International Journal of Engineering & Technology, 7 (4.29) (2018) 239-246

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Privacy and Security of Cloud Computing: A Comprehensive Review of Techniques and Challenges

Marwan Adnan Darwish [1]*, Eiad Yafi [2], Abdullah H. Almasri [3], Megat F Zuhairi[4]

[2,1] University Kuala Lumpur, Malaysian Institute of Information Technology
[4,3] Unitar International University
**Corresponding author E-mail:Marwan.khabbaz1@gmail.com*

Abstract

Cloud computing usage is rapidly increasing in a various range of services and it is seen on trend to revolutionize the way the IT companies doing businesses. The recent advances in mobile, social media companies and online businesses have given rise to success and propagation for the environment of the cloud. However, When uploading the users' data from the local device to the nature of the cloud that considered as a third party , major challenges cloud-computing model jeopardizes privacy and security issues and threats on data security and reliability. These threats constitute data breaches, loss of control, unauthorized uses at the different layers of the cloud models and these issues hinder the adoption of cloud and slow down acceptance in many sectors in IT. In this review, we present and summarize major articles in cloud computing and its multiple layers with a focus on security and privacy challenges (such as integrity, confidentiality and data privacy). We also intend to review the latest approaches regarding identity management inside the cloud, cryptography and steganography techniques that have been used inside the cloud platforms.

Keywords: *Cloud computing ; Privacy ;security ;identity cloud management ;cryptography; steganography*

1. Introduction

At the beginning of the 19th century, the computers were huge in size and needed large rooms to put with refrigerating capacity and the processing output was very limited. However, the invention of transistors and processors led to mini-computers with high and efficient computational output. The magnitude of computing had increased in the last century with transforming the infrastructure into a distributed systems form to guarantee more efficient and fast processing [1]. Therefore, the limitations of the traditional local components that prevented users from accessing and storing data online (ex: video conferencing, online surfing). Furthermore, the increasing of cost of the hardware and software were all important factors impacted the Cloud Computing development. The term “cloud” was coined in 1994 [67]. Cloud computing is a new generation dream as a utility because of transforming the software to more attractive way and present it as a service to change the form of IT industry and designing IT hardware and purchased [2]. NIST defined the cloud environment concept [3] is "an enabling ubiquitous model, provides network access based on demand and offers a convenient aid of collection of configurable resources like servers, networks and storage applications, various services, which has the ability to be quickly provisioned and released with minimum effort from service provider interface or minimal management effort". Besides the potential of cloud-computing concept, its model has been facing critical challenges which is the absence of standards to preserve the users' privacy [13]. Many organizations are reluctant to take full advantage of the benefits that have given from the cloud services, with the reason of the main concerns about the privacy of data and illegal access and uses and are hesitant to trust the cloud's providers to overcome the privacy obstacles. According to D. Chen and H. Zhao [74], the critical impediment to transferring data and relying on the cloud services are information privacy and security issues. Also , N. Vasanthi et al, [81] claimed that the major barriers in front of the growing of cloud environment from IT industry and consumers is privacy concern and the absence of efficient and standard evaluation mechanism for privacy preservation . Many data breach incidents took place in recent history. Some of the familiar examples: 1) The Sony PS (PlayStation) was hacked by external intrusions that led to interrupt the network 1 and steal sensitive and personal data from around 77 million accounts. 2) a few days' downtimes at Drobox [23,21] which allowed the visitors temporarily to sign into 25 million accounts due to a problem of misconfiguration 3) Private photos for celebrities have been leaked from Apple ICloud (2014) because of the poor protection inside the login credentials [24]. Furthermore, a report conducted by the FTC (Federal Commission) mentioned that users' private data had been used systematically by cloud providers for collection and analysis without owners' permissions, for example, cloud service providers (CSP) share the information about users that have diabetics because they are able to detect those users by their interest in sugar-free products and then insurers classify these users as a higher risk [25]. In addition, 39% of companies (57% of large enterprises) that used cloud services stated the main issue is the data breaches that have an impact on the security standard for adopting and using of cloud computing services in the EU statistics [20]. CSA (cloud security alliance)has done an investigation about the weak points in the cloud environment and released an analysis about the main problems [14, 12] and revealed the main threats of adopting cloud services, the threats were : 1)Insecure application programming interface 2) Malignant insiders 3) Data leakage. On the basis of architecture, cloud services are divided into three service models classified in the order 1)Software as a Service (SaaS),2) Platform as a Service (PaaS) and 3)Infrastructure as a Service (IaaS) and

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

four deployment models classified in the order : 1)public cloud, 2)private cloud, 3)hybrid cloud and 4)community cloud [10,11].

2. Architecture of Cloud Computing

Cloud environment is a model that provides access to a customized platform for a shared resource set such as : (services, storage, servers, and networks).This access can rapidly be granted with minimal effort and easy connect to service provider. The biggest benefits of cloud is automation so when the organization use the cloud layers it clearly lead to minimizing the cost and time spent on hardware and instead focus on innovation on application and take advantage on cloud strategies .

2.1 The Service Models

The service models mean the reference of a cloud computing that indicates which cloud environment relies on and works. These models can be classified with three basic layers as listed below. SPI is an acronym for the service models that defined as SaaS, PaaS and IaaS as explained in figure 1.

2.1.1 Software as a Service (SaaS)

It is used to rent services as a software. The applications installed on cloud by cloud providers can be used with no need to install any application or tools on the local desktops [4]. It is giving the user on demand ability via internet to use the software and its functions remotely [80]. SaaS is quite similar to the application's providers (ASP) and delivery services on cloud where the service provider hosts the customers' software and delivers back the software to end-user. In this layer the provider hosts the software and gives the access to the customers to reach and access the application on the network , while the core code of the software is same for all customers but each one access to his specific copy of application. So when there are some updated functions or features, they are rolled out into the source application for all customers regarding SLA (Service Level Agreement) [66]. Examples of Software as a Service providers are: Google App, Concur, Zendesk and Dropbox

2.1.2 Platform as a Service (PaaS)

This layer offers more features like providing tools for development, deployment, and management for the applications. This will help the developers to develop their apps without worrying about the maintenance or resources capacity. [76]. The PaaS is considered as the medium used to create applications. PaaS providers rely on key services, such as application hosting or Java development. It offers an optimized environment for the users to install their applications and datasets [80]. For example: Aprenda and Red hat openshift.

