Chapter 6
Cloud-Based Information Security

6.1 Introduction

Cloud computing facilitates on-demand service model and provides resources, information and software on sharable basis to their users. It supports heterogeneous connectivity of systems and can interact with each other at same time. The cloud computing provides various dynamically scalable resources as a service over the Internet. There are several economic benefits of using cloud computing as it reduces the overall expenditure and provides better performance and data storage capacity. However, there are still some potential challenges left to focus such as security, privacy and trust. The data that is being communicated between users, and cloud systems need to be secured from different threats and attackers. In [1], Shaikh and Haider have stated that one of the reasons why the cloud computing is not fully accepted by the users is the security. The users are always in fear of losing their data as well as privacy. They have identified various thrust area of cloud security and categorized them. Alassafi et al. [2] have emphasized on secure use of information technology (IT) to reduce risks and for further possible improvement of confidence and trust among the customers. They have stated that IT governance and information security governance (ISG) are two major factors for an organization to promote and use of cloud successfully. While implementing cloud security, security risks are associated with various infrastructure layers like application layer, virtualization layer, trust layer, authentication layer, access control layer, etc., the cloud computing can introduce the variety of risks and threats related to these layers. In [3], Tianfield has discussed about the various issues of security in cloud computing. They have analysed the cloud security requirements in terms of fundamental issues like trust, availability, audit, integrity and confidentiality. As the security is a major issue, it should be applied at different levels to ensure right implementation of cloud computing such as: security of host server, security of data storage, network security and security of application. In [4], Gugnani et al. have focused on cloud-based web services and proposed an approach for selective encryption of

P.K. Gupta et al., *Predictive Computing and Information Security*,
DOI 10.1007/978-981-10-5107-4_6

XML elements. They have used deoxyribonucleic acid (DNA) encryption technique for selective XML elements.

The cloud architecture is classified into four different layers [5] as shown in Fig. 6.1:

(a) Physical layer—The hardware level resources like network resources, computing resources and storage resources are all contained in this layer.
(b) Resource layer—All the resources that have been virtualized lie in this layer. These resources can be used by upper layers and end users further.
(c) Service layer—It supports various services, and software tool, middleware and provides development and deployment of platform.
(d) Application layer—It consists of all the executable applications in the clouds.

The cloud computing models are generally classified into three service models and four deployment models. The service models, as shown in Fig. 6.2 which can be categorized into further three categories: (i) Software as a Service (SaaS), (ii) Infrastructure as a Service (IaaS) and (iii) Platform as a Service (PaaS). On the other hand, the deployment models typically consist of (i) private cloud, (ii) public cloud, (iii) hybrid cloud and (iv) community cloud.

6.2 Related Work

Though the cloud computing architecture and its models are widely adopted by the industries, it still has certain drawbacks. The foremost issue in cloud computing is of security and privacy related to the data of the users. The cloud computing model leaves the clients vulnerable to different types of attacks and threats. Due to this, the client may suffer from a heavy loss of any confidential data or may lose any confidential information. An attacker may eavesdrop the conversation between two clients on cloud or between client and cloud. The users who move their data onto

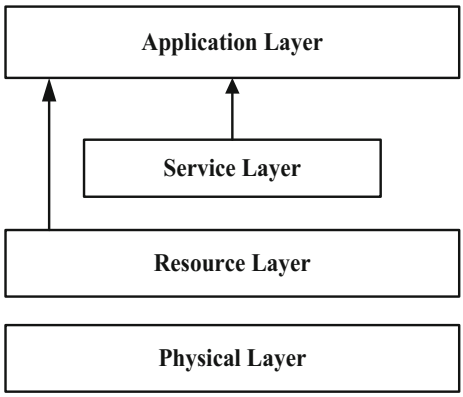

Fig. 6.1 The cloud architecture [5]

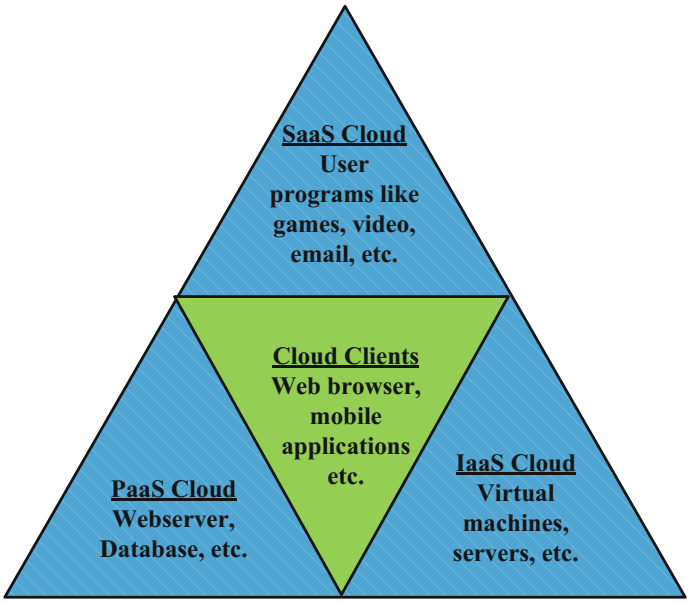

Fig. 6.2 The cloud computing service models

the cloud are unaware of the integrity of their data. They do not know as to where their data is getting stored. Due to these reasons, some users are still adamant of making use of this technology. So, there is a great need to protect the clients from such type of attacks.

The cloud security refers to a broad variety of technologies, policies, mechanisms, frameworks and controls deployed to protect data, applications and the associated infrastructure of cloud computing model. The potential areas that require focus to embed security features are:

- To safeguard all end cloud—user activities, actions regardless of device,
- To protect cloud, database and data centres, and
- To facilitate superior cyber security against various attacks.

The cloud security mechanism must ensure the implementation of correct defensive implementations. The well-organized cloud security mechanism should recognize and address the various security-related issues. Implementation of effective security mechanism and controls defend the system from flaws and decrease the possibility of an attack. These security controls can be categorized under the following category [1]:

- **Deterrent controls**—are anticipated to decrease attacks on a cloud. These deterrent controls typically diminish the effect of threat by notifying the attackers that there will be poor consequences for them if they continue further or move forward in that particular direction.

- **Preventive controls**—toughen the system against threats and attacks, and vulnerabilities. However, the well-built authentication of cloud customer stops unauthorized cloud access by the customers.
- **Detective controls**—are proposed to sense and respond to any accidents that occur. When an attack occurs, this control will sign the anticipatory or remedial controls to tackle the issue. The system and network sanctuary monitoring, intrusion detection and prevention arrangements, are typically engaged to sense attacks on cloud systems.
- **Corrective controls**—these controls decrease the result of a threat, usually by restricting the harm. These controls generally come into effect during or after an attack has occurred. Re-establishing system backup so as to reconstruct a cooperated system can be seen as a paradigm of a corrective control.

Since accessing of information in heterogeneous environment at a time, the integrity and privacy can be breached and always at risk. The cloud computing provides distribution of data over computers. When data is sent by the user to be processed in the cloud; the control of the data is given to a remote party that may not address security concerns of the user. As a user has no physical access to the data, he/she is unaware about the location of his/her data and is not sure whether the integrity of his/her data is maintained or compromised in the cloud. It is important to ensure that the information being processed on cloud is secure and no tampering of information is done when previously unknown parties may be present [6].

