office under Digital India Mission, thus enhancing the transparency of the government machinery has posed an extremity of cyber or digital forensics into e-governance. Cyber forensics is a requisition of inquiry and anatomy to convene and desiccate evidences from electronic devices. E-governance is the wielding of information and communication technologies in the administration of public entanglement. The paper focusses on the desideratum of the cyber or digital forensics in the occurrence of e-governance.*

***Keywords:*** *Digital forensics, E-governance, Digital attestation, Insider threats.*

## 1. INTRODUCTION:

The burgeon of the internetworking technologies has augmented various domains in varied fields of correlation to cyber security. One such domain is the domain of cyber forensics or digital forensics. Cyber forensics refers to the subpoena of bracketing, desiccating, perusing and according computerized denotation in a way that it is legit in the court of law[1]. It deals with the examination of what and how of the occurrence of the event. Cyber forensics is a terms which can deal with both criminal as well as undisclosed events. The area of examination concerns primarily with shielding of particulars, accession of particulars, envisioning, uprooting, cross-questioning, homogenization and promulgation.
The prima facie goal of the cyber or digital forensics is to discern computerized attestation for examination with the empirical methodology to come to the conclusion in its native form. The prominence of the domain is considerate in pronouncing the faults by an administrator and transposing perception anomaly with dynamic forensics.

The breaches attempted in the CIA triad i.e. confidentiality, integrity and availability of the cyber security domain often results in the roaring of digital forensics[2]. As per the Locard's exchange principle, in every misdemeanor, the malefactor will transmute the scenario of crime by upbringing some entity or abandoning some entity[3], leading to the establishment of LEAs i.e. Law Enforcement Agencies to tackle the cases leading to the forensics in well established and defined laboratories. The preliminary linchpin was investigating the unaided computer systems to recuperate expunged or demolished files from the hardware disks, but with the passage of time, extended to several other characteristics like imaging, analysing among others.

Since the perception of the conceptualization of e-office to boost transparency and empower trust of the natives has posed critical dangers on the covertness of the government data. The menaces can be internal or external. The internal menaces are most common and are often termed as insider threats[4] with the ability to escapade practical and viable susceptibilities. The connoisseur in governance can be expounded as a person who possesses: (a) *cognizance* of full unrolled entrance of systems in an organization with security deficit within the operations, (b) a *certitude person* of the government agency and (c) *paroxysm individual* with the possession of entire authorization of the security operations and systems entrance.

Insider threats can be recognized based on their activity analysis[5], cross examining of their access logs[6], and a precise intrusion detection system[7] and on the basis of suspicious activities performed using the organisation's networking protocols with location as prime identifier[8].

