EasyChair Preprint

№ 6836

Cloud Computing Security Solutions and Privacy.

Nashwan Al-Thobhani and Methaq Salam

October 12, 2021

Cloud computing Security Solutions and Privacy.

Nashwan Saeed M. Ghaleb Al-Thobhani,
Modern University Science & Sana'a Community College, Sana'a, Yemen
nashwansg@gmail.com

Methaq Ali Mohammed Salam,
Lebanese International University (LIU Yemen),
Sana'a, Yemen.

ABSTRACT.

In recent years, cloud computing has emerged as a new concept for delivering various online services. Cloud computing has become an indispensable part of corporate and public enterprise. It eliminates the need for users to plan for the future in order to provide services. It also allows companies to start small and increase resources only when there is growth in demand for services. However, despite the fact that cloud computing provides huge opportunities for the IT industry, the development of cloud computing technology is now in its infancy, with unresolved issues in this article, we offer a simplified review of cloud computing, highlighting basic concepts, architectural principles, and reviewed various security practices and challenges associated with both the software and hardware aspects of protecting data in the cloud, and improving data security and privacy protection for a secure cloud environment. We conducted a comparative research analysis of the current research work regarding data security and privacy protection techniques used in cloud computing.

Keywords: Cloud; Computing; privacy; Encryption; Security; Data; integrity; confidentiality; availability.

1. Introduction

Cloud is an expression that was originally used to refer to the Internet in network diagrams. It is defined as the initial cloud diagram used to represent the transfer of data from data centers to its final location on the other side of the cloud. The idea for software-as-a-service came about when John McCarthy of Stanford University said that "computing could be organized into a public service one day". [1] [2] He believed that timeshares could bring a future in which computing power and even private applications would be sold as a service through a business model. The idea was very popular in cottages, but disappeared in the mid-1970s when it became clear that current IT technologies could not support this computing model in the future. But this idea has recently become a popular term in technology circles and organizations of our time. Cloud computing is re-emerging as a method of computing in which computing resources are delivered as a service and are available to users through the cloud without the need for knowledge, experience, or even control over the infrastructure supporting those services. Cloud computing can also be considered as a general concept that includes software as a service and other current technology trends that share the idea of grid computing to meet the computing needs of users. In terms of commercial cloud computing platforms, these include Amazon EC2 [19] Services, Microsoft Azure Services Platform, and Google App Engine [1], which gives many companies flexible access to the computing resources they need and helps lower infrastructure costs for startups. But reliability was not without its problems. When it comes to the cloud, they raise issues such as privacy, security, etc. Hence, there is a growing interest in open-source cloud computing tools that allow companies to create and customize their own “clouds” to work together. With stronger business solutions. The concept of cloud computing revolutionized the ideas and applications of information technology services, especially with regard to the infrastructure solutions that organizations rely on to facilitate their functions, and it was found that many large and small companies participate in this new system. The concept of cloud computing has become one of the most important topics of discussion in the industry during the last period. Therefore, the focus of this study will be to discuss this concept and its main impact on small and medium-sized companies, as well as study the risks and challenges facing the transformation of this new concept of IT governance.

1.1 Cloud computing architecture

NIST (National Institute of Standards and Technology) is an organization that is well accepted worldwide for its work in the field of information technology. I will present the working definition provided by NIST for cloud computing. NIST

defines the architecture of cloud computing by describing five basic characteristics, three cloud service models, and four cloud deployment models (Cloud Security Alliance, 2009, p. 14) [5].

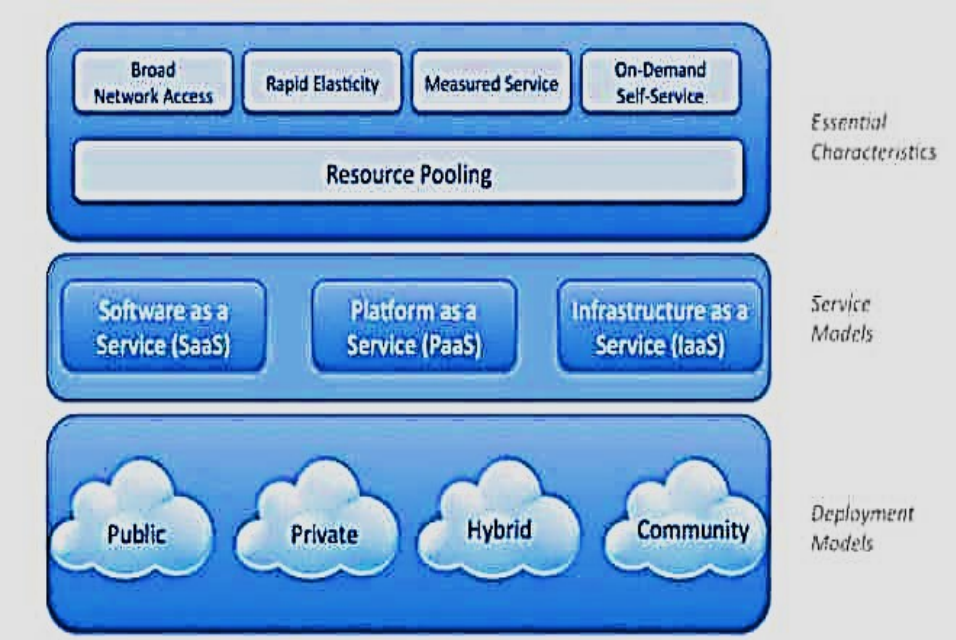

Figure 1: Visual model of NIST Working Definition of Cloud Computing (Cloud Security Alliance, 2009, p14) [5]

1.2 Cloud Computing Definition

The main idea behind cloud computing is not new. Already in the 1960s, John McCarthy envisioned that computing facilities would be made available to the general public as utilities [3]. The term "cloud" has also been used in various contexts such as describing large ATM networks in the 1990s. However, after Eric Schmidt, CEO of Google, used the word to describe the business model of providing online services in 2006, the term is already gaining popularity. Since then, the term cloud computing has been used primarily as a marketing term in a variety of contexts to represent many different ideas. Certainly, the lack of a standard definition of cloud computing [4]. National Institute of Standards and Technology (NIST) [5], as it covers, in our opinion, all essential aspects of cloud computing: networks, servers, storage, applications and services) that can be provisioned and released quickly with minimal administrative effort or interaction with the service provider. Figure 1: Visual model of NIST Working Definition of Cloud Computing

1.3 The essential characteristics of cloud computing

The five characteristics of the cloud computing model were originally defined by the National Institute of Standards and Technology (NIST) and have since been revised by a number of experts such as security.

1. **Self-service upon request.** You can quickly and easily configure the computing resources you need yourself, without filling out forms or emailing a service provider. The point is that what you're using is service-based ("I need 15 compute units"), not resource-based ("I need an HP ProLiant DL380 G6 with 32GB of RAM"). Your computing needs are drawn from what is truly customized for you. You don't know, and in most cases you shouldn't care. This is one of the biggest hurdles for IT departments that want to create their own on-premises cloud computing environment [6].
2. **Access to a wide network.** You can access these resources from anywhere you have access to the Internet, and you can access them from a browser, from a desktop with applications designed to work with them, or from a mobile device. One of the most popular application models (such as iPhone apps) is a mobile application that connects to a cloud-based back end [6].
3. **Pooling of resources.** Your cloud service provider, whether it's your organization or your IT department, manages all of the cloud's physical resources; Create a set of virtual processor, storage and network resources; It distributes it securely among all its clients. [6]
4. **Quick flexibility.** You can scale up and shrink the capacity (processing, storage, and network power) very quickly in a matter of minutes or hours. Self-service and resource pooling are what makes rapid flexibility possible. At the request of the customer, the service provider can

allocate more or less resources automatically from the available repository [6].

