EasyChair Preprint

№ 8473

A Survey of Cloud Computing Intrusion Detection System and Forensics Approaches

Muskan Khan

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

July 14, 2022

Research Article

A survey of cloud computing intrusion detection system and forensics approaches

Muskan Khan[3]

Department of computer science, Univeristy of manday, India[1]

Using cloud computing, businesses can adopt IT without incurring a significant upfront cost. The Internet has numerous benefits, but model security remains a concern, which affects cloud embracing negatively. The security challenge gets too difficult underneath data center, while additional dimensions such as model design, multitenancy, elasticity, and the layers dependency stack have been added to the problem scope. We present a thorough examination of the cloud security challenge in this article. We looked at the issue from the standpoints of network infrastructure: cloud-provided features, cloud consumers, and cloud service delivery methods. Based on this research, we developed an in-depth characterization of the data protection challenge and recommended security solutions that should address the critical aspects of the issue. Cloud computing is an exploding field of research that relies on distributing computing power instead of using dedicated computers or smart devices. Most of the growth in this sector is attributed to the indispensability of electronic and digital gadgets and the shift from a traditional IT subscription model to a unique cloud model. Cloud computing offered a significant danger and difficulty for information system projects, but it also provided them with several possibilities to improve their data processing. It has also been noted that cloud users and consumers do not yet have the necessary forensic skills to detect illegal activity in the cloud. Although the cloud offers potential technological and economic advantages, consumers have been reluctant to adopt it primarily due to security concerns and the difficulty of conducting an appropriate investigation into the cloud. Some study has been done in this area, and strategies for conducting forensic investigations have been proposed. In this research paper, we begin by analyzing the intrusion detection progress made by other academics, and then we analyze and evaluate our conclusions in order to assess the potential difficulties that cloud forensics face based on these findings.

Introduction

Cloud technology is the next phase of Intertubes, realistically distributed databases that deliver computing power “as a service [1].” NIST [2]proposes the most frequently used descrip- tion of the cloud services concept as “a paradigm for providing on-demand networking provisioning of cus- tomizable computational power (e.g., networking, com- puters, memory, programs, and activities) that may be swiftly provided and dispersed with minimum adminis- trative labor or network operator ability to interact.” Figure 1shows the structure of cloud computing. A cloud can be

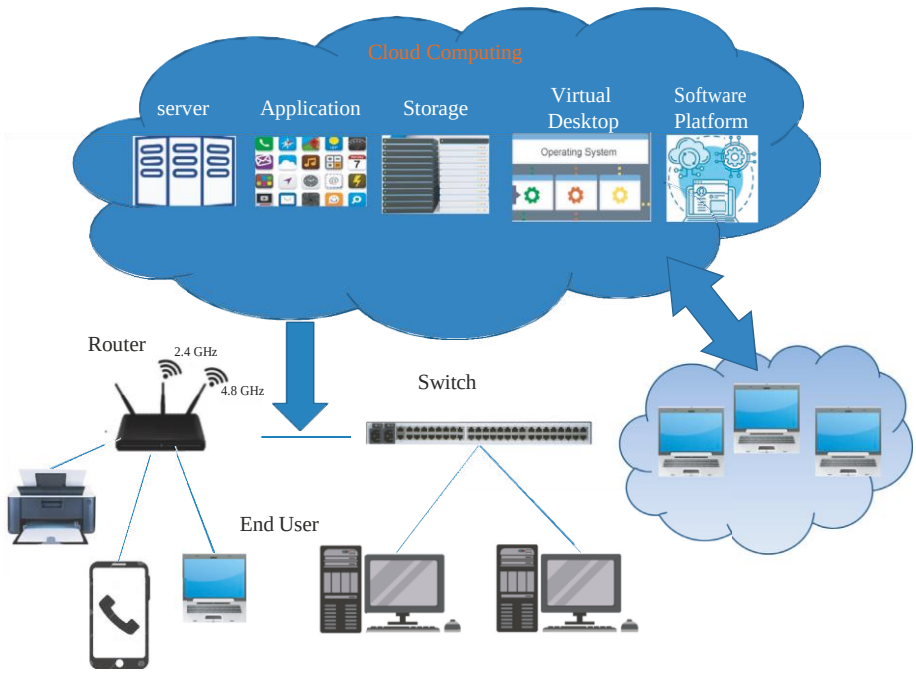


Figure 1: Cloud computing.

either private or public. Anyone with access to the Internet can purchase services from a public cloud. A private cloud is a closed network or data center that offers platform as a service to a small number of individuals who have particular access and rights. The goal of cloud computing, whether private or public, is to provide speedy, scalable access to data and information technology services [3, 4]

Cloud computing refers to a collection of networks and the data that flows across them. Users typically choose to use a third-party intermediary source for Internet connection instead of creating their personal physical systems in cloud computing, and they can use its ways forever.

In other words, the cloud is a browser technology that offers quality services to its clients, such as data and software, over distant servers. People can get beneficial results from the cloud without spending more time and money on things like computers and software to manage the data. When using cloud computing, clients' needs and applications are met without an entire physical and logical platform. Data can be accessed from almost anywhere, which has primary advantages of cloud computing for consumers. For example, cloud-based apps such as e-mail, video calling, and customer relationship management (CRM) operate on the cloud.

Furthermore, it presents its users with several features such as access to a large number of purposes without the need for permission, purchasing, or downloading files from any of these services. Cloud computing networks manage a service load because the workload is moved to mitigate the demand. As a result, client system requirements are reduced since the demand for local computers is not high, while the activity is operating. High-speed Internet service and a web browser are necessary for all cloud apps, and customers only pay for the services they have actually used. Cloud computing is an intriguing idea since it provides a viable opportunity for a new educational approach. On-demand web browsers encourage students and managers to swiftly and affordably access a broad range of different apps and services. This instantly decreases organizational expenditures while also providing more robust operational capacity. For academy operations, the progressive reduction of software licensing expenses, cost of data, and infrastructure costs provides considerable scalability. IT employees at academic institutions can get a lot of help from the advantages of the cloud. They do not have to keep the university's computer systems up and running, which is a huge help. Cloud computing gives quick universal systems, removes the need for hardware and software licensing, improves efficiency, and facilitates scaling. It is helpful to minimize the problems and expenses associated with backup and recovery by using a redundant cloud network. However, there are also several drawbacks to consider. There are always shortcomings with service providers, service-level agreements (SLAs), and cybersecurity. Furthermore, cloud service providers have varying degrees of technical expertise. In addition, we do not claim that cloud computing is a perfect solution for every company, so companies should conduct a well-informed analysis of its impact before adopting it.

Industry benefits of cloud computing are several; the first is that cloud computing greatly helps decrease the obstacle for smaller businesses to benefit from computation-intensive digital marketing, which was formerly only available to the larger enterprises. These analytical activities often need a considerable number of physical systems for a brief period, and cloud computing enables optimal resources available for small companies. Furthermore, cloud computing allows businesses to grow their services, which are progressively

dependent on precise information, to meet customer re-quirements. Because hardware resources are controlled by software, they would be efficiently applied as new procedures occur. Finally, cloud computing has the potential to decrease IT constraints. For example, as seen by the numerous po- tential startups, from the enormously powerful web pro- grams such as Facebook and YouTube to more specialized applications such as TripIt (for organizing one's trip) or Mint (for planning one's money).