2.1.3 Infrastructure as a Service (IaaS)

It represents the back-end service and located at the bottom of the cloud environment and refers to the physical hardware equipment. This layer deals with the memory, data center (DB), virtual machines (VMware), processors, network components like routers and switches. [80]. It is used to deploy and develop the layers SaaS and PaaS. Furthermore, it provides a set of physical services that helps users to maintain their application and evaluate its performance by giving them different components like load balancing, firewall, log monitoring, mirroring for backups and data recovery. For example, Amazon offers (EC2) "The Amazon Elastic Cloud Computing Service" where virtual servers can be selected and configured by users and many interfaces can be used by having the ability to run difference operating systems on the Internet within minutes.

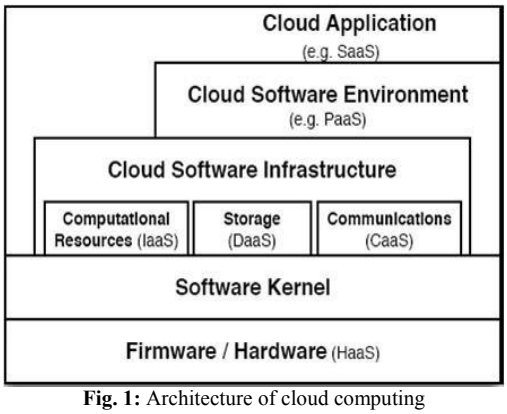


Fig. 1: Architecture of cloud computing

2.2 The Deployment Models

The deployment models refer to the location of cloud provider and mainly how users/ customers access the machines with different types of access: Public, Private, Community and Hybrid (See figure 2).

2.2.1 Public Cloud

This type of deployment model is used and accessible by public users or an industry groups to use the services offered by the cloud service provider [76]. An example of public cloud is Microsoft, Amazon and Google. The users here can access the services on the internet in which there share the identical architecture but with different constrained configurations and separation between the shared resources. This model follow the principle of pay-per-use. Although it is highly exposed for attackers, invaders and data breaches [6].

2.2.2 Private Cloud

Private cloud means the infrastructure is given to specific company or organization managed by multi customers, however it is much expensive compared to the public model [82]. In this model, users gain a specific data centre to share and store their confidential data privately. The data centre in this model guarantee the organizations/users a no participatory working environment in contrast to other models such as OPENStack [8].

2.2.3 Community Cloud

The infrastructure in this model allow services to be shared with a bunch of organizations that have the same concerns so they can share the same infrastructure [9]. For example, all government organizations in Washington may share the use of same cloud infrastructure to collect and process the data that belongs to the citizens who are living in the same state in America [76].

2.2.4 Hybrid Cloud

This type of cloud consists of different deployment cloud models (community, private, or public). The combination of models leads to having unique entities needed by users/organization to be used for multiple purposes in compliance with the standards technology [85]. The hybrid model is the most common design among the others. However, it is more secure and organized than public cloud when it comes to access the structure online. In addition, the Hybrid offers multiple benefits from the other types of cloud deployment models.

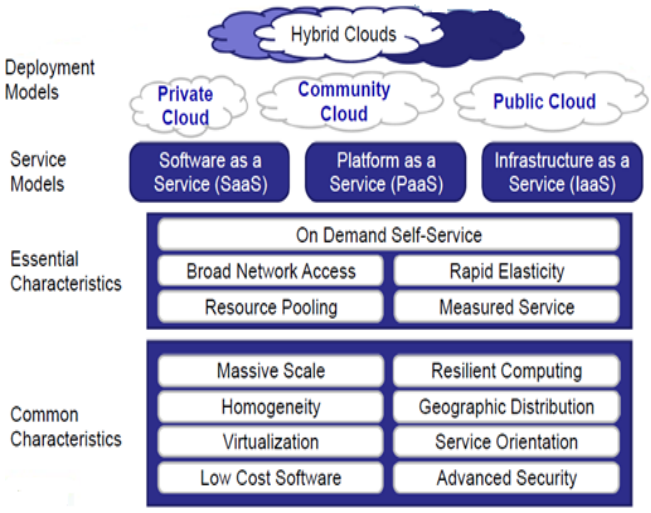


Fig. 2: General scope of cloud deployments models

3. Methodology

The methodology used in this article comprises the collection of journals and conference papers in the cloud computing domain with focus on privacy and security. Eighty-six papers published between 2000 and 2017 were collected and classified into three main categories IEEE, Science-Direct and Scopus. Further analysis was carried out by classifying the articles into three other categories named: Security, Privacy, Technologies. The method used in this review includes the following main steps: 1) Studying the background of cloud computing and analyzing the architecture of cloud environment, 2) Revising previous literature review and issues that related to the cloud environment 3) Analyzing cloud-computing challenges and issues by classifying them into privacy issues and security issues. Detecting vulnerabilities of cloud computing model was also included 4) Reviewing the approaches and techniques applied in the literature to tackle the cloud issues. Table 1 illustrate the number of articles used in the review and the classification of papers into different categories.