5. **Measured service.** It is also described as a subscription-based metered service meaning that the resources you use are measured and reported to you. You only pay for the resources you need, so you don't waste processing power like you do when you have to buy them on a server-by-server basis [1].
6. **Security.** Security complexity increases dramatically when data is distributed over a larger area or a larger number of devices and in multi-tenant systems, which is shared by unconnected users. Cloud security systems provide a rich set of integrated network and security gateway services to protect virtual data centers and optimize resource usage. Some of the key benefits are reduced cost and complexity, the ability to efficiently manage computing resources across group and subnet boundaries and a scalable secure network with simplified security management [1].

2. Services Models of cloud computing

2.1 Software as a Service (SaaS) [7] The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. Examples of SaaS providers include Salesforce.com [11], Rackspace [12] and SAP Business ByDesign [13].

2.2 Platform as a Service (PaaS) [7] The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

2.3 Infrastructure as a Service (IaaS) [7] Examples of PaaS providers include Google App Engine [14], Microsoft Windows Azure [15] and Force.com [16].

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). Examples of IaaS providers include Amazon EC2 [8], GoGrid [9] and Flexiscale [10].

3. The deployment models of cloud computing

NIST defines four deployment models [5]: private cloud, public cloud, community cloud, and hybrid cloud. Figure 2 Percentage of cloud computing models.

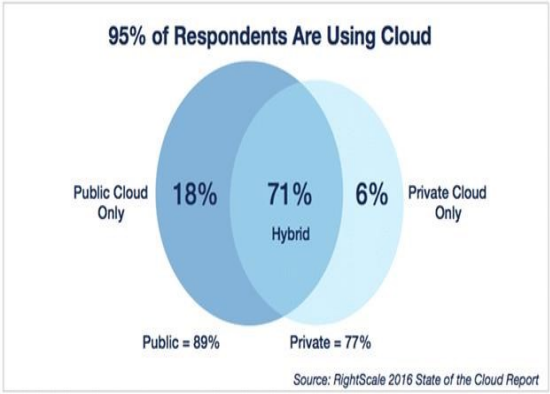

Figure 2: Percentage of cloud computing models[5]

3.1 Public clouds: A cloud in which service providers deliver their resources as a service to the general public. Public clouds offer several key benefits to service providers, including no upfront investment in infrastructure and transfer of risk to infrastructure providers. However, the public cloud lacks tight control over data, network, and security settings, which makes it less effective in many business scenarios [1].

3.2 Private clouds: Also known as inner draws, they are designed for the exclusive use of one organization. The private cloud may be created and managed by the organization or by external service providers. The private cloud provides the highest degree of control over performance, reliability, and security. However, they are often criticized for being similar to traditional proprietary server farms and not offering benefits such as no upfront capital costs [1].

3.3 Hybrid clouds: Hybrid cloud is a mixture of public and private cloud models that attempt to address the limitations of each approach. In a hybrid cloud, a portion of the service infrastructure operates in private clouds while the remaining portion operates in public clouds. Hybrid clouds offer greater flexibility than public and private clouds. Specifically, it

provides tighter control and security over application data than public clouds, while still making it easier to scale and contract on-demand service. On the downside, designing a hybrid cloud requires carefully defining the best division between public and private cloud components [1].

3.4 Virtual Private Cloud: An alternative solution to address the limitations of both public and private cloud is called Virtual Private Cloud (VPC). VPC is basically a platform that runs on top of public clouds. The main difference is that VPC makes use of Virtual Private Network (VPN) technology that allows service providers to design their own topology and security settings such as reallocation rules. VPC is basically a more comprehensive design because it not only virtualizes servers and applications, but the underlying network as well. In addition, for most companies, VPC provides a smooth transition from a proprietary service infrastructure to a cloud-based infrastructure, due to the virtual network layer [1].

4. Advantages and disadvantages of adapting to the cloud

The cloud computing system and its spread left all the previous data storage devices in which users kept their digital files, and all digital data and information can be dumped into one large cloud that is saved on the Internet. The computing system is a modern storage system for digital information and files on the Internet inside giant data storage centers that consume huge energy, so they can do their part to save digital user data and return it on demand [1].

4.1 The Advantages:

4.1 Fresh Software

With SaaS, the latest versions of applications needed to run the business are made available to all customers as soon as they are released. Instant upgrades put new features and functionality in the hands of workers to make them more productive. Moreover, software improvements are usually released frequently. This contrasts with locally developed or purchased software that may have major new releases only once a year or so and take a long time to publish [6].

4.2 Do more with less.

With cloud computing, companies can reduce the size of their own data centers or eliminate their data center footprint altogether. The reduction of the numbers of servers, the software cost, and the number of staff can significantly reduce IT costs without impacting an organization's IT capabilities [6].

4.3 Flexible costs

The costs of cloud computing are much more flexible than traditional methods. Companies only need to commission – and thus only pay for – server and infrastructure capacity as and when it is needed. More capacity can be provisioned for peak times and then de-provisioned when no longer needed. Traditional computing requires buying capacity sufficient for peak times and allowing it to sit idle the rest of the time [1].

4.4 Always-on availability

Most cloud providers are extremely reliable in providing their services, with many maintaining 99.99% uptime. The connection is always on and as long as workers have an Internet connection, they can get to the applications they need from practically anywhere. Some applications even work off-line [1].

4.5 Improved mobility

Data and applications are available to employees no matter where they are in the world. Workers can take their work anywhere via smart phones and tablets—roaming through a retail store to check customers out, visiting customers in their homes or offices, working in the field or at a plant, etc [1].

4.6 Improved collaboration

Cloud applications improve collaboration by allowing dispersed groups of people to meet virtually and easily share information in real time and via shared storage. This capability can reduce time-to-market and improve product development and customer service.

4.7 Cloud computing is more cost effective

Because companies don't have to purchase equipment and build out and operate a data center, they don't have to spend significant money on hardware, facilities, utilities and other aspects of operations. With traditional computing, a company can spend millions before it gets any value from its investment in the data center [1].

4.8 Expenses can be quickly reduced

During times of recession or business cut-backs (like the energy industry is currently experiencing), loud computing offers a flexible cost structure, thereby limiting exposure [1].

4.9 Flexible capacity

Cloud is the flexible facility that can be turned up, down or off depending upon circumstances. For example, a sales promotion might be wildly popular, and capacity can be added quickly to avoid crashing servers and losing sales. When the sale is over, capacity can shrink to reduce costs [6].

4.10 Facilitate M&A activity

Cloud computing accommodates faster changes so that two companies can become one much faster and more efficiently. Traditional computing might require years of migrating applications and decommissioning data centers before two companies are running on the same IT stack [1].

4.11 Less environmental impact

With fewer data centers worldwide and more efficient operations, we are collectively having less of an impact on the environment. Companies who use shared resources improve their 'green' credentials [1].