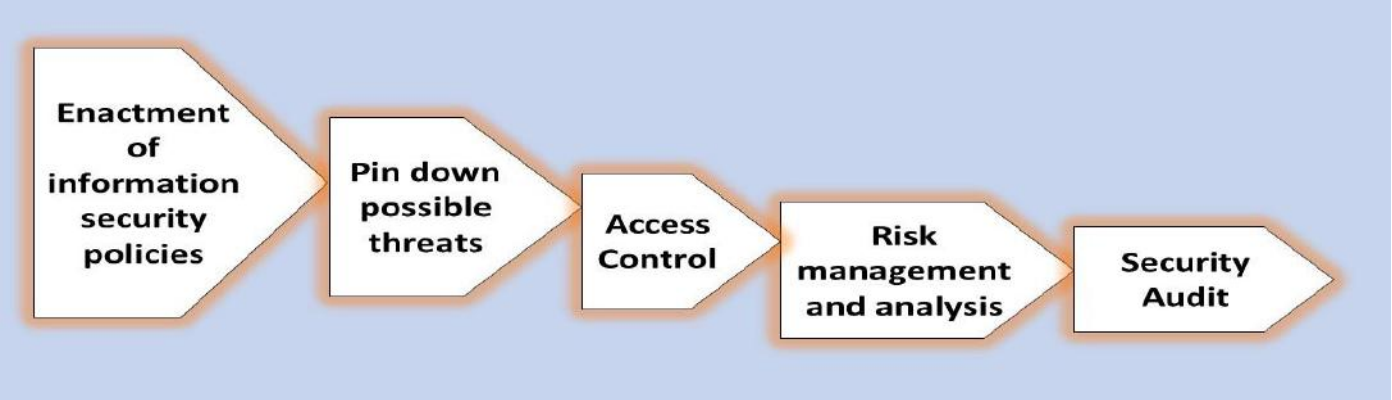


Fig 1: Insider Threat Detection

*Enactment of information security policies:*
The extant of the policies related to security of an organization is to be scrutinized and if found scarce, needs to be redesigned. The compliancy of security operation needs to be corroborated at the level of staff.

*Pin down possible threats:*
Probing of the mal-intended insiders' activity are enacted and recorded against the individual access mechanization of the security operations of the organization.

*Access control:*
Designating the role and responsibilities of each and every individual of the organization from entry to the highest level of operation.

*Risk management and analysis:*
The step encompasses succession of measures to be waged in an organization in order to fend off the event or acknowledge the eradication of risks.

*Security audit:*
The systematized summing up of security operations of an organization by quantifying the how well it is in accordance with entrenched set of criterion.

The recognisation methodology for threats related to insider vectors deals with three major mechanization. The first is *peculiarity* based which determines unanticipated disparities in the activities of the insiders of an organization from the normalcy. The second is the *endorsement* based where the individual system provides with the endorsement of the ancestral attacks. Lastly, the third one is the conglomeration of above two methodologies with the majority of the approaches believed to be on the first approach of detection.

One of the leading causes of the threat in an organization whether private or governmental depends on insider threat and more prominent in e-governance activities.

E-governance entails the tactical manoeuvre of information and communication technologies(ICT) to recast governance model presuming alliance between government machinery, natives and business entities along with other governmental agencies[9]. In the contemporary world, the manoeuvre of e-governance has shown colossal eventualities in the mutiny of the ever advancing world with profitable economic conditions through speedy service delivery mechanisms. In other terms, e-governance is an enterprise resource planning(ERP) [10] which holds communication between government and its natives including the business entities where there exists reciprocity and negotiations or proceedings among them.
There exists a need to establish sophisticated paradigm in the domain of e-governance is deliberated. A sophisticated paradigm by itself lays down an assemblage of comprehensive precept of development abilities of an organization with specified aims to be achieved. Depending upon the categorization of resource utilization, there exists four different categories.

Table 1: Categorisation of resource utilization

| S.No. | Resource Utilisation | Acronym |
|---|---|---|
| 1. | Government to Government | G2G |
| 2. | Government to Citizen | G2C |
| 3. | Government to Business | G2B |
| 4. | Government to Non-Profit | G2N |

*Government to Government*
The edifice of the Constitution of India lays down the federal architecture where the central, state and various district level organisations have to work hand in hand. Therefore, a sturdy intercommunication between the organs of the government at various levels for coherent functioning by minimizing the prolixity.

*Government to Citizen*
The prima facie objective of the resource utilization is coherent exchange of particulars between the government machinery and its natives by ensuring transparency in the service delivery mechanism at all levels of government and safeguard the citizens from the clutches of the corrupt third party alliances who by crooked means snatch the people of their valuables.

*Government to Business*
The prime objective of this resource utilization is the targeted service delivery to its citizens by eliminating the need of middle man and ensuring more transparency in public procedures and opening doors to small business entities like MSMEs to reach out to more and more of its population via government machinery by launching websites like local nation among others.

*Government to Non-Profit*
The exchange of particulars between government agencies and non profit organisations, social groups, NGO among others with the provision of funding and other resources facilities at doorstep availability. The digitalization of resource utilization should be sheltered, unshaken and effortlessly workable with the provision of examining of documents to be true and valid.

