Indian Journal of Forensic Medicine and Pathology
Volume 14 Number 2, April - June 2021 (Special Issue)
DOI: http://dx.doi.org/10.21088/ijfmp.0974.3383.14221.27

ORIGINAL ARTICLE

The Forensic Investigation of Cloud Computing Using Different Techniques: Challenges, Issues & Security Risks

Anjanee Kumar[1], Monika Chauhan[2], A K Jain[3]

Authors' Affiliations:
[1]Research Scholar, School of Basic and Applied Sciences, Galgotias University, Greater Noida 201310, Uttar Pradesh, India.

[2] Associate Professor, School of Basic and Applied Sciences Galgotias University, Greater Noida 201310, Uttar Pradesh, India.

[3] Dean & Professor, Schoolof Basic and Applied Sciences, Galgotias University, Greater Noida 201310, Uttar Pradesh, India.

Corresponding Author:
Monika Chauhan, Associate Professor, School of Basic and Applied Sciences, Galgotias University, Greater Noida 201310, Uttar Pradesh, India.

Email: *monika.chauhan@galgotiasuniversity.edu.in*

How to cite this article
Anjanee Kumar. The Forensic Investigation of Cloud Computing Using Different Techniques: Challenges, Issues & Security Risks. Indian J Forensic Med Pathol. 2021;14(2 Special):202-209.

ABSTRACT

Cloud computing is the most important and almost universally desired administration for all organisations because it allows organisations to exchange resources such as calculating, stocking, and programming units while also ensuring ease of use and management of virtualization technologies. Viva supports the internet. Comfort, mobility, stability, adaptability, speed, tremendous bandwidth limits, availability, and on-demand network access are just a few of the major benefits of cloud computing. The flexibility of options for cloud computing solutions has made it impossible for hackers to seek successful and pervasive future surveillance and security openings as emerging innovation. This paper examines cloud crime scene investigation research in order to include potential options, including questions and challenges, as well as several recommendations for overcoming these challenges.

KEYWORDS | cyber security, cloud computing, digital forensic, phishing

INTRODUCTION

In recent years, there has been a significant increase in the number of formal & informal online organizations, such as Facebook, Twitter, MySpace, and Friendster, which function with high levels of client personalization and client intercommunication. Online informal organizations, which can be described as cloud-based electronic administrations, which will allow each and every individual in a restricted context to create a public or semi-public identity, clarifying many clients they share with. Do, see, and overcome their relationships and the people they make. Some items inside the cloud-based structure.[1]

Sudden growth of the World Wide Web and disconnected clients with many gadgets are moving towards cloud computing for customer support. Along the main path in innovation there are potential threats to the client's data and if any attack is made by cyber criminals on the cloud, it calls for researching the cloud in light of an incredibly huge size. The most vexing difficulties to manage the diverse current liability on the classification of information received in different areas would be the issue of obtaining confirmation from the clouds and the capture of actual evidence for a coordinated effort of approval or proof of computerized crime. Does. Visual investigation in distributed computing starts from there. Cyber crime is a

fascinating field to examine non-ethical practices being used in the cloud. This happens with different types if examination and evaluation on a wide range of data on distributed computing. Completed in this area.[12]

Increasing cyberattacks and many offenses in the increasingly complex multi-legal and multi-local cloud world mean that the implementation of investigative processes in the cloud is urgently needed.[13]

METHOD & MATERIALS

The term "cloud" is being bandied around everywhere these days. This mysterious word seems to include almost every aspect of our lives. Although "the cloud" is merely a metaphor for the internet, cloud computing is a hot topic of conversation these days. It improves data collection, security, flexibility, and employee teamwork, as well as changing the workflow of small and large companies to help them make smarter choices while lowering costs.[14,15,16]

It is undeniable that cloud computing is becoming increasingly popular. The role and deployment of the cloud in companies like Alibaba, Amazon, Google, and Microsoft has already been predicted in our market intelligence trends report.

The cloud's importance is growing at an exponential rate. According to Gartner, the cloud computing industry grew to 17.3% in 2019 (US$206.2 billion), with 90% of the companies adopting cloud services by 2022.

Cloud Computing

The distribution of numerous hardware and software resources over the internet through a network of remote servers is referred to as cloud computing. These remote servers are collecting, handling, and processing information that allows users to extend or update their current networks.