Table 1: Number of articles and classification

Article / Headlines	IEEE	Science-Direct	SCOPUS
Privacy	38	19	5
Security	15	8	5
Solutions	10	8	3

4. Data Privacy and Security Approaches

Here are some of the approaches and techniques that have been used to tackle and enhance the level of security and privacy on cloud computing environment with different categories including identity cloud management, cryptography and steganography methods:

4.1 Identity Cloud Management

Identity management describes the authentication, authorization, managing individual's identities and permissions. The main goal of IDM is to enhance and increase security and privacy. To achieve this, systems require a trusted third party that fails to work on untrusted hosts. The first approach in data privacy was building **PRIME** (Project for privacy and identity management) – PRIME was developed between 2004 and 2008 and funded by EU (European Union) [45]. The project strived to enhance the privacy level by developing a prototype system for identity management, which strived to reduce the users' need in fully trust with other parties. This project was concerned to secure the interaction to track the user's data with the proliferation of sensitive data from users [46]. PRIME gave a new solution of the implementation of the agreed data depending on the handling policies. Another approach called **PRIMELIFE**– The PRIMELIFE project was developed between 2008 and 2011 [47] and it is cooperation between (IBM, W3C, Microsoft, and others) with some institutions from Europe. This project focused to understand the identity systems for the practical side, like enhance the privacy on the web applications by developing tools to manage the identity on the cloud computing platform[48]. However, PRIMELIFE has shown privacy technologies so the users can execute their legal rights on their personal and sensitive data. Another approach was named **ABC4Trust** – was developed between 2010 and 2015. ABC4Trust is a research and development project funded by European Union (EU) promoting the federation and exchange between supporting technologies of trust while maintaining the confidentiality of users' credentials (ABC , Privacy concept)[49]. Anonymous credential was proposed by this project to ensure the privacy for the users and using of tough policy. Identification profiles are used by access model for authentication and ensure the privacy for each user, which requires proper devices for participants entry [50]. **GÉANT**- was developed between 2015 and 2016. This project was managed from association of members in Netherlands and UK(United Kingdom).GÉANT helps to deliver innovative networks and technologies in Europe. The current research and education networking group named by GN4-1has done research about the identity and trustworthiness technologies called (JRA3) [51]. A project named by OIDC (Open-ID Connect) aimed to integrate different types of existing federation technologies to authenticate the username and password license[50]. **PRISMACLOUD** (Project for security and privacy in the cloud) –was developed between 2015 and 2018. PRISMACLOUD has funded by the EU's Innovation program [52]. This study focused on three substantial concerns: users-privacy that adopting cloud computing environment, data confidentiality and verifiability of the services based-cloud computing. The purpose of this research to develop accessible and novel cryptographic tools to ensure the security and data privacy for the cloud's customers from being stolen or disclosure during the lifecycle phases inside the cloud storage for users and cloud service providers. Specifically to develop an efficient storage solution to conserve the data privacy and integrity. This project was proposed to apply different strategies such as data minimization and data anonymization. Different use-cases will be implemented to assess the project results. **CREDENTIAL** – was developed between 2015 and 2018 .Credential research aimed to develop friendly ways to secure the data in the storage phase and sharing process and to keep the level of privacy for users. It also aimed to provide a service system for identity and access management to support the certified identity. The main idea beyond CREDENTIAL to develop crypto-graphical solutions to preserve user's data from being stolen or misused. which means to manage the identity first by specific credentials then cryptography algorithms. This project funded by the EU's Innovation program [53]. **PRAIS (Privacy Impact Assessment):** Project to assess strength Privacy, developer By scientists in University of London and experts Protect children from coram and teachers Information Technology From Logica UK [78]. **HPPA(Hewlett Privacy Advisor),** is a data discovery system from business operations to increase the level of privacy that helps organizations overcome privacy issues [79].

4.2 Cryptography Methods

Cryptography means to secure the communication between two parties while sending and receiving data to obfuscate the data from the adversaries and to transmit data privately between the parties and Cryptography stands for Greek word "Kryptos" [75]. Cryptography schemes use different types of theoretic concepts like factorization or discrete algorithms to generate digital signatures and secretly key exchange. Public- key cryptosystems is used because

the large key-sizes are unbreakable ordinary computers, supercomputers or special hardware. There are three types of algorithms: 1) Symmetric(Private) Key Cryptography, This algorithm uses one private key for whole the algorithm steps starting with encrypting data and ending with decrypting it. When the data sent between A(source) and B(destination) the encryption phase will use the private key to cipher the data and keep it privately[54], then when the cipher data arrives at the destination the algorithm will decrypt the data using the same key to obtain the original data. For example (AES, DES, BLOWFISH, RC6). 2) Asymmetric(Public) Key Cryptography, This algorithm will use unique pair of keys, When the data sent between A(source) and B(destination) the encryption phase will use the public key to cipher the data and keep it privately ,then when the cipher data arrives at the destination the algorithm will use the private key to decrypt the data to extract the readable data. Both pair keys are mathematically linked. For example (RSA, ECC) [55]. 3) Hash Cryptography - The hash function cryptography , this algorithm will take different types of entry as an input and the output data will always be the same fixed-size block and it called one-way encryption because there is not decryption phase . It is known as fingerprint of the data or one-way encryption. For example (MD5, SHA1, etc.) [55] Furthermore, additional tools have been developed and used to transform data from clear form to obfuscated form before uploading it into the cloud machines and decrypt it on the local PC: 1) **Boxcryptor** uses the local computer for the encryption the files locally at the client end before uploading to the cloud by using virtual drive as a medium for the process It uses the AES-256 private-key and RSA public-key algorithms. 2) **Veracrypt** is a free software for establishing encrypted volume (OTFE)by creating virtual disk inside the file or inside the storage device. The software uses AES-128 bit, Serpent and two fish encryption algorithms for data encryption. 3) **AxCrypt** it is an open source software for encryption on windows operating systems. This software used for compression, encryption, decryption with single files or folders easily integrated to windows. it uses AES-128 key in CBC mode after initiating random IV for encryption and then using a hashing algorithm for authentication using SHA1-128 and the key for integrity. 4) **SpiderOk** uses a layered approach for encryption, using a combination of RSA-2048 bit key and AES-256 bit key.