6.2.1 Security Issues

Security is termed as the prevention of any unauthorized access, unauthorized deletion or amendment of the information. ISO 27001 defines the security as: '*Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved*'. Cloud computing may introduce many risks to cloud service and cloud deployment model. In [7], Aluvalu and Mundane have presented various access control techniques and models and stated that privacy, trust and access control are important factor to maintain the security in cloud. Rashdi et al. [8] have defined the term cloud computing security as, '*The set of control-based technologies and policies designed to follow to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use*'. The main dimensions of security that should be kept in mind for providing user satisfaction are confidentiality, integrity and availability, (CIA) [9]. CIA provides the basis for implementing security principles, as shown in Fig. 6.3, to known set of threats and can be known as follows:

- Confidentiality—stands to keep the user's data secret. According to Xiao and Xiao [10], confidentiality is one of the major issues in cloud because the information that is outsourced by users on cloud servers is managed and

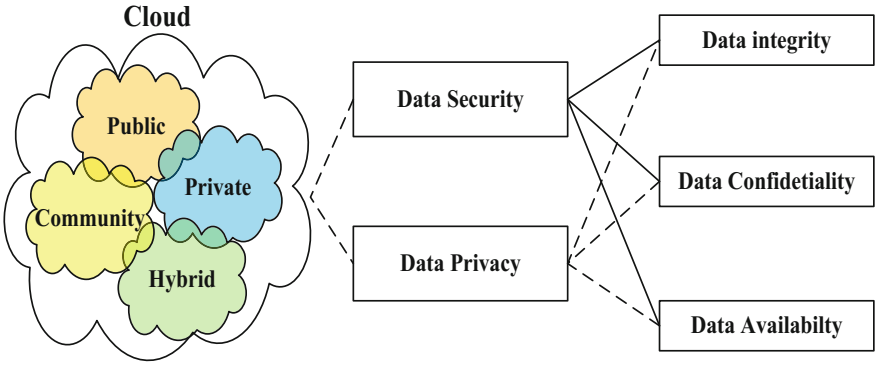

Fig. 6.3 Organizing security and privacy for various cloud deployment models

controlled by untrustworthy cloud providers. In [3], Tianfield also mentioned that threat to data increases because of increased number of applications, parties and devices which leads to increase in number of point of access. One way to achieve confidentiality is to encrypt the information sent by user before placing it in cloud.

- Integrity—stands to preserve the integrity of the information. It should be checked that the information is not lost or modified by unauthorized user. One technique to maintain the integrity is usage of digital signature. In [3], the authors have stated that by using service level agreement (SLA), information is protected while it is on cloud, preventing intrusion or attack on data and responding swiftly to attacks such that damage is limited.
- Availability—The users can access the resources, information from any place and at any time. Denial of service attacks, equipment outages and natural disasters are all threats to availability of information in clouds. According to Zissis and Lekkas [12], the availability should not only be in terms of information, software but also hardware being available to authorized users upon demand.

The risks associated to stored information in clouds can vary according to cloud service models deployed by the organization. Some risks can affect all the cloud service models including SaaS, PaaS and IaaS, whereas some are limited to one or two models only. Table 6.1 represents some of the major risks of cloud computing associated to CIA security principles.

6.2.2 Privacy Issues

The cloud computing uses different ways to manage the information and user-related personal data. The privacy refers to the right to self-determination, i.e. the ability of individual or group to seclude them from access of information and

Table 6.1 Various risks associated to CIA security principles and cloud service models

CIA security principles	Associated risks	Cloud service models		
		SaaS	PaaS	IaaS
Confidentiality	Users from organization	•	•	•
	Attacker(s)	•	•	
	Data leakage	•	•	
Integrity	User access	•	•	•
	Data segregation	•	•	
	Quality of data	•	•	
Availability	Change of policies or management	•	•	•
	Denial of service	•	•	•
	Physical disruption			•
	Lack of recovery methods	•	•	•

then selectively reveal them. Privacy issues are becoming more important while using Internet-based transactions. Lack of effective security mechanism and loss of control could result in serious threat to data integrity, confidentiality and privacy principles [13]. In terms of organization, personally identifiable information is managed by providing privacy which involves the application of processes, standards, laws and mechanisms. Xiao and Xiao [10] have considered the emerging cloud platform and used an attribute-driven methodology to design security and privacy paradigm. They have used attributes like confidentiality, availability, integrity, accountability and privacy-preservability. In [14], Chen and Zhao have analysed the data security and privacy-related issues using various algorithms. They have stated that because of these issues, many large organizations still do not share their data on cloud. In [15], Sun et al. have identified the various elements related to privacy and categorized them in three groups known as (i) *When*—a user is more cautious about the use of information which is either being accessed or will be accessed, (ii) *How*—user must ensure the way for accessing this information manually or automatically, (iii) *Extent*—user can define the several points as an ambiguous region and can only be used by group of users those who have the precise access to that region. Privacy issues vary according to different cloud scenario. In [16], Pearson has mentioned that existing cloud services impose a lot of challenges to privacy of data while handling sensitive data, and data leakage related issues and suggested that this type of data cannot be stored in public clouds of various cloud service providers in an unencrypted form. Pearson [16] and Guilloteau et al. [13] have identified the key potential privacy issues as follows:

- Lack of user control—As the user stores their data over public cloud, then cloud service providers become responsible for further handling and managing of data. Users have limited control over the stored data in public clouds. There is always an issue of transparency in between the cloud user and service providers as the stored data over clouds can be analysed by security agencies or law enforcement

agencies. A trust is required between both of the parties while transferring data rights and providers must ensure the data integrity throughout its lifecycle.

- Lack of training and expertise—Developers are focusing more on easy to design and deployment models of clouds rather the handling of privacy concerns to their models. They need to be trained with existing information security laws and practices to maintain the privacy of data. By ensuring privacy of users data, one can build the trust over the period of time.
- Unauthorized use of data by third party—There is always a risk associated with the stored data in the clouds that it can be used by the third party for their own purpose. Nowadays, it is getting more common as users may get annoying advertisements while accessing or using of stored information. Currently, there is no such arrangement to stop this unauthorized use of data by third party.
- Achieving regulatory compliance—Global use of cloud computing makes it complex as user never knows about the exact location of data that is being stored in clouds. These cloud servers can be in the same country or may be located globally. Things become complex if cloud is located in different country as many legislations in place around the world. It is always difficult to ensure compliance with all the legislations. The cloud computing may exacerbate the transborder data flow issue that may restrict the flow of information.

6.2.3 Trust Issues

Trust is a measureable belief that is used to make trustworthy decisions based on experience and it is a major issue with cloud computing irrespective of the cloud model being deployed. The security and privacy challenges discussed above are also relevant to the general requirement upon cloud suppliers to provide trustworthy services. Trust relationships are very much at the centre of certain security and privacy solution. To build trust, one need to ensure security and privacy of data is intact and foolproof. This situation is also depicted in the Fig. 6.4, where trust lies in between security and privacy. Trust has several different attributes like reliability, confidence, dependability, honesty, etc., to obtain various cloud services. Sun et al. [9] and Pearson [16] have identified various issues of trust in cloud computing:

- The attributes of cloud computing environment are unique, so the definition and evaluation of trust become difficult.
- Based on the degree of trust, how to provide different security level of services.
- The trust relationship in cloud computing is temporary and dynamic, so handling of malicious information is a tough task.
- Lack of consumer trust is another major reason for avoiding the cloud adoption. Various critical challenges like vendor's lock-in, cloud availability, cloud performance, cloud data security, etc., need to be addressed to encourage cloud adoption. In clouds, customers have limited control of resources that is why they cannot protect their data against unauthorized access or its misuse.

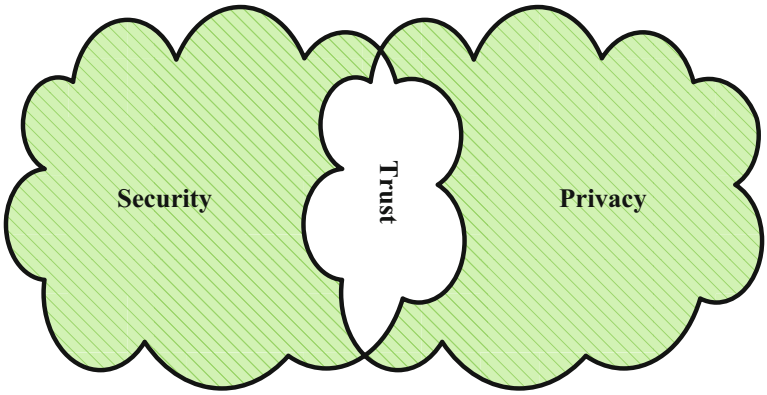

Fig. 6.4 Obtaining trust from security and privacy of data

- Weak trust relationships and lack of transparency between cloud user and service provider may lead to failure of cloud service delivery chain.
- Lack of knowledge and consensus for using standardized trust models and approaches for cloud environment [17].

