Cloud Forensics: Threat Assessment and Proposed Mitigations

Abstract. Cloud Computing is a broad but ambiguous term that can refer to a variety of dynamically allocated services. Cloud Computing may be viewed as a two-edged sword in terms of law enforcement and forensic inquiry. On the one hand, acquiring digital evidence from cloud sources may present difficult technological and inter-jurisdictional legal challenges. Using cloud storage and processing capabilities, on the other hand, can help to speed up the forensics process and focus the investigation on significant evidence earlier in the investigation. It is possible that traditional evidence gathering and recovery methods may no longer be relevant in the cloud due to the dispersed nature of data processing. Because of the dynamic genre of Cloud Computing, digital forensics has had to deal with new issues. Throughout this article, the foundations of Cloud Computing architecture will be discussed in depth. As well as that, we give thorough research of forensic threats in Cloud Computing and provide viable solutions.

Keywords: Cloud Computing, Cloud Forensics, Threats, Possible Mitigations, Digital Investigations.

1 Introduction

1.1 Cloud Computing

Computing in the cloud refers to the continuous availability of computer system resources in certain specified data storage and processing ability, without any client having direct effective participation. There are a variety of meanings attached to the word for many people who enjoy looking for information in the cloud. Easy to reconfigure, the shared array of efficient resources on the network may be rearranged in a straightforward manner [1]. Payment-per-use (PPP) is how the cloud works. Users make requests for services they require, and service providers respond to those requests. Multiple users can share the same instance of software in the cloud thanks to multi-tenancy. Elasticity is another essential aspect of the cloud that allows for the scaling of resources up and down based on demand. All of the characteristics described above are targeted at improving cloud services.

Concerns have been expressed about data privacy and security if sensitive company data is outsourced to the cloud. The most essential pillar for every respectable business is its security policies, and applying them across virtual cloud environments is a difficult challenge. The unidentified physical location of the organization's assets complicates matters even further. If a security breach occurs, the corporate security team wants to be able to conduct its own investigation without the aid of a third party. However, in the cloud, this is no longer possible: all sources of evidence are controlled by the Cloud Service Provider (CSP), as the CSP has complete control over the environment. In the best-case situation, a trustworthy third party acts as a trustee and ensures the CSP's trustworthiness.

The National Institute of Standards and Technology has developed five key Cloud Computing characteristics: “on-demand self-service, broad network access, resource pooling, rapid flexibility or growth, and measured service.” Others characterized Cloud Computing as being dynamic and easily extensible to deliver virtualized resources to clients via the Internet. Users do not need to know the physical characteristics of the cloud.

1.2 Cloud Forensics

Cloud forensics refers to a multidisciplinary approach to Cloud Computing and digital forensics. It is, without a doubt, separate from standard forensic PCs. It is a subfield of network forensics that deals with forensic investigators on any type of public or private network. Companies are embracing cloud computing, but they are concerned about compliance and the rising number of cybercrimes committed in cloud settings. Using cloud-based architecture, detectives must carry out digital forensic-style investigations to assess, preserve, gather, and find all evidence so it may be handled correctly in a jurisdiction. This method of identifying, storing, collecting, and analyzing all evidence information is commonly referred to as cloud forensics [11].

The capacity of cloud forensic investigators to perform an investigation is mostly determined by the methodology and tools used to extract useful digital evidence from a system. The digital forensic procedures and frameworks used today to conduct digital investigations are incapable of meeting the cloud environment's criteria and expectations for contemporary innovation. This is because computer technology is always evolving, and forensic technology appears to be falling behind.

To combat digital crimes, law enforcement has turned to cloud forensics. These difficulties include accessing numerous copies of stored data and tracing evidence across various countries, as well as the reliability of the evidence, ownership of the evidence, and most crucially, preserving chain-of-custody during the whole inquiry.

Within this paper, the focus will be mainly on the threats placed in the era of cloud forensics and their different types along with possible solutions.

2 Background Theory

2.1 Cloud Computing Architecture

People use the Internet to gain access to cloud-based apps, storage, and services. The cloud may be accessed by any device that is linked to the Internet, such as computers, tablets, mobile phones, and so on. Users can obtain cloud services from cloud service providers. Depending on the user, cloud services can be classified into a variety of categories. Major service delivery models are SaaS, PaaS, and IaaS.