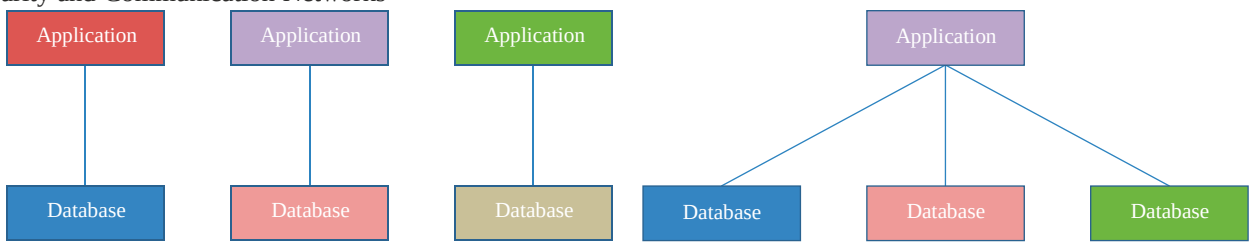
Needless to say, cloud computing has its own set of disadvantages for the industry as well; first and foremost, there are political issues arising due to international re-strictions imposed by governments. It is critical to maintain cloud computing apart from political concerns if it is to keep developing throughout the globe. Several leading world countries are considering legislation that sometimes im-pedes the expansion of the international cloud. There is a risk of losing information security if systems belonging to Canadians are used on American networks, such as those belonging to the US Patriot Act. Thus, corporation can not maintain that company data was on a certain centralized server in a given area. The second one is Security and Privacy. When it comes to cloud computing security, there is a considerable amount of ambiguity since it is a new novel technology (e.g., host and application). Because of this unpredictability, information experts have increasingly said that security is their top worry using cloud computing. In today's world, organizations confront several rules and regulations aimed at protecting the security of users' valu- able data. It is unclear if the cloud computing platform appropriately shields such data; rather, it causes firms to break the legislation.

The cloud model has two main elements: multitenancy and elasticity. Multitenancy allows several tenants to share the same service instance. Figure 2 shows the Multitenancy path for resource sharing [3]. The connection between the front and rear ends is managed by a centralized computer. The central server uses protocols to make data exchange easier. The central server uses both software and middleware to manage communication between many client devices and cloud servers. Each program or job usually has its own dedicated server [4, 5].

Elasticity allows a service's resources to be scaled up and down in response to the current service needs. Figure 3 shows the classification of the elasticity mechanisms [6]. Both features are aimed at maximizing resource usage, lowering costs, and increasing accessibility. Industry and academics have embraced cloud services to serve a broad range of applications, from cognitively complex queries to lighter services, thanks to the virtual machine. Small and medium enterprises will benefit from the approach since it allows them to embrace IT without having to spend on infrastructure, software licensing, or other necessary items upfront [7]. Furthermore, governments are becoming in- creasingly crucial of cloud computing to decrease

IT ex- penses while also increasing the abilities and mobility of their offered services. In [5] author presented a framework for practical mutation testing at binary level, named SNK4. To fully benefit from these modern computing models, which provide a creative economic structure for businesses to use IT without a large upfront investment, increased security risks must be addressed. Although virtualization can help businesses achieve more through splitting the physical bonds that exist among an infor- mation systems infrastructure and its consumers, it should be conquered in order to profit from this modern computing framework, which provides e-commerce strategy for businesses to implement IT beyond a large capital outlay [8, 9]. Cloud computing is now one of the most contentious problems in the telecommunication sector, prompting many businesses to move their infor- mation to the server since it offers several technological and economic advantages. Figure 4 shows the data or- ganization mechanisms under cloud Competitive servers include Google, Microsoft's Cloud Data Capa- bilities, and Amazon Web Services. In addition, several open-source web platforms, such as Solar Common Cloud Infrastructure and Phoenix, have persuaded con- sumers to use the Internet than in the past [6] When telecommunication companies began selling virtual pri- vate networks, the term "cloud" was coined. McCarthy proposed the fundamental notion of cloud computing, stating that "calculation may ultimately be structured as a public service." Prior to VPN, telecommunication pro- viders offered specialized step data connections, which squandered capacity. As a result, VPN connections are often used to transfer traffic in order to manage net- working use, and information technology expands this to include servers and network architecture. According to a Gartner assessment on cloud services sales in 2009, the cloud sector was worth USD 58.6 billion, USD 68 billion in 2010, and USD 148 billion by 2014. Cloud computing appears to be a viable platform; on the other side, it piques hackers' attention in exploiting any known flaws in the design

Overall, in terms of the goal of cloud technology in information technology services, cloud computing is so termed since the data collected resides in the cloud. Com- panies' cloud computing services allow clients to access information and programs on distant data centers and transfer the files over the network, notably the Internet. There is no need for a certain location to obtain it; thus, the user can operate from anywhere. In other words, it removes the burden of handling and storing data from the gadget you carried or interacted with. Additionally, it sends the workload to robust systems in cyberspace far away. As a result, the Internet acts as a cloud, allowing users to access their data and online services from virtually anywhere on the planet. Data processing has evolved into numerical com- putation, edge computing, and, most frequently, cloud computing over the network. However, the effectiveness of global norms, the convenience of final consumers, and, very prominently, the level of information security and privacy provided by modern technologies are all significant aspects in their success. Cloud computing is a new and fast expanding information tech- nology that is transforming the way IT building solutions are created, put, and presented as a result of a change in emphasis to the issue of data storage virtualization and local network.



(a)

Figure 2: Multitenancy path for resource sharing.

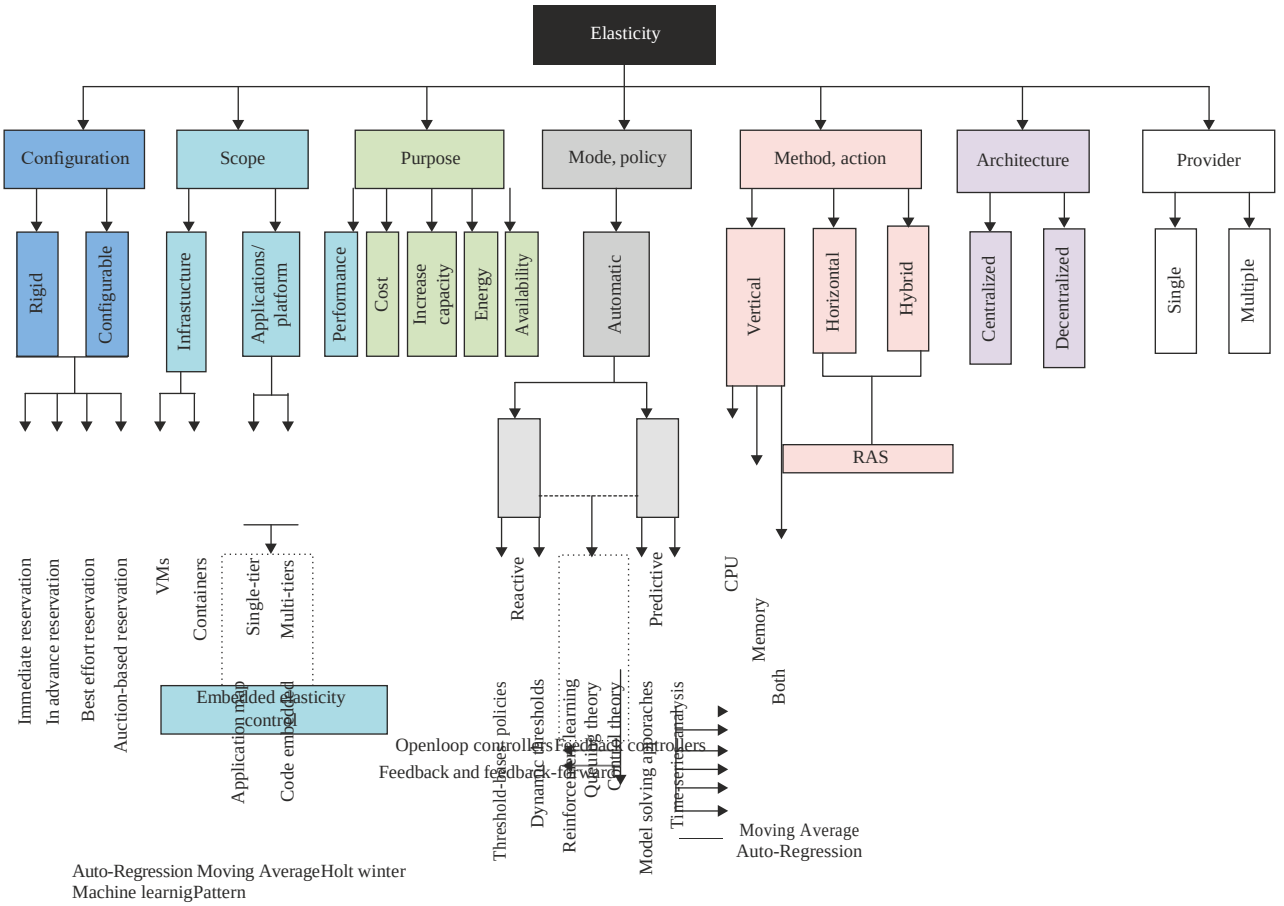


Figure 3: Classification of the elasticity mechanisms.