6.2.4 Issues with Cloud Service Models

Apart from the issues as stated in the preceding sections, there are many other issues of cloud computing pertaining to its different service models known as IaaS, PaaS and SaaS. In [18], Rana et al. have proposed a combined and improved IaaS and PaaS architecture to remove their drawbacks.

- **IaaS issues**—It provides only basic level of security like load balancing, firewall, etc. The applications moving to the cloud require high degree of security. One company may be hosting many other companies' workloads and data in a shared environment. In such cases, it may expose all parties to a higher risk of security- or privacy-related incidents [19]. In [20], Joshi et al. have listed the component wise security issues in IaaS like SLA issue for monitoring of quality of services to cloud users and enforces trust between cloud service provider and user, and cloud software related issues which coins the cloud component together to make them act as a single component so that attackers cannot easily target the SOAP envelop or XML signature. The different issues in IaaS are summarized as follows in Table 6.2 [21]:
- **PaaS issues**—The hacker can use the advantages of PaaS to influence the PaaS cloud infrastructure for malware command and control. One major challenge is the interoperability of PaaS as most of the applications, APIs, database are vendor specific. The various issues in PaaS are summarized in Table 6.3 [21].

Table 6.2 Issues in IaaS

Area	Security	Privacy	Trust
DOS (denial of service)	Misconfiguration, vulnerabilities in system or OS	Access control compromised	Service not available
Robustness of virtual machine-level Isolation	Vulnerabilities in hypervisor	Internal network probing may occur	Compromised virtual machines/hypervisors permit the loss of trust
EDOS (economic denial of service)	Authentication, authorization, and accounting (AAA) vulnerabilities	User provisioning, de-provisioning vulnerabilities	Access control compromised

Table 6.3 Issues in PaaS

Area	Security	Privacy	Trust
Technical immaturity	Compliance challenges	Storage of data in multiple jurisdiction and lack of transparency about this	Lack of information on jurisdictions
Lack of portability	Non availability of common authentication interface	'Data hostage' clause in supplier outsourcing contracts	Liquidate damage for lost business
Protecting API keys	Bad key management procedures	Service information leakage	Lack of sensitivity

- **SaaS issues**—The main focus is not only on application's portability but also on migration of data and enhancement of security functionalities. For development and deployment of SaaS application, the order of following security elements must be ensured. The following should be kept in mind:
  - *Data security*—In SaaS model, the data is stored at the vendor's end. The SaaS vendor should acquire additional security checks so as to ensure security of data and prevent data breach through unauthorized users. The strong encryption techniques should be involved for data security. Due to loophole in data security model, malicious users can gain access to the data.
  - *Network security*—The sensitive data that is obtained from the users/organizations are stored at SaaS vendor end. All the data over the network must be protected to prevent leakage of data. This is achieved by using strong encryption techniques to manage network traffic like SSL and TLS.
  - *Data locality*—The applications provided by SaaS are used by consumers and then data processing is done. The consumers are unaware of the fact as to where their data is getting stored. Example: In many European countries, certain type of data cannot leave the country because of the information being sensitive. The SaaS model should provide reliability to the customer in terms of location of data
  - *Data integrity*—It is easier to achieve data integrity in a single system with single database by making use of database constraints and transactions. Transactions follow ACID properties. The problem of data integrity gets magnified in case of cloud computing. The SaaS vendors unveil their web service APIs without any support for transactions. There are different levels of availability and SLA in each SaaS application which makes it difficult to manage the transactions and provide data integrity
  - *Data segregation*—Due to multi-tenancy feature in cloud computing, multiple users can store their data on cloud. The data of various users will reside at same location. Intrusion in user's data by another user becomes easy in such environment. Intrusion can be done by hacking or by injecting client's code into SaaS system. Therefore, SaaS model should ensure boundary for each user's data not only at physical level but also at application level

Table 6.4 Issues in SaaS

Area	Security	Privacy	Trust
Unauthorized access	Data integrity and confidentiality loss	Compromised communications secrecy	Loss of trust in service
Physical risks	Physically destroyed data	–	–
Browser-based risks	Loss of data integrity, and confidentiality	Loss of user secret credentials	Loss of confidence upon channel
Network dependence	Loss of availability	–	Trust on service reduces

- *Data access*—Various security policies are provided by the organization to the users when accessing the data. Based on these policies, each employee can access limited information. Cloud must stick to these security policies in order to avoid intrusion of data.
- *Authentication and authorization*—The authentication is assurance that the communicating entity is the one that it claims to be that is 'who are you?' and authorization is a kind of access control 'what you can do'. This means that no unknown or harmful entity should able to pretend that he or she is the authenticated one and even authenticated persons should have a limited access to the data.

The various issues in SaaS are summarized in Table 6.4 [22].

6.2.5 Threats in Cloud Computing

The cloud security alliance has presented a primary draft for threats relevant to the security architecture of cloud services. In this section, we have given few potential threats related to the cloud [23, 24].

(a) **Malicious insiders**—Majority of the companies conceal their strategies about the height of access to their staff. Though, via superior level of access, a member of staff can grow access to top secret data and services. As there is deficiency in transparency of cloud provider's policies, processes and procedures, some insiders can frequently have the privilege to access the client's data. Malicious insiders (employee) actions are often evaded by a firewall or infringement discovery system considering it to be an authorized action. Though, a trusted member of staff may also convert into an opponent. In these kinds of scenarios, insiders can source a significant effect on cloud services. Let us take an instance —here malicious insiders can access top secret data and put on control over the cloud services without any jeopardy of revealing his identity. These kinds of threats may be applicable to any cloud service SaaS, PaaS and IaaS. So as to avoid these kinds of risks, there is the need of more transparency in security and management process together with compliance reporting and breach

notification. This is amplified in the cloud via the meeting of IT services and client over a single management domain which is united within a general transparency deficiency into the service supplier process and procedure [25].

(b) **Shared technology issues/multi-tenancy nature**—Virtualization in multi-tenant architecture is used to provide shared on-demand services. Different users who have access to the virtual machine may use the same shared application. Though, as mentioned above, via some attacks and threats, some malicious entities can gain access and control of the lawful users' virtual machine. In multi-tenant architecture through shared resources, IaaS services are delivered which sometimes are not designed to give sufficiently strong isolation. Giving permission to one tenant to interfere in the other can cause serious affect on the cloud architecture which can affect its regular operations. Generally, these types of threats have an effect on IaaS. Transparency in SLA for patching, well-formed authentication system and access control mechanisms to administrative tasks are some of the solutions to resolve this issue.

(c) **Insecure Interfaces and APIs**—Cloud providers offer their services by using the various types of APIs, available for different cloud service models like SaaS, PaaS and IaaS. These weak set of APIs and interfaces can result in many security-related issues in cloud which includes unauthorized access of security key and data, insufficient input data validation, weak credentials that lead to loss of data integrity and CIA [26, 27].

(d) **Data threats**—In [27], Kazim and Zhu have stated that in cloud computing, data is the valuable resource for any organization, and security of the data is the biggest challenge for cloud service providers. Major data security threats that may arise over the period of time are data breaches, data loss, unauthorized access and integrity violations.

- **Data breaches**—are also commonly known as data leakage of stored information in cloud via unauthorized access. The major reasons of data breaches are poor application designing, flaws in operational and infrastructure setup, insufficiency of authentication, authorization and audit controls [27].
- **Data loss**—Information can be exchanged in many ways. This can incorporate data insertion, data compromise, deletion or modification. Data loss occurs because of many reasons like malicious attackers, data deletion, data corruption, etc. [27]. As the cloud is shared and dynamic in nature, so these threats could prove to be of a foremost concern leading to data theft.

(e) **Service hijacking**—is a very serious threat. In this, the hijacker may forward the cloud customer to an illegal website. For attackers, service instances and user accounts can serve as a new base for attack. This threat can have great impact on IaaS, PaaS and SaaS. There are some of the solutions to resolve this threat which include safety policies, strong authentication and activity monitoring.

