American Journal of Systems and Software, 2016, Vol. 4, No. 1, 14-26
Available online at http://pubs.sciepub.com/ajss/4/1/2

DOI:10.12691/ajss-4-1-2

A Survey on Secure Cloud: Security and Privacy in Cloud Computing

Shyam Nandan Kumar[1,*], Amit Vajpayee[2]

[1]M.Tech-Computer Science and Engineering, Lakshmi Narain College of Technology-Indore (RGPV, Bhopal), MP, India
[2]Department of Computer Science and Engineering, Lakshmi Narain College of Technology-Indore (RGPV, Bhopal), MP, India
*Corresponding author: shyamnandan.mec@gmail.com

Abstract Cloud computing is an emerging technology that is still unclear to many security problems. The security problem becomes amplified under the cloud model as new dimensions enter into the problem scope related to the architecture, multi-tenancy, layer dependency, and elasticity. This survey paper introduces a detailed analysis of the cloud security problem. In this paper various existing approaches related to data encryption and message authentications are discussed. After study the existing approaches, issues and challenges are point out during data processing over the cloud. Instead of only encryption or authentication, this paper suggests attribute based encryption and attribute based authentication together, during communication over the cloud for achieving better security.

Keywords: *cloud computing, data sharing, decryption, encryption, concurrent access, distributed system, web, message signing and verification, data confidentiality, message authentication, cloud security*

Cite This Article: Shyam Nandan Kumar, and Amit Vajpayee, "A Survey on Secure Cloud: Security and Privacy in Cloud Computing." *American Journal of Systems and Software*, vol. 4, no. 1 (2016): 14-26. doi: 10.12691/ajss-4-1-2.

1. Introduction

Cloud Computing is continuously evolving and showing consistent growth in the field of computing. Cloud computing (so-called, cloud) represents one of the magnificent shifts in information technology which can enhance collaboration, agility, scaling and availability, and provide the potential for cost reduction through optimized and efficient computing [1,2]. Cloud computing is emerging from recent advances in technologies such as hardware virtualization, Web services, distributed computing, utility computing and system automation. With virtualization, one or more physical servers can be configured and partitioned into multiple independent "virtual" servers, all functioning independently and appearing to the user to be a single physical device. Such virtual servers are in essence disassociated from their physical server, and with this added flexibility, they can be moved around and scaled up or down on the fly without affecting the end user. The difference with cloud computing is that the computing process may run on one or many connected computers at the same time, utilizing the concept of virtualization.

Different from the existing technologies and computing approaches, cloud is defined with five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), SPI service models (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)), and deployment models (Public, Private, Hybrid, Community) [1,2]. In SaaS, users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. IaaS refers to the sharing of hardware resources for executing services, typically using virtualization technology. Potentially, with IaaS approach, multiple users use available resources. IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw block storage, and file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. PaaS model aims to protect data, which is especially important in case of storage as a service. In case of congestion, there is the problem of outage from a cloud environment. Thus the need for security against outage is important to ensure load balanced service. The data needs to be encrypted when hosted on a platform for security reasons.

The fundamental factor defining the success of any new computing technology is the level of security it provides. Cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. To enable

data access control in the Cloud, it is imperative that only authorized users are able to get access to data stored in the Cloud. In enterprise settings, we see the rise in demand for data outsourcing, which assists in the strategic management of corporate data [1,2]. It is also used as a core technology behind many online services for personal applications. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security. Various access control models are in use, including the most common Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these models are known as identity based access control models. In all these access control models, user (subjects) and resources (objects) are identified by unique names. Identification may be done directly or through roles assigned to the subjects. These access control methods are effective in unchangeable distributed system, where there are only a set of Users with a known set of services [1]. In DAC, information may be accessed by unauthorized users because there is no control on copies of objects. MAC deals with information flow and solves this problem by attaching security levels on both users and objects. All users are required to obtain certain clearance to access objects. Security labels propagate to derivative objects, including copies. However, the policies in DAC and MAC are fixed and there is no room for flexible access control. RBAC emerged due to increasing practitioner dissatisfaction with the then dominant DAC and MAC paradigms, inspiring academic research on RBAC. Since then RBAC has become the dominant form of access control in practice.

Communication over web [4] must be protected. Encryption provides data protection while key management enables access to protected data. It is strongly recommended to encrypt data in transit over networks, at rest, and on backup media. In particular, data encryption at rest (e.g., for long-term archival storage) can avoid the risk of malicious cloud service providers or malicious multi-tenants abuse. At the same time, secure key stores (including key backup and recoverability) and access to key stores must be securely implemented since improper (or access to) key storage could lead to the compromise of all encrypted data. Most Cloud service provider's provide basic key encryption schemes for protecting data or may leave it to the user to encrypt their own data. Both encryption and key management are very important to help secure applications and data stored in the Cloud. Requirements of effective key management are discuss below [1,3]. Tthe stored data must be protected against unauthorized access. Also, both the data and the access to data need to be protected from cloud storage service providers (e.g., cloud system administrators). In these scenarios, relying on password and other access control mechanisms is insufficient. Cryptographic encryption mechanisms [2,3] are typically employed. However, simply having encryption and decryption implemented in the cloud database systems is insufficient. In order to support both challenges, data should be encrypted first by users before it is outsourced to a remote cloud storage service and both data security and data access privacy should be protected such that cloud storage service providers have no abilities to decrypt the data, and when the user wants to search some parts of the whole data, the cloud storage system will provide the accessibility without knowing what the portion of the encrypted data returned to the user is about [1,2].

The Cloud however is susceptible to many privacy and security attacks. The biggest obstacle hindering the progress and the wide adoption of the Cloud is the privacy and security issues associated with it. Evidently, many privacy and security attacks occur from within the Cloud provider themselves as they usually have direct access to stored data and steal the data to sell to third parties in order to gain profit. The main aim of the paper is to finds out the problem associated with cloud security. Paper extracts the issues and focuses on data security and privacy during communication on the clouds.

2. Security Issue with Cloud Deployment Model

In the given scenario, a constant research effort in the area of cloud storage and cloud computing security will help achieve the balance between economic feasibility, ease of deployment and a suitable collection of security considerations for each cloud service (CS) client.