The cloud's strengths and scope are immense. To further identify usage cases, the IT industry divided it into three groups.

a) Software as a Service (SaaS) – one or more vendors own, distribute, and operate software remotely. To begin, Software-as-a-Service, or SaaS, is a widely used method of obtaining and paying for software. Rather than downloading software on your own computers, SaaS companies allow you to rent software that is hosted, usually for a monthly or annual subscription fee. SaaS business intelligence and technology is being used by an increasing number of CRM, communications, and finance-related resources, and even Adobe's Creative Suite has followed the concept.

b) Infrastructure as a Service (IaaS) – operators own and host computing services, as well as storage and networking facilities, and make them accessible to consumers on request.

c) Platform as a Service (PaaS) is a term that refers to a group of providers that provide platform infrastructure (middleware). Application platform, automation, enterprise process management, and storage services are among these services.

Cloud Forensics

Cloud legal science or cloud forensics can be characterized as the use of advanced criminology in distributed computing for investigating crimes. Distributed computing is advantageous to the extent that it is making the legal local area so concerned about customer data. Adaptation of the cloud occurs at a certain point, information from different sources may include similar areas inside the capacity media that makes a commonality during e-disclosure, while an organization is being investigated; the expert unknowingly distributes the remaining information to another organization. The development of capacity limits in distributed computing is a hindrance to advanced criminology because more legal information and extra time will be used to examine the information, obviously, if nothing turns out badly. Traditional computerized criminology techniques (e.g., encoding) have different inadequacies and inefficiencies in distributed computing, in such a way that it is important to find out about advanced legal science information and set assessment in distributed computing to create fruitful pathways in distributed computing.

Towards declining cloud security opportunities

Distributed computing is another model and the computerized crime scene investigation local area is yet to investigate what inconvenience this new time innovation is. Countless creators of this sort expressed potential experienced troubles during the time spent maintaining a series of coherence.[5,6,7]

In any event, driving associations have not yet introduced a set of ideas or can be made to follow a definite arrangement of instructions when the most efficient method for moving the cloud across the associations is in the cloud or on the rules. A safety accident occurs inside. Many times, distributed computing and computing enabled to help network exams in their online exams for misdeeds. Lawbreakers can manipulate efficient free interchange frameworks, for example, Tor and Anonimizer which were initially shown to secure network client structure personalities criminals and delineations. In this manner, the law requires that many Amazon EC2 VMs be purchased, using the Tor network as a watchdog that can skip routes to the Tor circuit and leave the hub and attack inside the fitting. May examine sources [8]. Amazon Web Administration (AWS) is a more realistic model that can provide MD5 of every document that is on the framework, so when a bit of duplicate is being created, Microsoft continues to include the metadata record. Ease of use in the office, email store and careful reinforcement.

Related Work

Frank Y.W. Law et al.[4] has suggested a data-protection solution that is irrelevant with cryptographic aid to the investigative situation. The research begins with some insight into the situation, some keywords in the text base case may be. The suggested solution enables investigators to use approved keywords to scan for encrypted records. For an email server, the device is tested consisting containing 120 GB of 100,000 emails of which 600 words are used for all emails. Among all the addresses, 25% contain protection, and 25% contain both security and forensics, while 25% contain security. In order to create an index register, the system took 3536.984 seconds and calculated trapdoors took 0.25 seconds. To search through the whole emails and return the index file name which contains the text, protection or forensic, took 1705.672 seconds.

In the year of 2011, Ruan et al.[2] In the United Arab Emirates, a paper was distributed among advanced legal experts and experts around the world proposing another definition for the cloud exam in view of a review directive, facilitated by Zayed University. The review was planning to show a better understanding of some ideas, for example, cloud legal science definitions, difficult issues, most urgent investigative titles, and basic measures for cloud exam ability. In view of Ruan et al., By definition, cloud legal science is a cross layer between computerized distributed computing and advanced digital mis-examination. Additionally, it is a subset of the organization's wrongdoing experts that manage measurable examinations in any type of organizations, with current existing methods tailored for the distributed computing climate. Cloud Criminology can be extended into three components of special, authoritative and valid measurements.