4.3 Steganography

It is the art of hiding the data. In the process of steganography, we hide the secret message within an ordinary or chosen one (image, video, text and audio) and extract the message in the destination. There are three categories of steganography: Public key steganography, private key steganography and pure one . the benefits of the steganography overhead the cryptography that the messages do not catch the attention by the third party. Sending and storing data using steganography technique is very safe on web. We summarize here the latest work related to steganography methods: Marwa E. Saleh [83] proposed a hybrid technique for data security and reliability. Firstly, the technique uses AES cryptography algorithm to encrypt data then steganography to hide the secret message using PVD_MPK. Alok and Bhonsle [84] investigated ways to secure data inside the third party(cloud) as it proposed to encrypt the data using AES algorithm then applied hash function on hash based least bit for the cover image to produce steganography image. Suhad Shakir Jaber [64], introduced schema that combines the two methods cryptography and steganography by using AES algorithm for encryption then, PRT_PVD steganography method to hide the output of encryption process.

5. Privacy Challenges

As mentioned earlier, the critical issue on cloud is privacy and data reliability. Privacy in the Cloud Computing denotes different types of private information like :

(a)Personal Information (PII) : this kind of information define the person's identity for sure (name , national identity number , phone number ,...etc.)[5].(b)Sensitive information : like private information (membership , demography , health insurance , ...etc.) [27]. This information must be guaranteed in cloud storage where services are executed instead of cloud's customers like storage and processing operations on the storage device that the clients do not control. This model is a ubiquitous and adopted in new technologies of IT industry. The user uploaded the data to the cloud, which means that the data after uploading will be in clear on the storage machine that users do not own. This situation led to serious privacy challenges. The risk of data to be disclosed from the storage devices, by fraudsters clerks or from hackers or attackers to steal sensitive data from the machines. Maybe the customers of the same service steal the data from other users if the isolation is not adequate between services in the same virtual machines that hosted inside the cloud computing environment[26, 22]. In some countries where data is stored, governments can access data legally to view it under some circumstances. In this case may the data leaked to some untrusted parties. Selling data is like business trend on cloud to get profits and revenues after sharing the data with marketing and advertisements companies. [77**]**. The following key privacy challenges should be carefully addressed: 1) Data Confidentiality: confidentiality is an agreement with constraints among the service providers and owner of the data to retain sensitive data secrets inaccessible from unauthorized uses. It keeps the data secret and not exposed to any unauthorized parties. In addition, outsourced data are stored far away from users management on cloud machines, out of their control or manage [7]. Data confidentiality is an essential concept for the customers to use the cloud and move their data to this new model [62]. Providers use different ways to retain data like capture images for VM, backups, and logs because data is stored in different locations according to its server [61]. The shared storage is used by different users or clients to share their data and applications. In this situation, the problem of lack of confidentiality arises because of malicious attacks or system failure[62]. Furthermore, most cloud users in the SaaS model are always worried about their confidential data as it can be used for illegal motives [68]. 2) Data Integrity: the concept of data integrity that achieves the completeness and accuracy of the data. Users of the cloud expect that their outsourced data on the remote storage machines is correct and stored without and misused attempts. In another word, it should not have tampered or deletion by a third party [7]. This is a new challenge on this model platform. Securing data without fabrications or maliciously deleting to gain integrity from the CSP. This attribute is easy to get on the independent system, not like the cloud, it is hard to get because a cloud is contained by multiple operating systems, servers and databases [58, 59]. This attribute is very essential in any system whatever it was. We can acquire this attribute in a single database belong to the single system, but very hard to achieve because of the magnitude of computing on distributed systems. Is it worth mentioning that data integrity is always managed via database transactions [69]. 3) Data Acquisition: That means a mechanization to obtain data from different hardware devices (using suitable tools or technologies to accumulate the results of data). Cloud users and service providers should aware about P2P operation , the streaming of the data and data access[60]. The fear from intruders to obtain data illegally during the data collection(during the processing on data before storing it or when it already stored inside the hardware). 4) Loss of Control: As long as the users are adopting the cloud services, so their data will certainly be possessed by the third party [58].In this case, the user's control is limited because if he wants to transfer the data from the current provider to a different one, the data will be vulnerable to tamper or misuse attempts and this shows the loss of user's control of his data [72]. 5) Data Exposure: The data that is outsourced into cloud machines are more vulnerable to be disclosed from adversaries or hackers. The number of hackers is increased, such as fraudulent employees inside the cloud providers, Revocation of members from different