In a public cloud enabling a shared multi-tenant environment, as the number of users increase, security risks get more intensified and diverse. It is necessary to identify the attack surfaces which are prone to security attacks and mechanisms ensuring successful client-side and server-side protection [18]. Because of the multifarious security issues in a public cloud, adopting a private cloud solution is more secure with an option to move to a public cloud in future, if needed [21]. Based on the deployment model of cloud, security issues are classified as:

2.1. Issues with Public Cloud

In a public cloud, there exist many clients on a shared platform and infrastructure security is provided by the service provider. A few of the key security issues in a public cloud include:

- In case of a public cloud, the same infrastructure is shared between multiple tenants and the chances of data leakage between these tenants are very high. However, most of the service providers run a multitenant infrastructure. Proper investigations at the time of choosing the service provider must be done in order to avoid any such risk [15,16].
- The three basic requirements of security: confidentiality, integrity and availability are required to protect data throughout its lifecycle. Data must be protected during the various stages of creation, sharing, archiving, processing etc. However, situations become more complicated in case of a public cloud where we do not have any control over the service provider's security practices [15].

Although data is stored outside the confines of the client organization in a public cloud, we cannot deny the possibility of an insider attack originating from service provider's end. Moving the data to a cloud computing

environment expands the circle of insiders to the service provider's staff and subcontractors [18]. An access control policy based on the inputs from the client and provider to prevent insider attacks has been proposed in [17]. Policy enforcement implemented at the nodes and the data-centers can prevent a system administrator from carrying out any malicious action. The three major steps to achieve this are: defining a policy, propagating the policy by means of a secure policy propagation module and enforcing it through a policy enforcement module.

The Guidelines on Security and Privacy in Public Cloud Computing published by NIST offer an overview of the security, privacy and availability risks of cloud computing [18]. The NIST guidelines identify, among other points, the following risks related to the use of cloud computing by organizations:

- **Trust**: Through the use of cloud computing and CS the organization relinquishes control over significant parts of aspects of security and privacy. As a result of this, the organization makes a commitment and places trust into the control mechanisms and processes employed by the cloud provider. One risk is the potential for insider access to the information, provoking both intentional incidents leading to loss or corruption of data, or unintentional errors, leading to massive unavailability of the CS. Another risk is the potential lack of clarity over data ownership, especially in border cases such as transaction data generated through the use of CS.
- **Data protection**: From the CS customer perspective, there are fewer mechanisms for data protection when data is created through CS or maintained in cloud storage. Two aspects of data protection are considered, namely data availability and data access control. The first aspect depends on the migration and backup capabilities offered by the type of the CS chosen by the client. The second aspect is less trivial, due to the specifics of the shared multi-tenant environment in which CS are deployed.
- **Governance**: Due to their wide availability and in many cases high degree of usability, CS (especially on the SaaS level) can easily bypass the security, privacy and software use policies adopted by the organization. While ensuring that systems are secure and risk is managed is possible (although not trivial) in the case of in-house system deployments, that is far more difficult in the case of cloud services.

2.2. Issues with Private Cloud

In a private cloud, customers have total control over the network. Private cloud provides the flexibility to the customer to implement any traditional network perimeter security practice. Although the security architecture is more reliable in a private cloud, yet there are issues/risks that need to be considered: A few of the key security issues in a private cloud include:

- In a private cloud, users are facilitated with an option to be able to manage portions of the cloud, and access to the infrastructure is provided through a web interface or an HTTP end point. There are two ways of implementing a web-interface, either by writing a whole application stack or by using a standard applicative stack, to develop the web interface using common languages such as Java, PHP, and Python etc. As part of screening process, Eucalyptus web interface has been found to have a bug, allowing any user to perform internal port scanning or HTTP requests through the management node which he should not be allowed to do. In the nutshell, interfaces need to be properly developed and standard web application security techniques need to be deployed to protect the diverse HTTP requests being performed [20].
- Virtualization techniques are quite popular in private clouds. In such a scenario, risks to the hypervisor should be carefully analyzed. There have been instances when a guest operating system has been able to run processes on other guest VMs or host. In a virtual environment it may happen that virtual machines are able to communicate with all the VMs including the ones who they are not supposed to. To ensure that they only communicate with the ones which they are supposed to, proper authentication and encryption techniques such as IPsec [IP level Security] etc. should be implemented [19].

Private clouds are considered safer in comparison to public clouds; still they have multiple issues which if unattended may lead to major security loopholes. Hybrid cloud model is a combination of both public and private cloud and hence the security issues discussed with respect to both are applicable in case of hybrid cloud.

3. Security and Privacy in Cloud

Cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. There is a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud) [23]. The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures. We need to consider the security problem level classification as follows [34]: (1) server deposit security, (2) Internet deposit security, (3) database deposit security, (4) material privacy security, and (5) program deposit security. Security issues can be categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing [24]. Therefore, Cloud

Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity. It is generally recommended that information security controls be selected and implemented according and in proportion to the risks, typically by assessing the threats, vulnerabilities and impacts.

Cloud providers help ensure that customers can rely on access to their data and applications, at least in part. Cloud providers also ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment. With respect to cloud computing environment, privacy is defined as "the ability of an entity to control what information it reveals about itself to the cloud/cloud SP, and the ability to control who can access that information" [25]. The ability of cloud computing to adequately address privacy regulations has been called into question. Organizations today face numerous different requirements attempting to protect the privacy of individuals' information, and it is not clear whether the cloud computing model provides adequate protection of such information, or whether organizations will be found in violation of regulations because of this new model.

Security is one of the key requirements to enable privacy. This principle specifies that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Cloud Security Alliance (CSA) is a non-profit organization that promotes the use of best practices in order to provide security in cloud environments. CSA has issued an Identity and Access Management Guidance [37] which provides a list of recommended best practiced to assure identities and secure access management. This report includes centralized directory, access management, identity management, role-based access control, user access certifications, privileged user and access management, separation of duties, and identity and access reporting.

4. Cloud Service Security

Based on Cloud Service Model, security issues can be categorized [2]. It can be categorized into network level, user authentication level, data level, and generic issues. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. Before analyzing security challenges in Cloud Computing, we need to understand the relationships and dependencies between these cloud service models [38]. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it may be true on the other way around. However, we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a consequence of these deep dependencies, any attack to any cloud service layer can compromise the upper layers. These relationships and dependencies between cloud models may also be a source of security risks. A SaaS provider may rent a development environment from a PaaS provider, which might also rent an infrastructure from an IaaS provider. Each provider is responsible for securing his own services, which may result in an inconsistent combination of security models. It also creates confusion over which service provider is responsible once an attack happens. Topic wise cloud security survey is given in Table 1. Security monitoring for Cloud Service is shown in Table 2.