Software as a Service (SaaS). Third party providers host software or applications and allow customers to use them on a demand basis, in this form of Cloud Computing.

Platform as a service (PaaS). According to this concept, it gives users with a platform and an environment in which to create their own apps or service.

Infrastructure as a service (IaaS). They give you with a virtualized computing machine and help you save money on server and data-center purchases.

Lately, in Cloud Community, there are four cloud deployment models:

Private Cloud. Cloud infrastructure is controlled by the business or a third party and operates entirely within a single organization, whether on-premises or off-premises. A company may be motivated to establish a private cloud for a variety of reasons. These characteristics are explored in the following order: The priority is to maximize and optimize the usage of current in-house resources. Furthermore, Private Cloud businesses include characteristics such as data security, data privacy, and trust, making them an appealing alternative. Third, even now, the cost of transferring data from a local IT infrastructure to a Public Cloud might be prohibitively high. Fourth, corporations always seek total control over key operations that take place outside of their own country. Researchers and teachers often use private clouds for research and teaching.

Community Cloud. Businesses collaborate to create a cloud infrastructure that is compatible with their demands and laws as well as their goals and concerns. A degree of economic scalability and democratic balance exists in the cloud community. One of the community's organizations, or a third party supplier, may host the cloud infrastructure.

Public Cloud. Essentially, this is a better version of the current Cloud Computing deployment model. People utilize the public cloud, and CSPs have total control over it, with their own policies, value and profit models, pricing, and invoicing. Force.com, Google App Engine, and Amazon S3, EC2 are just a few examples of public clouds.

Hybrid Cloud. There are numerous clouds (private, communal, or public) in this cloud architecture that remain independent entities but are linked by proprietary technology that enables data and application mobility (e.g., cloud bursting for load-balancing between clouds). Associations, for example, might use the hybrid cloud model to restructure their fundamental capabilities by transferring peripheral business tasks to the cloud while maintaining control over vital activities on-premises via the private cloud.

The essential components of cloud architecture are as follows:

Virtualization. Cloud Computing is based on the virtualization of servers, storage, and networks. This layer allows several applications to seamlessly use the same physical resources, increasing the efficiency of servers, storage, and networking throughout the organization.

Infrastructure. There are, in fact, actual servers. All of the traditional data center components, such as servers, persistent storage, and networking equipment such as switches and routers, are included in the cloud infrastructure.

Middleware. As in traditional data centers, networked components, applications, and software may connect with one another thanks to software components such as databases and communications applications.

Management. These technologies allow for continuous monitoring of the performance and capacity of a cloud environment. From a single console, tracking the usage, deploying new apps, integrating data, and ensuring disaster recovery can be managed by the IT Teams.

Automation Software. Automation and pre-defined policies can help to save costs, streamline application delivery, relieve IT workloads, and offer vital IT services. Automation is utilized in a cloud system not just to easily scale up system resources to meet a surge in demand for processing capacity, but also to install applications to suit ever-changing market demands or to assure administration throughout a cloud environment.

3 Related Work

3.1 Literature Survey

Cloud computing provides significant technological and legal challenges for digital investigators, and solutions to many of these concerns are in their early stages. Cloud computing is always changing. As a result, many of the existing recommended solutions to these problems rely on CSP co-operation. According to [6], CSPs are capable of providing law enforcement with tools and systems through forensic preparedness, such as data collection methodologies, thorough log management, safe and trustworthy data provenance, and so on. Adoption of these solutions may not improve the CSP's bottom line, but it should be a priority on ethical and legal grounds.

The use of evidence reduction to establish a parallel process through the deletion of known superfluous material and deduplication is one strategy given in numerous literary works. This parallel process would deal with a smaller collection of information and attempt to answer fewer perplexing questions, functioning as a type of triage for the overall investigation process. The complete dataset would be scrutinized only if the triage revealed possibly suspicious activities. This reduction process introduces additional issues, such as the collecting method, the reduction process itself to guarantee as little loss of detail as feasible, and what data mining approach may be employed with as low supposition as plausible.

