Journal of Network and Computer Applications 75 (2016) 200–222

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A survey on cloud computing security: Issues, threats, and solutions

Saurabh Singh [a], Young-Sik Jeong [b], Jong Hyuk Park [a,*]

[a] Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul 01811, Republic of Korea
[b] Department of Multimedia Engineering, Dongguk University, Seoul 04620, Republic of Korea

ARTICLE INFO

Article history:
Received 12 April 2016
Received in revised form
21 August 2016
Accepted 1 September 2016
Available online 7 September 2016

Keywords:
Cloud computing
Security
Embedded system
Resource pooling

ABSTRACT

Over the internet, the cloud computing reveals a remarkable potential to provide on-demand services to consumers with greater flexibility in a cost effective manner. While moving towards the concept of on-demand service, resource pooling, shifting everything on the distributive environment, security is the major obstacle for this new dreamed vision of computing capability. This survey present a comprehensive overview of the security issues for different factors affecting cloud computing. Furthermore, a detailed discussion on several key topics regarding embedded system, application, storage system, clustering related issues and many more. This paper works on some public cloud and private cloud authorities as well as related security concerns. Additionally, it encompasses the requirements for better security management and suggests 3-tier security architecture. Open issues with discussion in which some new security concepts and recommendations are also provided.

1. Introduction

In the first years of the 60s, computers needed large rooms and consumed large amounts of electricity, had expensive electronic parts and produced very little processing output. However, smaller computers eventually replaced those room-size computers. At the end of the last century, the magnitude of computing and infrastructure node organized to form a distributed system, which provided an increase in efficiency (Modi et al., 2013). In recent years, when the demand of data and online users has vastly increased, the traditional computing infrastructure is becoming costlier and harder to manage. Traditional computing is not suitable for accessing data anywhere and at any time. In order to do so, we need to save the data on an external storage system. Additionally, the increase of online users on networking sites, online surfing, video conferencing, and such cannot be handled by traditional computing (Modi et al., 2013). This rapid increase in global internet usage needs new ways of managing the volume, variety and availability of data, therefore, we are moving towards cloud computing.

Cloud computing is one of the hottest core technical topics in the modern era. It has emerged with broad ranging effects across IT, businesses, software engineering and data storage. One of the main effects is the increase of their capability. This increase in capability does not necessarily mean an increase in expenses in hardware, software, and training of personal to mention a few. According to the National Institute of Standards and Technology (NIST) definition, "the cloud computing is a model for enabling convenient, resource pooling, ubiquitous, on-demand access which can be easily delivered with different types of service provider interaction" (Zissis and Lekkas, 2012). The cloud computing follows simple "pay as you go (PAYG) model, where you pay for the services you've used (Subashini and Kavitha, 2011). One of the major benefits of PAYG model is that we can reduce our expenditure by provisioning a certain amount of resources. The user can select processor, memory, hard disk, operating system, networking, access control and any additional new software as required to their environment. The resources provided on-demand to the customer or end users. It provides tremendous benefits to industry and home users and attracts the attention of the research community (Fotiou et al., 2015).

Cloud computing implements virtualization technique is to provide resources efficiently to the end user. The characteristics of cloud computing include manageability, scalability, and availability. In addition, cloud computing is also economical, on-demand service, expedient, ubiquitous, multitenant, elasticity, and stability. Cloud computing offers mainly three service delivery models; Infrastructure as a Service (IaaS), Platform as a Services (PaaS) and Software as a Service (SaaS) (Hashizume et al., 2013). NIST defines four-development model of the cloud: public, private, hybrid and community. Cloud computing uses cloud server stack where the client or user is on the front end and server on the back

* Corresponding author.
E-mail addresses: singh1989@seoultech.ac.kr (S. Singh), ysjeong@dongguk.edu (Y.-S. Jeong), jhpark1@seoultech.ac.kr (J.H. Park).

http://dx.doi.org/10.1016/j.jnca.2016.09.002
1084-8045/

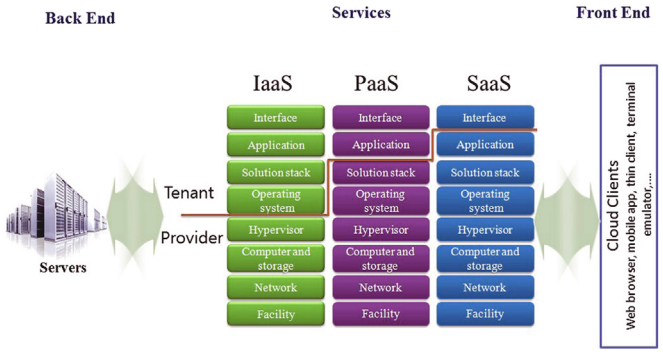

Fig. 1. Cloud service stack.

end. Services reside in middleware of stack as shown in Fig. 1. At the top level resides the application, which directly delivers the outsourced software to the client and eliminates sophisticated software. Customers do no need to expend money to install software, only they pay for their usage (Ku and Chiu, 2013).