virtualization, which are two instances of virtualization (in- frastructure). In the current study, we express the existing problems and issues surrounding security and efficiency [7] These concerns are divided into four categories: architectural design concerns, process improvement design concerns, cloud particular type concerns, and cloud decision maker concerns. Our goal is to figure out where the cloud model's flaws are. We provide a thorough study of each shortcoming to highlight the underlying causes. The securitychallenge turns to be very challenging underneath the cloudparagon at fresh aspects such as model design, elasticity, andlayer dependency stack, which are introduced into the problem scope [8]These findings will support cloud suppliers and security sellers to understand the problem well.Moreover, it allows investigators to determine the current scale and flaws of the problem.The following is a breakdown of our paper's structure. Inpart two, we look back at prior attempts to define cloud security issues and concerns. Parts III through VII look at analyzing the security issue from several angles. The major security enablers in the cloud paradigm are discussed in Section 8. Section 9 summarizes our findings and identifies the essential characteristics that some cloud security answersshould address. Furthermore, in part *X*, we talk about up- coming effort focused on privacy factors we talked about previously. Figure 5 shows the flow of paper.

1. Literature Review

Numerous authors address the problems and problems related to cloud computing security. The Cloud Services Use Factors division delves into the many usage event

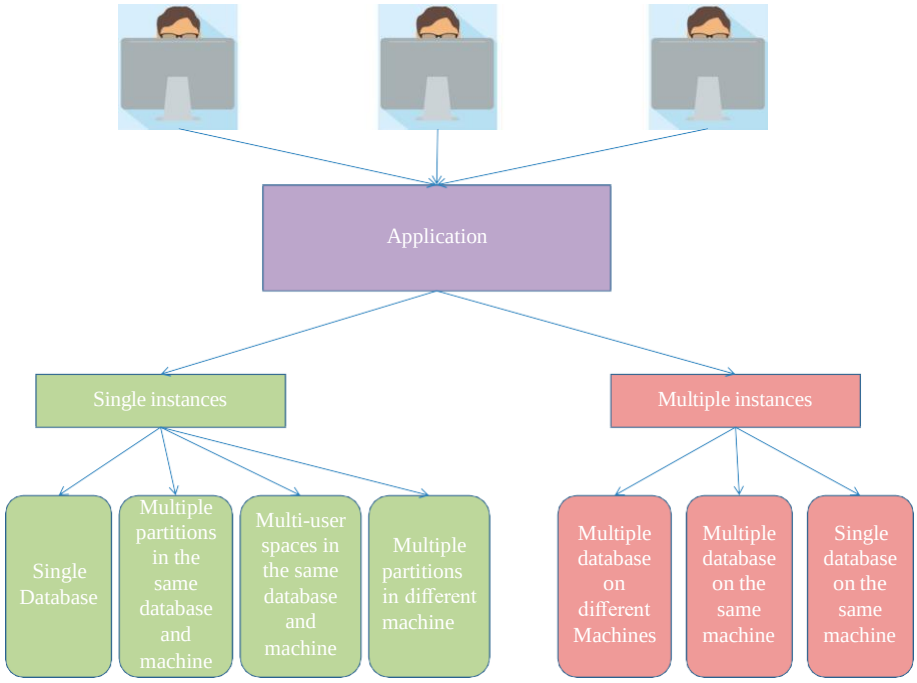


Figure 4: Data organization mechanisms under the cloud.

situations and connected needs that might be found in the cloud computing platform. Users, designers, and system administrators all contribute to their analysis of use cases. ENISA looked into the many security concerns related to cyber adoption, the assets involved, and the hazards' probability and effects. CSA discusses similar attempts.. Problems with high-level security in the cloud computing paradigm, like data quality, in- voicing, and confidential information protection, are reviewed by Popovic and Hocenski, talked on ITIL, ISO/ IEC 27001, and the Open, Virtualization Format, among other incident response standards (OVF) [18]. XML-at- tacks, browser-related assaults, and flooding attacks are among the technological security concerns raised by implementing the cloud computing architecture, accord- ing to Jensen et al. [. Grobauer and his colleagues ex- amine the cloud network's security flaws [20]. In [9] presented a novel scheme of privacy preservation in location based mobile coupon system using ananomous authentication schem. In [10] author presented evaluation system of effectiveness in social media. The system divides the critical threats into three categories: innova- tion, cloud-related, and security controls-related. Sub- ashini and Kavitha, concentrating on the SaaS model, examine the security problems of cloud service delivery models [21].in [11] the author participate in reducing maleware analysis overhead with covering. [12]The CSA addresses the most important as- pects of cloud computing. In each category, they suggest a series of cloud provider best practices, customers, and campaign featured to monitor. For several of these topics, the CSA produced a set of thorough reports. In our study, we looked at the cloud model in depth to determine the fundamental causes and major contributing aspects in the privacy problems addressed in earlier studies It will aid in a greater understanding of the issue and the delivery of remedies [13].Data Analysis

To support this research, we gathered 47 relevant articles on forensic investigation and subjected them to a study quality evaluation, keyword research, and the research framework, which served as a data collecting technique. This is critical to research since it gives a clear picture of the research topic in the subject. As shown in Figure 6, recent research advances in cyber forensics are mostly focused on concerns and dangers in cloud computing, as well as the obstacles that cloud forensic poses. In this sense, several publications are either two or three types of study. There are a total of 22 articles that discuss these concerns, indicating that knowl- edge of cloud security vulnerabilities has grown over time ascomputing evolved.

The lowest amount of study attention is on articles that illustrate existing forensic processes and legislative strategy towards the web platform; this may imply that the present forensic strategy has failed to address cloud computing.Scientists, on either side, are suggesting new regulations, techniques, and frameworks to improve the capacity to do cloud forensics, as seen by the 18 papers we examined in this area. Moreover, phrases convey to users the overall theme of a document. Strong relevance was carried out in this study to determine the pattern of presence of specific terms in the cyber science industry among the evaluated articles, as shown in Figure 7.

Information technology is mentioned 21 times out of 47 times in all the articles. Computer evidence and data en- cryption are both close behind, with 15 and 14 times, re- spectively. Specific keywords like digital attribution, incident generation, and 16 additional phrases, on either side, have only been mentioned once. The importance of the findings

main contributions. Figure 8 demonstrates different types ofcloud computing. Also, Figure 9 shows different layers in cloud computing.

The following are examples of cloud initiatives, as shown in Figure 10.As shown in Figure 10, every care model contains a variety of alternative solutions, complicating the creation ofa common security architecture for every service delivery model. Furthermore, various service provision methods maycohabit in a single virtual machine, complicating the risk management further. *Infrastructure-as-a-Service (IaaS)*: cloud services offer computational power, memory, and networking as web operations. The network virtualization underpins this ser- vice architecture. The most well-known IaaS supplier is Amazon EC2. Figure 11 shows the offering services and their connections by IaaS.*Platform-as-a-Service (PaaS)*: cloud services give sys- tems, resources, and some other professional services that letclients create, publish, and maintain their own apps while configuring some of these systems or supplementary services through their own computers The PaaS paradigm can be built on top of an IaaS model or immediately in front of data centers. The most well-known PaaS is the Google App Engine and Windows Server Azure. Figure 12 shows the offering services and their connections by PaaS.*Software-as-a-Service (SaaS)*: when cloud suppliers provide programs housed on network infrastructure as aweb resource to end customers, rather than needing theconsumers to download the apps on their PCs. This ap- proach may be served in front of PaaS, IaaS, or network infrastructure directly. Salesforce CRM is an instance of a SaaS application. Figure 13 shows the offering services andtheir connections by SaaS.

reveals that the majority of studies focused on the overall field of cloud forensics rather than a specialized one.