Reconstructing the crime scene is critical in order to understand how unlawful actions were carried out. Unfortunately, in the cloud environment, this might be an issue. For example, if an opponent shuts down her virtual instance after engaging in specific criminal behaviors, it will be hard to reconstruct the crime scene. However, a regeneration event can be employed in cases when a snapshot is taken as a result of each strike. Finally, it is proposed that the investigators see incoming and exiting data over the cloud [1].

Several strategies for minimizing cloud issues have been offered. Regardless, the great majority of these concepts are hypothetical and have not been tested in real-world circumstances. Regardless of the differences between performing digital investigations in cloud architecture and traditional computer settings, established methodologies such as Encase and FTK are still widely used in obtaining evidence from the cloud. Data gathering is the first practical duty that digital investigators must do. Just one study analyzed and investigated the present tools utilized in remotely data gathering. This tool is known as Forensics OpenStack tools (FROST). Rather than communicating with the operating system within the guest virtual machines, it talks with the cloud administrative plane. FROST is the first forensics capability built into an Infrastructure-as-a-Service cloud model. The CSP, on the other hand, employs FROST. As a result, faith in the CSP is still required, but not in the guest machine. Furthermore, trust must be placed in the cloud infrastructure, which comprises hardware, the host operating system, the hypervisor, and the cloud employees.

4 Threats

Cloud Computing's ubiquity has led to a proliferation of security and privacy concerns. Cyber-threats are also on the rise as demand-based and pay-per-use services become more prevalent. Since user information is freely accessible, identity theft has become quite frequent. The reason behind such an increase is the ever-growing online transactions in which the users have to provide their identification. Let us discuss some threats faced in cloud forensics.

4.1 Data Breach

Leakage of data in any case, whether it is an insider of the data center or an outsider with illegal access. The extent of the harm is determined by the data's sensitivity. It is possible that the data also contains financial information, which might cause serious harm. To access a large company's data center, you must provide your footprints and fingerprints as well as a valid cause for entering the server room Organizations like Google, Microsoft, et al. have armed guards outside of their data center, so that nobody tries to break in the room [3].

4.2 Data Locality

The cloud's data shouldn't all be in one place. Different backups should be available for the data. Only High Clearance officials should know the location of data centers and not anyone else in the organization.

4.3 Insecure Interfaces and API

Interfaces and APIs are commonly exposed to unauthorized access, plain text content transfer authentication, and cloud software exposure due to the open nature of cloud services and their interfaces and APIs. There are three main locations in which this threat is concentrated: Data tampering, repudiation, information disclosure, and privilege elevation [5].

Malicious users and developers can manipulate cloud services via application programming interfaces. APIs which users use should not be shallow. APIs are responsible for cloud service monitoring, provisioning, and administration. Weak APIs can cause application configuration settings to be changed, sensitive data to be leaked, servers to be disabled, and so on. By only utilizing encrypted keys to access cloud service APIs, which will authenticate the API user, this issue may be reduced to a certain extent. They should be kept on a secure hardware device.

4.4 Malicious Insiders

When a current or former employee with authorized access to an organization's data and network maliciously abuses his access privileges, the CSP's reputation suffers as a consequence. After analyzing this threat, the threat was found to be focused on the following areas: Repudiation, Denial of Service, Elevation of Privilege.

You can't protect yourself against such a danger. In this scenario, an insider employee may modify or delete critical data, or update or disclose it. Everyone on his team is trustworthy according to the cloud provider. An employee's history may be checked before they are hired. They can be given only what they need to accomplish their job [4].

4.5 Insufficient Due Diligence

Not having a defined plan to reach security goals, resources, and accurate policies for an organization regarding the cloud can be a serious threat. They migrate data to the cloud without fully comprehending the implications of doing so, the CSP's security procedures, and their own obligation to offer security safeguards. They decide to employ cloud services without fully comprehending how those services must be safeguarded. When evaluating technologies and CSPs, creating a strong roadmap and specification list is critical for the extreme gamble of success.

4.6 Multi-Tenancy

Under Multi-tenancy, numerous tenants share many resources. The most significant advantage of multi-tenancy is cost savings. However, multi-tenancy can lead to:

Interference. When a renter creates an unfavorable circumstance, it has the potential to affect another tenant.

Data Isolation. In a shared server environment, it is possible for one tenant to access data from another.

Riskier Change Management. It is possible that changing a tenant's settings will affect another tenant.