(f) **Identity theft**—The identity theft is a kind of scam in which one acts as if to be someone else so as to access resources or obtain credit and other benefits. The casualty (of identity theft) can undergo undesirable consequences and losses and held responsible for the criminal's activity. Some of the security perils are phishing attacks, weak password, recovery workflows, key loggers, etc. This threat can have significant impact on SaaS, PaaS and IaaS and some of the solution includes the use of powerful encryption, authentication and authorization mechanisms.

(g) **Denial of Service (DOS)/Distributed Denial of Service (DDOS)**—DOS attacks prevent users from accessing of cloud services, network and other services whereas in DDOS, attackers use the multiple network sources to send a large number of requests to the cloud for consuming its resources [27, 28].

(h) **Online Cyber theft**—In [29], Chou has stated that as the cloud-based services are becoming popular among the customers and organizations for storage of information, stored sensitive data is becoming an attractive target to online cyber theft. Online cyber thieves can make the use of stolen password and user IDs or can take the advantage of computing power offered by cloud service providers to launch attacks or to access user accounts.

6.2.6 *Attacks on Cloud*

There is number of security risks and issues as shown in Fig. 6.5, associated with cloud computing but they are grouped in two categories: (i) security issues faced by cloud provider and (ii) security issues faced by their customers. Various types of attacks in cloud are listed as follows:

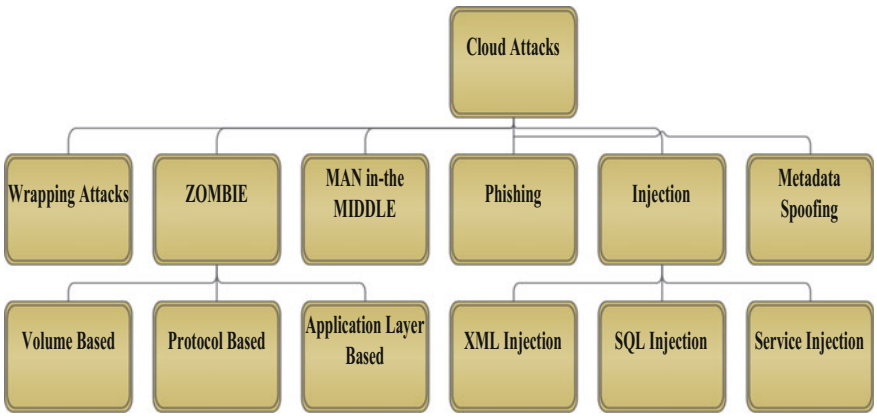

Fig. 6.5 Various types of cloud attacks

(a) **Zombie Attack**—An attacker can overflow the huge number of requests via *zombies*. This kind of attack disrupts the normal performance of cloud, disturbing the availability of cloud services. This cause cloud to be overloaded to serve a huge number of requests and therefore all its resources get exhausted, which can further originate DoS (Denial of Service). In DoS, in cloud due to the presence of invader's overflow of requests, cloud becomes unavailable to serve legitimate user's requests. Nevertheless, strong authentication and authorization and IDS/IPS can offer defense in opposition to such type of attack.

(b) **Injection attack**—Injection attacks are such attacks where intentionally malicious data is included as the input to disrupt the normal functioning of the cloud. A few of the injection attacks are:

- *XPath Injection:* When user and the cloud communicate, they communicate through XML files. XPath is a kind of query language for XML document as for relational databases we have SQL. Dissimilarity among SQL and XPath is that XPath is implementation independent [30]. XPath injection can occur by querying the XML database or when a service is invoked.
- *SQL injection:* In such kind of attacks, user injects malicious SQL statements into an entry field for execution. SQL injection is generally recognized as an attack vector for websites but can be used to attack any type of SQL database.
- *Service Injection:* An opponent attempts to insert a suspicious service or new illegal virtual machine into the cloud system and could supply malicious service to users. Cloud malware deforms the cloud services by changing (or blocking) cloud functionalities. Let us take an example in which an opponent makes its own malicious services like SaaS, PaaS or IaaS and attach it to the cloud system. In case, an opponent becomes successful to perform this, then legitimate requests are readdressed to the malicious services automatically. To protect against such an attack, there is a need to implement the service modules.

(c) **Man-in-the-Middle attack**—An attacker is capable of accessing the data exchange between two parties, if SSL is not configured properly. In case of cloud, an attacker is capable of accessing the data communication between data centres. To reduce or to prevent cloud from man-in-the-middle attack, proper configuration of SSL and data communication tests between cloud and its client are required.

(d) **Metadata spoofing attack**—In such kind of attack, an opponent amends or changes the service's Web Services Description Language (WSDL) file where descriptions about service instances are stored. In case, if the opponent succeeds to suspend service invocation code from WSDL file at delivering time, then metadata spoofing attack can be feasible. So as to triumph over such an attack, information about services and applications should be kept in ciphered form. Currently, WS-Security Service is broadly used in cloud to endow with security for the system [31].

(e) **Phishing attack**—is famous for manipulating a hyperlink and sends false link to obtain confidential information from the user. In cloud, sometimes it might be possible that an adversary uses the cloud service to host a phishing attack site to hack accounts and services of other cloud users.
(f) **Wrapping attack**—In [29], Chou has mentioned that web service security mechanism is used to ensure the confidentiality and integrity of SOAP messages communicated between user and cloud service providers. Wrapping attacks use XML signature wrapping to exploit a weakness when web servers validate signed requests [32]. These attacks generally take place during the translation of SOAP message between users and web servers. Since cloud users normally request services from cloud computing service providers through a web browser, wrapping attacks can cause damage to cloud systems as well. In [33], a group of researchers have demonstrated the use of XML signature wrapping technique for hijacking of an account that exploited vulnerability in the Amazon web service.

6.2.7 Cloud-Based Information Security Models

To ensure cloud security at various levels from information retrieval to its storage, security models are implemented. These security models must ensure the support for cloud security issues related to security issues, privacy issues, and trust issues as discussed in previous section. These security models also build the user's confidence by deploying various techniques for handling the various cloud-related threats. In [34], Mushtaq et al. have proposed the quad-layered framework for data security, data privacy, data breaches and process associated aspects. This proposed layered framework prevents the confidential information and try to build user's trust on cloud computing. In [35], Kritikos and Massonet have proposed a security meta-model for clouds. This model captures the high-level and low-level security requirements and capabilities to derive application deployment. Nafi et al. [36] have proposed a security model for cloud and implemented various security algorithms like RSA, AES and MD5 for secure communication of information between users and servers. To resolve the problem of privacy in the clouds, Metri and Sarote [37] have introduced a threat model known as STRIDE which helps in analysing a problem, designing appropriate strategies and evaluating the solutions. They have listed the following steps to ensure the privacy:

(a) Identify—attacks, and threats
(b) Prioritize threats—according to the impact using STRIDE model.

- Spoofing identity—means an attacker poses as another user or a machine poses as a valid machine.
- Tampering with data—means to maliciously modify the data.
- Repudiation.
- Information disclosure—means to expose the information to the unauthorized users.

- Denial of Service (DoS)—means to deny any service to valid users. Example: web browser made temporarily unavailable.
- Elevation of privilege—means the privileged access is gained by unprivileged users to destroy entire system.

(c) Select appropriate strategies for threats

In [38], Mathew has presented a model to help the cloud users and cloud providers to ensure the safety of data. He has used the secured virtual private network (VPN) for accessing clients and providers. In [39], a privacy protection framework was proposed by Gajanayake et al. based on information accountability (IA) components. They have used IA agent for accessing of information by the users. In case of any misuse of information, IA agent implements various methods to stop this. In [40], Chidambaram et al. have proposed a secure storage system to handle sensitive data in clouds. They have introduced a user authentication mechanism to prevent unauthorized access to data. RSA algorithm has been used for encryption of files in cloud and MD5 has been used to generate the digital fingerprint. Hamlen et al. [41] have proposed a framework consisting of layers for cloud security and focused on two of the layers known as the storage layer and the data layer. A bottom-up approach to security was also proposed, where work is done on small problems in the cloud to solve the larger problem of cloud security. First, the various methods have been discussed for securing of documents. Second, how security can be enhanced by using secure coprocessors is discussed. Juels et al. [42] described a formal 'Proof of Retrievability' (POR) model as shown in Fig. 7.6 for ensuring the remote data integrity. This model utilizes the error correction code approach to verify the validity of data. In POR protocol, the verifier stores only a single key for each file. This scheme requires that only a small portion of file F is accessed by the prover in course of a POR. POR encrypts file F and randomly valued check blocks called *sentinels* are embedded. The prover is challenged by the verifier by specifying position of collection of sentinels and asking the prover to return associated sentinel values. If any modifications are made on file F by the prover, then large number of sentinels is likely to be compressed. To protect corruption of file F by the prover, error correcting codes are employed.