2. The Cloud Computing Architecture andSecurity Implications

There are three performance management methods and three major technology architectures in the Cloud Com- puting paradigm [23, 24]. The three existing solutions are (1)private cloud, that is, a database server specific to a given organization, (2) public cloud, that is, a cloud platform publicly accessible for registration and use of basic facilities,and (3) hybrid cloud, that is, a hybrid cloud that can be broadened to usage funds in community clouds. Since cloudservices are open for customers to serve their operations, including malevolent users, they are the most susceptible

2.1. Identify the Objects under Protection. This study iden- tifies seven protection layers as per the cloud service's de- livery method . Control points in cloud information management include standard control points as well as cloud-related control points. Cloud-based protection objectsand traditional approaches are compared in Table 1. It is alsovital that the cloud system protect the abstract resourcesecurity and the software platform layers. In the end, vir- tualization devices must be protected on the host side and inthe network layer .

2.2. Trust and Security Models in Cloud Computing. The capacity to interact with AR displays is perhaps one of the most important features. A partnership of five Japaneseinstitutions, comprising JAIST, launched the enPiT-Securitytraining plan (also known as SecCap) in April 2013. TohokuUniversity, Nara University of Science and Technology, Keio University, and the University of Management Safety are allthe other cooperation participants.

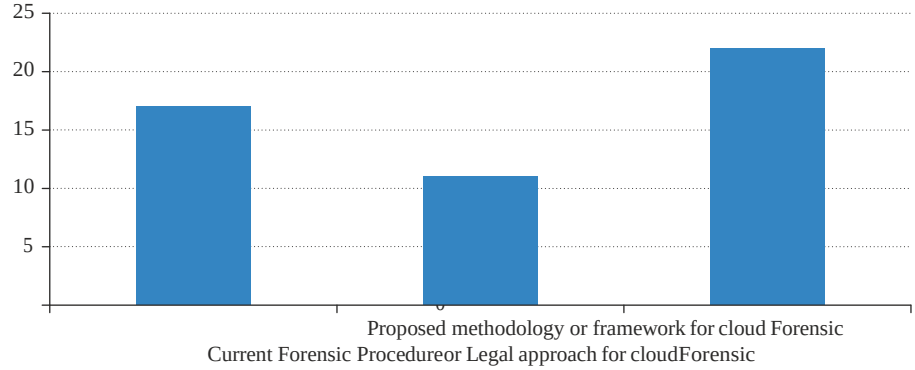


Figure 6: Research nature.

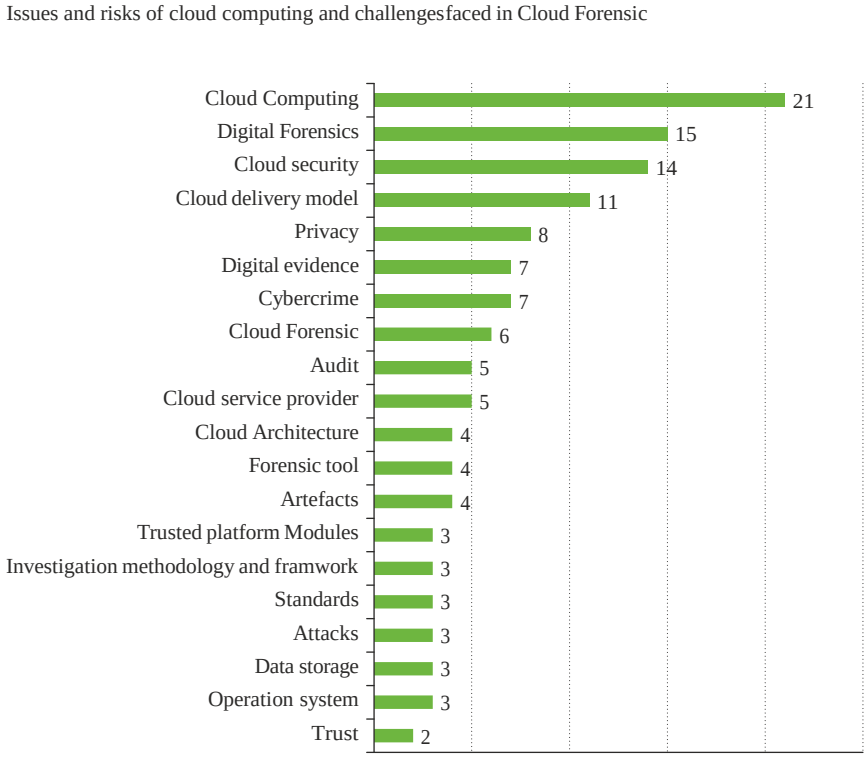


Figure 7: Keyword frequency analysis.

The SecCap program is intended for undergraduates and aims to acquire the skills needed by IT security professionals through lectures and hands-on actions on protection ele- ments of web browsers, programs, networking, and mali- cious software defenses and techniques

3. Cloud Computing Characteristics andSecurity Implications

Cloud services must enhance resource usage and, yet, lowercosts in order to achieve effective resource use. At the sametime, users must be able to acquire assets only as far as theyare required, with the ability to raise or reduce energy usagein response to real demand . The cloud computing model provides a win-win solution by including two es- sential features: integrons and mobility. All traits have majorconsequences for the privacy of the cloud paradigm.

Multitenancy means that tenants share computing re- sources, storage, services, and applications . Figure 15 depicts the various ways to multitenancy implementation. Each tenant has their own dedicated instance with their ownmodifications in method 1 (customization may include special development to meet customer needs).

Approach 1 is called the single Tenant. A single client is served by a single instance of the application and its corresponding infrastructure. There is just one instance of the program running on a single computer with a single tenant. In essence, this choice does not allow for any kind of sharing. Essentially, there is no sharing happening with this option. It has some advantages and disadvantages. There are several advantages to a single-client environment, such as increasedsecurity and dependability due to the abundance of re- sources and safe physical systems that come with having a whole environment devoted to just one client and always accessible. Furthermore, it benefits from customization since

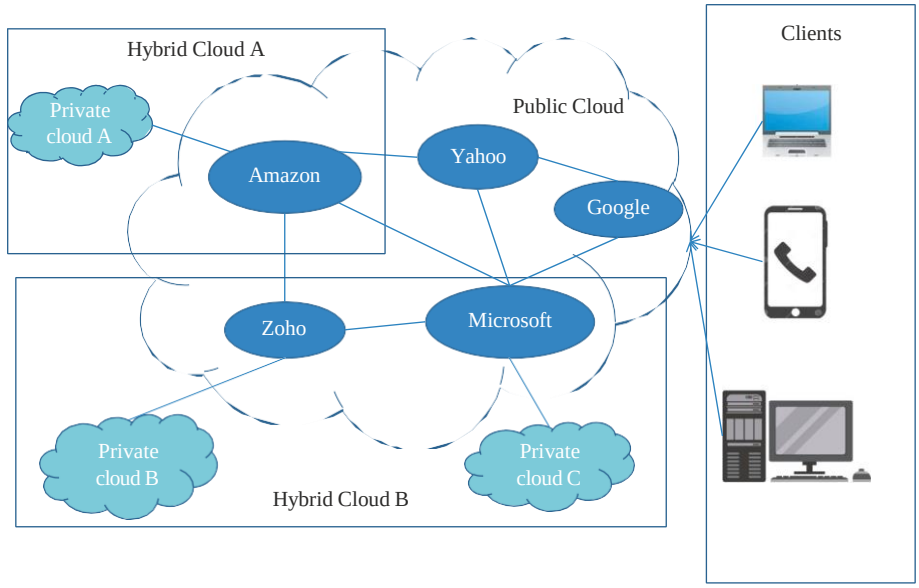


Figure 8: Types of cloud computing: private cloud, public cloud, and hybrid cloud.