Table 1. Cloud Security Survey

Reference	[38]	[49]	[63]	[64]	[60]	[41]	[45]	[56]	[55]
Threats			Y	Y	Y	Y	Y	Y	Y
Data Security	Y	Y						Y	
Vulnerabilities			Y	Y	Y	Y		Y	Y
Security Need	Y	Y				Y			
Cloud Service Model Security				Y		Y			Y
Trust		Y				Y			
Security Standards							Y	Y	
Recommendations	Y		Y		Y				Y

4.1. Security Issues with SaaS

SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM [39]. SaaS users have less control over security among the three fundamental delivery models in the cloud. The adoption of SaaS applications may raise some security concerns.

Data Security: Data security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security [40,41,42]. Data security includes the specific controls and technologies used to enforce information governance. This has been broken out into three sections to cover detection of data migration to cloud, protecting data in transit to the cloud and between different providers and protecting data once it's within the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and stored [30]. In SaaS, organizational data is often processed in plaintext and stored in the cloud. Also, data backup is a critical aspect in order to facilitate recovery in case of disaster, but it introduces security concerns as well [41]. Also cloud providers can subcontract other services such as backup from third-party service providers, which may raise concerns. Moreover, most compliance standards do not envision compliance with regulations in a world of Cloud Computing [40]. In SaaS model, the process of compliance is complex because data is located in the

provider's datacenters, which may introduce regulatory compliance issues such as data privacy, segregation, and security, that must be enforced by the provider.

Application Security: Since applications are typically delivered via the Internet through a Web browser [40,45]. However, flaws in web applications may create vulnerabilities for the SaaS applications. Security challenges in SaaS applications are not different from any web application technology, but traditional security solutions do not effectively protect it from attacks, so new approaches are necessary [41]. Attackers have been using the web to compromise user's computers and perform malicious activities such as steal sensitive data [43]. The Open Web Application Security Project (OWASP) has identified the ten most critical web applications security threats [46]. There are more security issues, but it is a good start for securing web applications.

Multi-Tenancy: The impact of multi-tenancy is visibility of residual data or trace of operations by other user or tenant. In this case, multiple consumers with same or different organization use same resources or applications. Information security is one of the prime factors for this phase. Since data from multiple tenants is likely to be stored in the same database, the risk of data leakage between these tenants is high. Security policies are needed to ensure that customer's data are kept separate from other customers [47].

Access Control: Accessing applications over the internet via web browser makes access from any network device easier, including public computers and mobile devices. However, it also exposes the service to additional security risks. The Cloud Security Alliance [48] has released a document that describes the current state of mobile computing and the top threats in this area such as information stealing mobile malware, insecure networks (WiFi), vulnerabilities found in the device OS and official applications, insecure marketplaces, and proximity-based hacking.

4.2. Security Issues with PaaS

PaaS cloud (public or private) offers an integrated environment to design, develop, test, deploy, and support custom applications developed in the language the platform supports. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform [49]. PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications.

Mashups combine more than one source element into a single integrated unit. Thus, PaaS models also inherit security issues related to mashups such as data and network security [50]. Also, PaaS users have to depend on both the security of web-hosted development tools and third-party services.

From the perspective of the application development, developers face the complexity of building secure applications that may be hosted in the cloud. However, developers also have to understand that any changes in PaaS components can compromise the security of their applications. Besides secure development techniques, developers need to be educated about data legal issues as well, so that data is not stored in inappropriate locations. Data may be stored on different places with different legal regimes that can compromise its privacy and security. In PaaS, developers do not usually have access to the underlying layers, so providers are responsible for securing the underlying infrastructure as well as the applications services [51]. Even when developers are in control of the security of their applications, they do not have the assurance that the development environment tools provided by a PaaS provider are secure.

Access Control: In the PaaS delivery model, the CSP is responsible for managing access control to the network, servers, and application platform infrastructure. However, the customer is responsible for access control to the applications deployed on a PaaS platform. Access control to applications manifests as end user access management, which includes provisioning and authentication of users.

Table 2. Security Monitoring for Cloud Service

	SaaS	PaaS	IaaS
Application monitoring	Allow	Monitor application logs for vulnerabilities (may be available via the PaaS platform)	Monitor application vulnerabilities (OWASP Top 10) and application event logs for intrusions
Network monitoring	Allow	Provider responsibility	Monitor the network interfaces of virtual instances
Database monitoring	Allow	Provider responsibility	Install database security monitoring tool on VMs hosting database and log events to a dedicated and persistent log server
Host monitoring	Allow	Provider responsibility	Monitor security events from host IDSs such as OSSEC Log events to a dedicated and persistent log server Monitor security events from VMs stored in system logs

4.3. Security Issues with IaaS

With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor [41]. They control the software running in their virtual machines, and they are responsible to configure security policies correctly [52]. However, the underlying compute, network, and storage infrastructure is controlled by cloud providers. IaaS provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet [55]. IaaS providers must undertake a substantial effort to secure their systems in order to minimize these threats that result from creation, communication, monitoring, modification, and mobility [53]. Unlike PaaS and SaaS, IaaS customers are primarily responsible for securing the hosts provisioned in the cloud. Customers of IaaS have full access to the virtualized guest VMs that are hosted and isolated from each other by hypervisor technology. Hence customers are responsible for securing and ongoing security management of the guest VM. Some of the new host security threats in the public IaaS include:

- Attacking unpatched, vulnerable services listening on standard ports (e.g., FTP, NetBIOS, SSH)
- Hijacking accounts that are not properly secured (i.e., weak or no passwords for standard accounts)
- Stealing keys used to access and manage hosts (e.g., SSH private keys)
- Deploying Trojans embedded in the software component in the VM or within the VM image (the OS) itself
- Attacking systems that are not properly secured by host firewalls

Virtualization: It allows users to create, copy, share, migrate, and roll back virtual machines, which may allow them to run a variety of applications [53,54]. However, it also introduces new opportunities for attackers because of the extra layer that must be secured [43]. Virtual machine security becomes as important as physical machine security, and any flaw in either one may affect the other [56]. Virtualized environments are vulnerable to all types of attacks for normal infrastructures; however, security is a greater challenge as virtualization adds more points of entry and more interconnection complexity [45].

Virtual Machine Monitor (VMM): VMM or ***hypervisor*** is responsible for virtual machines isolation; therefore, if the VMM is compromised, its virtual machines may potentially be compromised as well. The VMM is low-level software that controls and monitors its virtual machines, so as any traditional software it entails security flaws [57]. A vulnerable hypervisor could expose all user domains to malicious insiders. An attacker can compromise the migration module in the VMM and transfer a victim virtual machine to a malicious server. Keeping the VMM as simple and small as possible reduces the risk of security vulnerabilities, since it will be easier to find and fix any vulnerability. A malicious VM can infer some information about other VMs through shared memory or other shared resources without need of compromising the hypervisor [58]. Using covert channels, two VMs can communicate bypassing all the rules defined by the security module of the VMM [59]. Thus, a malicious Virtual Machine can monitor shared resources without being noticed by its VMM, so the attacker can infer some information about other virtual machines.