In Fig. 6.6, by using encoding algorithm, raw file F is transformed into file F' and is stored with the prover/archive. A key K is produced by using the key generation algorithm and it is stored by the verifier. The key K is used in encoding mechanism. A challenge–response protocol is performed by the verifier with the prover to check that file F can be retrieved by the verifier. The drawback of the approach is that there is computational overhead. In [21], Mohta et al. have discussed about the implementation of TPA for verifying the cloud service provider (CSP). A protocol was proposed that is used for supporting various operations which also maintains privacy and integrity. The architecture is shown in Fig. 6.7

In [43], Chalse et al. provide a detailed analysis of the cloud security problem. The different problems in a cloud computing system and their effect upon the different cloud users are also analysed. This architecture is shown in Fig. 6.8 and consider the following:

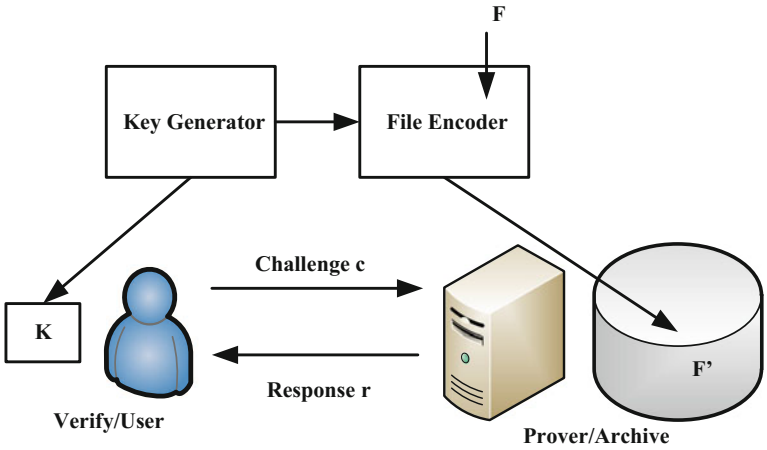

Fig. 6.6 Schematic of a POR system

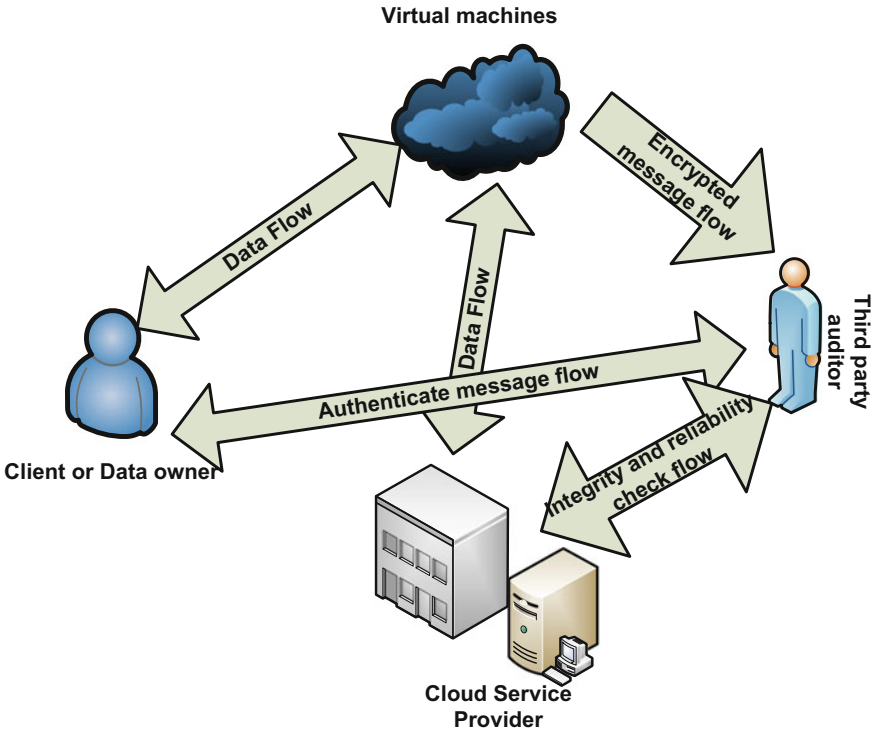

Fig. 6.7 Architecture for client, third party auditor and cloud service provider

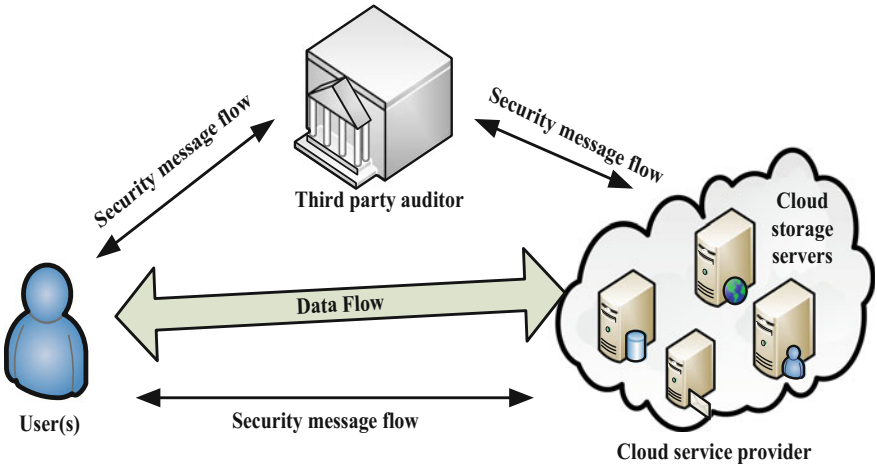

Fig. 6.8 Cloud data storage architecture

- A client who wants to store large amount of data in multiple clouds and has the permissions to access and manipulate stored data.
- Cloud service providers (CSP) support various services related to data storage and its usage and have sufficient resources available for computation.
- Trusted third party (TTP) ensures various parameters related to storage and use of data and provides appropriate public query services available to these parameters.

6.3 Framework to Maintain Data Integrity

This section defines the proposed framework to provide data integrity in multi-cloud system. Proposed framework shown in Fig. 6.9 has three main roles [11]:

- *Users*—who will store the data by selecting appropriate layer depending on the level of security needed for the data stored on cloud.
- *Cloud service provider (CSP)*—provides the storage of data service with flexible resources to keep the user data. The CSP manages cloud server (CS) which informs the user about the intrusion of data on cloud.
- *Third party auditor (TPA)*—verifies the cloud server and checks whether there is any manipulation of user data by the cloud server. It then sends a report to the user stating that the cloud server (CS) was trusted or not.

There are many cloud service providers and each of them provides different storage plan along with different QoS parameters so it becomes a tough task for users to keep moving their data from one cloud to another based on QoS and cost optimization [14]. In the proposed model, concept of multi-cloud is used to provide best cost optimization for various requirements of user.