Inadequate Logical Security Controls. Reliance on logical segregation to guarantee that one tenant does not purposefully interfere with the security of the other tenants.

4.7 Denial of Service

Compel chosen cloud service providers to consume excessive amounts of limited system resources such as CPU power, memory, disc space, or network bandwidth - as in distributed denial-of-service (DDoS) attacks. Such attacks cause the system's functionalities to slow down and frustrate genuine system users.

4.8 Encryption

Lack of data security planning while implementing cloud encryption from the organization can lead to complexities and financial problems. The greatest threat in encryption is the use of weak and common passwords, which makes the encryption easier to bypass. Total encryption is also not guaranteed in the cloud because of the false sense of security organizations have regarding encryption. Even if the cloud is encrypted adequately, improper handling of key management could lead to a serious threat for an organization.

4.9 Dependance on Cloud Providers

CSPs are constantly competing and spending millions to be the most secure cloud service. But it is dangerous to assume for the organizations that their data will have full security under these providers. Contrary to a study, all the CSPs state that cloud consumers have the most responsibility in securing their cloud environment.

4.10 CMIA (Cloud Malware Injection Attack)

In the cloud environment, an unwelcome party tries to attack or infiltrate virtual machines or harmful services inside it. A hostile third party creates harmful implementation modules such as SaaS, PaaS, or VM's such as IaaS, and tries to introduce them into the cloud system in such assaults. As a cloud-based service, the body appears to be a new service that is comparable to previous services, but it is not. As soon as the malicious service is activated, the cloud redirects permitted body requests to it. Classified as an assault on the service to cloud attack surface [2].

5 Proposed Mitigation

We discuss potential solutions to some of the risks associated with cloud forensics and investigations.

5.1 Adopted Strategy

As an investigator, you will be looking for digital evidence that may be utilized in an internal inquiry or in court. This includes data preservation and validation as well as data collection, identification and analysis along with documentation and presentation. As a result, a large number of them recognize the urgent need for cloud-forensics tools, registration, and processes. Forensics cloud procedures are shown in Fig. 1.

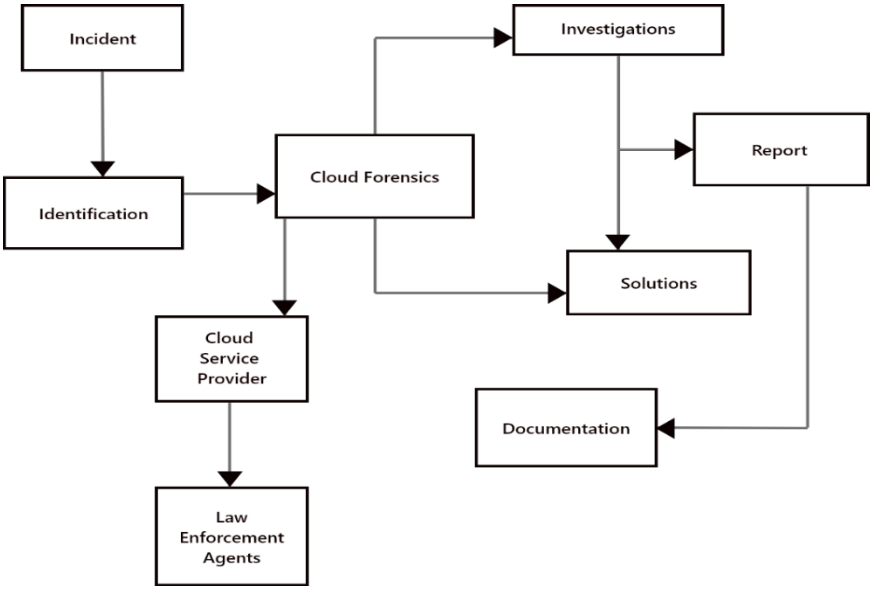

Fig. 1. Block Diagram of Processes in Cloud Forensics

Identification. The process of identifying and gathering data in the cloud via various processes is referred to as data collection. The data is made up of client-side and provider-side infrastructure artifacts. Traditional digital forensics consists of a data collection process that must maintain data integrity while not violating the laws and regulations of the authority where the data is gathered. This strategy should not infringe on the privacy of other tenants who share the resource.