Advantages	Disadvantages
Low or no cost infrastructure	Requires High speed internet connection.
Least administration cost	Downtime or stoppage time
No management hassles	Partial control of infrastructure
Very easy accessibility	Restricted or limited flexibility
Pay per use	Ongoing more costly
Better reliability	Security & security breaches issues
Data control	Vendor lock- in
Easier Data backup and recovery	Technical related Issues
Massive cloud storage available	Not available

Table 1 Advantages and Disadvantages of Cloud Computing

CONCLUSION

Advantages of Cloud Computing

1. *Low or no charge on infrastructure:* Distributed cloud-based computing that are separated into the three most popular significant classifications according to the administrations: Infrastructure as a Services (IaaS), Platform as a Services (PaaS) and Software as a Services (SaaS).

Each and every one of these classes, one thing that is normal that you don't have to put resources into equipment or any foundation. When all is said in done, each association needs to spend a ton on their IT foundation to set up and enlist a particular group.

Workers, network gadgets, ISP associations, stockpiling, and programming – these are the significant things on which you need to contribute on the off chance that we talk about broad IT framework. Yet, on the off chance

 copyright © 2021 red flower publications pvt. ltd

that you move to distributed computing administrations, you don't have to put resources into these. You just go to a cloud administrations supplier and purchase a cloud administration.[8]

2. *Minutest management and cost:* By selecting the cloud-based services, you must be saved the cost in multiple points of ways:
3. *Least administration cost:* You don't want to claim the foundation, you don't spend anything on its administration of the organization or staff to oversee it.

Cloud chips away at pay more only as costs arise model, so you spend just on assets of resources that you need. That's it!

At the point when you select the cloud-based services, the administration of its foundation is the sole obligation, commitment of the cloud service provider and none of the client or cloud-based customer.

4. *No managerial or management hassles:* At whatever point there is a buy or up-degree of equipment, a ton of time is squandered searching for best sellers, welcoming citations, arranging rates, taking endorsements, creating POs and sitting tight for conveyance and afterward in setting up the framework.

This entire interaction incorporates loads of authoritative/administrative errands that burn through a ton of time.

With cloud administrations, you simply need to look at the best cloud specialist co-ops and their arrangements and purchase from the one that coordinates with your necessities. Furthermore, this entire interaction doesn't take a lot of time and saves you a great deal of endeavors. Your framework support undertakings are additionally disposed of in the cloud.

5. *Easier Accessibility and pay-per-use:* Cloud assets are effectively open from around the globe – whenever, anyplace and from any gadget and you have total admittance to your assets.

This determines the charging as well - you only pay for what you need and how much you need. It seems like a phone bill or a fuel bill. However, like other IT foundations, the entire amount is spent all at once, and it is exceedingly rare if such funds are invested optimally, resulting in the investment being squandered.[17]

6. *Better Reliability:* Your foundation in the cloud expands the unwavering quality and accessibility of utilizations and administrations. Cloud administrations run on pooled and repetitive foundation which furnishes you with a higher accessibility of IT administrations.
7. *Data Control:* Another essential benefit of the cloud is that it concentrates all the information from different ventures and branch workplaces to a solitary area. You oversee the information without visiting singular spots for checking the data.
8. *Easier Data back-up & Recovery:* Loss of information can fundamentally affect your business. You may lose basic data which can cost you an immense amount of cash, burn through your important time and damage your coroprate image.

To forestall it, you can consequently reinforcement all the information to the cloud consistently. This assists you with recuperating any information in the event of unintentional erasure, misfortune in view of regular catastrophe or if the hard drive crashes.[18]

9. *Found Massive cloud storage:* Most cloud platforms give you a free, secure and enormous storage to store all your data.

Albeit most distributed storage administrations like OneDrive offer you a decent measure of free stockpiling, on the off chance that you use everything, you can generally go for purchasing safer capacity in the cloud.

10. *Automatic software updates for security purposes:* Refreshing a framework once in a while can be a disappointing undertaking for endeavors. The IT office needs to refresh the framework for each person which sits around idly as well as influences efficiency. Yet, in the event that you are utilizing cloud-based applications, they will get naturally refreshed, with no contribution from the clients.

Subsequent to examining the advantages of distributed computing, how about we currently examine a few burdens of distributed computing.[8]

Disadvantages of Cloud Computing

1. Required High-speed internet connection:

To get to your cloud administrations, you need to

have a decent web association consistently with great data transmission to transfer or download documents to/from the cloud

2. Downtime: Since the cloud requires high web speed and great transmission capacity, there is consistently a chance of administration blackout, which can bring about business vacation. Today, no business can bear the cost of income or business misfortune because of vacation or delayed down from a break in basic business measures.