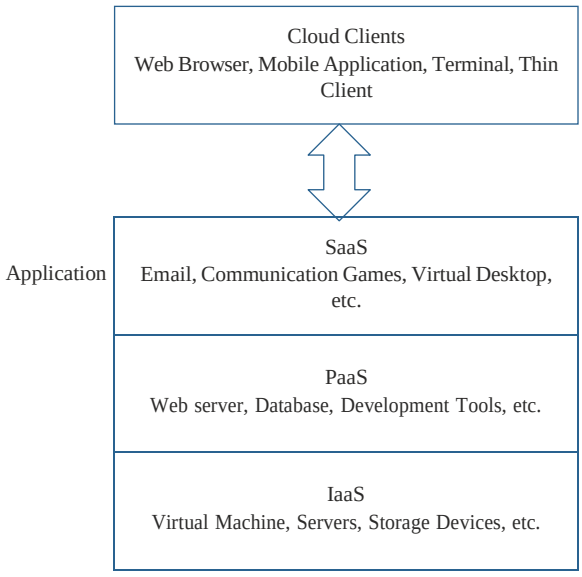


Figure 9: Cloud computing layers.

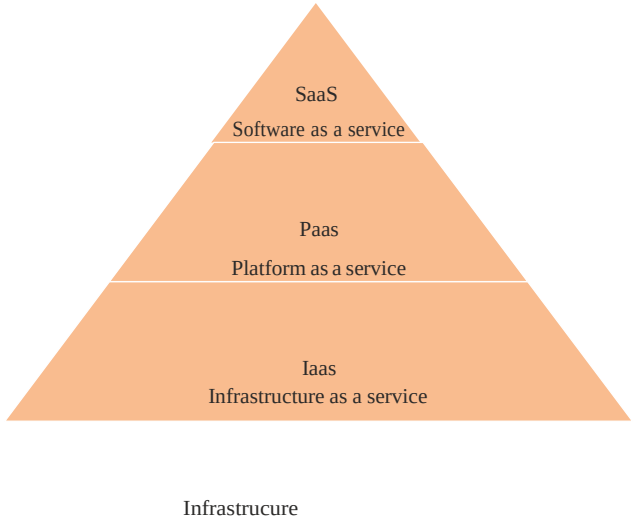


Figure 10: Cloud service delivery models.

separated into main network elements and additional components that are launched given current tenant requests, similar to Amazon web services .

In method 4, tenants are routed to a cloud infrastructure, which routes their requests to the most appropriate example

it has complete control over the data, making it possible forcustomization and new features if necessary.

On the other side, the drawbacks of a single-client en- vironment include the need for frequent maintenance tokeep the system operating smoothly and effectively since a single-tenant system often involves more jobs. Additionally, setup/management is a disadvantage since SaaS multitenant configurations are simple to install and run. Last but not least, there is Cost, which is single-tenant that often providesfor greater resources, however, at a more significant expensesince there is just one user for the whole system.

In method 2, every tenant has their own specialized server, similar to strategy 1; however, all versions have distinct settings. All tenants utilize the same example with real-time customization in method 3 (the program is depending on the load on the current context. The most dangerous approaches are 3 and 4 because tenants share the same storage and equipment . This information sharing compromises the anonymity of tenants' IT property, ne- cessitating the use of protected virtualization. To prevent coordinated attacks that tries to founder with the accuser funds, there must be segregation between tenants' infor- mation (at remainder, storing, and transformation) and destination accountability, during which tenants have reallyno expertise or regulate from over particular location of theirassets (could have a high ranking influence on data pres- ervation like nation or continent extent) .

Separation in IaaS must take into account VM capacity, processor, cognition, cached storage, and networking. Segregation in PaaS must comprise isolating among

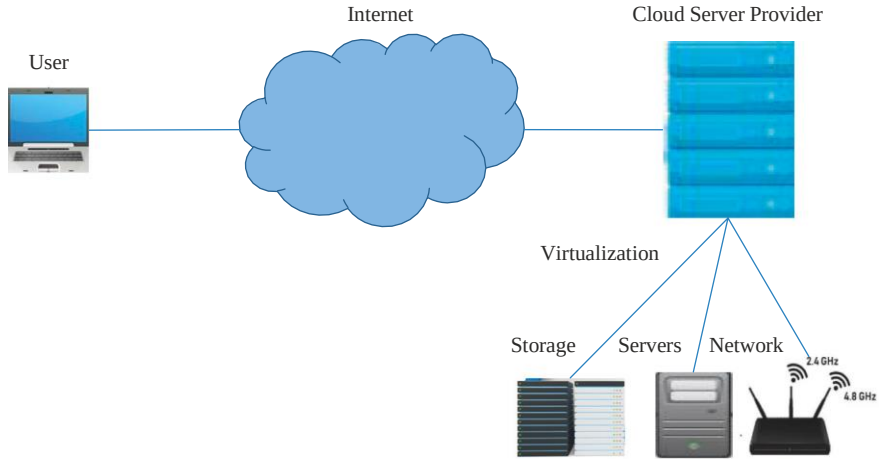


Figure 11: Infrastructure as a service (IaaS).

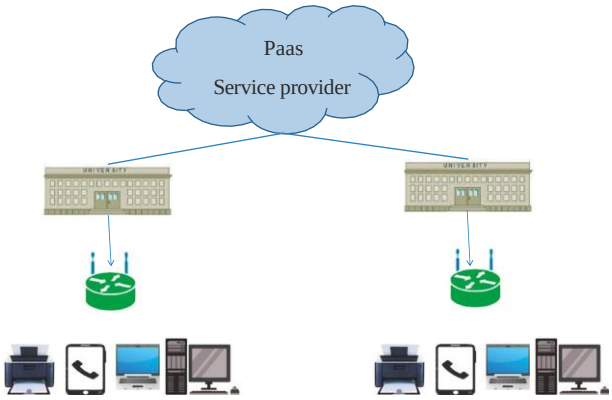


Figure 12: Platform-as-a-service (PaaS).

operating services and API calls . Separation in SaaS must be applied to distinct telecommunications service in the same example by numerous occupants, in addition to tenant information.

Flexibility is the capability of adjusting the amount of resources given to an on-demand based system . Tenant contributions can be scaled up and down to use the tenant's given threshold value assets in the development of other tenants. But this could cause security concerns . The reduction of tenant A frees up resources, which are now shared by tenant A and tenant B, allowing them to determine tenant A's former contents. In addition, flexibility provides a mechanism for allocating resources based on the number of eligible assets attributed to a vendor [10].

4. Cloud Computing Stakeholders and Security Implications

Various people are engaged in the cloud computing plat- form: private cloud (an entity that schedules to cloud users), Internet supplier, and trade customer . Every participant has its current security technologies, as well as obligations (specifications)

and abilities (provided) from many other participants. As a result, (1) a collection of protection criteria defined on a system by several tenants may be incompatible As a result, every provider's protection specifica- tions must be preserved and implemented at the provider recommended intervals and at execution time, taking into consideration the potential of new conditions given current users' requirements to ameliorate potential risk; (2) the user and provider must try negotiating and cooperate on the imposed system security. However, there are no basic se- curity specification expressions that cloud participants may use to describe and argue about the security features they offer/require.; and (3) every participant can have their safety new strategies for defining resources, anticipated risks, and their consequences, as well as how to avoid problems. Both cloud service suppliers and cloud users (who are unaware of the materials and security measures of activities based on their technologies) lose control when they embrace the public cloud. Security SLA was made critical as an element of the strategy for defining, enforcing, and analyzing security characteristics . SLAs, on the other hand, still leave security characteristics out of their requirements. Further- more, SLAs are greater contracts that do not include the specifics of security rules and controls, as well as how to alter them in real-time. Data centers, on the other hand, can not implement efficient and safe security measures since they are unaware of the designs of managed services [6]. Moreover, computing resources are confronted with a slew of new safety regula- tions, even while maintaining a diverse set of security controls that must be maintained. The protection control- lers' jobs are made much more difficult by this . Between cloud producers and recipients, they must be informed about what safety is implemented, what dangers are present, and what breakdowns happen on the cloud infrastructure and infrastructure components . This is referred to as "trust but verify," in which cloud users should have faith in their suppliers, but cloud services should give tools to assist users in verifying and monitoring privacy compliance .

5. Security and Trust Model in Cloud

Aside from a basic inspection, numerous associated recent studies have generated many approaches for forensic.