groups or even rogue administrators. In addition, because of the servers that located in some countries and due to the law that allowed the government to access the users' data without their permissions may lead to data exposure[7]. 6) Unauthorized Access and usage: This matter is not insignificant because of the importance to grant rights to users and revoke them back. However, data access in cloud environments need flexible rights and distinguishability policies between different users. Various users belonging to dynamic groups can share the data between them. The problem here is to find the proper repeal methods to avoid the unauthorized usage [7]. Also, the cloud providers may collect data for junk ads and share this information with different companies or competitors even when the users do not want to expose their data publicly to get commercialization profits [76].7) Data loss and manipulation: Cloud providers claim to use redundancy and mirroring to make multiple copies of the data to protect against data loss [59]. In addition, the data is stored separately across different places of storage to avoid hardware failure. However to reduce storage and operation costs may rogue administrators of the cloud might intend to ignore the other copies from the redundancy and this is cost data losses and errors. This traitor way may expand the data into a very large magnitude of data (i.e data stored without users' awareness)"[7]. The data can be accessed through weak configurations of accounts , so the attacker will perform different attacks to manipulate data and data theft [12]. 8) SLA-Violation: SLA means the Service Level Agreement between service providers and clients depends on a contract signed between them that included two types of services functional and non-functional [7, 9]. SLA recognizes obligations, service prices and penalties in case of violation of the convention. However, because the metaphysical of the cloud environment the violation of the service agreement is multifaceted [10, 11]. 9) Invaders Attacks: may the attackers exploit the security vulnerabilities to recover the data after deletion process [13]. the report that have conducted by the Verizon stated that the external intrusions comprise the critical troubles for data privacy by (73%), with less impact. Because of the vulnerability virtualization can increase the chances of data breaches result [70]. On other hand, may the attackers detect the stream on data collection between the providers and users to hack the data illegally. 10) Lack of consumer trust: (70%) of citizens of Europe are worried about data privacy protection on the cloud platforms as a result of a survey on European citizen on data privacy [71]. Another survey conducted in 2012 on cloud industry investigating consumers trust revealed that (28%) of the sample do trust reputation for providers, (26%), trust in a third party, (21%) trial experience, (19%) contractual, (6%) others [41]. That is why it is very important for users to have trust in their cloud provider to store data on its storage without any doubt. Unfortunately, users still do not fully trust to store their sensitive data as they afraid of misuse or steal of their data. Because of that, cloud providers should build a trust relation with its users [72]. 11) Data Breaches: Data Breaches means loss of privacy, trust and SLA policy violation between clients and cloud service providers. The external intrusion may lead to data loss or when the disk drive dies without making any backups copies. This breach may affect web applications, so the attackers will take the advantages of permissions in the implementations of the cloud [43]. At the end, the chances of data breaches are increasing day per day. Furthermore, Intel report titled Blue Skies Ahead has shown that the perception and reality: 1 in 5 participants indicated that their main concern is the data breaches in Software as a service (SaaS). Data breaches are very critical to be tackled especially on infrastructure as a service (IaaS). Although, results show that (23%) know about the security breaches from the cloud machines[56]. 12) Data Privacy: user privacy is the major challenge that is facing the cloud model on the users' confidential data or applications that moved from local devices to heterogeneously distributed cloud servers to gain the benefits from cloud services. The privacy means to protect the data information and ensure the stability between different accesses to outsourced data [7, 39]. The servers of cloud located in several places and owned by multiple services providers. So, The privacy challenges are in the providers' hands because the users can manage or control the data center where the data is stored, so the only side that is responsible for the privacy level is the cloud service providers [44].The users should be confident that the data is secured and private by the cloud providers and nobody can't access the data without granting a right to be authorized [63, 57]. Nowadays a recent survey was conducted in 2015 interviewed 675 decisions makers who belong to different countries stated that the organizations now are focusing more on privacy, security, CRM, and trust [42]. 13) Multi Tenancy: multi-tenancy refers to multiple users can use the same architecture, storage, and services as a tenant with some constraints from the providers. In spite of the shared architecture, the attacks still arise using malicious injection code in the packet header to expose and steal the data . Those attacks may lead to data errors and identity theft from the data center of the cloud machines. [62, 56]. 14) Data availability: This expression means that the data is always available anytime and anywhere for all data owners without any problems or limitations. In the cloud case, the data availability property may not be guaranteed one hundred percent. So the users are worried about the data center that located in different countries, and the cloud providers are subject to enforce laws for some countries. The best solution to this issue that all procedures should be transparent for the data owners [73, 37].

6. Security Challenges

The security issues in the cloud related to the communication between the customers from one side and the cloud machines on the other side. The cloud provider should ensure the data security and privacy to gain the trustworthiness from the customers. The data packets that uploaded from the customers to store and process it inside the cloud And vice versa ,data can easily be tracked and stolen from the attackers because of the untrusted environment of the internet. The cloud is susceptible for different ways of attacks and thefts [65]. The last twenty years of information and communication technologies development witnessed fundamental security flaws such as Spectre and Meltdown. These vulnerabilities allow programs to steal data from memory on processed hardware. Spectre and Meltdown are still considered critical problems in the modern processors. Normal programs have prevented from reading or accessing data from different programs, in contrast, the malign software could gain data from memory like Spectre and Meltdown could expose the data from current programs that are running on physical memory. This information may contain password, personal photos, emails or even business documents. Spectre is security vulnerability that encourage the customers to do some operations during the programs running that should not be run with the correct path of the program source code and may be led to leaking the data to the adversary. Spectre is all about breaking the isolation between the applications for different users[86]. On the other hand, Meltdown refers to break the isolation inside the CPU's memory. So it will allow unauthorized operations to gain the data in the kernel space, such as entire memory in Linux, OSX and a big portion of the memory on Windows. This attack breaks the isolation between the applications and the operating systems to gain sensitive data from the memory [85]. Network attacks can be classified into the following:

i. Port scanning: A port may be checked on a server to detect the service status that being performed on the goal device. Scanning of the port needs an access via a network that hosts the objective device. This attack used to expose the gaps in the goal device leading to denial-of-service [28]. This attack uses DOS to interrupt the service during the server port by listening on which ports are available and then sending packets to server machine to get an idea about the OS and the services that have used on.

ii. Botnets: A botnet word formed from the word 'robot' and 'network' is used to steal data using special Trojan viruses from a host machine. The botnets can reach the victim device illegally from the downloading of some software or maybe installing Trojans without realizing that. These botnets will crawl from the internet to the local device trying to exploit and expose the users' data and hack the data automatically. When the botnet is successfully downloaded, it will immediately connect with the master-computers (bot-master) to give them the sign to start stealing the sensitive data [29].