There exists variety of hindrances in the proper execution of e-governance such as:

(a) Lack of cooperation between various organs of governmental machinery which adds to the poor execution and distribution of resources available at hand.
(b) Existence of atypical processes between different governmental machinery.
(c) Technology at odds with the familiarity of citizens
(d) Lack of embracing issues by the natives

The Section II of the paper deals with the related work in the domain of digital forensics in e-governance though the information is limited to an extent. The Section III deals with the taxonomy of various digital forensics present and used especially while dealing with the conceptualization of e-governance in recent times. The Section IV inter-relates the core of this research study- digital forensics and e-governance. The Section V concludes the empirical work in a way to throw future aspects of the same.

## 2. LITERATURE REVIEW:

As stated earlier, with the augmentation of internetworking facilities, a need to boost the digital forensics especially in the government sector is essential. Kim et. al. in his literary work focused on the need to have an AI based digital forensics with respect to developing sustainable cities[15].

Chauhan R. in his literary threw light on the aspect of using reactive procedure for investigating and surveying the insider cyber threats and proposed the combined procedure of digital forensics along with anomaly detection to prevent the loss and avoid the occurrence of attack[4].

Beena et al. in the work highlighted the conceptualization of insider threat vectors and the challenges associated in dealing with them in respect to the information systems and highlighted the panacea which could be adopted in the emergent situations[5].

Javed et al. showcased the modern trailblazing on forensics of computer systems and the menaces in the research of the same with the potentiality of freely available as well as paid tools used for the investigation of the same[11] with the future intent on registry forensics while manoeuvring machine and deep learning.

Khanra et al. examined the vital dimensionality in regard to full-ledged machinery of the governance in relation to the existing modulations by patronaging the meta-ethnographic[9] perspective and also highlighted the issues related to security and privacy of data of various individuals.

Yuanfeng et al. propounded a framework in connection with nurturing, coping and refining particulars relevant in forensics at fastened rate keeping in place higher bandwidth requirements and costly transmission of data with anticipated policies[16].

Anand in his work highlighted the augmenting need of ICT in the domain of e-governance while highlighting the initiatives taken by the modern government machinery to bolster transparency, zero corruption, authenticity and coherence[10].

Arafat et al. in the research work proposed the essentiality of database forensics as well as highlighting the menaces in the forensics conducted in this domain and future scope by applying the methodology of semantic modelling and the establishment of warehouse for depot and recuperation of data[13].

M.I Cohen et al. has demonstrated far off, instantaneously and uninterrupted forensic analysis at corporate level with the help of freely available tools with mindboggling aftermath on retrenchment, monetary and efforts with the limitation of purloining the data of users from devices acting as a proctor[17].

Though the related work in relation to digital forensics in e-governance is limited and not much of the information is available at hand, this paper provides a comprehensive requirement and need of it by analysing the modern state of the art based on previously attempted works.

## 3. QUINTESSENCE OF DIGITAL FORENSICS:

*Computer forensics*
With the augmenting manoeuvre of electronic devices, the techniques and technologies prevalent in computer forensics to pin down, accumulate and preserve the attestation of data to recuperate the astray or destructed information present on the electronic devices.
The recuperated data involves:

(a) Erased files retrieval: It indulges with retrieval of the files that has been accidentally or intentionally erased from the electronic device in order to escapade the investigation scenario.
(b) Countermand steganography: The endeavor to conceal particulars inside the digital message or file is retrieved by specialists which examines the hashing functionality of original and the modified content on the system files.
(c) Juncture analysis: It deals with examining the particulars across varied systems with the help of planning interdependence and quoting of occurrences from one electronic device to another to ascertain peculiarities.
(d) Alive investigation: The investigation of non-permanent memory of the computer systems, RAM or cache memory.

There are various tools available with some open source and other licensed to investigate forensics analysis of electronic devices like Autopsy, FTK, OS Forensics, Magnet Axiom[11] among others.

*Network Forensics*
The process of regulating the provenance of castigation and preservation of attestation by dynamic surveillance and probing internetworking congestion that is highly non-permanent. The essentiality of the components comprises of switch, hub, firewall, router, among others. The process also permits the self defence electronic devices to inspect and fathom the causes and aftermath of an unfamiliar earlier confronted threat[12].