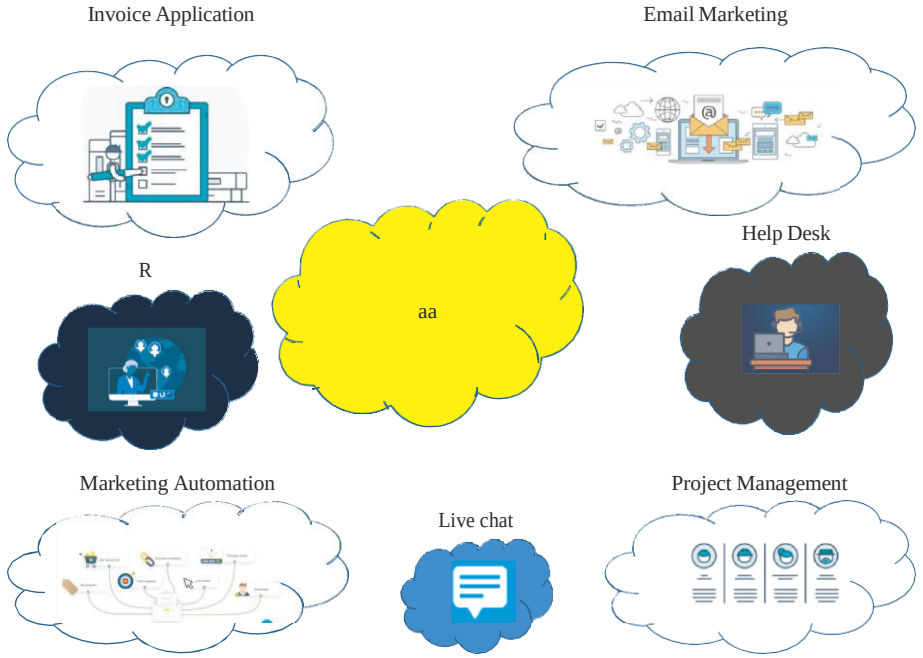


Figure 13: Software-as-a-service (SaaS).

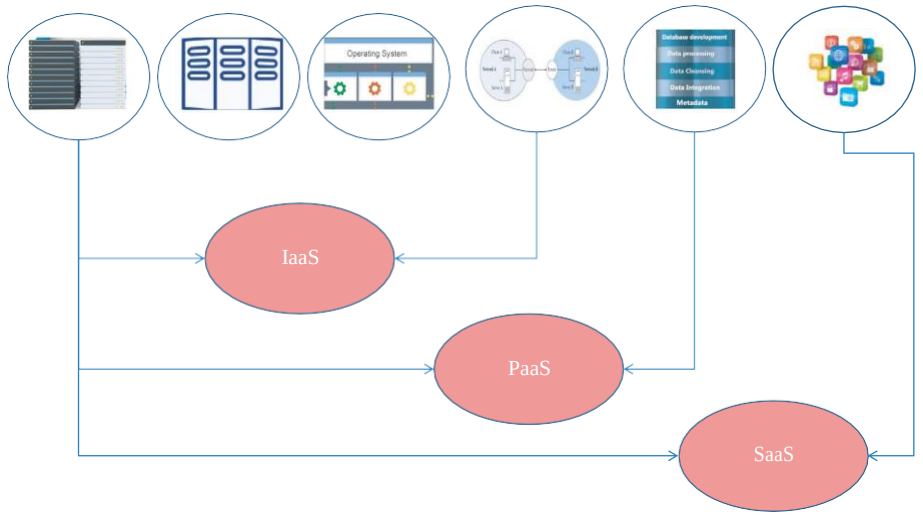


Figure 14: An overview of three cloud computing models.

investigation, particularly in the security and trust areas. Thereare some who use the Internet who are not necessarily specialists in the area of computers. Traditional firms handle allsensitive information inside and have total control over their personnel, which is one of the most noticeable issues found .According to Dimitri , cloud migration has reducedthe development of effective security procedures. Since thecloud's characteristics vary from architectural design, this isbeing reevaluated. So, as to secure the secrecy and reliabilityof data, it is advised that you use a suggested trustworthythird party; it can be regarded as a protection system in the cloud that forms a network of confidence. In this context, it is argued that even if the cloud model isnot completely open, suppliers can exercise some openness in order to outline what is really being performed in a certainregion and also discusses the necessity of cloud providers proposing security rules and the many types of security problems . In terms of privacy, corporation is ac- countable for all of their sensitive data; moreover, there is a fundamental weakness in organizations that are unfamiliar with data storage and contro.The major barrier foradopting cloud services, as shown in Figure 16, is data protection safety problems around the cloud, which span over seven phases of the information life cycle, including

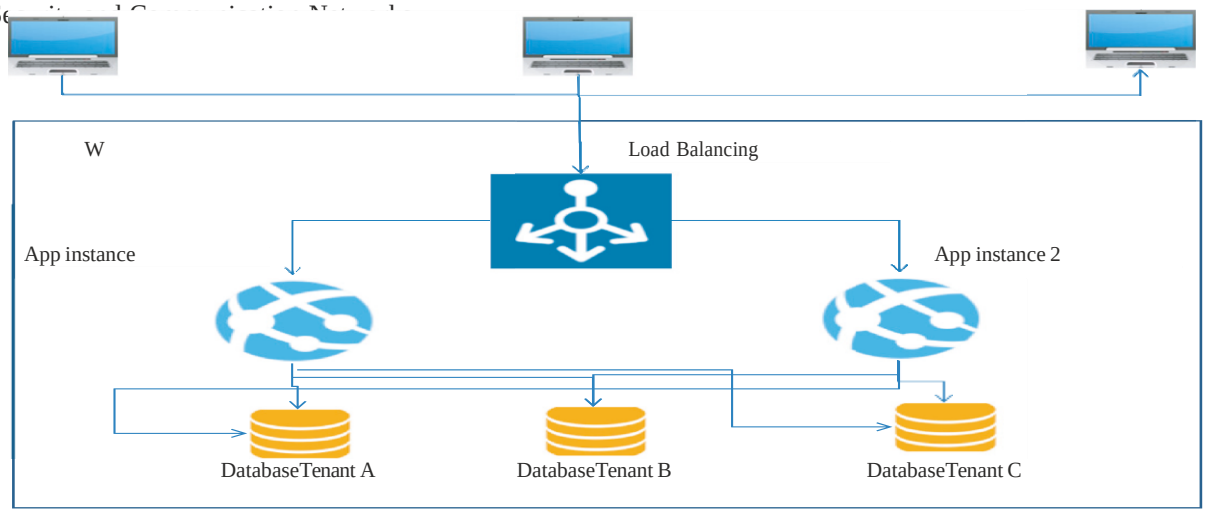


Figure 15: A different approach in multi-tenancy.

data production, transmission, usage, sharing, storage, ar- chive, and elimination.

They do, however, give a few information securities thatare now available. Standard process techniques are not designed for companies and data in the cloud since orga- nizational borders have been stretched to the cloud. They also bring up the question of computer security.

5.1. Cloud Forensic Issues and Challenges. Scientists have attempted to develop conceptualizations to solve these challenges; nevertheless, only a few of these accepted standards for data gathering and proper work on the In- ternet [48]. They suggest an iteration platform based on the currently utilized McCamish and NIST frameworks, which have common similarities but different methods. They propose that forensic experts produce evidence using a methodology in addition to current forensic methods. Re- garding trust in a cloud context, it emphasizes the need for asecurity-based certification that includes technology in order to improve cloud service confidence. It also demonstrates that the present use of SAS 70 (II) certification as an business standard is merely the start and that it currently can not offerconsumers the safety features that they want . In ad- dition to targeting consumers who profit from cloud plat- form providers' offerings, criminals will look at cloud computing to exploit any potential vulnerability in this new architecture and operating model . They argued that, in order to prevent cybercrime, service providers (SLAs) should be strong. They also stress that safety must be a typeof cloud solution, with designers focusing on management, hazard, and management as part of the design. There appears to be a tendency in existing standards to a better knowledge of the cloud environment and tailoring business standards toit. We stated that while cloud service providers can be used for a variety of purposes, they can also be misused bycustomers with bad intentions; for instance, a consumer canuse the public cloud to launch a Dispersed Rejection of Service (DDoS) offensive on other customers or the cloud on its own, causing the services to go inactive. It is difficult to tell the difference between legal content demands and malicious ones, but cloud services can deliver resources quickly in the case of a DDoS attack . The cloud is subject to the same types of assaults as other Internet services, which makes appropriate management challenging. According to the authors, cloud providers should establish tight access controls to prevent unauthorized access by users who abusethe network and limit access to customers' data in order to improve data security.