An attacker with a valid account can create an image containing malicious code such as a Trojan horse. If another customer uses this image, the virtual machine that this customer creates will be infected with the hidden malware. Moreover, unintentionally data leakage can be introduced by VM replication [60]. Some confidential information such as passwords or cryptographic keys can be recorded while an image is being created. If the image is not “cleaned”, this sensitive information can be exposed to other users.

Virtual Networks: Virtual Networks increase the VMs interconnectivity, an important security challenge in Cloud Computing [61]. The most secure way is to hook each VM with its host by using dedicated physical channels. However, most hypervisors use virtual networks to link VMs to communicate more directly and efficiently. For instance, most virtualization platforms such as Xen provide two ways to configure virtual networks: bridged and routed, but these techniques increase the possibility to perform some attacks such as sniffing and spoofing virtual network [57, 62].

Availability Management: Availability considerations for the IaaS delivery model should include both a computing and storage (persistent and ephemeral) infrastructure in the cloud. IaaS providers may also offer other services such as account management, a message queue service, an identity and authentication service, a database service, a billing service, and monitoring services. Hence, availability management should take into consideration all the services that user depends on for his IT and business needs.

5. Attacks on Cloud Data

Attacks on cloud data is increasing day by day with various techniques. Table 3 shows the idea about threats, attacking type with layer where it occurs mostly. A ***threat*** is a potential attack that may lead to a misuse of information or resources, and the term ***vulnerability*** refers to the flaws in a system that allows an attack to be successful. Some of them are:

Cross Site Scripting (*XSS*) attacks: Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts (also commonly referred to as a malicious payload) into a legitimate website or web application. XSS is amongst the most rampant of web application vulnerabilities and occurs when a web application makes use of un-validated or un-encoded user input within the output it generates. In order for an XSS attack to take place the vulnerable website needs to directly include user input in its pages. An attacker can then insert a string that will be used within the web page and treated as code by the victim’s browser [26]. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec as of 2007 [27]. It can be classified as: *non-persistent* and *persistent*.

In non-persistent, holes show up when the data provided by a web client, most commonly in HTTP query parameters or in HTML form submissions, is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the request.

Persistent ***XSS*** occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users in the course of regular browsing, without proper HTML escaping. A classic example of this is with online message boards where users are allowed to post HTML formatted messages for other users to read.

SQL injection attacks: Here malicious code is inserted into a standard SQL code. Thus the attackers gain unauthorized access to a database and are able to access sensitive information [28]. Sometimes the hacker’s input data is misunderstood by the web-site as the user data and allows it to be accessed by the SQL server and this lets the attacker to have know-how of the functioning of the website and make changes into that. Various techniques like: avoiding the usage of dynamically generated SQL in the code, using filtering techniques to sanitize the user input etc. are used to check the SQL injection attacks. A proxy based architecture towards preventing SQL

Injection attacks which dynamically detects and extracts users' inputs for suspected SQL control sequences has been proposed in [29].

Man in the Middle attacks (MITM): Another class of attacks, quite popular to SaaS, is termed as MITM. In such an attack, an entity tries to intrude in an ongoing conversation between a sender and a client to inject false information and to have knowledge of the important data transferred between them. Various tools implementing strong encryption technologies like: Dsniff, Cain, Ettercap, Wsniff, Airjack etc. have been developed in order to provide safeguard against them. A detailed study towards preventing man in the middle attacks has been presented in [30].

DoS/DDos Attacks: In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service (DDoS) is where the attack source is more than one–and often thousands of-unique IP addresses. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks, credit card payment gateways. A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services. Permanent denial-of-service (PDoS), also known loosely as phlashing, [35] is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. [36] Unlike the distributed denial-of-service attack, a PDoS attack exploits security flaws which allow remote administration on the management interfaces of the victim's hardware, such as routers, printers, or other networking hardware. The attacker uses these vulnerabilities to replace a device's firmware with a modified, corrupt, or defective firmware image—a process which when done legitimately is known as flashing. This therefore "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced.

Table 3. Cloud Threads

Threats	Attack type	Layer
Data leakage	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed [64,63,60].	SPI
Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.	SPI
Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction [63].	SPI
Data manipulation	Users attack web applications by manipulating data sent from their application component to the server's application [60,46]. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.	S
Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs [57,61].	I
Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository [60].	I
VM hopping	It happens when a VM is able to gain access to another VM (i.e. by exploting some hypervisor vulnerability) [64,53]	I

6. Cloud Security Controls

Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management [22]. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of the attack. While there are many types of controls behind the cloud security architecture, they can usually be found in one of the following categories [22]:

- **Preventive controls**: Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.
- **Detective controls**: Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue [22]. System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.
- **Deterrent controls**: Deterrent controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed.
- **Corrective controls:** Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

7. Security Approach through Existing Technologies

Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters [44]. Because Cloud Computing represents a relatively new computing model, there is a

great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing [2, 65]. That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing [49]. Literature review is presented in this section that deals with existing cloud security models, methodology and algorithms.

Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds [66] is presented by Gonzales, D. et. all. It is a cloud architecture reference model that incorporates a wide range of security controls and best practices, and a cloud security assessment model – Cloud-Trust – that estimates high level security metrics to quantify the degree of confidentiality and integrity offered by a Cloud Computing Systems (CSS) or cloud service provider (CSP). Cloud-Trust is used to assess the security level of four multi-tenant IaaS cloud architectures equipped with alternative cloud security controls and to show the probability of CCS penetration (high value data compromise) is high if a minimal set of security controls are implemented. CCS penetration probability drops substantially if a cloud defense in depth security architecture is adopted that protects virtual machine (VM) images at rest, strengthens CSP and cloud tenant system administrator access controls, and which employs other network security controls to minimize cloud network surveillance and discovery of live VMs. In optimized fine-grained and fair pricing scheme [67], two tough issues are addressed for IaaS platform: (1) the profits of resource providers and customers often contradict mutually; (2) VM-maintenance overhead like startup cost is often too huge to be neglected.

Biometric encryption [5] is proposed to improve the confidentiality in Cloud computing for biometric data. The privacy of a particular user is an issue in biometric data i.e. the face reorganization data for a famous and important people. Also, this paper discussed virtualization for Cloud computing, as well as biometrics encryption.