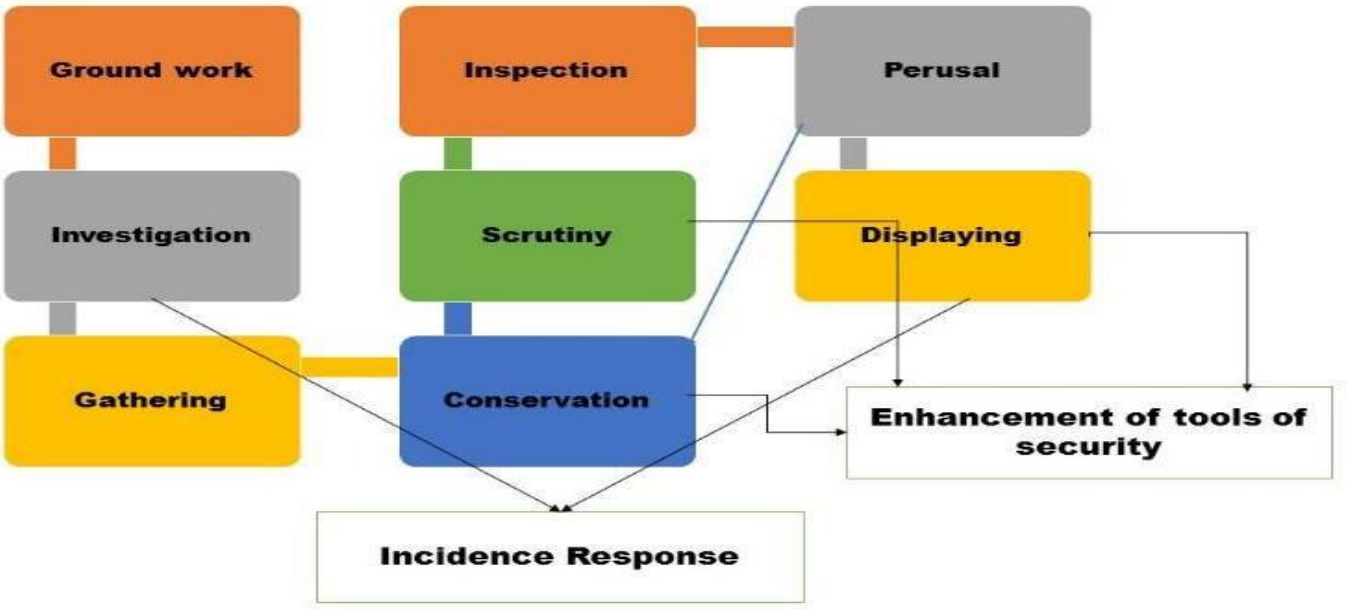


Fig 2: Subpoena modulation of network forensics

*Database Forensics*

To minimize obscurity in terminologies used in the process of digital forensics, it particularly obligatory to uniquely distinguish each and every terminology manoeuvred in the procedure to prevent lawsuit dereliction[13]. The forensics involved in the process of database deals with the conservation and investigation of concomitant and non concomitant databases which track downs the ancient venture, recuperate the erased data before hand and govern the earlier and former states of the particulars.

*Mobile Forensics*

The category of science with prima facie focus on recuperating of electronic attestation from devices such as mobile phones or smart phones[14] whose manoeuvring is most relevant in the Industry 4.0 though one of the tedious tasks involved in the procedure of forensics of mobile devices.