3. Partial control of infrastructure: Since you are not the proprietor of the framework of the cloud, thus you don't have any control or have restricted admittance to the cloud infra.

4. Restricted or limited flexibility: The cloud gives an immense rundown of administrations, however devouring them accompanies a ton of limitations and restricted adaptability for your applications or advancements. Additionally, stage reliance or 'merchant lock-in' can now and then make it hard for you to relocate starting with one supplier then onto the next.

5. Ongoing more costly: Despite the fact that you save your expense of expenditure on entire framework and its administration, on the cloud, you need to continue to pay for administrations as long as you use them. In any case, in customary strategies, you just need to contribute once.

6. Security & security breaches issues: Everyone is concerned about information security. Since the public cloud is built on the internet, the data can become powerless.

Since it is a public cloud, it is up to the cloud provider to handle the data. As a result, before settling on cloud administrations, it is critical that you locate a provider who adheres to the most stringent information management strategies.

For full cloud protection, one must choose a much more expensive private cloud option or the crossover cloud solution, in which nonexclusive information can be stored on the public cloud and business-basic information is kept on the secret cloud.

7. Vendor Lock-in: It's better to sign a cloud computing contract than it is to break one. When switching suppliers is either prohibitively costly or impossible, "vendor lock-in" occurs. It's possible that the offering isn't standard or that there aren't any suitable vendor alternatives.[12]

It all boils down to prudence on the part of the consumer. Ensure that the services you use are standard and transferable to other suppliers, and that you are aware of the standards.[13]

While you are guaranteed to be able to turn to a specialized cooperative at some other point in time in cloud organizations, it is an extremely troubling interaction.

You may believe that moving all of the cloud administrations, beginning with one expert co-op and progressing to the next, is difficult. Similarity, interoperability, and backing issues can arise during the relocation process. To avoid these problems, often customers opt not to switch sellers.

8. Technical related issues: If you're a computer prodigy or not, specialized challenges will arise, and they can't all be resolved in-house. To avoid interfering with your work, you should seek assistance from your specialist co-op. In any case, only one out of every odd retailer provides day-to-day assistance to their clients, although emerging service providers are unable to do so.[8]

RESULT & DISCUSSION

In January 2018, RighScale published its annual report on emerging cloud dynamics. They polled 997 technology leaders from a wide variety of companies on their cloud computing practices. Their findings were eye-opening, especially in light of today's cloud computing challenges. To answer the main question on the challenges of cloud infrastructure, we've expanded on some of their findings and introduced additional cloud computing topics that businesses will need to address further down.

In terms of forensic science, we will not able to map entire events in traditional forensic cloud-based computing environments, any of which are mentioned below:

i) The majority of problems encountered during a criminological review of the cloud are a lack of customer data during the preparation period for a variety of reasons, such as worker closure, which can conflict with equivalent or random administrations.

ii) Not simple to get to all organize switches, network-based router, load balancers and other

 copyright © 2021 red flower publications pvt. ltd

systems administration gadgets.

iii) Access to a massive firewall is denied.

iv) Imaging challenges that bounce from one to the next but remain constant across cloud steering plans.

v) The issue was discovered through a log analysis of cloud apps.

vi) Log reinforcement and bendability.

vii) Log data access is limited.

viii) Assaulting Velocity is higher.

ix) At the time of the investigation, malicious hubs are present.

x) Clients will cancel or hide the majority of information.

xi) Hypervisor-level of research. Experts conducted a classification of research, for example, Lu *et al.,* to discuss the challenges of cloud-based distributed computing. In distributed computing, it was suggested that a stable installation be developed and managed to devise and monitor the history of knowledge properties. He stated that the secure starting point should address the two states' impossibility and protection issues, and then suggested a fair specification based on bilinear pairs after using the security technique to ensure their personal safety in the standard model.