NIST is responsible for developing guidelines and standards to provide security in cloud environment. Here we define the cloud architecture as a fourfold, which is composed of: (a) cloud computing concept and characteristics (b) cloud deployed models (c) cloud service delivery models (d) cloud security concept. The details of the cloud architecture are given below:

1.1. Cloud service delivery models

As internet technology and big data cloud computing grow, they raise a new concept of services. This new services are able to interconnect the growing number of online activities. According to a survey from Cisco, the Internet of Things (IoT) is progressively increasing the capabilities of the cloud (Subashini and Kavitha, 2011). After many researches, the major three delivery models are IaaS, PaaS, and SaaS. Still many service models are available as per their functionality and service providing capabilities, which have led to the creation of Anything-as-a–service 'AaaS' delivery models. In this section, we discuss the different types of service models as shown Fig. 2.

- *Infrastructure as a service (IaaS)* belongs to the bottom of the model. IaaS deals with computer hardware (network storage, virtual server/machine, data center, processor, and memory) as a service. IaaS supports the revolution in the business investment in IT infrastructure (Madjid et al., 2013). The elasticity of allocating physical or virtual resources helps providing the infrastructure in an abstract manner. It also provides scalability and provisions (such as hypervisor) issues of infrastructure without the need of spending huge amount of funds and time. IaaS also focuses on security areas like firewall, intrusion detection, and prevention (IDS/IPS), virtual machine monitor (Flavio and Pietro, 2011). However, IaaS has still many security issues. We will explain those issues in Section 2.
- *Platform as a service (PaaS)*: It is in middleware of service model and it delivers the services in the form of development tools, framework, architecture, programs, and Integrated Development Environments (IDE). In other words, the customers are able to control the applications but do not have any means to manage the underlying infrastructure. It can be helpful in situations where multiple developers located in different physical locations need to work together. A popular *PaaS* provider is Google App Engine. It is a Software Development Kit (SDK) which provides an environment that supports Python, Java, and Go programming languages. As it provides features that are ready for the customer, PaaS is more extensible and more flexible than SaaS model. PaaS security can compromise in the runtime of application or in the customer application deployment. It has some challenges like third party relationship, development of lifecycle, and underlying infrastructure security (Sun et al., 2011).
- *Software as a service (SaaS)* is a collection of remote computing services. SaaS is at the top model among the delivery models. It allows the applications to deploy remotely by third-party vendors. It allows the customer to use cloud service provider's application (CSP's) running on cloud infrastructure via the internet. SaaS is the prevalent cloud market and still keeps growing quickly. Google App and Salesforce are examples of SaaS providers, which is a collection of remote computing services. When we talk about the security from the customer point of view, many errors that lead to vulnerabilities are being discovered (Fan et al., 2015).
- *Anything as a service (AaaS)* is a collective term which combines a number of things as X as a service. X may be anything or everything as a service. This service becomes interchangeable in cloud landscape. The cloud system are able to support the large resource to specific, personal and granular requirements using Monitor as a Services (MaaS), Data as a Service (DaaS), Communication as a Service (CaaS), Security as a Service (SecaaS), Routing as a Service (RaaS) (Ali et al., 2015).

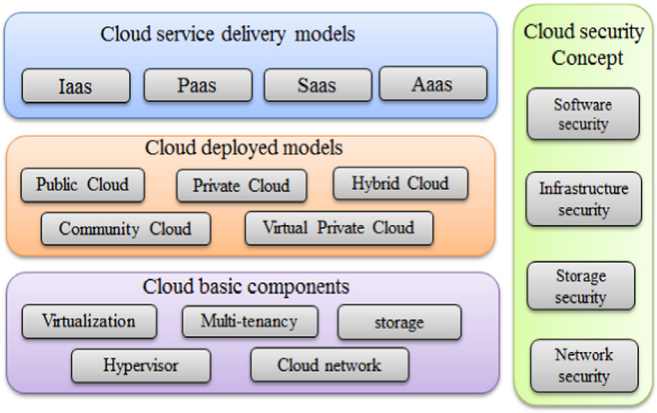

Fig. 2. Cloud computing framework.