Despite these advantages, Cloud Security Alliance has identified several obstacles to the introduction of clouds. In 73% of enterprises, data security is one of the main problems that constrains cloud projects. This is accompanied by concern about regulatory requirements (38%), as well as loss of control over information technology services (38%), as well as knowledge and experience as IT managers and business executives (34%). While organizations concern about security and compliance are seen through the expansion of corporate data policies in the cloud and investments in bridging the gap in cloud skills can fully take advantage of cloud services.[17]. Figure 3: Cloud Computing Security Concerns

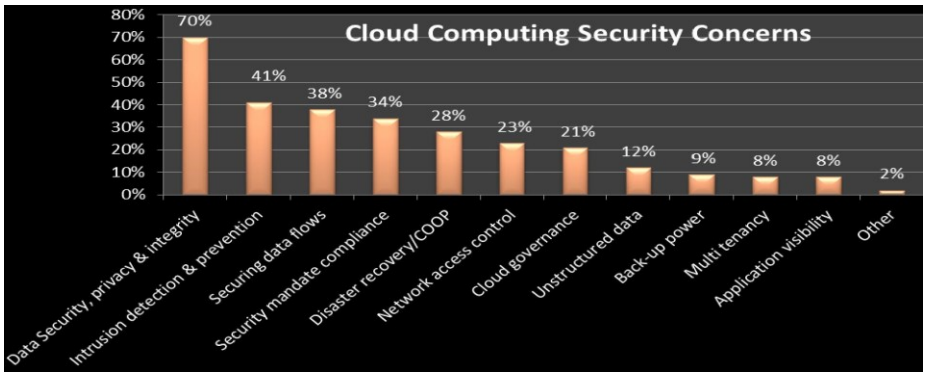

Figure 3: Cloud Computing Security Concerns [44]

5. Challenges to Cloud Computing:

The new cloud-computing model offers a number of benefits and advantages that outperform previous computing models and there are many organizations that adopt and adopt it. However, there are still a number of challenges, which are currently being addressed by researchers and practitioners on the ground. These challenges are summarized below [1].

5.1 Performance: The biggest performance problem may be for some transaction-oriented applications and other dense data applications, and cloud computing may lack proper performance. Users away from cloud providers may also experience delays and sluggishness [1].

5.2 Security and privacy: Companies are still concerned about security when using cloud computing. Customers are concerned about attacks when important information and IT sources are outside the firewall. Solving the security problem assumes that cloud providers follow standard security practices [1].

5.3 Control: Some IT departments are concerned that cloud providers have full control over the platforms. Cloud providers do not usually design platforms for specific companies and their business practices [1].

5.4 Data transfer costs: With cloud computing, companies can save money on hardware and software, but they can afford high network data transfer charges. The cost of the data transfer rate may be low for small Internet applications, which are not data intensive, but can increase significantly for heavy data applications [1].

5.5 Accuracy and reliability: Cloud computing still does not provide lasting reliability around the clock. Where there have been some cases where cloud services suffer from power outages for a few hours. In the future, we expect to see more cloud computing providers, richer services, standards in place, and better practices.

6. Case Studies

6.1. Case Study1.

Saleem (January, 2011), "cloud computing efficient on enterprise in terms of cost and security" [18] The studies of the effects of cloud computing on companies have been seen as a relatively recent subject with a desire for enterprises to shift to cloud work. The researcher looked at specific areas that he considered most influential - cost and data security. The study found the following results:

6. There is still confusion about the true definition of cloud computing.

7. Institutions that use network computing are better able to understand cloud computing.
8. The first feature that makes enterprises think about cloud computing is the cost effect.
9. Many factors or characteristics affect the cost of cloud computing for enterprises.
10. The study concluded that institutions can save their capital by not building their data centers and not hiring employees to manage them. Along with that flexibility and different pricing models makes the cost of cloud computing more effective for enterprises.
11. The most important finding is that the Cloud Computing is ideal for medium and small sized enterprises both in terms of cost benefits. However, in terms of security, it is not so beneficial for medium and small enterprises to adopt Cloud Computing. For large enterprises, it is more effective to adopt private cloud because with private cloud they can save cost and have better security.
12. The impact of cloud computing on enterprise structure and enterprise success.

The study conclusions were:

1. Cloud computing is a way to deliver services to customers.
2. Cloud computing has a positive impact on implementation details.
3. There are multiple restrictions on the cloud service developed for organizations that can be overcome by building a private cloud.
4. The adoption of cloud computing leads to the best results in terms of success of the project; in terms of the efficient use of costs, time and implementation and limited impacts on the infrastructure of the user.

6.2. Case Study2.

Ronald Beaubrun and Alejandro Quintero (April 2021), "A Secure Access Control Architecture for Multi-Tenancy Cloud Environments" [38]. The researchers in this paper propose a secure access control architecture for multi-tenancy cloud environments, in which physical resources are transparently shared by multiple virtual machines (VMs) belonging to multiple users. Implementing an effective access control mechanism in such environments can prevent unauthorized access to cloud resources. In this paper, we propose an access control mechanism that provides scalable and secure control of cloud access in the context of multi-tenant cloud environments. This mechanism will prevent malicious tenants from creating and sending unauthorized traffic to the cloud network. The study found the following results:

6.2.1. Main assumptions

The proposed architecture deals with the concept of Inter-VM traffic, which is the transmission of any data packet to and from one virtual machine. In other words, when the hypervisor encounters inter-VM traffic, the traffic does not pass through the physical switch or router, as the virtual switch that is located at the hypervisor forwards the packet to the destination VM. At this point, the following assumptions need to be done:

a) The virtual machines and physical servers are collocated at the same cloud provider. If the entire system is not part of the Cloud, then for sending traffic to another Cloud, the traffic should pass through a real router or firewall. In this case, the policies that are implemented in the firewall should be enforced [50].
b) Each physical server has only one hypervisor. In this case, the security attributes and access control lists of all virtual machines that belong to a physical server are located at one hypervisor. If we have multiple hypervisors on a physical server, we should apply an extra process for realizing which hypervisor contains the access control lists of certain virtual machines.
c) Each physical server is hosting at least one tenant, and each tenant has at least one virtual machine. Since each virtual machine should be registered as a tenant, if a tenant is registered in the Cloud, a virtual machine should be assigned to that tenant.
d) All access control lists are defined and stored in the hypervisor.
e) In its startup process, a hypervisor sends an update message to the other hypervisors that are located at the same Cloud. This update message contains the IP address and the ID of virtual machines that are located at that hypervisor.

6.2.2. Architecture principles

The principles of the proposed architecture are based on control packets, which is the core element for verifying security permissions of virtual machines in multi-tenancy Cloud environments. In this section, we explain the elements of the proposed access control architecture, which is illustrated in Figure 4.