Despite the suggested stable root plot computing being acknowledged as proof in the knowledge question, it was argued that the inquiry was conducted hypothetically and that there is no evidence that the administration and conscious models are distinct. Worked in conjunction with [6]

Digital Forensics Investigation Procedures

The event entails a series of tools and processes for remotely investigating the process of crimes in a cloud computing environment, with the following main aspects:

Figure 1 Digital forensic investigation: the process after the attack

Diagnosis Determine whether an unlawful act or indeed fraudulent activity is involved in IT based programs. These actions can include complaints submitted by an individual, irregularities noticed by IDS, tracking and profiling as a result of audit trail, and unusual events in a cloud. The use of deployment models (i.e., private, public, community and hybrid), the type of cloud resources (i.e., SaaS, Paas and IaaS) and the geographic region chosen for deployment.[10]

Clues Identification

The cloud as a concept has been shared as proof of finding possible validation wells, which is almost a concern. In this part, we'll look at the problems that the examinee can see at this point in more detail. The main problem in the Proof ID process is the log entry for validation. The testing framework is a piece of status and log record validation that isn't particularly noteworthy in SaaS and PaaS since the client's access is entirely restricted to the API or preplanned interface. Since it returns a virtual machine that behaves like a real machine, this is suitable for the IaaS cloud model.

Forensic Collection of Data

It is either the source-side or purpose-side to obtain, characterize, remove, and retrieve information about antiquities from other potential wells of information from the cloud. Due to the diverse cloud benefits and sent models, obligations begin with a help or conveyance model, then on the next in the cloud along these lines, requiring different tools and methods.

Preservation of Data

In a criminal investigation, proof is a confirmation of a crime, and no offence may use it to attach testimony. It is possible to assure the user that his or her recognition was taken and abused from someone in situations enabling evidence that the client is concerned in unethical activities. This is unlikely to refute the situation since the client will automatically and individually associate with the cloud.

Analysis of Data

The knowledge test is another crucial stage in a mediocre exam; in fact, in a PC science review, it necessitates a more sensitive assessment when the volume and quantity of objects to be tested is increased. It may also be referred to as a catastrophe

in distributed computing because the concept of distributed computing entails the utilisation of a vast number of properties with a reasonable chance of validation. This is a different viewpoint on cloud observable examination, owing to the difficulty of processing and distinguishing large amounts of data.

Reconstruction

The information recreation process of the science investigation yields a variety of dissect findings. As a characteristic of knowledge collection steps, computerised science practices are of concern for the era of brief inquiry to reliably replicate the non-moral demonstration. Because of the different ideas of distributed computation, which involve exploiting and distributing properties, any piece of misconduct could have arisen in a better position in distributed computing; this creates a problem that interferes with the era of the transitory test.

Reporting and Presentation

The final stage in scientific agents' trials entails selecting the appropriate court for the case's declaration. It is not difficult to select the court in a general PC criminal examination, and the matter will be taken to court in the country where the crime was wrongfully committed; however, it is totally muddled due to the virtue of distributed computing in accumulated networks, and especially in distributed computing.

It is not certain where the wrongdoing has been done and where the confirmation is actually located as cloud assets are usually split between different customers in many countries. This clearly enables the examinee to choose where and how the suit should be used in the overall set of laws.

CONCLUSION

Currently, there are no complete cloud-specific forensic solutions on the market. Despite this, forensic analysts continue to use existing technologies to collect data from the Cloud.

Stacks of wishes for organizations and organizations with issues of distributed computing and restricted processing assets with the beautiful proposition of PCs as administration. As the generality of cloud processing increases, digital faults associated with the cloud or direct tilt of the cloud are noted. In this paper, we examined and dissected the inconveniences and difficulties observed by computerized criminology experts when they were experiencing non-ethical practices related to the cloud and presented our ideas about cloud legal sciences, including most of the exam items, the discovery of the cycle and its requirements were included, and the final proposition 3 is the fundamental crime potential that agents must measure.

My future work will focus on developing the nonstop enhancement inspection methodology for cloud-related digital missteps, proposing a cloud legal science paradigm, and demonstrating policy and models using some of the cases that we've encountered. IJFMP

Acknowledgement:

The author would like to express his gratitude to the authority of Division of Forensic Science and School of Basic and Applied Sciencies, Galgotias University, Greater Noida, UP., India, for giving him an opportunity to work on this project.

Conflict of Interest:

The author declares there is no conflict of interest in this project.

Source of Funding:

The author declares that there is no funding for this project.