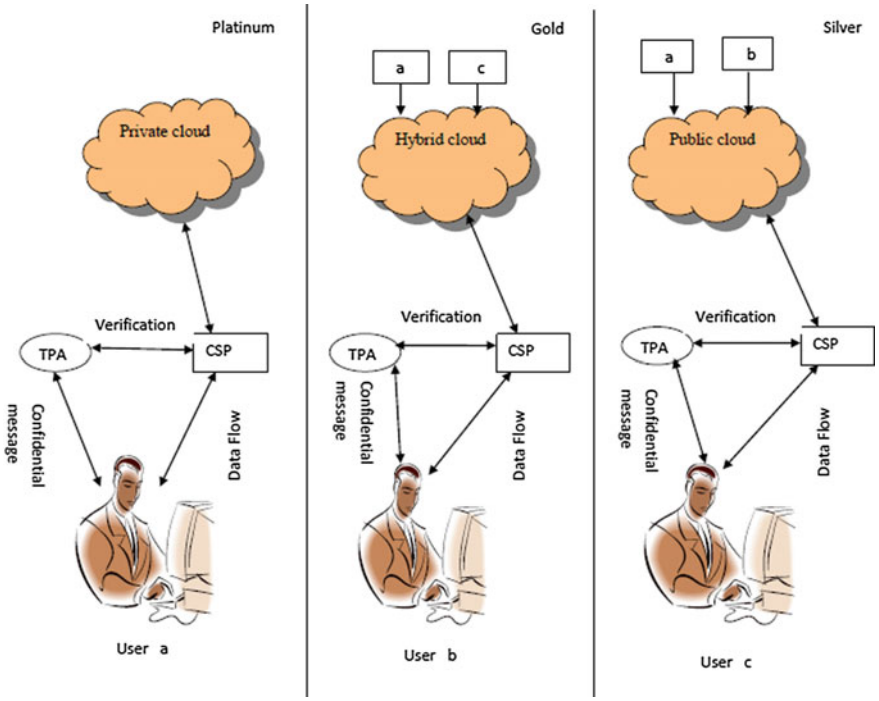

Fig. 6.9 Data integrity framework

It can clearly be seen that depending on type of data, the user can move from one service provider to another, e.g. the user 'a' can put his data over hybrid or public cloud depending on the security needed for the data stored. The same thing can be applied by other two users. Depending on the type of data to be stored on various clouds, there are three main platforms in the model namely:

- *Platinum*—To store sensitive data like data related to transactions of ATMs, bank account information along with high level of security on the data. The data will be stored on a private cloud.
- *Gold*—To store data related to simple login on any page like Facebook, ebooking and email login is stored. The level of security needed is not that high. Security only on password is required.
- *Silver*—To store data related to only simple browsing of sites, uploading of images, downloading of files like downloading of music files or images are stored. The level of security needed is the least.

Based on these levels, the user will decide the platform to store the data.

6.3.1 Data Integrity Algorithms

In this section, we have discussed various algorithms which are used to implement the proposed framework.

Algorithm 6.1: SaaS cloud integrity

```
/* Variables used for:
        User => u,
        Platinum => p,
        Gold => g
        Silver => s
 */
 Begin
        If u chooses p
          Then call module m1;
        If u chooses g
          Then call module m2;
        If u chooses s
          Then call module m3;
 End

Module m1:
  Begin
     User's data is encrypted using RSA and sent to CSP;
     Data is verified by CSP;
     If data is valid
           success message;
      Go To Module T
  End

Module m2:
  Begin
     Data stored is encrypted using Bcrypt algorithm;
     Data is verified by CSP;
     If data is valid
           success message;
     Go to module T
  End

Module m3:
   Begin
     Data is encrypted using AES algorithm;
     Verification of data is done by CSP;
     If data is valid
       success message;
     Go To Module T
    End

Module T:
  Begin
     Check the data stored.
     If  user's data == cloud data then
       data valid;
     Else
       corrupted data;
  End
```

In module m1, RSA algorithm [44] is used to provide integrity of data because for storing sensitive information on cloud, hashing algorithms are used. RSA is based on the difficulty of factoring large numbers. There are various advantages of RSA due to which it is preferred over DSA.

- DSA can only be used for authentication while RSA can be used for both authentication and to encrypt a message.
- A bad random number generator will leak DSA key bits.
- Faster at encrypting than DSA.

In module m2, Bcrypt algorithm is used for hashing the passwords over algorithms like MD-5, SHA-1, SHA-2 and SHA-3. A password hashing algorithm should preferably be slow in order to prevent brute force attacks; it should have features which actually decrease the feasibility of a distributed brute force attack on the hashes. Bcrypt algorithm is derived from the Blowfish block cipher which uses lookup tables that are initiated in memory to generate the hash.

In module m3, AES algorithm is used to provide security on the stored data. AES is asymmetric encryption algorithm which is used to encrypt the message. Here, sender uses the public key of receiver and receiver uses its private key to decrypt the message. The following features of AES over DES describe its usability for the framework presented in Fig. 6.10.

- AES is more secure in comparison to DES algorithm.
- AES data encryption is mathematically more efficient and elegant cryptographic algorithm. Key length option is the main strength of the algorithm. Time required to crack an encryption algorithm is directly related to the length of the key used to secure the communication. AES gives an option to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger as compared to the 56-bit key of DES.
- Block size of DES is small compared to AES algorithm.
- A balanced Feistel structure is used by DES while substitution-permutation is used by AES.

6.3.2 Performance Analysis of Security Techniques

In order to provide assurance of characteristics in cloud systems like reliability, security, fault tolerance, sustainability and scalability, computational services timely, repeatable and controllable methodologies are required for evaluation of new cloud applications and policies before actual development of cloud products. In [45], Thakur et al. have presented the simulations of above mentioned algorithm using CloudSim. Algorithmic analysis and obtained results using RSA, AES and Bcrypt for the presented framework in Fig. 6.9.

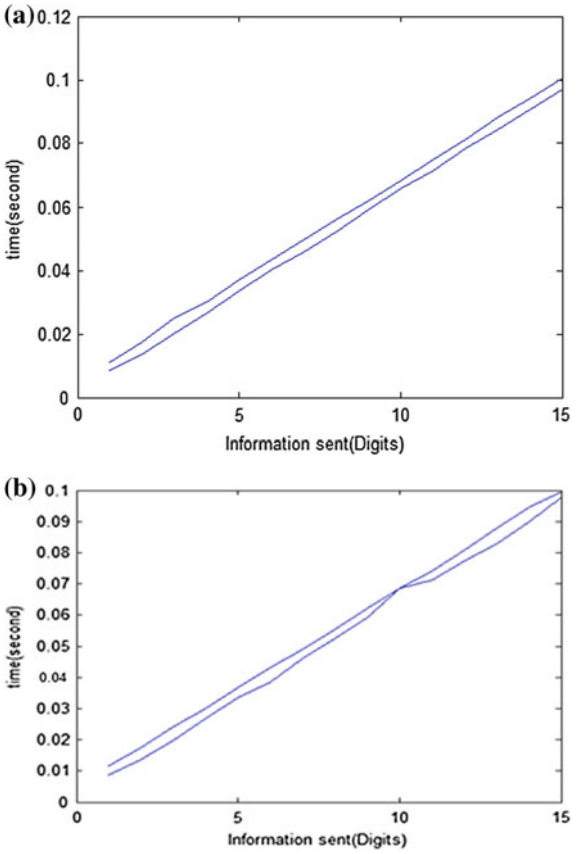

Fig. 6.10 Message length versus time. **a** $p = 3$ and $q = 7$, **b** $p = 23$ and $q = 17$

- *RSA Algorithm Analysis*

RSA algorithm is tested for integer numbers ranging from a single digit message length to 16-digit message length. The execution time t is in seconds. The execution time depends on the values of p and q which are prime numbers. Different values of p and q have been considered and depending on these values, graph between message length and time is plotted (Fig. 6.10a, b).

- *AES Algorithm Analysis*

AES is used here to provide data integrity while simple browsing of webpages over Internet. Plain text is encrypted to hexadecimal format. The change in graph depends on the value of plain text. The time taken increases if there is a use of combination of text and digits. A graph between information sent and time is plotted (Fig. 6.11).

Now by using the discussed framework and the type of information that has to be stored, multilevel security can be provided on different files. Tables 6.5, 6.6 and 6.7 summarize the execution time of four different files using RSA algorithm, Bcrypt algorithm, AES algorithm, respectively.