iii. Spoofing attacks: This attack means to impersonate with fake IP address trying to gain the sensitive data and harm the user's privacy. A faked IP will manipulate the original IP in the network packet with a forged one that means faked IP different from the original one. DNS Spoofing is a similar way to IP spoofing that makes the DNS return faked IP address to transfer the data packet path from the original network to the hacker's device. ARP (Address Resolution Protocol) Spoofing is to link the MAC of the attackers with legal IP of the computer over the virtual network. [30, 38]. These attacks are the most common for intruders to steal data from the machine. Another common networks attack is called **VM attacks.** This type of attacks is using malicious VM on a physical device resource like Hypervisor to gain the cryptographic keys with some private information, then to extract sensitive data and to do multiple attacks like side channel attack , DOS (Denial of attack) and keystroke monitor ,then to reach the bridge between the VMs inside the cloud platforms. The VM attack is the main concern and vulnerability hole inside the security system of the cloud machines[15]. **storage attacks** is another threat targeting that are facing hardware components, which means an attacker from outside or even from the inside system, may steal sensitive and private information that being stored inside the cloud machines[32, 33, 34]. Should implement and apply strict methods to eliminate the hackers illegal uses and avoid accessing the data and exposing it [35,36]. the hackers aim to use the cloud services without paying the rental charges and to access to the different resources of the date [19]. 90% from the hackers are using the extracted data illegally to illegal motives. [15]. The last threat to list here is happening on application level and called **application attacks.** The application that running on with cloud may get attacks in very various ways such as injecting code to track the execution path and avail this information for different ways of illegal motives. A virtualization attack on software may force the ability to scan and steal private information using VM to trigger the attack which is mistakenly issued [17]. In a similar way, the protocols that used to provide the services alongside with cloud platforms are vulnerable to attacks from different applications as an intrusion. the architecture of the cloud also is vulnerable to application attacks [35]. Below are the three types of threatens that can considered as application attacks:

i. Malware injection and interface attacks: if the cloud platform allowed the malicious code to be inserted because of the weak and insecure interface for applications [36, 37]. With steganography attacks, the attackers Included malicious code inside files that are transferred via the network [38]. May the attack will reach to the root level on the cloud platform after successful interface attacks [15]. The attacks included two types (XML Signature, Exploits the vulnerability in XSS).

ii. Shared architectures: On a multi-tenant architecture, the account can be hijacked and stolen by tracing the execution's path of the victim's application because of the share architecture [39]. The multi-tenant process in cloud computing refers to a software that runs on the same physical server for multiple tenants or customers [18]. Because of this architecture, the cloud is facing different types of aggression for example: man-in-the-middle during VM migration. VM insertion is a rootkit root during memory modification. Side channel attack to steal sensitive data[15].

iii. Web services and SSH attacks: Web services used different protocols, for example SOAP, to process their message address to contain incorrect requests (40). Attacks on Shell Secure (SSH), the main method used to establish trust and connect with the cloud services, pose the most serious threat to trust in control. With reference to the weak security report of Ponemon 2014 [15, 16], 74% of organizations do not have control over the provision, routing, tracking and removal of SSH keys.

7. Conclusions and Future Work

In spite of many advantages associate with cloud computing, there are many vulnerabilities and challenges associated with cloud security and privacy. In this review, we analysed latest literature related to the service models and deployment models of cloud computing, latest threats, security, privacy issues, trending approaches and solutions tackling privacy such as identity cloud management, cryptography and steganography. Many approaches and solution are included to tackle privacy and security issues. However, those solutions must be implemented at SaaS level for higher level of security to individuals and corporates. Several techniques have been proposed for data privacy and reliability inside the cloud environment. This article strives to be the latest review article in area of cloud computing and its techniques and challenges. We also believe that this is the comprehensive and to serve as main reference in privacy and security of could computing. The future work we intend to pave the way with incorporating a special layer into the cloud computing environment. This planned layer will be specialized on Privacy As a Service relying between SaaS and IaaS layers and built on NFV architecture so we can enhance the level of privacy for users and companies.

References

[1] Modi, Chirag,Patel ,Dhiren, Borisaniya, Bhavesh ,Pat Avi , Rajarajan, Muttukrishnan,2013 A survey on security issues and solutions at different layers of Cloud computing..J.Supercomput.63(2),5612.

[2] Armbrust , Micheal, et al. Above the Clouds: A Berekely View of Cloud. Technical Report No. UCB/EECS-2009-28, Berkeley: Electrical Engineering and Computer Sciences, 2009.

[3] Mell, P. & Grance, T (2009). The NIST Definition of Cloud Computing.

[4] Subashini,Subashini,Kavitha,Veeraruna,2011.A survey on security issues in service delivery models of cloud computing.J.Netw.Comput.Appl.34(1),111.

[5] Syrine Sahmim , Hamza Gharsellaouib.2017 France Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review

[6] IDC, Spending on it Infrastructure for Cloud Environments in 2016 will be Strong Despite First Quarter Slowdown, 2016.

[7] Nesrine Kaaniche , Maryline Laurent], 2017 Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms

[8] A.N. Toosi , R.N. Calheiros ,R. Buyya, Interconnected Cloud Computing Environ- ments: Challenges, Taxonomy, and Survey, 47, ACM, New York, NY, USA, 2014 .

[9] G. Aceto , A. Botta , W. De Donato , A. Pescapè, Survey cloud monitoring: a sur vey, Comput . Net w. 57 (9) (2013) 2093–2115 .

[10] Z. Xiao, Y. Xiao, Security and Privacy in Cloud Computing, 2012, pp. 1–17.

[11] A. Haeberlen , A Case for the Accountable Cloud, 44, ACM, New York, NY, USA, 2010 .

[12] Cloud Security Alliance, Top Threats to Cloud Computing V1.0, 2010.

[13] Jansen WA,“ Cloud Hooks: Security and Privacy Issues in Cloud Computing, Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, Kauai, HI. IEEE Computer Society, Washington, DC, USA, 2011, pp 1–10.

[14] Cloud Security Alliance, 2010. Online: http://www.cert.uy/wps/wcm/connect/975494804fdf89eaabbdab1805790cc9/Cloud_Computing_Vulnerability_Incidents.pdf/?MOD=AJPERES.