REFERENCES

1. ***D. M. Boyd and N. B. Ellison,*** *"Social Network Sites: Definition, History, and Scholarship," vol. 13, no. 1, pp. 210-230, 2008.*
2. ***Angus McKenzie Marshall.*** *Digital Forensics: Digital Evidence in Criminal Investigations. John Wiley, 2009.*
3. ***M Reith, C. Carr, G Gunsch.*** *An Examination of Digital Forensic Models. International Journal of Digital Evidence, 2002.*
4. ***Brian Carrier.*** *Defining Digital Forensic Examination and Analysis Tools. Digital Research Workshop II, 2002.*
5. ***Yiu S. Chow K. Kwan M. Tse H. Law F., et al.*** *" Protecting digital data privacy in computer forensic examination. Technical report".*
6. ***Eoghan Casey.*** *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press,2011.*
7. ***No author listed.*** *Bangor University. 2021. Bangor University. [online] Available forensic investigation at:<https://www.bangor.ac.uk/> [Accessed 12 May 2021].*
8. ***No author listed.*** *Wikipedia. Digital Forensics July 2021. http://en.wikipedia.org/wiki/Digital/forensics.*
9. ***Maricela-Georgiana Avram*** */ Procedia Technology 12 (2014) 529 – 534*
10. ***Jyotsna Gupta,*** *what are the pros and cons of cloud computing? ZNetLive Blog - A Guide to Domains, Web Hosting & Cloud Computing https://www.znetlive.com/blog/pros-and-cons-of-cloud-computing/*

 copyright © 2021 red flower publications pvt. ltd

REFERENCES

11. ***Shivam, K. (2020, April 11).*** *https://kumarshivam-66534.medium.com/cloud-forensics-be18e14230de*
12. ***Zargari, Shahrzad, and David Benford.*** *"Cloud Forensics: Concepts, Issues, and Challenges." 2012 Third International Conference on Emerging Intelligent Data and Web Technologies, 2012, doi:10.1109/eidwt.2012.44.*
13. ***Birk, D. and C. Wegener.*** *Technical issues of forensic investigations in cloud computing environments. in Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on. 2011. IEEE.*
14. ***Ruan, K., et al.*** *Key Terms for Service Level Agreements to Support Cloud Forensics. in IFIP Int. Conf. Digital Forensics. 2012. Springer.*
15. ***Martini, B. and K.-K.R. Choo,*** *An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 2012. 9(2): p. 71-80.*
16. ***Nasreldin, M.M., et al.,*** *Digital Forensics Evidence Acquisition and Chain of Custody in Cloud Computing. International Journal of Computer Science Issues (IJCSI), 2015. 12(1): p. 153.*
17. ***Pichan, A., M. Lazarescu, and S.T. Soh,*** *Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation, 2015. 13: p. 38-57.*
18. ***Palmer, G.,*** *A Road Map for Digital Forensic Research: Report from the First Digital Forensic Workshop, 7–8 August 2001. DFRWS Technical Report DTR-T001-01, 2001.*
19. ***McKemmish, R.,*** *What is forensic computing? 1999: Australian Institute of Criminology Canberra.*
20. ***Kruse II, W.G. and J.G. Heiser,*** *Computer forensics: incident response essentials. 2001: Pearson Education.*
21. ***Ahmed Alenezi, Nurul H N Zulkipli,*** *Hany F Atlam, Robert J Walters, and Gary B Wills. 2017. The Impact of Cloud Forensic Readiness on Security. 7th Int. Conf. Cloud Comput. Serv. Sci. Closer (2017), 511–517. DOI:https://doi.org/10.5220/0006332705390545*
22. ***M. Edington Alex and R. Kishore.*** *2017. Forensics framework for cloud computing. Comput. Electr. Eng. 60, (2017), 193–205. DOI:https://doi.org/10.1016/j.compeleceng.2017.02.006.*
23. ***Pranay Chauhan and Pratosh Bansal.*** *2017. Emphasizing on Various Security Issues in Cloud Forensic Framework. Indian J. Sci. Technol. 10, 18 (2017), 1–7. DOI:https://doi.org/10.17485/ijst/2017/v10i18/112116.*
24. ***Suchana Datta. 2016.*** *Review on Cloud Forensics : An Open Discussion on Challenges and Capabilities. 145, 1 (2016), 1–8.*
25. ***Muhammad Irfan, Haider Abbas,*** *Yunchuan Sun, Anam Sajid, and Maruf Pasha. 2016. A framework for cloud forensics evidence collection and analysis using security information and event management. (2016). DOI:https://doi.org/10.1002/sec.*
26. ***Suleman Khan, Ejaz Ahmad,*** *Muhammad Shiraz, Abdullah Gani, Ainuddin Wahid Abdul Wahab, and Mustapha Aminu Bagiwa. 2014. Forensic challenges in mobile cloud computing. 2014 Int. Conf. Comput. Commun. Control.*