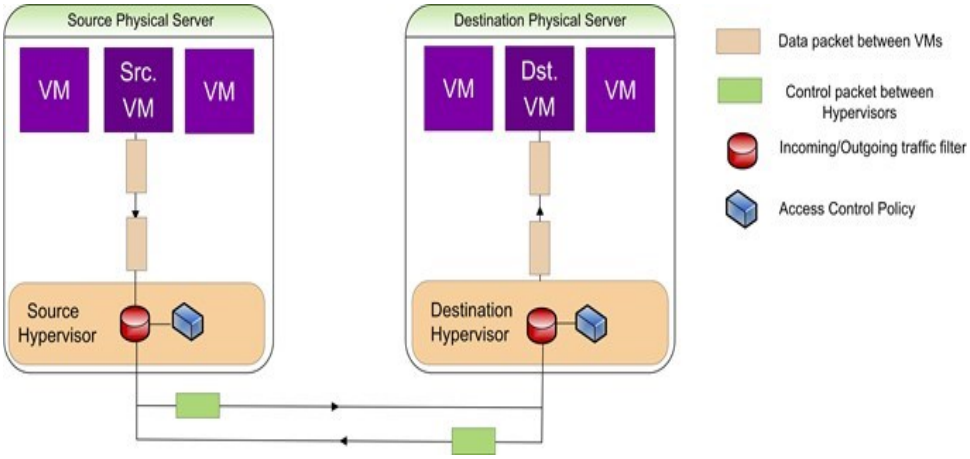

Figure 4: Principles of the proposed architecture [38].

a) Source (Src.) VM is a virtual machine that is installed on the source hypervisor, as the latter is located at the physical source server. The source VM is then sending traffic packets to a virtual machine in the same Cloud called Dst. VM.
b) Destination (Dst.) VM is installed at the destination hypervisor, and this hypervisor is located at the destination physical server.
c) A data packet is a packet that the source VM wants to send to the destination VM.
d) A control packet is a special packet that is generated by the source hypervisor. Its content represents the specifications of the source and destination VMs.
e) Incoming/outgoing traffic filter is a lightweight IDS that is integrated in the hypervisor. It compares the control packet with the access control lists of destination VM.
f) An access control list is a set of security permission that defines the level of security of each virtual machine.

6.2.3. Architecture design

The main goal of the proposed architecture is to block and drop unwanted packets as close as possible to the source hypervisor. As shown in Figure 2, when the source VM sends traffic to the destination VM, this traffic must pass through the source hypervisor. Once the data packet arrives at the hypervisor, it creates a control packet consisting of the necessary information for the access control check, such as the source IP address, destination IP address, port numbers as well as the protocol type. This control packet must be sent to the destination hypervisor which checks its content and decides whether the traffic can be delivered to the destination hypervisor. If the source virtual machine is allowed to send so-called traffic to the destination VM, the destination monitor adds a pass or drop value to the control packet's payload, and sends it back to the source hypervisor. According to this value, the source hypervisor threatens the waiting traffic. As shown in Figure 4, the process starts when a virtual machine starts sending some traffic to another virtual machine. Once such traffic is received by the source hypervisor, it checks the packet and looks for the destination address that is in the header of the inserted IP packet. If the destination address belongs to a virtual machine in the same cloud, we will have two possibilities. The first case considers that the destination address is on the same physical server. In this case, the architecture checks the access control policy of the destination VM, and can decide whether to pass or drop traffic. The second case occurs when the destination address is on a different physical server. In this case, the source hypervisor creates the control packet and sends it to the destination hypervisor. Then it waits for the response control packet [38].

Beside these possibilities, there may be an exception, when the destination address does not belong to any virtual machine in this cloud, which means that the source and destination addresses belong to two devices that are not in the same cloud. In this case, the architecture only has to pass the traffic to the default gateway to the source hypervisor (router, switch or firewall) [38].

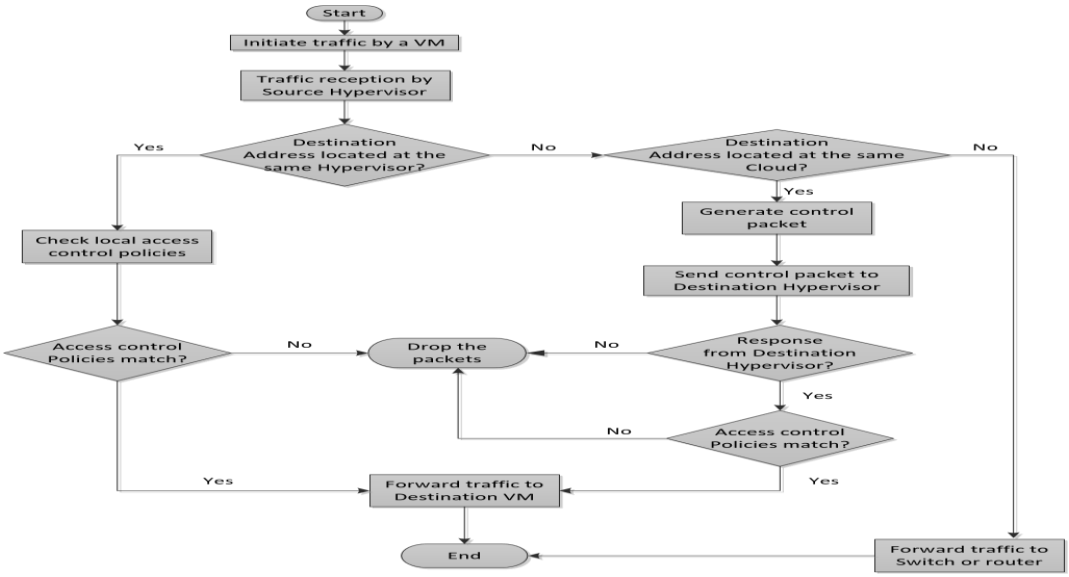

Figure 5: General mechanism flowchart [38].

6.2.4. The study conclusions were:

a) Scalability and security.
b) This architecture is scalable in the sense that if the number of virtual machines increases, we only need to implement this architecture in the hypervisor of each physical server without any additional changes in the system.
c) The architecture enables information security in the cloud by controlling the traffic sent from one hypervisor to another hypervisor and enforcing the hypervisor's security policies.
d) Using such an architecture leads to better performance by avoiding unnecessary traffic and allocating cloud resources to the necessary traffic.

6.3. Case Study 3

Rasavarna, Medu & Karlapudi, Medu. (18 December 2020), "Security in cloud computing" [45]. In this paper, researchers present that cloud computing tools are compatible with the computing environment. In the event of a mismatch, the cloud computing environment will likely have control and visibility loopholes that can be a vulnerability that cybercriminals can exploit. Incompatibility in the cloud computing environment raises several security issues that the service provider must consider. These issues include compliance issues with applications, platforms, networks, and data stores, increased vulnerabilities in the cloud computing environment, data leaks, risks from misconfigured services, and excessive access to privileges [45]. While selecting an enterprise service provider, the organization has to select the cloud computing services that are compatible with the required infrastructure. Also, the organization must understand the approach of cloud suppliers to security matters. The service provider must meet specific security standards and management models for business organizations and large organizations [45]. Organizations should also consider the relevant services, applications, platforms, and infrastructure offered by a service provider to avoid incompatibilities. This helps reduce security issues and cyber-attacks. The results of this study were as follows:

1) It is essential to deploy high-end security mechanisms to protect the network security from malware and malicious content.
2) To allow access to sensitive data and restrict access based on needs and preferences, you should use the principle of minimal privilege.
3) All the devices we use must be protected by antivirus software at all times.
4) The Internet connection is shield by using a firewall and Wi-Fi masking.
5) Use the least specific concepts to allow and limit access to sensitive data according to your needs and preferences.
6) The user must follow a two-step verification process where authorization steps must obey to prevent data loss.
7) A good network connection is a counsel to use with additional security layers like firewall, Virtual Private Network, and security provisions that enable adequate security measures.
8) Human errors and system crash are common issues which will penetrate to further loss of data. The organization must focus on core business activities associated with sensitive data security policies with strict rules and regulations.
9) Third-party users and external providers should not be allowed to access sensitive data.