According to Birk and Wegener, cloud computing offers significant technological and economic benefits; neverthe- less, many chambers are still uncertain to change their systems to the cloud because of cloud security fears and unknown dangers . The researchers looked at a variety of cloud settings and came up with methods to help these systems overcome their flaws. To summarize, security concerns in the virtual environment are primarily driven by the lack of a uniform worldwide cloud specification.

5.2. Cloud Forensic. Currently, digital gadgets are growing at a breakneck pace, and analyzing the data created by these devices necessitates a massive amount of processing power [49]. The notion of a "Forensic Cloud" has been presented, with the goal of allowing a researcher to concentrate entirelyon the investigative process .

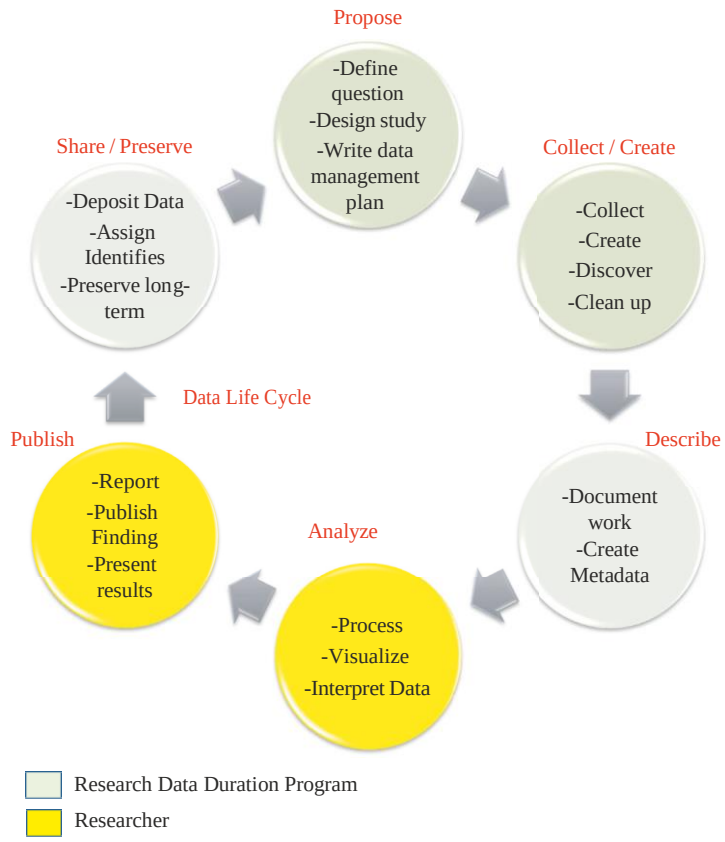


Figure 16: Data life cycle.

In terms of cloud computing, according to Biggs and Vidalis, criminal users represent significant difficulties and dangers to end customers who use the cloud service sup- plier's products . The hackers will also investigate big data to see if there are any flaws in this new idea, archi- tecture, or business strategy in cloud forensics. They argued that, in order to prevent cybercrime, service level agreements (SLAs) must be strong. They also mention bridge laws as a key concern. Various nations, digital investigators, and theircapacity to perform successful investigations may be harmed. They also looked at the influence of cloud tech- nology on criminal examination and discovered that, despiteits efforts to be safe, cloud technology is still not suited for forensic science. Yan addressed the present cloud system's dangers, which include big data, individual rights, and provider (CSP) trust issues . He claimed that the cloud ecosystem is more vulnerable to cybercrime than in the past,necessitating the use of digital forensics. In terms of the CSP,it claims that finale consumer data are kept and housed in the data center of the cloud provider, which saves business money on equipment and operations. Some organizations are unsure about the legal consequences of how CSP manages data passed over by consumers, which is one of theprimary reasons to designate data centers to maintain the benefits of cloud computing. He also mentioned that the cloud ecosystem had issues with cybercrime forensics and proof retention. In the article, he also suggested architecture for the cloud process that involves a dynamic allocation

management system and an information gathering and analysis engine to address these challenges. Mason and George discuss the data flow of electronic data and the use ofcloud computing for forensic investigation as a trend . That has gotten greater attention in recent years and, as a result, generates uncertainty in the present judicial system, which is not equipped to deal with cloud technology. The scientists clearly illustrate how to conduct an inquiry using the UK legal system, as well as how to collect evidence fromforeign countries, in their article.

5.3. Concerns about Cloud Computing's Privacy and Associ- ated Risks. Cloud technology is a technical system in which users entrust their data to third parties who store it on a webcomputer . As stated, virtualization has received only a small level of publicity from a private and legal standpoint. As Hou et al. pointed out, cloud computing comes with clearprivacy and user hazards that must be addressed . Re- mote forensics, also known as cloud forensics, allowed re- searchers to gather evidence without physically visiting the place and examining the storage devices. The danger act, risk cause, and risky things of a cloud system can all be analyzedand created on a cloud system's protection matters. In Table 2, some of the risks associated with cloud computing are described briefly .

the virtual machine itself or its OS (operation system). Because monitoring software is running on a virtual ma- chine, they are vulnerable to being attacked since the software does not have enough shield to protect users' privacy. Also, when the protection object is cloud data, the administrators can misuse and mismanage information since all of the information is in their hands, and each user does not have access to them at a higher level. Finally, when business application systems are considered as a protection object, the attacker again can take advantage of them and sabotage not only OS, but also associated databases with them, for example, in a PaaS.

Parts of the cloud's fragmented data may belong to numerous data owners, while other parts are useless to a computer crime investigation. Evidence may disperse, resulting in the cloning of data exposing unnecessary fea- tures to investigators without the authorization of cloud providers [58]. When a search is obtained, the server su- pervisor could collect necessary data and pass it on to de- tective, but this is contradictory to the objective of the case's secrecy [59]. Rather than relying on individual keywords to find relevant evidence across many files, he offers a system that maintains the inquiry's confidentiality while only extracting data that's relevant to the inquiry.

Zhu et al. [14] developed the concepts of proof of retrievability (POR) and proven data presence (PDP) in this respect, arguing that audit services are essential for ensuring data integrity and availability. They suggested that audit services may be implemented using cryptographic tech- niques such as PDP. They also talked about the present challenges of checking the accuracy of data in a cloud context. Key encryption solutions for data integrity, depending on neural networks and sign systems, they claim, cannot operate on data owners without a local memory of the information. They claim that most current systems cannot provide security properties versus untrustworthy CSP's deceit and forgery. As a result, they argued that a new framework is needed in cloud inspection services that enable the safety of the traditional authentication method. They suggested an analytical review exporting infrastructure for validating the security of contracted online storage using the cryptography evaluation method. They also construct a sample of an inspection system to assess the suggested technique. The efficiency of the aforementioned techniques and algorithms has been confirmed by their experimental findings. Their solution also has a reduced computationally and requires less additional storage for validation, according to the results. To assess the suggested method, they designed an architecture for audit service outsourced and built a prototype. The efficacy of mentioned methods and algo- rithms has been confirmed by their experimental findings. By understanding the prevalent digital forensic investigation methods that are linked with security, they are confident that the cloud computing model is in straight contradiction with a numerical forensic investigation.

6. Cloud Forensic Investigations

In the case of cybercriminals or other illegal activity, various police authorities frequently conduct digital forensics in- quiries[15] . They follow processes and standards that must be obeyed when dealing with evidence collected, which are outlined in standards. This is required to guarantee that the information found during the procedure meets legal stan- dards and may be presented in court . Because of its fleeting nature, cloud inquiries provide a unique set of challenges for these forensic experts.