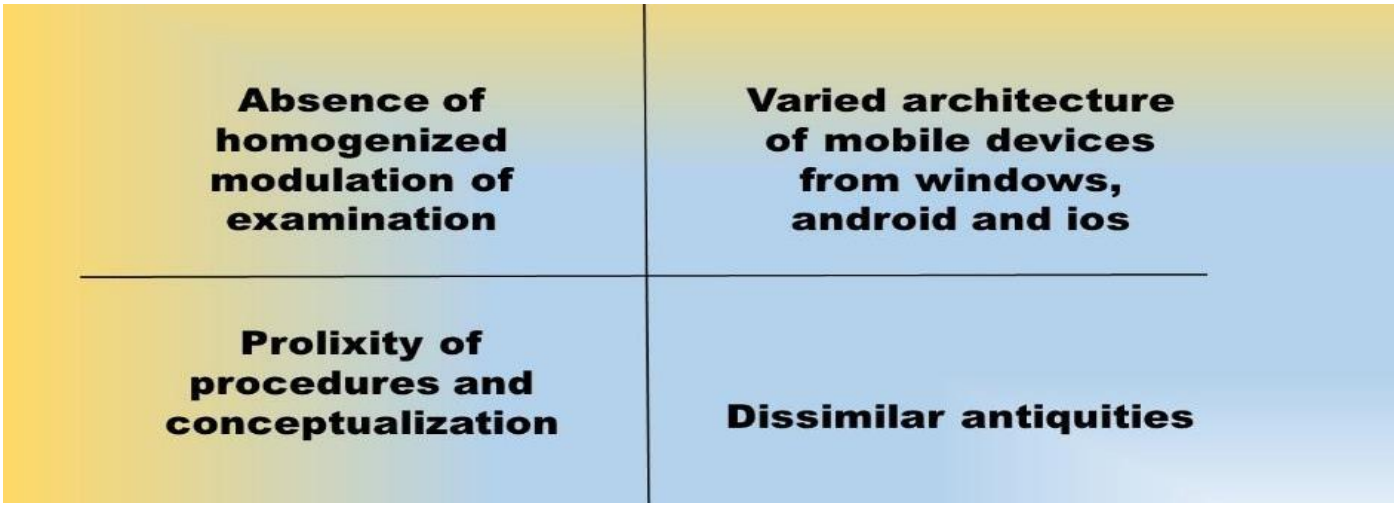


Fig 3: Challenges to mobile forensics

**4. DIGITAL FORENSICS AND E-GOVERNANCE :**

The terminology of digital forensics is not new. With the advent of new fangled technologies and the augmenting rate of cyber crimes, there exists a necessity of the domain of forensics in order to capture the psychology, recognize the

pattern of attack and recuperate the data lost during the threat attack without the requirement to pay any ransom and mitigate ways to prevent them in future.

Digital forensics plays a crucial role in introspecting the crime scene while gathering attestations and moving it carefully without damage to the forensics labs for further investigation and analysis. But there exists subcategorization of forensics which needs to be applied dynamically especially the network forensics to trace the activities of each and every member of the organization and prevent from any insider attack.

The digital forensics plays a vital role in the functioning and implementation of e-governance where government repository comprises of humongous particulars of its natives, externalities and neighbourhood. The applications created or the websites developed for the ease and transparency of working of government machinery needs to be protected 24/7 without fail. The failure can lead to huge loss of data and put the security of country at stake.

Network forensics is one of the domains of digital forensics which needs to be up to date, traced and restricted while dealing things at the national and international level. Though there has been use of VPN in many government organisations to safeguard their potentialities but, there still exists a risk as the service providers are limited and there is an absence of skilled workforce in regard to the ever advancing technologies.

Government of India or any other government holds a colossal sum of data from hospitality, to various license details, medical sector, defence among others which gets updated very often and needs to be safeguarded from the nefarious actors who off and on plan the cyber terrorism attacks on the nations.

There ways in which digital forensics can help in e-governance:

(a) Speedy perception of insider threat actors
(b) Quick recuperation of data lost during the attack
(c) Segregation of work with specialized persons in different domains to safeguard the machinery
(d) Establishment of concentrated infrastructure on digital forensics can improve the policy implementation and generate new opportunities for young mindset

The limitation of the digital forensics in e-governance:

(a) Absence of proper infrastructure facilities
(b) Lack of skilled personnel
(c) Secrecy in policy formulation and implementation among various ministries and departments
(d) Lack of guidelines for security framework to deal with newer threats

The domains of digital forensics, namely, network, computer and database forensics plays a crucial role in the investigation and prevention of attacks in government machinery and a need to develop more stringent tools and policy measures for coherence and ease.