In decentralized multi-authority attribute-based signature (DMA-ABS) scheme [68], no central authority and no trusted setup are required. The proposed DMA-ABS scheme for a large class of (non-monotone) predicates is fully secure (adaptive-predicate unforgivable and perfectly private) under a standard assumption, the decisional linear (DLIN) assumption, in the random oracle model. In Outsourced ABS [69], the computational overhead at user side is greatly reduced through outsourcing intensive computations to an untrusted signing-cloud service provider (S-CSP).

Multi-factor authentication (MFA) [10] is an approach to user validation that requires the presentation of two or more authentication factors. Given the popularity of cloud systems, MFA systems become vital in authenticating users. A privacy-preserving multi-factor authentication system utilizing the features of big data called MACA [10]. In MACA, the first factor is a password while the second factor is a hybrid profile of user behavior. The hybrid profile is based on users' integrated behavior, which includes both host-based characteristics and network flow-based features. MACA is the first MFA that considers both user privacy and usability combining big data features.

Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. Fully Homomorphic encryption (FHE) [31] allows straightforward computations on encrypted information, and also allows computing sum and product for the encrypted data without decryption. In addition the homomorphic property of various cryptosystems can be used to create many other secure systems, for example secure voting systems,[32] collision-resistant hash functions, private information retrieval schemes, and many more. Craig Gentry [33] using lattice-based cryptography, described the first plausible construction for a fully homomorphic encryption scheme. Gentry's scheme supports both addition and multiplication operations on cipher texts, from which it is possible to construct circuits for performing arbitrary computation.

An ID-Based User Authentication Scheme for Cloud Computing [11] supports higher security levels and lower computation costs. An efficient authentication scheme for distributed mobile cloud computing services is proposed in [12]. The proposed scheme provides security and convenience for mobile users to access multiple mobile cloud computing services from multiple service providers using only a single private key. The security strength of the proposed scheme is based on bilinear pairing cryptosystem and dynamic nonce generation. Security Enhanced Anonymous Remote User Authentication and Key Agreement for Cloud Computing are proposed in [13]. It enables a user and a cloud server to authenticate each other anonymously and establish a secure channel between them. Thus, only the user and the cloud server may learn the messages exchanged and no entity except themselves can learn the real identities of the message senders.

A new scheme is proposed [14] for mutual authentication where the user and cloud server can authenticate one another. The protocol is designed in such a way that it uses steganography as an additional encryption scheme. The scheme achieves authentication using secret sharing. Secret sharing allows a part of the secret to be kept in both sides which when combined becomes the complete secret. The secret contains information about both parties involved. Further, out of band authentication has been used which provides additional security. The proposed protocol provides mutual authentication and session key establishment between the users and the cloud server. Also, the users have been given the flexibility to change the password.

7.1. ABE Schemes

Sahai and Waters proposed a new type of IBE – Fuzzy Identity-Based Encryption [7]. It is also known as Attribute-Based Encryption (ABE). In their work, an identity is viewed as a set of descriptive attributes. Different from the IBE, where the receiver could decrypt the message if and only if his identity is exactly the same as what specified by the sender, this fuzzy IBE enables the decryption if there are identity overlaps‘ exceeding a pre-set threshold between the one specified by sender and the one belongs to receiver. However, this kind of threshold-based scheme was limited for designing more general

system because the threshold based semantic cannot express a general condition. In ABE, a user has a set of attributes in addition to its unique ID. It can be divided into two main categories: KP-ABE scheme and CP-ABE scheme.

7.2. KP-ABE Scheme

In Key-policy ABE or KP-ABE (Goyal et al. [8]), the sender has an access policy to encrypt data. Cipher-text is associated with a set of attributes, which partially represents the cipher-text‘s encryption policy. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is able to decrypt information if it has matching attributes.

Unfortunately, with a drawback that the access policy is built into the secret key, the data owner in a KP-ABE scheme cannot decide the one who can decrypt the cipher text, and he can only choose a set of attributes to control the access of cipher texts. Besides, the access structure is a monotonic access structure which cannot express the negative attribute to exclude the participants with whom the data owner does not want to share data. Subsequently, Ostrovsky et al. [70] proposed a scheme with a non-monotonic access structure where the secret keys are labeled with a set of attributes including positive and negative attributes. Comparatively, the ABE scheme with non-monotonic access structure can express a more complicated access policy. Unfortunately, this mechanism doubles the size of the cipher text and secret key and adds encryption/decryption overheads at the same time. Ostrovsky et al.’s initial construction is recently improved by Lewko et al. [71] who us a new technique to achieve user revocation and design the most efficient non-monotonic KP-ABE scheme. KP-ABE schemes, In this methodology the cipher text size grows linearly with the number of cipher text attributes and the only known exception only supports restricted forms of threshold access policies.

7.3. CP-ABE Scheme

In 2007, using a monotonic access tree as access structure, Bethencourt et al. [72] proposed the first CP-ABE construction. Their scheme can support flexible access control policies like the KP-ABE [8] scheme, but the security proof is in the generic group model. Cheung and Newport [73] provided a provably secure CP-ABE scheme which is proved to be secure under the standard model and their scheme supports AND gate on positive and negative attributes as its access policy. In 2011, Waters [9] proposed a new methodology for realizing CP-ABE under concrete and non-interactive cryptographic assumptions in the standard model. He expressed access control by a linear secret sharing scheme (LSSS) matrix over the attributes in the system (previously used structures can be expressed succinctly in terms of an LSSS). In this most efficient scheme, the cipher text size and the encryption/decryption overheads increase linearly with the complexity of the access formula. As a result, his scheme achieves the same performance and functionality as Bethencourt et al.’s [72]. Finally, Lewko et al. [74] recently leveraged the encoding technique from Waters’s scheme [9] to propose an ABE scheme that achieves adaptive (nonselective) security. Their scheme is based on the Composite order groups, which results in some loss of practical efficiency when compared with Water’s. Emura et al. [84] improved the efficiency and achieved hidden policies.

Table 4 shows the comparison among various existing CP-ABE based Encryption/Security systems.

Table 4. CP-ABE Technologies Comparison

	Access structure	Supported policy	Assumption	Model
Waters’ [9]	LSSS matrix	And, or, threshold	DPBDHE	Selective
Lewko et al.’s [74]	LSSS matrix	And, or, threshold	3P-SDP	Adaptive
Bethencourt et al.’s [72]	Tree without bound	And, or, threshold	Generic group	Adaptive
Cheung and Newport [73]	AND gate between two-value attributes	And, non	DBDH	Selective
Emura et al.’s [84]	AND gate among multivalue attributes	And	DBDH	Selective

7.4. Dual-Policy ABE Scheme

In 2009, Attrapadung and Imai [75] presented a new ABE scheme called the Dual-Policy ABE. Basically, it is a conjunctively combined scheme of Goyal et al.’s KP-ABE scheme [8] and Waters’ CP-ABE scheme [9]. It allows simultaneously two access control mechanisms over encrypted data. One involves policies over objective attributes ascribed to data and the other involves policies over subjective attributes ascribed to user credentials. These two access control mechanisms can only allow either functionality above one at a time. What is more, the security proof is based on decisional bilinear Diffie-Hellman exponent (DBDHE) assumption.