1.2. Cloud deployed models

Cloud computing generally depends on shared resources by local servers or individual devices (Laura, 2011). Therefore, it is able to achieve consistency by taking the advantage of resource sharing. Deployed model tells what is the purpose and nature of the cloud. By doing this, it reduces the power of servers, capital expenditure and control the operating cost. NIST defines five types of deployed models:

- *Private cloud*: Cloud computing operates and manages within the data center of an organization is called a *private cloud*. Many consumers of cloud infrastructure (eg, business units) have been including provision for exclusive use by a single organization. In a private cloud, it is much easier to identify the customer and vendor relationship because the infrastructure owned and operated by the same organization. Therefore, security risks are easier to detect.
- *Public cloud:* It is the true representation of cloud hosting where the customer and provider have a strong Service Level Agreement (SLA) to maintain the trust between them. In this cloud infrastructure, open access to the public and organization provided. Businesses, academics, or governmental organizations

own public cloud environments. This means multiple entities may own and operate a public cloud. This creates many issues, as we don't know where the resources are located or who owns them, increasing the difficulty of protecting them from attack (Modi et al., 2013).

- *Community cloud:* Cloud infrastructure of the organizations shared concerns (mission, security requirements, policy, and compliance considerations) of consumers a special provision has been made for exclusive use by the community model. It is owned, managed, and community organizations, a third party, or some combination of them is driven by one or more, and that may be present on or off campus. In simple words, a community cloud is being shared and controlled by multiple organizations (Ali et al., 2015). It also reduces the security risk in the public cloud and reduces the cost of private cloud.
- *Hybrid cloud:* It is the combination of two or more clouds (public, private, community). Usually, the data and application are bound together by standardized and propriety technology. Hybrid cloud offers the advantages of different clouds deployment models. However, it is well organized and more secure than public cloud while accessing the entities over the internet.
- *Virtual private cloud:* It is a semi-private cloud, which is fewer resources, and it consists of virtual private network (VPN). It is on demand configurable pool of shared resources allocated within the cloud environment.

1.3. Cloud computing basic component

In this section, we will discuss the basic components on which cloud computing deployed. These components consist of a wide range of services that we can use all over the internet. Here we discuss some important component:

- *Virtualization:* It plays an important role in deploying the cloud. It is the strategic component in the cloud, which allows the physical resources by multiple consumers. It creates the virtual instance of resource or device such as operating system, servers, network resources and storage devices wherein the framework utilize the resources into more than one execution environment (Subashini and Kavitha, 2011).
- *Multi-tenancy:* Multi-tenant environment can have multiple customers or users who does not see or share each other's data but can share resource or application in an execution environment, even if they may not belong to the same organization. Multi-tenancy results the optimal utilization of hardware and data storage mechanism (Tan and Ai, 2011).
- *Cloud storage:* It is a component, which maintained, managed, and backed up remotely and it made available over the network where the users can access data (Feng et al., 2011).
- *The hypervisor:* The So called virtual machine monitor or manager is a key module of virtualization. It allows multiple Virtual Machines (VMs) to run on a single hardware host. It manages and monitors the various operating systems, which run in a shared physical system (Li et al., 2012).
- *Cloud Network:* It can operate more than one conventional data centers; a typical data center contains hundreds or thousands of servers (Tianfield, 2012). To efficiently build and manage the storages the cloud requires a secure network infrastructure called cloud networking. It requires an internet connection and similar with a virtual private network which enables the user to securely access printers, applications, files etc.

1.4. Cloud computing security concept

Nowadays, cyber warfare is arguably the most complex challenge in a distributed and multi- tenant environment. It is a complex job within the client-server architecture. When the data transfer to the cloud services, the requirements of security should be the most important. The European Network Information Security Agency (ENISA) enumerated the risks, recommendations and benefits for cloud computing (Somorovsky et al., 2011). It also lists the infection on confidential document, loss of governance, malicious insider, and insecure incomplete data. The Elastica 2015 shadow data report (Zhaolong et al., 2016) it focuses on unauthorized apps discovered in an organization. It examines which type of data typically found in sharing apps, riskiest exposure, and what steps take to mitigate these security problems. The CSA and ElasticaQ2 2015 also examine how to build an effective cloud app security architecture, which provides control, visibility, and remediation. In this section, we briefly introduce about the major security concerns of cloud computing.