10) High-end advanced security systems must be deployed with disaster recovery plans and procedures which provide an alternate source of data if a backup provision countenance by the management every year [45].
11) Encryption of data must be followed irrespective of its privacy to data and data transfer mechanism through the web, and Network sources addressed with encrypted codes. The receiver must have decryption codes to view the message.
12) Use strong passwords and change them frequently to protect yourself from attackers/hackers.
13) Finally, it is crucial to educate the employees and train them regularly with modern technologies and create awareness on cyber-attacks about controlling them on a primary level and how to protect their data from malware [45].

7. Cloud Security Solutions and Privacy.

Security is a big challenge in cloud system due to its nature of outsourced computing. Mainly, confidentiality, integrity and authentication are the primary pain areas. Unless robust security scheme and user-centric security policy is implemented, cloud system would be vulnerable to different attacks and susceptible by the users. Below we mention the key issues of ensuring the cloud security and the open challenges to be addressed for making cloud security system at least at the level of current IT systems [20].

Cloud storage security and privacy is a major concern, especially if your company handles sensitive data such as company data, credit card information, and medical records, among others. However, if you want to keep the information by default, we must take into account the additional risk that your information may be reached by other potential people that you do not want to access. Cloud subscribers want to ensure that their data is protected from cyber threats using the latest methods [21]. You will need multi-layered security and privacy solutions for the subscriber in the cloud, including endpoint protection, content and email filtering, threat intelligence, and best practices such as regular updates and patches. We need clear access and authentication policies and privacy policies. This section proposes a number of techniques to protect data and achieve the highest level of security and privacy for data in the cloud [21].

7.1. Ongoing security updates.

How often do you ignore requests to update your operating system, browser, or email client? In the field of computer security, this is not the case. These updates often include capabilities to protect your devices from the latest viruses and malware. However, when you store your data in the cloud, server companies must update their security measures. You don't have to worry about forgetting to run the update. The security procedures of the cloud provider will be updated regularly [21].

7.2 The Encryption

Encryption is commonly used to ensure the confidentiality of data. Homomorphic encryption is a variation of the encryption system proposed by Rivest et al. [22].

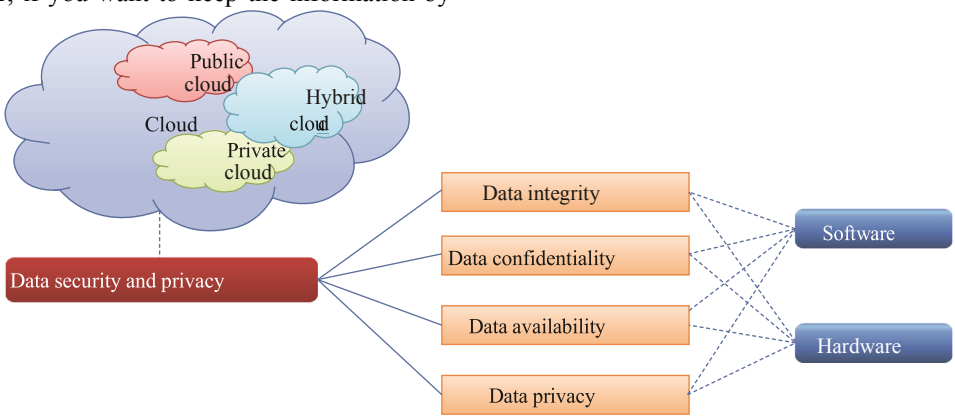

Figure 6: Organization of data security and privacy in cloud computing [23].

This ensures that the results of the cipher text algebra operation are consistent with the results of the post-encryption cleanup operation; moreover, the whole process does not require data decryption. Implementation of this method may well solve the problem of data confidentiality and data operations in the cloud.

Gentry was the first to propose a completely homomorphic encryption method [24] that can perform any operation that can be performed in plaintext without decryption. This is an important breakthrough in homomorphic encryption technology. However, the encryption system requires very complex computations, and the computation and storage costs are very high. This leads to the fact that completely homomorphic encryption is still far from real applications.

For secure communication, the Diffie-Hellman cryptographic algorithm [25] is proposed, which is very different from the key distribution control mechanism.

For greater flexibility and increased security, a hybrid method has been proposed that combines several encryption algorithms such as RSA, 3DES, and a random number generator [26]. RSA is useful for establishing a secure communication connection through digital signature authentication, while 3DES is especially useful for encrypting block data. In addition, several encryption algorithms are discussed to ensure the security of user data in cloud computing. Since the homomorphic encryption algorithm is ineffective, researchers turn to the study of applications of the restricted homomorphic encryption algorithm in the cloud. Encrypted search is a common operation [23].

Manivannan and Sugarani [27] proposed a lightweight database encryption mechanism known as the transform, replace, fold, and shift (TSFS) algorithm. However, as the number of keys increases, the amount of computation and processing increases.

An in-memory database encryption method has been proposed to ensure the confidentiality and security of sensitive data in an unreliable cloud environment [28]. There is a synchronization tool between owner and customer to find access to data. The client will need a key from the synchronizer to decrypt the encrypted shared data it receives from the owner. Synchronizer is used to store related shared data. In figure 5 shown, the easier for us to understand how homomorphic encryption works in cloud.

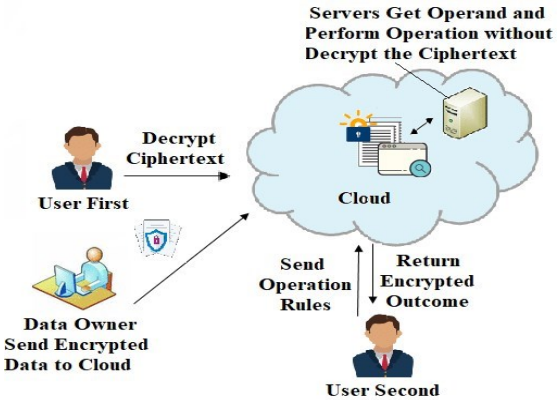

Figure 7: Homomorphic Encryption [21]

7.3 Access Control in Cloud Computing

In cloud computing, access control is an important security method to ensure data security. It ensures that only authorized users can access the cloud-based data they requested. In cloud computing, there are a variety of security technologies that allow proper access management. On separate network and cloud layers, intrusion detection systems, firewalls, and separation of responsibility can be deployed. Only restricted content is allowed to enter through the cloud due to the firewall. The firewall is usually configured according to the user's applicable security policies [21].

7.4 Secure Data Destruction

When data must be destroyed, it must be done safely. There are risks of data leakage if data destruction is not protected. When data is not securely destroyed, anyone can recover it. If you store classified and sensitive data on the cloud and the vendor fails to properly destroy the data from defunct equipment, the data is unnecessarily compromised. The purpose of the data deletion service is to completely obliterate sensitive or important data. Third party software or proprietary software is used to make this possible. After this process, it is expected that the data can no longer be recovered and used for any unauthorized or fraudulent purposes [21].