## 5. CONCLUSION:

The work proposed throws light on the need to establish a well delineated and properly implemented infrastructure corresponding to the manoeuvre of digital forensics in e-governance or government machinery which acts a base for many modern organisations and businesses on national and international levels. Thus, a need to safeguard and protect the particulars of individuals along with the identification of threat actors whether internal or external is the need of the hour in the ever advancing technological developments and augmentation of cyber crimes and threats like cyber warfare, ransomware, phishing among others.

## 6. FUTURE SCOPE:

A well defined policy framework along with skilled manpower and well equipped infrastructure is the need of the hour and an indulgence of the professionals in the domain of digital forensics is desirous especially in developing countries like India whose ever growing data needs to be protected, maintained and recuperated without the slightest delay.

**ACKNOWLEDGEMENT**

I would like to thank my masters faculty for providing an insight into the topic of digital forensics and linking it with e-governance sector.

**REFERENCES:**

1. Saurabh, P., & Roy, A. J. K. (2021). Role of Cyber Forensics in Investigation of Cyber Crimes. *Issue 3 Int'l JL Mgmt. & Human.*, *4*, 786.
2. Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Abd Razak, S., Grispos, G., Choo, K. K. R., ... & Alsewari, A. A. (2021). Digital forensics subdomains: the state of the art and future directions. *IEEE Access*, *9*, 152476-152502.
3. Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., ... & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, *10*, 25464-25493.
4. Chauhan R., 2017. An architecture for detection and incidence response of insider cyber threats. *International Journal for Technological Research In Engineering Volume 4, Issue 5, January-2017* pp. 838-841.
5. B. A. L and D. H. K. S, "Information Security Insider Threats in Organizations and Mitigation Techniques," *2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC)*, Nagercoil, India, 2019, pp. 1-4
6. Chen, Y., Nyemba, S., & Malin, B. (2012). Detecting anomalous insiders in collaborative information systems. *IEEE transactions on dependable and secure computing*, *9*(3), 332-344.
7. Ray, D., & Bradford, P. (2007). An integrated system for insider threat detection. In *Advances in Digital Forensics III: IFIP International Conference on Digital Forensics, National Centre for Forensic Science, Orlando, Florida, January 28-January 31, 2007 3* (pp. 75-86). Springer New York.
8. Choi, S., & Zage, D. (2012, October). Addressing insider threat using "where you are" as fourth factor authentication. In *2012 IEEE International Carnahan Conference on Security Technology (ICCST)* (pp. 147-153). IEEE.
9. Khanra, S., & Joseph, R. P. (2019). E-governance maturity models: a meta-ethnographic study. *The International Technology Management Review*, *8*(1), 1-9.
10. Anand, D., & Khemchandani, V. (2019). Study of e-governance in India: a survey. *International Journal of Electronic Security and Digital Forensics*, *11*(2), 119-144.
11. Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*, *10*, 11065-11089.
12. Rizvi, S., Scanlon, M., Mcgibney, J., & Sheppard, J. (2022). Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions. *IEEE Access*, *10*, 110362-110384.
13. Al-Dhaqm, A., Abd Razak, S., Dampier, D. A., Choo, K. K. R., Siddique, K., Ikuesan, R. A., ... & Kebande, V. R. (2020). Categorization and organization of database forensic investigation processes. *IEEE Access*, *8*, 112846-112858.
14. Al-Dhaqm, A., Abd Razak, S., Ikuesan, R. A., Kebande, V. R., & Siddique, K. (2020). A review of mobile forensic investigation process models. *IEEE access*, *8*, 173359-173375.
15. Kim, S., Jo, W., Lee, J., & Shon, T. (2022). AI-enabled device digital forensics for smart cities. *The Journal of Supercomputing*, 1-16.
16. Wen, Y., Man, X., Le, K., & Shi, W. (2013, May). Forensics-as-a-service (faas): computer forensic workflow management and processing using cloud. In *The Fifth International Conferences on Pervasive Patterns and Applications* (pp. 1-7).
17. Cohen, M. I., Bilby, D., & Caronni, G. (2011). Distributed forensics and incident response in the enterprise. *digital investigation*, *8*, S101-S110.