- *Software security:* It provides basic idea of software security come from the engineering software department that it continues to function correctly under the malicious activities. To build a cloud environment a central and critical problem is software security problem. It defects with security including implementation bugs, buffer overflow, designed flaws, error handling promises and much more (Sun et al., 2011).
- *Infrastructure security:* The most common and fundamental challenges is to demonstrate that the virtual and physical infrastructure of the cloud can be trusted. The attestation of the third party is not enough for the critical business process. It's absolutely essential for the organization to be able to verify business requirements that the underlying infrastructure is secure.
- *Storage security:* In cloud storage system, end user stores the data in the cloud and no longer owns the data and where it's stored. This always has been an important aspect of quality of service. It ensures the correctness of user's data in the cloud and by utilizing homomorphic token with distributed verification of erasure-coded data (Thanh Cuong et al., 2015). Storage security concerns about data sanitization, cryptography, data-Remanence, data leakage, snooping of data availability and malware.
- *Network security:* In cloud computing, communication is via the internet and it is the backbone of the cloud environment. Network security concerns about both internal and external attacks. These attacks in the network can either occur in the virtual or physical network. Wu et al. (2010) focuses on the virtual network in a Xen platform by discussing and analyzing its security problems.

Flavio and Pietro (2011) present a novel virtual network framework aimed to control intercommunications and provide high-security level. Some attacks like DoS or DDoS, DNS, ARP spoofing, IP spoofing phishing attack and port scanning are aimed to gain access to the resources in a cloud network.

We have discussed cloud computing and its characteristics, which are well understood, but still the security state of it is still puzzling. Security is the biggest concerns for IT businesses who are considering to join the cloud computing. Currently, security is one of biggest obstacles for cloud computing service adoption.

Security issues in the cloud environment are caused by its essential characteristics such as resource pooling, virtualized nature, elasticity, and some measured services.

There was an increase of 70% Advance Persistence Threat (APT) attacks (Ussath et al., 2016), 68% suspicious activities, and 56% brute force attacks on a cloud environment in 2015. APT attack is network attack in which an unauthorized identity gain access to a network and remain undetected for a long period. The International Data Center (IDC) is an analysis and research firm that takes the opinion of companies' chiefs on cloud challenges. The results

show that security is most concerned topic for 87% of respondents (Fernandes et al., 2014; Singh and Pandey, 2013).

Some business organizations are reluctant to completely believing the third party service providers. Security in cloud computing is managed through policy and Service Level Agreement (SLA) which is the foundation of expectation of service between consumer and provider (Chang et al., 2016). It is the common belief too many IT professional that cloud computing distributes the data openly at much higher risk (Ali et al., 2015).

Many researchers have studied and discussed the security issues of cloud computing. Fernandes et al. (2014) suggested making comprehensive reviews on cloud security issue, it addresses many several key topics namely threats, vulnerability, attacks proposing and taxonomy for their classification. Ali et al. (2015) explained the security survey highlighted on communication, architectural, contractual and legal aspects. It also discusses the countermeasure for communication issues, it also surveys on the vulnerability of virtual machine like VM migration, VM image, hypervisor, and discusses security in future direction. Flavio and Pietro (2011) gave the detailed knowledge on critical infrastructure for the secure cloud. Moreover in Subashini and Kavitha (2011) has emanated the security issue in service delivery models of cloud computing system and provide some solution regarding these issues.

Saripalli and Walters (2010) surveyed the most relevant privacy and trust issue and analyzing privacy, security and trust threats and provide solution a secure trustworthy and dependable cloud computing. This paper provides the security requirements regarding effective governance, personal requirements, some better encryption techniques, disaster and backup recovery management and good scheme for secure virtualization in the cloud system.

Liu et al. (2015) surveyed critical privacy and security challenges in cloud computing, categorized diverse existing solutions, compared their strengths and limitations, and envisioned future research directions.

Zhaolong et al. (2016) discussed recent developments in cloud computing, various security issues and challenges in cloud computing environment, various existing approach and solutions provided for dealing with these security threats and will deliver a comparative analysis of these approaches.

Zhifeng and Xiao. (2013) provided a systematic review of security issues in clouds based on an attribute-driven methodology. The attributes used were confidentiality, integrity, availability, accountability, and privacy-preservability. For each attribute, a few threats were reviewed along with the corresponding defense solutions.