7.5 Distributive Storage.

Distributive storage of data is also a promising approach in the cloud environment. AlZain et al. [30] discussed the security issues related to data privacy in the cloud computing including integrity of data, intrusion, and availability of service in the cloud. To ensure the data integrity, one option could be to store data in multiple clouds or cloud databases. The data to be protected from internal or external unauthorized access are divided into chunks and Shamir's secret algorithm is used to generate a polynomial function against each chunk. Ram and Sreenivaasan [31] have proposed a technique known as security as a service for securing cloud data. The proposed technique can achieve maximum security by dividing the user's data into pieces. These data chunks are then encrypted and stored in separated databases which follow the concept of data distribution over cloud. Because each segment of data is encrypted and separately distributed in databases over cloud, this provides enhanced security against different types of attacks.

Arfeen et al. [32] describe the distribution of resources for cloud computing based on the tailored active measurement. The tailored measurement technique is based on the network design and the

specific routes for the incoming and outgoing traffic and gradually changing the resources according to the user needs. Tailored measurement depends on the computing resources and storage resources. Because of the variable nature of networks, the allocation of resources at a particular time based on the tailored active method does not remain optimal. The resources may increase or decrease, so the system has to optimize changes in the user requirement either offline or on-line and the resource connectivity [23]. The HAIL system uses POR mechanism to check the storage of data in different clouds, and it can ensure the redundancy of different copies and realize the availability and integrity checking [33]

7.6 Security policy plan

Data security will be ensured if the cloud service provider has a written security plan of policies. If the cloud service provider does not have a written security policy plan, the cloud is not secure and the data security cannot be guaranteed because they do not have a written security policy plan. This indicates that they are working on data security software. Organizations that have not formalized their security strategies cannot be trusted with your sensitive company/customer information. Strategies of order, establishment and without security are just an idea later [21].

7.7. Correct use of administrative privileges

Administrative authority should be limited in cloud computing organizations, and administrative accounts should only be used when absolutely necessary. All administrator accounts must be inventoried using automated methods, and every user with administrative access on laptops, desktops, and servers must be delegated by a senior manager. All administrator passwords must be complex, contain a combination of numbers, letters and special characters, and must not contain lexical words [21]. Before introducing any new devices to network systems, you must change all default passwords for operating systems, applications, firewalls, routers, wireless access points, and other systems. Passwords for service accounts should be changed regularly and should be long and difficult to guess. Passwords must be encrypted or hashed before they can be stored. Hashed passwords must comply with the instructions in NIST SP 800-132 or equivalent. The administrator must use unique and different passwords for their administrative and non-administrative accounts. This goal can be achieved by applying policies and increasing user knowledge [21].

7.8 Multi-tenancy access control model

As shown in Figure 8, a multi-tenant cloud service provider has three basic components: cloud manager, hypervisor, and virtual machines (VMs) [34]. Cloud Manager is a management console that is provided to customers in order to manage their cloud infrastructure, which means creating, shutting down or starting up instances. A hypervisor, also known as a Virtual Machine Manager (VMM), allows multiple operating systems (guests or virtual machines) to run concurrently on a host server. Its main responsibility is to manage application operating systems (OSs) and their use of system resources (such as CPU, memory, and storage). Its role is to control the processor and host resources, as well as allocate what is required for each operating system. A virtual machine is an isolated guest operating system installation within a regular host operating system. In this context, each client may have one or more VMs, where a single physical server can host multiple VMs. In such an environment, one client can send an unlimited amount of traffic to another client. Accordingly, the malicious agent can rent a virtual machine on the same host where the target virtual machine is located. This malicious agent can send unauthorized traffic to the target virtual machine and violate the security of the target virtual machine [39].

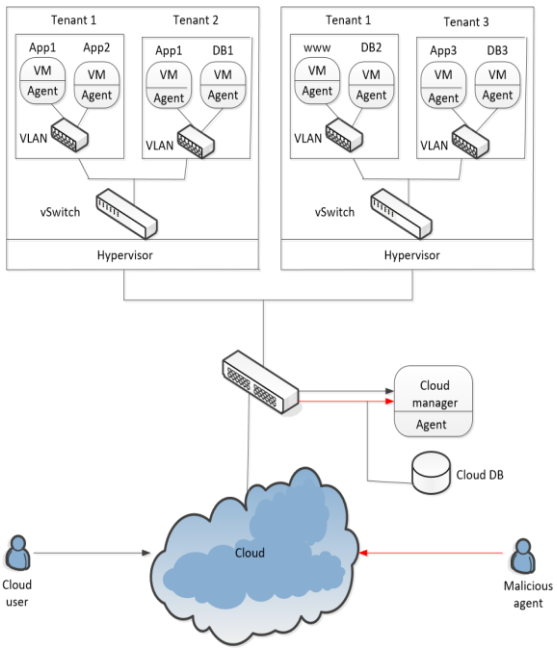

Figure 8. A model for a multi-tenant cloud service provider [38].

Unauthorized traffic may contain some scripts or malware that violate the confidentiality or integrity of the target virtual machine's data. Sending such traffic to another virtual machine makes it possible to carry out other types of attacks. For example, a

malicious proxy that owns a virtual machine can perform VM hopping on another user who is on the same host. By hopping between virtual machines, an attacker takes control of one virtual machine and tries to take control of another virtual machine. Navigating virtual machines allows an attacker to move from one virtual server to the next, or even gain root access to physical machines. Moving between virtual machines is a huge threat because multiple virtual machines can run on the same host, making them targets for an attacker. By carrying out this attack, a malicious user can breach security and steal data of other users on the same server while compromising the hypervisor file system [37] In addition, a malicious user can perform Denial of Service (DoS) attacks. These types of attacks deplete cloud network resources, such as bandwidth and computing power, by sending a large amount of unauthorized traffic to other virtual machines.

7.7.1. The Multi-Tenant Access Control (MTACM) model is a security architecture that incorporates the principle of separation of security duty in multi-tenant cloud environments [35]. The main idea of MTACM is to restrict the administrative privilege of the CSP and allow customers to manage the security of their own business. In this model, the mechanism of separation of tasks between the cloud service provider and the cloud client is handled through a management module. However, the management module is not user friendly for clients, as the cloud client has to take care of data security.

7.7.2. Role-based Multi-Rental Access Control (RB-MTAC) applies identity management to identify the user's identity and applicable roles [36]. This model combines two important concepts of access control in a multi-tenant access environment: identity management and role-based access control. In this context, Yang et al. [36] They believe this combination facilitates the administration of privileges that protect application systems security and data privacy. Providing a set of privileges and identity management systems to companies in a cloud computing environment is the main contribution of this security model.

This system can be used to easily change employee privileges when an employee leaves an organization or when we want to give employees more access without having to modify all employee privileges one by one. However, RB-MTAC is not independent, and for its implementation in the cloud computing system, a directory service is needed [38].

7.8. Third-Party Security Testing

The cloud provider should hire third-party security services to regularly test their servers and software to ensure they are protected from hackers, cybercriminals, and the latest malware and viruses. This external testing increases the chances that your cloud provider will have the protection it needs to keep your files safe from hackers [21].