7. Cloud-Based Forensic Investigations: Issues to Consider

We explored the many types of difficulties that detectives face when working by Internet and discovered the exam- ining cloud services using the present methodologies, which were inefficient. The most important difficulties appeared to be the researchers' physical, personal, and legal restrictions. When it comes to cloud investigations, this can be much more difficult since it involves thousands of virtual ma- chines, many systems, and a huge number of cloud users, just one of which is relevant to the matter. It would cause service interruptions for people who are not participating in the lawsuit . The machines are connected to the data center and communicate with each other without the par- ticipant's awareness. Furthermore, because of the accessible nature of the cloud, the only way to maintain identification when there is no physical connection is to utilize user IDs

and passwords, which may be captured and misused by unauthorized users. As a result, there is a significant gap in the technologies that can help detectives in working with

cloud data centers. It is tough to build these technologies for forensic information gathering since there are a lot of bridge creation and a lack of resources standardization [3].

8. Summary of Solutions Presented

After some thought, we have included some of the answers given in the selected articles in this section. First, we looked for cloud-based digital forensics options. Cloud suppliers offer software as a service, which includes a specialized investigative system for researchers to use. Because the re- searchers would have to deal with huge disk disks, they alsooffer investigations as a service. This platform may offer investigators terabytes of data of memory to handle nu- merous pictures and can also assist them in cracking cryptography keys. Another suggested framework integratedthe conservation and recognition stages to aid data pro- tection; the framework's distinctiveness resides in the iter- ative process necessary for evaluating consumer equipment as evidence. In addition, to cope with the continuouslychanging cloud environment, a new data tracking system is recommended, as well as a data gathering and processing system to handle cloud-related difficulties. We have dis- covered solutions for specific stages of standard sensitivity analysis. For difficulties with the identification phase, it wasproposed that a capability to monitor the status of client usage and logging be added to the software as a service architecture. Some innovative approaches were also pre- sented. Afterward, there are approaches to safety, faith, andconfidentiality problems in the cloud, with a secure in-formed cloud that uses a cloud authentication scheme beingoffered as a solution. It has an inner confidence element, which is performed using the physical system's hardware security module. In summary, the majority of cloud securityissues are caused by the lack of a single standard paradigm.This can increase scientific researchers' capacity to conduct examinations by ensuring that worldwide standards are followed. Table 3 shows a comparison of cloud forensic, cloud computing's privacy and associated risks, and forensicapproach for cloud forensic, which are discussed in this paper.

9. Conclusion

After some thought, we have included some of the answers given in the selected articles in this section. First, we looked for cloud-based digital forensics options. Cloud suppliers offer software as a service, which includes a specialized scientific server for researchers to use. Because the re- searchers would have to deal with huge hard drives, they also offer investigations as a solution. This service may offer investigators terabytes of data of memory to handle nu- merous pictures and can also assist them in cracking security keys. One of the suggested systems integrated the conser- vation and recognition stages to aid data protection; the program's distinctiveness resides in the iterative process necessary for evaluating a client's equipment as proof. Additionally, a data management framework was presented as well as a data gathering and processing system to addressthe concerns of the continuously changing cloud environ- ment. We have discovered solutions for specific stages of standard forensics frameworks. For difficulties with the analysis phase, it was proposed that a capability to monitor the condition of customer consumption and reporting be added to the software as a service architecture. We also presented an innovative approach for establishing a mini- mum value for a remote monitoring system. There is now a way for a safe, trusted, and private cloud to be offered as a solution to the problems of security, trust, and privacy in thecloud. It has an inner trust component, which is performed using the physical system's trusted platform component.

increase forensic analysts' capacity to conduct examinations through the correct application of world standards. Despite the fact that governments can strive to establish agreements to protect privacy for the sake of bridge inquiry, choosing which court or judicial system to present the subject remains problematic. However, the tools that are ready to facilitate a thorough audit cannot be used to conduct a forensic ex- amination on the Internet. As a result, appropriate appli- cation of worldwide standards aids detectives in improving cloud performance. The big data paradigm is one of the most promising computing paradigms for telecom operators, virtual servers, and cloud clients. However, we must plug inthe present security weaknesses in order to get the most out of the model. The following is a summary of the Internet security concerns based on the facts supplied as follows:

(i) Many security vulnerabilities, like as virtualizationand SOA, are handed down from the technology used.

(ii) Multitenancy and isolation are significant aspects of the data protection challenges that necessitate a vertical approach from the SaaS level to physical infrastructure.

(iii) To oversee and monitor such a large number of needs and procedures, risk management is necessary.

(iv) As indicated in Figure 3, the hybrid cloud should have a thorough security layer such that everycontact with any cloud platform asset must first pass through security features. We propose that cloud computing security solutions be implemented:

(v) Focus on the abstract of the problem, using model-based approaches to capture several security per- spectives and connect them in a unified cloud security model.

(vi) A feature of the data center. A flexible regulatory interface should be provided through delivery mechanisms (such as flexibility motors) and APIs.

(vii) Project integration for multitenancy (each user canonly see their own contributed data) and flexibility(you can scale

up or down depending on the scenario).

(viii) Assist with the integration and coordination of other security measures at various tiers so that integrated security may be provided.

(ix) Adapt to environmental changes and the demands of users.

10. Future Work

We are taking a look at the current cloud security issue. As a consequence of the adoption of the cloud designer, a security gap has formed between cloud users' and cloud providers' system security measures. To solve this problem, we must

we suggest using an adaptive model-based method. Patterns will aid in the abstraction of problems and the capture of different stakeholders' security needs at various degrees of detail. Adaptability will aid in the delivery of a cloud security paradigm that is interconnected, flexible, and enforced. The vicious circle will track system security in order to improve the present cloud security paradigm and keep cloud users informed about the protection of their property.

Conflicts of Interest

There are no conflicts of interest.

References:

[1] S. Ma, C. Yu, and W. Gu, "Towards Cloud Computing Security Considerations in Smart Grid," 2014.

[2] P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," *NIST special publication*, vol. 800, no. 145, p. 7, 2011.

[3] N. Mazher and I. Ashraf, "A Survey on data security models in cloud computing," *International Journal of Engineering Research and Applications (IJERA)*, vol. 3, no. 6, pp. 413-417, 2013.

[4] N. Mazher, F. Riaz, M. Tariq, F. Ishaque, and H. S. Shakir, "Performance Comparison of Load Balancing Algorithms using Cloud Analyst in Cloud Computing," 2018.

[5] M. Ahmadi, P. Kiaei, and N. Emamdoost, "SN4KE: Practical Mutation Testing at Binary Level," *arXiv preprint arXiv:2102.05709*, 2021.

[6] J. Asad and N. Mazher, "Load Balancing Protocol for dynamic resource allocation in cloud computing," 2018.

[7] "An integrated conceptual digital forensic framework for cloud computing - r_6_130217100243.pdf." http://www.ccbc.ir/files_site/files/r_6_130217100243.pdf (accessed.

[8] "Security in the Cloud: The threat of coexist with an unknown tenant on a public environment - MA-2012-12.pdf." http://www.ma.rhul.ac.uk/static/techrep/2012/MA-2012-12.pdf (accessed.

[9] M. Ahmadi and B. S. Ghahfarokhi, "Preserving privacy in location based mobile coupon systems using anonymous authentication scheme," in *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 2016: IEEE, pp. 60-65.

[10] M. Ahmadi, "Hidden fear: Evaluating the effectiveness of messages on social media," Arizona State University, 2020.

[11] M. Ahmadi, K. Leach, R. Dougherty, S. Forrest, and W. Weimer, "Mimosa: Reducing malware analysis overhead with coverings," *arXiv preprint arXiv:2101.07328*, 2021.

[12] P. Kiaei, C.-B. Breunesse, M. Ahmadi, P. Schaumont, and J. Van Woudenberg, "Rewrite to reinforce: Rewriting the binary to apply countermeasures against fault injection," in *2021 58th ACM/IEEE Design Automation Conference (DAC)*, 2021: IEEE, pp. 319-324.

[13] M. Armbrust *et al.*, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50-58, 2010.

[14] N. Luong, D. Hoang, P. Wang, D. Niyato, D. Kim, and Z. Han, "Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey," *IEEE Communications Surveys & Tutorials*, 2016.

[15] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security," *University of California, Berkeley Report No. UCB/EECS-2010-5 January*, vol. 20, no. 2010, pp. 2010-5, 2010.