[15] Syed Asad Hussain , Mehwish Fatima , Atif Saeed ,Imran za ,Raja Khurram Shahzad,11 May 2015, Multilevel classification of security concerns in cloud computing

[16] L. Ponemon, Ponemon ,2014 , SSH security Vulnerability Report Retrieved ,website : http :// www.venafi.com/collateral/wp/ponemon-2014-ssh-security-vulnerability-report 2014.

[17] J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning, 2009,Managing security of virtual machine images in a cloud environment, in:ACM Cloud Computing Security Workshop (CCSW?09), ACM,

[18] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Get off of my cloud: exploring information leakage in third-party compute clouds, in: ACM Conference on Computer and Communications Security, ACM, 2009.

[19] P. Arora, R.C. Wadhawan, E.S.P. Ahuja, Cloud computing security issues in infrastructure as a service, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 2 (1) (2012) 1–7.

[20] David Sánchez , Montserrat Batet(2017), Privacy-preserving data outsourcing in the cloud via semantic data splitting

[21] Cloud Security Alliance, Cloud usage: risks and opportunities report, in, September 2014.

[22] European Network and Information Security Agency, Cloud computing. Benefits, risks and recommendations for information security. Revision B, in: L. Dupré, T. Haeberlen (Eds.), December 2012.

[23] http://money.cnn.com/2011/06/22/technology/dropbox _ passwords/ .

[24] http://www.bbc.com/news/technology-29237469 .

[25] E. Ramirez, J. Brill, M.K. Ohlhausen, J.D. Wright, T. McSweeny, Data Brokers, 2014: A call for transparency and accountability, in, federal trade commission, May

[26] IBM Corporation, The essential CIO, 2011. From www.ibm.com/businesscenter/cpe/download0/218842/2011mmciostudy.pdf .

[27] Symantec,2015,InternetSecurityThreatReport.URL⟨http://www.symantec.com/security_response/publications/threatreport.jsp⟩, April.

[28] Riquet,D.,Grimaud,G.,Hauspie,M.,2012.Large-scale coordinated attacks: Impact on the cloud security,2012, Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS),pp.558–563.

[29] InfoSecurity,2009.GoogleCloudPlatformUsedforBotnetControl.URL⟨http://www.infosecuritymagazine.com/news/google-cloud-platform-used-forbotnetcontrol/⟩.

[30] Wu,H.,Ding,Y.,Winer,C.,Yao,L.,2010.Network security for virtual machine in cloud computing In:20105th International Conference on Computer Sciences and Convergence Information Technology (ICCIT),pp.18–21.

[31] Tandon,S.,SB,S.,Agrawal,V.,2014.Cache-based side channel attack on AES in cloud computing environment .Int.J.Eng.Res.Technol.3(10),1080–1084

[32] Stefanov,E.,Shi,E.,2013.Oblivistore:high performance oblivious cloud storage In:2013IEEE Symposium on Security and Privacy (SP) ,pp.253267.

[33] Li,M.,Yu,S.,Ren,K.,Lou,W.,Hou,Y.,2013.Toward privacy assured and searchable cloud data storage services.IEEENetw.27(4),5662.

[34] Jung,T.,Li,X.Y.,Wan,Z.,Wan,M.,2013.Privacy preserving cloud data access with multi-authorities. In:2013Proceedings IEEE INFO COM,pp.2625–2633.

[35] Minhaj AhmadKhan ,2016,Review A survey of security issues for cloud computing ,Pakistan

[36] Ryan K L , Stephen G Lee, V Rajan, 2013 . Cloud Computing Vulnerability Incidents : A Statistical Overview.

[37] Owens, D ,2010. Securing elasticity in the cloud Queue8(5)10:1010:16.Paxson,V. , 1999.Bro: a system for detecting network intruders in real time Comput.Netw.31(2324),2435–2463.

[38] Mazurczyk , W, Szczypiorski ,K. , 2011.Is cloud computing steganography proof: In:2011Third International Conference on Multimedia Information Networking and Security(MINES), pp.441–442.

[39] Zhang,Y.,Juels,A.,Reiter,M.K.,Ristenpart,T.,2014. Cross-tenant side-channel attacks in PaaS clouds .In: Proceedings of the 2014 ACM SIG SAC Conference on Computer-and-Communications-Security,CCS'14.ACM,NewYork,NY,USA,pp.9901003

[40] Gruschka , N , Iacono , L.,2009.Vulnerable cloud : soap message security validation revisited . In : IEEE International Conference on Web Services ,2009 . ICWS2009 , pp. 625–631.

[41] Mansooreh, Moghadam, Sterkel, Wendy, 2012. Cloud Computing vs Traditional Internet Setting: Which One is More Secure.

[42] Chen, Deyan, Zhao, Hong,2012. Data security and privacy protection n issues in cloud computing . In : Proceedings of 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE) .I EEE,Vol.1,pp.647–651.

[43] Gupta, Sanchika, Kumar, Padam, 2013. Taxonomy of cloud security. Int. J. Comput. Sci. Eng. Appl. 3 (5).

[44] Muhammad Baqer Mollaha,, Md. Abul Kalam Azada, Athanasios Vasilakosb(2017)Security and privacy challenges in mobile cloud computing: Survey and way Ahead,

[45] D. Sommer , M. Casassa Mont , S. Pearson , PRIME Architecture V3, Tech. Rep. D14.2.d, PRIME, 2008 .

[46] Prime, Privacy and identity management for Europe, 2016, Retrieved: June, 2016 URL https://www.prime-project.eu/ .

[47] S. Górniak , J. Elliott , M. Ford , D. Birch , Managing multiple electronic identities, Technical Report, ENISA - European Network and Information Security Agency, 2011 .

[48] PrimeLife, Privacy and identity management for europe life, 2016, Retrieved: June, 2016 URL http://primelife.ercim.eu/ .

[49] ABC4Trust, Abc4trust, 2016, Retrieved: May, 2016 URL https://abc4trust.eu/ .