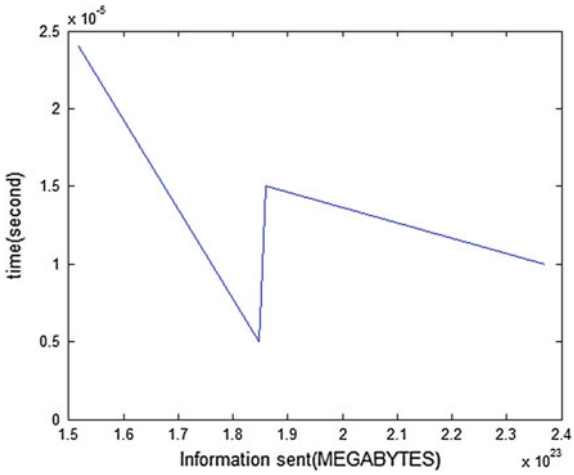

Fig. 6.11 AES algorithm

Table 6.5 File execution time using RSA algorithm

File size (MB)	RSA encryption (ms)	RSA decryption (ms)
1	66,787	720
2.9	2206	385
3.98	17,325	1081
4.65	40,441	1064

Table 6.6 File execution time using Bcrypt algorithm

File size (MB)	BCRYPT encryption (ms)	BCRYPT decryption (ms)
1	1306	447
2.9	1218	454
3.98	1225	510
4.65	1225	445

Table 6.7 File execution time using AES algorithm

File size (MB)	AES encryption (ms)	AES decryption (ms)
1	2129	234,229
2.9	3132	21,663
3.98	3276	71,129
4.65	2613	152,405

Table 6.8 Performance analysis of previous scheme versus proposed framework when number of requests is 8

No. of requests	Previous scheme [21] (time in ms)	Proposed scheme (time in ms)
1	3074	3074
2	3074	2917
3	3075	796
4	3009	1108
5	2995	1108
6	2905	796
7	3079	921
8	3420	827

Table 6.9 Performance analysis of previous scheme versus proposed scheme when number of requests increased to 16

No. of requests	Previous scheme [21] (time in ms)	Proposed scheme (time in ms)
1	3248	3006
2	3291	3110
3	3106	900
4	3341	1249
5	3570	1289
6	3320	1160
7	3334	1276
8	3456	900
9	3418	1000
10	3534	958
11	4018	2987
12	3987	3540
13	3765	3491
14	4211	4010
15	4300	2667
16	4696	3800

To analyse the performance of discussed algorithm, a comparative analysis is also done with previous algorithms using the presented framework. In [21], all files were provided same level of security irrespective of the type of data which is in contrast to the current framework that provides different levels of security on files with varying sizes. Tables 6.8, 6.9 and 6.10 present the comparison between the encryption time of previous scheme and the proposed scheme when the number of requests keeps on increasing. Figure 6.12a–c, represent this process.

Table 6.10 Performance analysis of previous scheme versus proposed scheme when number of requests increased to 32

No. of requests	Previous scheme [21] (time in ms)	Proposed scheme (time in ms)
1	3896	3694
2	3424	3341
3	3308	3208
4	3410	3400
5	3540	3459
6	3691	3576
7	3330	3200
8	3120	3110
9	3600	3567
10	3498	1000
11	3900	3741
12	4009	4003
13	3774	3669
14	4219	4198
15	4166	4047
16	4333	4216
17	3681	3538
18	3908	3497
19	3724	3623
20	3805	3551
21	3500	3348
22	4460	4234
23	4000	3811
24	4790	4626
25	4546	4377
26	3980	3694
27	2196	987
28	2897	1248
29	3071	2381
30	4298	3106
31	4571	3963
32	5168	4685

Tables 6.8, 6.9 and 6.10 show the average time taken for all three cases for proposed framework and performance is evaluated as shown in Table 6.11.

The average time taken by the schemes in both the cases is shown in Fig. 6.13. It can be predicted easily that the time taken by proposed scheme is less than the time taken by previous scheme.

In case, if the file is modified then the data in file will get encrypted using RSA algorithm but it will not be decrypted as shown in Table 6.12.

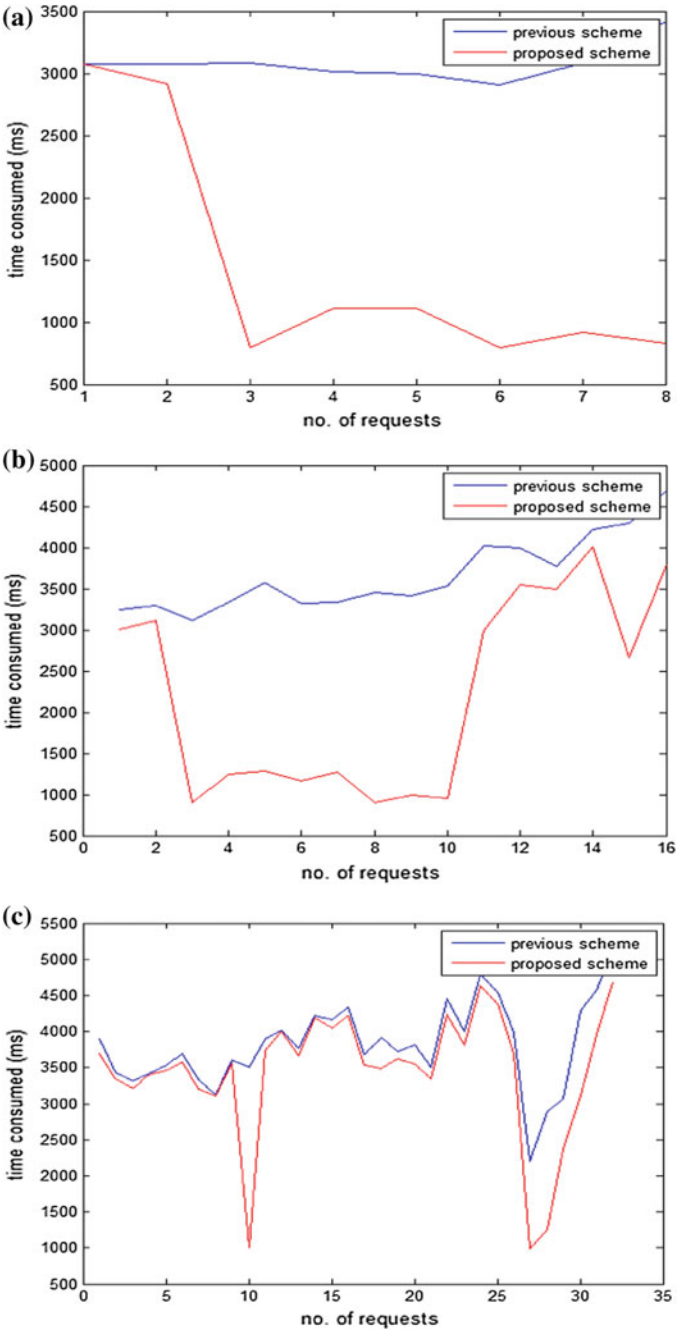

Fig. 6.12 Encryption time for previous scheme and proposed scheme: **a** number of requests = 8, **b** number of requests = 16, **c** number of requests = 32

Table 6.11 Average time taken by previous schemes and proposed scheme when requests vary from 8 to 32

No. of requests	Previous scheme [21] Avg. time (ms)	Proposed scheme Avg. time (ms)
8	3105.91	1086.3
16	3870.19	2519.88
32	3899.72	3149.19

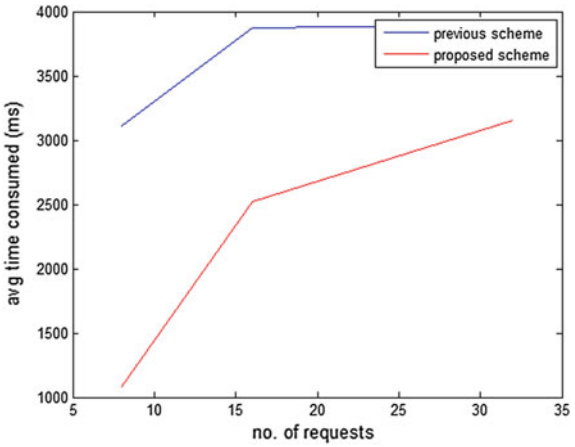

Fig. 6.13 Average time taken by both the schemes

Table 6.12 Encryption and decryption time when file is modified

File size (MB)	Algorithm	Encryption (ms)	Decryption (ms)
1	AES	1037	3184
2.90	Bcrypt	698	1786
3.98	RSA	1123	–
4.65	Bcrypt	695	1781

6.4 Summary

Cloud computing is becoming one of the crucial technologies and considered as a boon for the IT sector. It follows multi-tenancy where several users can share the resources at a given time over the Internet. Along with the benefits of cloud computing there are some drawbacks, in which security is major concern which causes hinderance in full acceptance of this technology. In this chapter, we have summarized various security issues and security threats related to each level of cloud. We have proposed a framework to maintain data integrity in SaaS. This framework also implements the various security algorithms at three different levels. The performance analysis of this framework represents that the proposed framework is easy to implement and can effectively maintain the information security in clouds.