7.5. MA-ABE Scheme

Multi-authority ABE schemes [76,77] can be divided into two types. One needs a central authority (CA, for short) which is used to guarantee the proper decryption and can also decrypt all cipher texts, such as schemes [76,78], while the other does not need a CA, such as schemes [79,80].

Table 5. Comparison of computational cost

Schemes	Authority setup	KeyGen	Encryption	Decryption
Chase’s [76]	$(\|U\|+1)E$	$(\|A_U\|+1)E$	$(\|A_C\|+2)E$	$\|A_C\|E+(\|A_C\|+1)P$
Han et al.’s [77]	$(\|U\|+2N)E$	$(\|A_U\|+3\|I_U\|)E$	$(\|A_C\|+3)E$	$\|A_C\|E+(\|A_C\|+\|I_C\|+1)P$
Chase and Chow [80]	$(\|U\|+2N)E$	$(\|U\|+\|I_U\|^2)E$	$(\|A_C\|+2)E$	$\|A_C\|E+(\|A_C\|+1)P$

Table 6. Working Idea Comparison for MA-ABE

Scheme	Security Model	Used ABE	Cipher text Length	Central Authority
Chase's [31]	Selective	KP-ABE	$(\|A_C\|+1)L_{G1} + L_{G2}$	Yes
Han et al.'s [37]	Selective	KP-ABE	$(\|A_C\|+2)L_{G1} + L_{G2}$	No
Lin et al.'s [32]	Selective	FIBE	$(\|A_C\|)L_{G1} + L_{G2}$	No
Chase and Chow [34]	Selective	KP-ABE	$(\|A_C\|+1)L_{G1} + L_{G2}$	No

The comparison between the different multi-authority schemes is shown in Table 5 and Table 6. By $|U|$, $|A_U|$, and $|A_C|$, we denote the number of the universal attributes, the attributes held by user U, and the attributes required by the cipher text, respectively. I_U and I_C denote the index set of the authorities. By E and P, we denote one exponential and one paring operation, respectively. By L_{G1} and L_{G2}, we denote one element in group G1 and one element in group G2, respectively. N denotes the number of the authorities in the systems. Table 5 shows the ideas about operation cost for various MA-ABE schemes while Table 6 shows the working ideas comparison of existing MA-ABE technologies.

7.6. Attribute-Based Proxy Re-encryption Scheme

To make data sharing more efficient, proxy re-encryption (PRE) is proposed. Introduced by Mambo and Okamoto [81] and first defined by Blaze et al. [82], PRE extends the traditional public key encryption (PKE) to support the delegation of decryption rights. It allows a semi-trusted party called proxy to transform a cipher text encrypted under Alice's public key into another cipher text of the same plaintext intended for Bob. The proxy, however, learns neither the decryption key nor the underlying plaintext.

7.7. HABE Scheme

Hierarchical attribute-based encryption scheme (HABE) [83] by combining a hierarchical identity-based encryption (HIBE) system and a cipher text-policy attribute-based encryption (CP-ABE) system, so as to provide not only fine-grained access control, but also full delegation and high performance. It supports a scalable revocation scheme by applying proxy re-encryption (PRE) and lazy re-encryption (LRE) to the HABE scheme, so as to efficiently revoke access rights from users.

This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys. Moreover, it used disjunctive normal form (DNF) to express the access control policy, and the same domain authority in this scheme administered all attributes in one conjunctive clause. There are five roles in this scheme: the cloud storage service, data owner, the root authority, the domain authority, and data users.

Existing work on access control in cloud are centralized in nature. Except and, all other schemes use attribute based encryption (ABE). The scheme uses a symmetric key approach and does not support authentication. One of the main efficiency drawbacks of the most existing Encryption schemes is that decryption is expensive for resource-limited devices due to pairing operations, and the number of pairing operations required to decrypt a cipher-text grows with the complexity of the access policy. Also these existing schemes are given in centralized manner and not support multiple read and multiple write. However, the authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. Concurrent data sharing and accessing is other important issue with existing system. Message Authentication with confidentiality is the most important requirement over the cloud.

8. Need of Technology for Cloud Security

In recent years, the research areas on secure data processing have gained more and more attention. Cloud computing security issues include preserving confidentiality and privacy of data. Only encryption or authentication cannot give suitable security service. They having individual feature. There are several expressive Attribute Based Encryption (ABE) schemes where the decryption algorithm only requires a constant number of pairing computations. Recently, some researcher focuses on only message signing to achieve authentication. A monetization of the risks involved for the main assets that need to be protected (data, algorithms, activity patterns or business reputation) would show that each of the aspects is likely to have a different value for each organization or person. Hence, cloud users would benefit from both a choice of different levels of security based on their requirements as well as different aspects of security (e.g. special attention to business reputation risks). Both cases bring along their own trade-offs and implementation peculiarities.

To achieve confidentiality, integrity and authentication of data, there should be encryption and decryption along with message signature and verification. Data Confidentiality and Message Authentication together will give better security than single encryption or single authentication during data processing over the cloud. The data objects should never be updated by unauthorized clients and in order to achieve this limitation the system ensures that only correct and authorized client are able to perform the updates. If attribute based encryption and attribute based authentication are applied, it supports multiple read and multiple write. Confidentiality assures that private or confidential information is not made available or disclosed to unauthorized individuals over the clouds. A loss of confidentiality is the unauthorized disclosure of information. Message authentication assures that data received are exactly as sent (i.e., contain no modification, insertion, deletion, or replay). In many cases, there is a requirement that the authentication mechanism assures that purported identity of the sender is valid. It verifies the integrity of message. For optimal authentication signing and verifying of message is need. Message authentication may also verify sequencing and timeliness.

Figure 1. Requirement for Cloud Security.

Lack of multiple KDCs is another issue with existing systems. There should be a decentralized approach, meaning that there can be several KDCs for key management, which allows concurrent access on the resource and data sharing. Since in the proposed approach KDCs are distributed across the cloud, so it helps in fault tolerance in case a KDC failure. Technology should collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized. Figure 1 gives the idea about the requirement for secure cloud.