Preservation. Due to the access limits of customers who have accessed material, SaaS providers will not allow access to IP data. The IaaS supplier would not provide you access to forensic evidence such as disc images or virtual machines. Customers will have restricted access to meta-data and other crucial fog files in the cloud. It will be impossible to investigate real-time monitoring for cloud customers on their own networks, as well as audit network operations.

When a malicious event is detected, the client and CSP seek assistance from a third party to take a snapshot of the present state independent of any data linked to the consumer. When data is "removed" in the cloud, the Service Level Agreement should notify you of the circumstances. Data purging on the cloud might be difficult, if not impossible. However, there are ways, such as crypto shredding, that may be used to retrieve lost data. Some data may have to be erased or rendered fully unavailable in order to meet regulatory requirements. There may come a time when data must be erased or minimized, in which case no one will be able to access it. The cloud provider's data management infrastructure should be ready and able to satisfy the destruction criteria; alternatively, other suitable methods, such as crypto shredding, must be used.

Examination. The forensic tools made available to the client by the CSP must be stated in the Service Level Agreement. Cloud computing relies heavily on rapid elasticity. Storage resources and Cloud Computing can be made available if there is a high demand. As a result, dynamic scalability in cloud forensic tools is critical. Most investigations will need the use of both live and static forensic technologies for data collection, e-discovery, evidence inspection, data recovery, and evidence analysis. Consumers must have access to scalable forensic data collection technologies for use in investigations.

At the CSP, incidents involving cloud forensics occur. All characteristics of evidence availability, transparency, and third-party trust are inextricably tied to CSPs. CSPs have complete control over the infrastructure's data; the personnel should be well-educated, and they should ensure that the staff is taught to conduct an investigation and that it is not tampered with.

Presentation. Documentation of investigation is critical in establishing any incident, and it is also applicable in cloud forensic investigation. Throughout the inquiry. During the investigation, the chain of custody and protocols are incorporated in the document. To maximize the chances of winning the case in court, the investigative documents must be kept in good condition and be attractive. When an event happens, the employees must take certain procedures. The record kept early in the incident allows the investigators to keep track of all the acts and proceed to retrieve the evidence using various tactics.

A chronology of evidences should be constructed in order to obtain precise answers to crucial questions. Data is highly important in the cloud environment, and it must be treated properly when it comes to multiple time zones.

5.2 Possible Solutions

Local Machine. Depending on the cloud model, the amount of access to forensic data varies greatly. When it comes to forensic data, IaaS users have unfettered access, whereas it is possible that SaaS clients will have restricted or no access to it. This means that the only software that connects to the cloud service on a client's side is their Web browser. The evidence found on a local computer may be the last hope. The local system will retain some file fragments and web cache when consumers interact with their devices in a Cloud Computing environment. Investigators may be able to retrieve this data to the greatest extent possible.

Between Cloud and Local Machine. Internet Service Provider (ISP) audit control nodes are another place to look for evidence of client activities. However, whether the ISP is in the cloud or not, they must follow the rules and regulations of their home country, making the audit control node of the ISP in the local region one of the most concerning objects in the investigation. Inquiry record and auditing may be time-consuming, yet it is possible that substantial evidence can only be uncovered through such tedious efforts.

In the Cloud. We propose that node data be received directly from the cloud service provider. Node data acquired by court order may provide unlawful evidence, as well as trace evidence. Also, use of Virtual Machine Monitor (VMM) is recommended. It is advised to use a cloud-based virtual environment and Virtual Introspection to monitor and investigate virtual machines from a VMM. Currently, data is obtained through a cloud provider. They look for, collect, and provide data to law enforcement using a search warrant or subpoena issued to the provider. Both examiners and jurors must have trust in a provider's technician, the technician's equipment and software used to collect data, and the cloud infrastructure via which evidence was obtained, compared, and reported on, as well as the provider's cloud architecture. After examining five different methods of obtaining data, we examined their efficacy as well as how much faith may be placed in such evidence. Although all of the tools and approaches were successful in producing proof, they all required a high level of faith in the cloud infrastructure. In order to address the multi-trust issue, we supplied four technologies: The cloud management plane, Trusted Platform Modules (TPMs), contract assistance, as well as forensic as a service. Remote acquisitions can be made more trustworthy by using any one or a combination of these methods.