References

1. Shaikh FB, Haider S (2011) Security threats in cloud computing. In: Proceeding of international conference for internet technology and secured transactions (ICITST). IEEE, pp 214–219
2. Alassafi MO, Hussain RK, Ghashgari G, Walters RJ, Wills GB (2017) Security in organisations: governance, risks and vulnerabilities in moving to the cloud. Enterp Secur 241–258
3. Tianfield H (2012) Security issues in cloud computing. In: Proceedings of IEEE international conference on systems, man, and cybernetics (SMC'12), Seoul, Korea, pp 1082–1089
4. Gugnani G, Ghrera SP, Gupta PK, Malekian R, and Maharaj BTJ (2016) Implementing DNA encryption technique in web services to embed confidentiality in cloud. In: Proceedings of the 2nd international conference on computer and communication technologies. Springer, pp 407–415
5. Magoulès F, Pan J, Teng F (2012) Cloud computing data-intensive computing and scheduling. CRC Press, Boca Raton, p 231
6. Naruchitparames J, Güneş MH (2011) Enhancing data privacy and integrity in the cloud. In: Proceedings of 2011 international conference on high performance computing and simulation (HPCS), pp 427–434
7. Aluvalu R, Muddana L (2015) A survey on access control models in cloud computing. In: Proceedings of 49th annual convention of the Computer Society of India (CSI) Emerging ICT for bridging the future, 1, pp 653–664
8. Rashdi A et al (2013) Cloud security standards. Oman National CERT Information Technology Authority, pp 1–28
9. Sun D, Chang G, Sun L, Wang X (2011) Surveying and analyzing security, privacy and trust issues in cloud computing environments. Proced Eng 15:2852–2856
10. Xiao Z, Xiao Y (2013) Security and privacy in cloud computing. IEEE Commun Surv Tutor 15(2):843–859
11. Thakur AS, Gupta PK (2014) Framework to improve data integrity in multi cloud environment. Int J Comput Appl 87(10):28–32
12. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Future Gener Comput Syst 28(3):583–592
13. Guilloteau S, Venkatesen M (2012) Privacy in cloud computing. ITU-T technology watch report, pp 1–26
14. Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. In: Proceedings of IEEE-conference on computer science and electronic engineering, pp 647–651
15. Sun Y, Zhang J, Xiong Y, Zhu G (2014) Data security and privacy in cloud computing. Int J Distrib Sens Netw 1–9
16. Pearson S (2013) Privacy, security and trust in cloud computing. Privacy and security for cloud computing, pp 3–42
17. Shin D, Ahn GJ (2005) Role-based privilege and trust management. Comput Syst Sci Eng J 20(6):401–410
18. Rana P, Gupta P, Siddavatam R (2014) Combined and improved framework of infrastructure as a service and platform as a service in cloud computing. In: Babu B et al (eds) Proceedings of the 2 nd international conference on soft computing for problem solving (SocProS 2012), December 28–30, 2012. Adv Intell Syst Comput 236:831–839
19. Eswaran S, Abburu S (2012) Identifying data integrity in the cloud storage. IJCSI Int J Comput Sci Issue 9(2):403–408
20. Joshi BK, Shrivastava MK, Joshi B (2016) Security threats and their mitigation in infrastructure as a service. Perspect Sci 8:462–464
21. Mohta A, Sahu RK, Awasthi LK (2012) Robust data security for cloud while using third party auditor. Int J Adv Res in Comput Sci Software Eng 2(2):1–5

22. 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
23. da Silva CMR, da Silva JLC, Rodrigues RB, Nascimento LMD, Garcia VC (2013) Systematic mapping study on security threats in cloud computing. Int J Comput Sci Inf Secur 11(3):1–10
24. Islam T, Manivannan D, Zeadally S (2016) A classification and characterization of security threats in cloud computing. Int J Next Gener Comput 7(1):1–20
25. Vaquero LM, Rodero-Merino L, Morán D (2011) Locking the sky: a survey on IaaS cloud security. Computing 91(1):93–118
26. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB (2013) An analysis of security issues for cloud computing. J Internet Serv Appl 4(1):1–13
27. Kazim M, Zhu SY (2015) A survey on top security threats in cloud computing. IJACSA 6 (3):109–113
28. TTW Group et al (2013) The notorious nine: cloud computing top threats in 2013. Cloud Security Alliance
29. Chou TS (2013) Security threats on cloud computing vulnerabilities. IJCSIT 5(3):79–88
30. Dillon T, Wu C, Chang E (2010) Cloud computing: issues and challenges. In: Proceedings of 24th IEEE international conference on advanced information networking and applications, pp 27–33
31. Yan L, Rong C, Zhao G (2009) Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In: Proceedings of international conference on cloud computing, IEEE, pp 167–177
32. McIntosh M, Austel P (2005) XML signature element wrapping attacks and countermeasures. In: Proceedings of workshop on secure web services.ACM, New York, USA, pp 20–27
33. Constantin L (2011) Researchers demo cloud security issue with AMAZON AWS attack. IDG News Service, Available via PCWorld. https://www.pcworld.idg.com.au/article/405419/researchers_demo_cloud_security_issue_amazon_aws_attack/. Accessed 15 Feb 2017
34. Mushtaq MO, Shahzad F, Tariq MO, Riaz M, Majeed B (2017) An efficient framework for information security in cloud computing using auditing algorithm shell (AAS). IJCSIS 14 (11):317–331
35. Kritikos K, Massonet P (2016) An integrated meta-model for cloud application security modeling. Proced Comput Sci 97:84–93
36. Nafi KW, Kar TS, Hoque SA, Hashem MMA (2012) A newer user authentication, file encryption and distributed server based cloud computing security architecture. Int J Adv Comput Sci Appl 3(10):181–186
37. Metri P, Sarote G (2011) Privacy issues and challenges in cloud computing. Int J Adv Eng Sci Technol 1(5):1–6
38. Mathew A (2012) Security and privacy issues of cloud computing; solutions and secure framework. Int J Multidiscip Res 2(4):182–193
39. Gajanayake R, Iannella R, Sahama T (2011) Sharing with care an information accountability perspective. Internet Comput 15:31–38
40. Chidambaram N, Raj P, Thenmozhi K, Amirtharajan R (2016) Enhancing the security of customer data in cloud environments using a novel digital fingerprinting technique. Int J Dig Multimed Broadcast 1–6
41. Hamlen K, Kantarcioglu M, Khan L, Thuraisingham B (2010) Security issues for cloud computing. Int J Inf Secur Priv 4(2):39–51
42. Juels A, Kaliski Jr BS (2007) PORs: proofs of retrievability for large files. In: Proceedings of 14th ACM conference on computer and communications security. ACM, pp 584–597
43. Chalse R, Selokar A, Katara A (2013) A new technique of data integrity for analysis of the cloud computing security. In: Proceedings of 5th IEEE international conference on computational intelligence and communication networks, pp 469–473
44. Singh S, Maakar SK, Kumar DS (2013) A performance analysis of DES and RSA cryptography. IJETTCS 2(3):418–423
45. Thakur AS, Gupta PK, Gupta P (2014) Handling data integrity issue in SaaS cloud. In: Proceedings of FICTA, Springer. pp 127–134