9. Conclusion and Future Work

Security concern has become the biggest obstacle to adoption of cloud because all information and data are completely under the control of cloud service providers. In the cloud, data and services are not restricted within a single organization's perimeter. This dynamism and fluidity of data introduces more risk and complicates the problem of access control. Therefore, compared with the traditional models, in cloud computing model ensuring confidentiality and integrity of the end-user's' data is far more challenging. Security issues can be categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues.

This paper finds out the problem associated with secure communication over the clouds. Paper extracts the issues and focuses on why is there need of encryption as well as message signing and verification for achieving confidentiality, data integrity and message authentication during service providing over the cloud? Optimal security services can be achieved if both encryption and authentication are applied on data processing over the cloud. Also Multiple ***KDCs*** are mandatory to handle fault tolerance. It is noted that solutions to various cloud security issues vary, from cryptography, particularly public key infrastructure (***PKI***), to use of multiple cloud providers, standardization of ***APIs***, and improving virtual machine support and legal support. Layered architecture of cloud computing requires different levels of security considerations.

Since security is one of the key requirements to enable privacy. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data. In the future, work can be done on Cloud Security System for secure communication over cloud.

References

[1] Shyam Nandan Kumar, "Cryptography during Data Sharing and Accessing Over Cloud." International Transaction of Electrical and Computer Engineers System, vol. 3, no. 1 (2015): 12-18.

[2] Shyam Nandan Kumar, "DecenCrypto Cloud: Decentralized Cryptography Technique for Secure Communication over the Clouds." Journal of Computer Sciences and Applications, vol. 3, no. 3 (2015): 73-78.

[3] Shyam Nandan Kumar, "Review on Network Security and Cryptography." International Transaction of Electrical and Computer Engineers System, vol. 3, no. 1 (2015): 1-11.

[4] Shyam Nandan Kumar, "World towards Advance Web Mining: A Review." American Journal of Systems and Software, vol. 3, no. 2 (2015): 44-61.

[5] Omar, M.N, Salleh, M., and Bakhtiari, M., "Biometric encryption to enhance confidentiality in Cloud computing", International Symposium on Biometrics and Security Technologies (ISBAST), 2014, IEEE, pp. 45-50, Kuala Lumpur.

[6] Chandar, P.P., Mutkuraman, D. and Rathinrai, M., "Hierarchical attribute based proxy re-encryption access control in cloud computing", International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2014, IEEE, pp. 1565-1570, Nagercoil.

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption", in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 3494. Springer, pp. 457-473, 2005.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89-98.

[9] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Public Key Cryptography (PKC '11), pp. 53-70, Springer, Berlin, Germany, 2011.

[10] Wenyi Liu, Uluagac, A.S. and Beyah, R., "MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data", IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2014, pp. 518-523, Toronto, ON.

[11] Jen Ho Yang and Pei Yu Lin, "An ID-Based User Authentication Scheme for Cloud Computing", Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014, IEEE, pp. 98-101, Kitakyushu.

[12] Jia-Lun Tsai and Nai-Wei Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services", Systems Journal, IEEE (Volume: 9, Issue: 3), pp. 805-815, 21 May 2015.

[13] Zheming Dong, Lei Zhang and Jiangtao Li, "Security Enhanced Anonymous Remote User Authentication and Key Agreement for Cloud Computing", IEEE 17th International Conference on Computational Science and Engineering (CSE), 2014, pp. 1746-1751, Chengdu.

[14] Nimmy, K., and Sethumadhavan, M., "Novel mutual authentication protocol for cloud computing using secret sharing and steganography", Fifth International Conference on the Applications of Digital Information and Web Technologies (ICADIWT), 2014, IEEE, pp. 101-106, Bangalore.

[15] A. Verma and S. Kaushal, "Cloud Computing Security Issues and Challenges: A Survey", Proceedings of Advances in Computing and Communications, Vol. 193, pp. 445-454, 2011.

[16] P. Sharma, S. K. Sood, and S. Kaur, "Security Issues in Cloud Computing", Proceedings of High Performance Architecture and Grid Computing, Vol. 169, pp. 36-45, 2011.

[17] Sudharsan Sundararajan, Hari Narayanan, Vipin Pavithran, Kaladhar Vorungati, Krishnashree Achuthan, "Preventing Insider

attacks in the Cloud", Communications in Computer and Information Science, vol. 190, issue. 5, pp. 488-500, 2011.

[18] Wayne Jansen, Timothy Grance, "NIST Guidelines on Security and Privacy in Public Cloud Computing", Draft Special Publication 800-144, 2011.

[19] Thomas W. Shinder, "Security Issues in Cloud Deployment models", TechNet Articles, Wiki, Microsoft, Aug, 2011.

[20] Alessandro Perilli, Claudio Criscione, "Securing the Private Cloud", Article on Secure Networks, Virtualization.info. http://virtualization.info/en/security/privatecloud.pdf

[21] Jon Marler, "Securing the Cloud: Addressing Cloud Computing Security Concerns with Private Cloud", Rackspace Knowledge Centre, March 27, 2011, Article Id: 1638.

[22] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80.

[23] "Swamp Computing a.k.a. Cloud Computing", Web Security Journal. 2009-12-28.

[24] "Top Threats Cloud Computing V1.0" , Cloud Security Alliance, 2010 https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[25] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing", The World Privacy Forum, 2009.

[26] Cross Site Scripting (XSS) attacks, http://www.acunetix.com/websitesecurity/cross-site-scripting/.

[27] During the second half of 2007, 11,253 site-specific cross-site vulnerabilities were documented by XSSed, compared to 2,134 "traditional" vulnerabilities documented by Symantec, in "Symantec Internet Security Threat Report: Trends for July–December 2007 (Executive Summary)".

[28] Justin Clarke; SQL Injection Attacks and Defense; Syngress 2009.

[29] A. Liu, Y. Yuan, A Stavrou, "SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks", SAC March 8-12, 2009, Honolulu, Hawaii, U.S.A.

[30] Jonathan Katz, "Efficient Cryptographic Protocols Preventing Man in the Middle Attacks", Doctoral Dissertation submitted at Columbia University, 2002.

[31] Craig Gentry, A FULLY HOMOMORPHIC ENCRYPTION SCHEME", PhD Thesis, STANFORD UNIVERSITY, September 2009.

[32] Ron Rivest (2002-10-29). "Lecture Notes 15: Voting, Homomorphic Encryption.

[33] Craig Gentry, "Fully Homomorphic Encryption Using Ideal Lattices", ACM 978-1-60558-506-2/09/05, STOC'09, May 31–June 2, 2009, Bethesda, Maryland, USA.

[34] B. R. Kandukuri, P. V. Ramakrishna, and A. Rakshit, "Cloud security issues," in Proceedings of the IEEE International Conference on Services Computing (SCC '09), pp. 517–520, September 2009.