7.9. Reliable Storage Agreement.

Safe storage agreement. The most common abnormal storage behavior is that cloud providers can discard some of the user's update data, which is difficult to verify only depending on simple data encryption. In addition, a good retention agreement should support simultaneous modification by multiple users. Mahajan et al. Proposed Depot that can guarantee the causal consistency of the fork joint and the ultimate consistency [40]. It can effectively resist attacks such as reset and can support other defenses to be implemented in a trusted cloud storage environment (such as Amazon S3). Feldman et al. proposed by SPORC [41], which can implement secure and reliable real-time communication and collaboration for multiple users using a trusted cloud environment, while untrusted cloud servers can only access encrypted data. However, the types of operations supported by a reliable storage protocol are limited, and most of the computation can only be performed on the client.

7.10. Perform Data Backups

Ensure that you only engage with cloud service providers who back up your data. We don't want all of your data to be stored on a single server. If that server goes offline, you won't be able to access your data. Even if you save your most sensitive data in the cloud, you should consider backing it up on your own external hard drives. This will provide you with an extra layer of protection should something happen with your cloud provider [21].

7.11. Deploying Multi-Factor Authentication (MFA)

Traditional username and password combinations are often not enough to secure user accounts from hackers, and stolen credentials are one of the most common ways hackers use to access your business data and applications on the Internet. They can log into all the cloud-based software and services that you use every day to run your organization once they have your user credentials [42]. Multi-Factor Authentication (MFA) protects all of your cloud users, ensuring that only authorized workers can log into your cloud applications and access critical data in your on-

premises or off-premise environment. MFA is one of the simplest and most effective security measures to prevent hackers from accessing your cloud applications. In fact, most security experts will warn you that failing to deploy MFA as part of an Infrastructure as a Service (IAAS) design is now considered careless [21].

6.13 IDS/IPS

IDS/IPS is a natural addition to any firewall setup. Both an IDS and an IPS watch for questionable network activity by using signature-based rules that search for predetermined patterns in network activity or by analyzing network traffic to identify deviations from the baseline. An IDS is able to identify anomalous traffic but does not block the traffic, while an IPS blocks traffic based upon a predefined set of rules. IDS/IPS in the cloud works similarly to an on-premises device. Many IDS/IPS vendors offer cloud-based solutions that security teams can deploy easily to protect against cloud-based traffic. Some vendors allow organizations to connect their cloud IDS/IPS deployment to their on-premises solution so that users have a single, comprehensive view [43].

8. Conclusion.

Cloud computing is a new way of delivering resources to users as a "service" over the Internet. Cloud consumers no longer fully own the infrastructure that these service providers control, as opposed to traditional approaches based on the ownership of the hardware that stores the data. You can sync cloud storage with your smartphone, tablet, or other mobile devices for easy access on the go by simply subscribing to it and uploading your files. Cloud computing is a computing model that provides on-demand network access to a custom pool [46].

Computing resources such as networks, services, storage, and applications that can be provisioned and released quickly with minimal effort by an administrator or service provider. Cloud computing is a new concept that allows users to access scalable and virtual resources such as bandwidth, software [47] and hardware on demand. Although this issue has received a lot of attention in recent years, the issue of privacy and data security is one of the main obstacles to the development of cloud computing. In this article, we looked at several of the significant security risks of cloud computing environments [48] from different perspectives, as well as decisions that all users and companies should be aware of when deciding whether to use the cloud or not. This work contributes to the discovery of solutions to security and privacy issues in cloud storage that have been identified in other technologies, and to the development of a new solution or approach [49] for securing the cloud.

9. Future work of cloud computing

In this paper, the researchers proposed a number of ways to protect data and achieve the highest level of data security in the cloud. However, there are still many gaps that need to be filled in to make these methods more effective. More work is required on cloud computing to make it acceptable to cloud consumers. This paper explored different technologies related to data security and privacy, with a focus on storing and using data in the cloud to protect data in cloud computing environments and build trust between cloud service providers and consumers.

10. Suggestions

Some cloud computing services will be made by the GOSI through cloud computing platforms for businesses where researchers have chosen Amazon. In 2002, Amazon launched its first cloud called the Amazon Web Services cloud, which contains cloud-based cloud services and AWAS. The tools necessary to work for your datacenter or company specific and the appropriate instance and booking Servers specifications you want as well as booking the databases of the type you want to provide several types of databases as well as work portfolio is the name that launched Amazon to back up of the data of the entity or company to which the service is performed.

There is no doubt that Amazon is the most important company in the field of cloud and distinctive in this company that it maintains its spirit of innovation as it always works as an emerging company in the market and Duma looks forward to step forward, becoming one of the largest companies that change the technology industry in general.

- Amazon provides an easy way to access servers, volumes, databases and a variety of service applications that work online.
- The Amazon service provider maintains and owns the network - in addition to the equipment needed for such service applications while you select and use exactly what you want through a web-related application.
- Amazon's cloud service provides a flexible, low-cost way to access the IT resources needed to support the diverse operations of e-business.

• More secure and reliable than any other provider due to global reputation and good reputation.
• Providing a large number of computing services in all fields in the fields of databases, networks, applications and storage.
• Unlimited storage.
• The flexibility to change the area and expand in a short time, where it is ordered in a few minutes.

11. References

[1] Al-Thobhani, dr.Nashwan S A E E D ghaleb. "Implementation of Cloud Computing in the General Authority for Insurance and Pensions." Al-Andlus University 1 (2017)., https://scholar.google.com/citations?view_op=view_citation&hl=en&user=cazJ2ncAAAAJ&citation_for_view=cazJ2ncAAAAJ:3fE2CSJIrl8C

[2] *Hassan, Qusay (2011).* "Demystifying Cloud Computing" *(PDF). The Journal of Defense Software Engineering. CrossTalk. 2011 (Jan/Feb): 16–21.* Retrieved 11 December 2008.

[3] Parkhill D (1966) The challenge of the computer utility. AddisonWesley,Reading

[4] Qi Zhang , Lu Cheng and Raouf Boutaba (2010) Cloud computing: state-of-the-art and research challenges J Internet Serv Appl 1: 7–18.

[5] NIST Definition of Cloud Computing v15, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[6] Mr. Mukesh Kumar, and Niraj Kuma (2016) cloud computing: architect and use of technology in the past, present and future v1, http://www.ijrets.com/wp-content/uploads/2016/08/160314084-11.pdf

[7] The NIST Definition of Cloud Computing. Retrieved November 1, 2015, from National Institute of Standards and Technology website: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[8] Amazon Elastic Computing Cloud, aws.amazon.com/ec2

[9] Cloud Hosting, CLoud Computing and Hybrid Infrastructure from GoGrid, http://www.gogrid.com

[10] Ghemawat S, Gobioff H, Leung S-T (2003) The Google file system. In: Proc of SOSP, October 2003

[11] Salesforce CRM, http://www.salesforce.com/platform

[12] Dedicated Server, Managed Hosting, Web Hosting by Rackspace Hosting, http://www.rackspace.com

[13] SAP Business ByDesign, www.sap.com/sme/solutions/businessmanagement/businessbydesign/index.epx

[14] Google App Engine, URL http://code.google.com/appengine

[15] Windows Azure, www.microsoft.com/azure

[16] Virtualization Resource Chargeback, www.vkernel.com/products/EnterpriseChargebackVirtualAppliance

[17] Thomas Sommer, Tanya Nobile, Paul Rozanski (2012) The Conundrum of Security in Modern Cloud Computing V12, scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1197&context=ciima context=ciima

[18] Saleem (January, 2011), cloud computing efficient on enterprise in terms of cost and security, Master Thesis Size: 89 Pages, https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1764306&fileOId=1764311

[19] Amazon EC2 Pricing, aws.amazon.com. Retrieved in 10/09/2017, http://aws.amazon.com/ec2/pric

[20] Arijit Ukil, Debasish Jana and Ajanta De Sarkar, " A SECURITY FRAMEWORK IN CLOUD COMPUTING INFRASTRUCTURE", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, pp. 11-24, September 2013.