TPMs deployed in each cloud server allow the hardware and associated software to verify what software is installed on each computer as well as the health and condition of each machine. TPMs deployed in each cloud server allow the hardware and associated software to examine what software is loaded on each computer as well as the health and condition of each machine. In summary, TPMs can validate the trust in Cloud Computing hardware, removing the need to rely on this layer.

Another method for assisting trustworthy forensics is data collecting from the management plane. The management plane may send log data, disc pictures, and packet captures to the provider, end users, and law enforcement on demand. Because this forensic gathering takes place within the hypervisor, accessing VM images and other data would need sole reliance on the Host OS and below, making it more admissible in court. In addition to virtual computers, cloud service providers may also preserve and collect data from infrastructure logging devices, packet captures, and billing information. If the company and its infrastructure are dependable, they can aid law enforcement with forensics. Furthermore, the supplier may offer these services to its consumers at a low cost and with minimal effort.

6 Conclusion

Cloud is a platform that is always evolving, and cloud users are also less familiar with cloud security when compared to other platforms. When events occur, cloud users and cloud providers must collaborate to establish an environment that fully supports forensics. To be better equipped to deal with incidents, forensics must continue to study risks to the cloud environment. It is also important to train and hire forensic investigators to solve the scarcity of cloud forensic experts. In future, we intend to deal for certain true situations and break down certain open regions in the regarded field that should be engaged upon.

References

1. S. Alqahtany., N. Clarke., S. Furnell., C. Reich.: Cloud Forensics: A Review of Challenges, Solutions and Open Problems. In: 2015 International Conference on Cloud Computing (ICCC), pp. 1-9, doi: 10.1109/CLOUDCOMP.2015.7149635 (2015).
2. A. Bedi., N. Pandey., S. K. Khatri.: Analysis of Detection and Prevention of Malware in Cloud Computing Environment. In: 2019 Amity International Conference on Artificial Intelligence (AICAI), pp. 918-921, doi: 10.1109/AICAI.2019.8701418 (2019).
3. M. Irfan., M. Usman., Y. Zhuang and S. Fong.: A Critical Review of Security Threats in Cloud Computing. In: 2015 3rd International Symposium on Computational and Business Intelligence (ISCBI), pp. 105-111, doi: 10.1109/ISCBI.2015.26 (2015).
4. S. Kumra., T. Choudhury., N. G. Nhu., T. Nalwa.: Challenges faced by Cloud Computing. In: 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pp. 50-56, doi: 10.1109/ICATCCT.2017.8389105 (2017).
5. G. Pandi., S. Shah., K.H. Wandra.: Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation. In:

International Conference on Computational Intelligence and Data Science (ICCIDS), pp. 163-173 (2019).

6. J. Farina., M. Scanlon., N. Le-Khac., M. Kechadi.: Overview of the Forensic Investigation of Cloud Services. In: 2015 10th International Conference on Availability, Reliability and Security, pp. 556-565, doi: 10.1109/ARES.2015.81 (2015).
7. S. Hraiz.: Challenges of digital forensic investigation in Cloud Computing. In: 2017 8th International Conference on Information Technology (ICIT), pp. 568-571, doi: 10.1109/ICITECH.2017.8080060 (2017).
8. P. Gayatri., M. Venunath., V. Subhashini., S. Umar.: Securities and threats of Cloud Computing and solutions. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 1162-1166, doi: 10.1109/ICISC.2018.8398987 (2018).
9. N. F. Efozia., E. Ariwa., D. C. Asogwa., O. Awonusi., S. O. Anigbogu.: A review of threats and vulnerabilities to Cloud Computing existence. In: 2017 Seventh International Conference on Innovative Computing Technology (INTECH), pp. 197-204, doi: 10.1109/INTECH.2017.8102448 (2017).
10. Z. Balani., H. Varol.: Cloud Computing Security Challenges and Threats. In: 2020 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-4, doi: 10.1109/ISDFS49300.2020.9116266 (2020).
11. R. Fernandes., R. M. Colaco., S. Shetty., R. Moorthy H.: A New Era of Digital Forensics in the form of Cloud Forensics: A Review. In: 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 422-427, doi: 10.1109/ICIRCA48905.2020.9182938 (2020).