[35] "Phlashing attack thrashes embedded systems" The Register. http://www.theregister.co.uk/2008/05/21/phlashing/.

[36] Jackson Higgins, Kelly (May 19, 2008). "Permanent Denial-of-Service Attack Sabotages Hardware", Dark Reading.

[37] Cloud Security Alliance (2012) SecaaS implementation guidance, category 1: identity and Access managament. Available: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf .

[38] Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[39] Ju J, Wang Y, Fu J, Wu J, Lin Z (2010) Research on Key Technology in SaaS. In: International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. IEEE Computer Society, Washington, DC, USA, pp 384-387.

[40] Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press.

[41] Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1-11.

[42] Viega J (2009) Cloud Computing and the common Man. Computer 42(8):106-108.

[43] Owens D (2010) Securing elasticity in the Cloud. Commun ACM 53(6):46-51.

[44] Ju KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey. Available: http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291.

[45] Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On technical Security issues in Cloud Computing. In: IEEE International conference on Cloud Computing (CLOUD'09). 116, 116, pp 109-116.

[46] OWASP (2010) The Ten most critical Web application Security risks. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

[47] Bezemer C-P, Zaidman A (2010) Multi-tenant SaaS applications: maintenance dream or nightmare? In: Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE), Antwerp, Belgium. ACM New York, NY, USA, pp 88-92.

[48] Cloud Security Alliance (2012) Security guidance for critical areas of Mobile Computing. Available: https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf.

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

[50] Xu K, Zhang X, Song M, Song J (2009) Mobile Mashup: Architecture, Challenges and Suggestions. In: International Conference on Management and Service Science. MASS'09. IEEE Computer Society, Washington, DC, USA, pp 1-4.

[51] Chandramouli R, Mell P (2010) State of Security readiness. Crossroads 16(3):23-25.

[52] Jaeger T, Schiffman J (2010) Outlook: cloudy with a chance of Security challenges and improvements. IEEE Security Privacy 8(1):77-80.

[53] Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA, pp 35-41.

[54] Garfinkel T, Rosenblum M (2005). When virtual is harder than real: Security challenges in virtual machine based computing environments. In: Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. Vol. 10. USENIX Association Berkeley, CA, USA, pp 227–-29.

[55] Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia.

[56] Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36-42.

[57] Reuben JS (2007) A survey on virtual machine Security. Seminar on Network Security. http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf. Technical report, Helsinki University of Technology, October 2007.

[58] Hashizume K, Yoshioka N, Fernandez EB (2013) Three misuse patterns for Cloud Computing. In: Rosado DG, Mellado D, Fernandez-Medina E, Piattini M (ed) Security engineering for Cloud Computing: approaches and Tools. IGI Global, Pennsylvania, United States, pp 36-53.

[59] Ranjith P, Chandran P, Kaleeswaran S (2012) On covert channels between virtual machines. Journal in Computer Virology Springer 8:85-97.

[60] Grobauer B, Walloschek T, Stocker E (2011) Understanding Cloud Computing vulnerabilities. IEEE Security Privacy 9(2): 50-57.

[61] Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine in Cloud Computing. In: 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18-21.

[62] Xiaopeng G, Sumei W, Xianqin C (2010) VNSS: a Network Security sandbox for virtual Computing environment. In: IEEE youth conference on information Computing and telecommunications (YC-ICT). IEEE Computer Society, Washington DC, USA, pp 395-398.

[63] Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0. Available: https://cloudsecurityalliance.org/research/top-threats.

[64] ENISA (2009) Cloud Computing: benefits, risks and recommendations for information Security. Available: http://www.enisa.europa.eu/activities/riskmanagement/files/deliverables/cloud-computing-risk-assessment.

[65] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469-487.

[66] Gonzales D, Kaplan J, Saltzman E, and Winkelman Z. "Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds", IEEE Transactions on Cloud Computing, pp 1. (2015).

[67] Hai Jin, Xinhou Wang, Song Wu and Sheng Di, "Towards Optimized Fine-Grained Pricing of IaaS Cloud Platform", IEEE Transactions on Cloud Computing. Vol 3, issue 4, pp. 436-448, (2015).

[68] Tatsuaki Okamoto and Katsuyuki Takashima, "Decentralized Attribute-Based Signatures" , Public-Key Cryptography – PKC 2013, Springer Berlin Heidelberg, pp 125-142.

[69] Xiaofeng Chen, Jin Li, Xinyi Huang, Jingwei Li, Yang Xiang and Duncan S. Wong, "Secure Outsourced Attribute-Based Signatures", pp: 3285-3294, IEEE, vol. 25, (2014).

[70] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 195-203, November 2007.

[71] A. Lewko, A. Sanais, and B. Waters, "Revocation systems with very small private keys," in Proceedings of the IEEE Symposium on Security and Privacy (SP '10), pp. 273-285, Oakland, Calif, USA, May 2010.

[72] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the IEEE Symposium on Security and Privacy (SP '07), pp. 321-334, May 2007.

[73] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 456–465, November 2007.

[74] A. Lewko, T. Okamoto, A. Sahai, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in Advances in Cryptology: EUROCRYPT 2010, vol. 6110 of Lecture Notes in Computer Science, pp. 62-91, Springer, Berlin, Germany, 2010.

[75] N. Attrapadung and H. Imai, "Dual-policy attribute based encryption," in Applied Cryptography and Network Security, pp. 168–185, Springer, Berlin, Germany, 2009.

[76] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography, vol. 4392 of Lecture Notes in Computer Science, pp. 515–534, Springer, Berlin, Germany, 2007.

[77] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 11, pp. 2150-2162, 2012.

[78] V. Bozovic, D. Socek, R. Steinwandt, and V. I. Villanyi, "Multi-authority attribute-based encryption with honest-but-curious central authority," International Journal of Computer Mathematics, vol. 89, no. 3, pp. 268-283, 2012.

[79] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Information Sciences, vol. 180, no. 13, pp. 2618-2632, 2010.

[80] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09), pp. 121–130, Chicago, Ill, USA, November 2009.

[81] M. Mambo and E. Okamoto, "Proxy cryptosystems: delegation of the power to decrypt ciphertexts," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 80, no. 1, pp. 54-62, 1997.

[82] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT '98), pp. 127-144, Espoo, Finland, 1998.

[83] Guojun Wang, Qin Liu, Jie Wu and Minyi Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", 2011.

[84] K. Emura, A. Miyaji, K. Omote, A. Nomura, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," International Journal of Applied Cryptography, vol. 2, no. 1, pp. 46-59, 2010.