[21] Dr. Nikhat Akhtar, Dr. Bedine Kerim, Dr. Yusuf Perwej, Dr. Anurag Tiwari, Dr. Sheeba Praveen, "A Comprehensive Overview of Privacy and Data Security for Cloud Storage", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 5, pp. 113-151, September-October 2021. Available at doi: https://doi.org/10.32628/IJSRSET21852,Journal URL : https://ijsrset.com/IJSRSET21852.

[22] R.L. Rivest,L.Adleman and M.L. Dertouzos,"On data banks and privacy homomorphisms," Foundations of Secure Compu-tation,vol.4,no.11,pp.169–180,1978.

[23] Yunchuan Sun, Junsheng Zhang, Yongping Xiong and Guangyu Zhu, "Data Security and Privacy in Cloud Computing", International

Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages http://dx.doi.org/10.1155/2014/190903.

[24] C. Gentry, A fully homomorphic encryption scheme [Ph.D. thesis], Stanford University, 2009.

[25] D. Boneh, “The decision Diffie-Hellman problem,” in Algorithmic Number Theory, vol. 1423, pp. 48–63, Springer, 1998.

[26] A. Kaur and M. Bhardwaj, “Hybrid encryption for cloud database security,” Journal of Engineering Science Technology, vol. 2, pp. 737–741, 2012.

[27] D. Manivannan and R. Sujarani, “Light weight and secure database encryption using tsfs algorithm,” in Proceedings of the International Conference on Computing Communication and Networking Technologies (ICCCNT '10), pp. 1–7, IEEE, 2010.

[28] F. Pagano and D. Pagano, “Using in-memory encrypted databases on the cloud,” in Proceedings of the 1st IEEE International Workshop on Securing Services on the Cloud (IWSSC ’11), pp. 30–37, September 2011.

[29] Y. Rouselakis and B. Waters, "Ef_cient statically-secure large-universe multiauthority attribute-based encryption," in Proc. Int. Conf. Financial Cryptogr. Data Secur., pp. 315-332, 2015.

[30] M. A. AlZain, B. Soh, and E. Pardede, “Mcdb: using multiclouds to ensure security in cloud computing,” in Proceedings of the IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC ’11), pp. 784–791, 2011.

[31] C. P. Ram and G. Sreenivaasan, “Security as a service (sass): securing user data by coprocessor and distributing the data,” in Proceedings of the 2nd International Conference on Trendz in Information Sciences and Computing, (TISC '10), pp. 152–155, IEEE, December 2010.

[32] M. Asad Arfeen, K. Pawlikowski, and A. Willig, “A framework for resource allocation strategies in cloud computing environment,” in Proceedings of the 35th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW ’11), pp. 261–266, July 2011.

[33] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: a high-availability and integrity layer for cloud storage,” in Proceedings of the 16th ACM conference on Computer and Communications Security,pp. 187–198, ACM, Chicago, Ill, USA, November 2009

[34] K. Benzidane, S. Khoudali, and A. Sekkaki, "Autonomous Agent-based Inspection for inter-VM Traffic in a Cloud Environment," in 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012), London, 2012, pp. 656-661.

[35] X.-Y. Li, Y. Shi, Y. Guo, and W. Ma, "Multi-Tenancy Based Access Control in Cloud," in International Conference on Computational Intelligence and Software Engineering (CiSE), Wuhan, pp. 1-4, 2010.

[36] S.-J. Yang, P.-C. Lai, and J. Lin, "Design Role-Based Multitenancy Access Control Scheme for Cloud Services," in International Symposium on Biometrics and Security Technologies (ISBAST), Chengdu, pp. 273-279, 2013.

[37] A. Jasti, P. Shah, R. Nagaraj, and R. Pendse, "Security in Multi-Tenancy Cloud," in International Carnahan Conference on Security Technology (ICCST), , San Jose, CA, 2010, pp. 35-41.

[38] Ronald Beaubrun and Alejandro Quintero, "A Secure Access Control Architecture for Multi-Tenancy Cloud Environments', CLOUDCOMPUTING 2021 Twelfth International Conference on Cloud Computing, GRIDs and Virtualization, ISBN: 978-1-61208845, April 18 -22,2021, pp. 48-53.

[39] S. J. De and S. Ruj, “Efficient Decentralized Attribute Based Access Control for Mobile Clouds,” IEEE Transactions on Cloud Computing, Vol. 8, No. 1, pp. 124-137, 2020.

[40] P. Mahajan, S. Setty, S. Lee et al., “Depot: cloud storage with minimal trust,” ACM Transactions on Computer Systems, vol. 29, no. 4, article 12, 2011.

[41] A. J. Feldman, W. P. Zeller, M. J. Freedman, and E. W. Felten, “SPORC: group collaboration using untrusted cloud resources,” in Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (OSDI ’10), vol. 10, pp. 337–350, 2010.

[42] D. Wang, D. He, P. Wang and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment", IEEE Trans. Dependable Secur. Comput., vol. 12, no. 4, pp. 428-442, 2015.

[43] Kevin Garvey, How to Protect Enterprise Systems with Cloud-Based Firewalls, July 2019.

[44] Yasir Saleem, Muhammad Munwar Iqbal, Muhammad Amjad, Muhammad Salman Bashir, Muhammad Faisal Hayat, Muhamamd Farhan, Amjad Farooq, Abad Ali Shah. High Security and Privacy in Cloud Computing Paradigm through Single Sign On. Life Sci J 2012;9(4):627-636] (ISSN:1097-8135). http://www.lifesciencesite.com. 96.

[45] Rasavarna, Medu & Karlapudi, Medu. (2020), "Security in cloud computing", 10.13140/RG.2.2.29168.28163.

[46] Yusuf Perwej, "An Experiential Study of the Big Data," for published in the International Transaction of Electrical and Computer Engineers System (ITECES), USA, Vol. 4, No. 1, page 14-25, March 2017, DOI:10.12691/iteces-4-1-3.

[47] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M.L. Stefanizzi, et al., "An iot-aware architecture for smart healthcare systems", IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515-526, 2015

[48] Nikhat Akhtar, Firoj Parwej, Yusuf Perwej, "A Perusal of Big Data Classification and Hadoop Technology", International Transaction of Electrical and Computer Engineers System (ITECES), USA, Volume 4, No. 1, Pages 26-38, 2017, DOI: 10.12691/iteces-4-1-4

[49] Y. Zhang, "Research on the security mechanism of cloud computing service model," Autom. Control Comput. Sci., vol. 50, no. 2, pp. 98-106, Mar. 2016.

[50] Al-Thobhani, Nashwan Ghaleb, and Naser Al-Maweri. Building A Secure Internet Banking Environment for the Bank. No. 4975. EasyChair, 2021. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=cazJ2ncAAAAJ&citation_for_view=cazJ2ncAAAAJ:YOwf2qJgpHMC