[50] Jorge Werner , CarlaMerkle Westphall, Carlos Becker Westphall [5 September 2016] Florianópolis, SC, Cloud identity management: A survey on privacy strategies ,

[51] GÉANT, Géant project, 2016, Retrieved: May, 2016 URL http://www.geant.org/ .

[52] PRISMACLOUD, Prismacloud project - privacy and security maintaining services in the cloud, 2016, Retrieved: August, 2016 URL http://www.prismacloud. eu/ .

[53] CREDENTIAL, Credential project - secure cloud identity wallet, 2016, Retrieved: August, 2016 URL http://www.credential.eu/ .

[54] Secure Computation over Cloud using Fully

[55] Homomorphic Encryption , G. K. Patra, Nilotpal Chakraborty, Anusha Bilakanti, Anjana.N.B,(2016)

[56] https://benlog.com/2011/12/

[57] Intel article, Blue Skies Ahead, Raj Samani, Chief Information Officer, EMEA Europe, Intel Security.[April 13, 2016] https://newsroom.intel.com/news-releases/news-release-new-report-reveals-critical-need-for-improved-trust-to-advance-cloud-adoption/

[58] Rohit Bhadauria, Sugata Sanyal, " Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques".2012

[59] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy.Sebastopol, CA: O'Reilly Media, Inc.

[60] Vinay Kumar Pant, Mr. Anshuman Saurabh, "Cloud Security Issues, Challenges And Their Optimal Solutions" International Journal of Engineering Research & Management Technology, ISSN: 2348-4039, Volume 2, Issue-3, May- 2015.

[61] G. Dr. Mohammad V. Malakooti and Nilofar Mansourzadeh, "A Two Level-Security Model for Cloud Computing based on the Biometric Features and Multi-Level Encryption", The Proceedings of the International Conference on Digital Information Processing, Data Mining, and Wireless Communications, Dubai, UAE, 2015.

[62] M.Marwaha, R.Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue I, No I, P. 367-370, January2013.

[63] Amit Asthana, Jyoti Prakash, Vinay kumar pant,2015, Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques,

[64] Randeep Kaur ,Supriya Kinger ,2014, Analysis of security algorithms in cloud computing", International journal of invocation in engineering and management(IJAIEM).

[65] Suhad Shakir Jaber, Hilal Adnan Fadhil, Zahereel I. Abdul khalib,Rasim Azeez Kadhim," Cloud Computing Data Security : AES Encryption Algorithm and PRT-PVD Steganography technique", Australian Journal of Basic and Applied Sciencesvol.9,2015.

[66] Beckham, The top five security risks of cloud computing, A vailable on internet : http : // blogs .cisco .com/smallbusiness/the-top-5-securityrisks-of-cloud-computing, 2011.

[67] Sichao Wang, 2015. Are enterprises really ready to move into the cloud? FromCSA,

[68] Gibbs. Steve, 2013,Cloud computing, International journal of innovative research in engineering and science, vol.1, issue 1, pp.10-17.

[69] T. Elahi, S. Pearson, 2007,Privacy assurance: Bridging the gap between preference and practice, trust, privacy and security in digital business, Springer Berlin, Heidelberg, vol. 4657, pp. 65-74.
[70] Eswaran S., Abburu S. , 2012, Identifying data integrity in the cloudstorage, International journal of computer science issues (IJCSI), vol.9(2), pp.403-408.
[71] Tsai W. T., Zhong P., Multi-tenancy and Sub-tenancy architecture in software-as-a-service (SaaS), In service oriented system engineering(SOSE), 8th International symposium on IEEE, pp.128-139, 2014.
[72] Kuyoro S.O., Ibikunle F. , Awodele O, Cloud computing security issues and challenges, International Journal of Computer Networks, vol. 3, issue 5,pp.11-14, 2011.
[73] Marston, Sean, et al. "Cloud computing—The business perspective." Decision Support Systems 2011.
[74] Vinay S, Arjun U, 2016, A Short Review on Data Security and Privacy Issues in Cloud Computing,
[75] D. Chen and H. Zhao, 2012, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 Int. Conf. Comput. Sci. Electron. Eng., no.973, pp. 647–651.
[76] Bharati Mishra, Debsish Jena, 2016 ,Securing Files in the Cloud, IEEE International Conference on Cloud Computing in Emerging Markets
[77] Rajat soni, Smrutee ambalkar, Dr.Pratosh bansal. 2016,security and privacy in cloud computing
[78] A Privacy Manager for Cloud Computing
[79] Siani Pearson, Yun Shen and Miranda Mowbray(2013)
[80] David Tancock ,Siani Pearson ,Andrew Charles worth , A Privacy Impact Assessment Tool For Cloud Computing.
[81] Siani Pearson, George Yee. Book- Privacy and Security for Cloud Computing- Hewlett Packard's Privacy Advisor.
[82] Serap Şahin , 2010,On Current Trends in Security and Privacy of Cloud Computing .
[83] M. S, E. Daniel, and N. Vasanthi, 2013, "Survey on Various Data Integrity Attacks in Cloud Environment and the Solutions," pp. 1076–1081.
[84] Yahya Kord Tamandani, Qahtan Makki Shallal, Mohammad Ubaidullah Bokhari ,security and privacy issues on cloud computing , (2016 IEEE)
[85] Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara ,2016," Data Security using Cryptography and Steganography techniques ", International Journal of Advanced Computer Science and Applications .
[86] Alok Ranjan, Mansi Bhonsle, 2016," Advanced System to Protect and Shared Cloud Storage Data using Multilayer Steganography and Cryptography", International Journal of Engineering Research.
[87] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas,Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, Mike Hamburg,2017, Meltdown.
[88] Paul Kocher, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg,Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, Yuval Yarom, 2017, Spectre Attacks: Exploiting Speculative Execution.