The security landscape concerning clouds is expansive and the previous works focus on specific areas, paying less attention to the role that clouds play in IT and cyber security, though favoring sometimes the technical depth description of the solutions to the problems. Table 1 compares the several existing works for different aspects, namely the topics they are focused in, the incorporation of industry references, the description of recommendations and solutions to the problems.

Our survey describes the security issue from a technological and operational point of view and it differs significantly from previous surveys. Our survey is different in terms of comprehensiveness, extensiveness and integrated discussion. In addition, it emphasizes the latest security solutions.

As said, our study is different from previous works. Rather than focusing on specific issues, we concentrate on a broader perspective of the state-of-the-art and high-level description. We discuss and provide various approaches proposed in the literature to counterattack the issues. The aim is to achieve an efficient, secure, good privacy, trustworthy and cost effective cloud system. Our paper is the only work that proposes taxonomy for the wide security landscape. Furthermore, an analysis for open issues and a discussion are provided at the end of the article. The comprehensive studies presented in our paper help to quickly understand basic concepts as well as review and understand the current security panorama of cloud systems. Our survey paper also includes ongoing project in various countries that aim to facilitate cloud computing in their smart cities. In addition, an analysis of the publications on the field throughout the years is presented in Table 1. The analysis of several topics covered in this survey paper provides the means to, also discuss the open issues and challenges, and consider some more factors for enhanced security in cloud. Moreover, it analyzes which security issues need to be addressed, and consequently, the paper identifies opportunities for future research work.

The researches for cloud computing have considered the unique advantages of empowered computing system, and a wide range of potential cloud applications have been recognized in the literature. One of the major drivers of cloud computing acceptance is economies of scale. It provides a pay-per-use type of service, thus eliminating the upfront investment in many cases.

Despite of all advantages, the lack of enthusiasm in other investigation topics shows that researchers are focused on the first mitigating security risks in *clouds* instead of digging into their wide area of potential applications. Therefore, addressing the security issues in *cloud computing* environments is of utmost importance. This would allow a better and more secure deployment of *clouds* over the industry. Despite all security measures available nowadays to counterattack the many security issues, one should always have in mind that no system is 100% secure. Previous security researches and events have proven that, no matter what kind of new technology is invented, it may be flawed due to human error. This was the main motivation of this survey.

The goal of this paper is to provide the major and important security concerns in a very efficient way. It also includes some public and private cloud authorities and their security concerns. This paper provides the security requirements regarding effective IT governance, personal requirements, some better encryption techniques, disaster and backup recovery management. Additionally, it suggests proper model and open issue along with discussion for secure cloud system.

Table 1
Contribution of our study related with existing surveys.

Research work	Year	Cloud overview	Security issue and attacks	Recommendations and solutions	Security projects	Open issues
(Flavio and Pietro, 2011)	2010	No	Limited	Limited	No	No
(Subashini and Kavitha, 2011)	2011	Yes	Yes	No	No	Yes
(Modi et al., 2013)	2012	Yes	Limited	No	No	Yes
(Zhifeng and Xiao, 2013)	2013	Limited	Yes	Limited	No	Limited
(Fernandes et al., 2014)	2014	Yes	Yes	Yes	No	Yes
(Ali et al., 2015)	2015	Yes	Yes	Yes	No	Yes
(Liu et al., 2015)	2015	No	Limited	Yes	No	Yes
(Zhaolong et al., 2016)	2016	Yes	Yes	Limited	No	Limited
This survey	2016	Yes	Yes (in detail)	Yes	Yes	Yes

The paper also aim to contribute a comprehensive taxonomic survey on security in cloud computing. Unlike the existing works, this survey paper effort is canalized to provide more complete and thorough view of research literature. The paper also aims to include publication from both industries and academia and it describe several key points of clouds.

The organization of the paper is as follows: Section 2 provides the architectural framework and classification in different issues. Section 3 provides a detailed discussion and a survey on security attacks on cloud. It also presents security concerns on public and private enterprises. The security requirements for cloud environments are illustrated in Section 4. Section 5 proposes a 3-tier security architecture and discusses open issues. This paper ends with the main conclusion in Section 6.

2. Cloud security issues and challenges

This chapter discusses the security state of cloud environments thoroughly by describing its security issues. Each section of this chapter represents a category of cloud computing environment as shown in Fig. 3. Moreover, each section is further divided to some topics that group security issues common in some property.

It elaborates the different security issues while developing on cloud computing environment. The classification discusses embedded security issue in which property of virtual machine arises many security issues like Cross-VM attack misconfiguration, in programmability single point failure. In addition, this chapter also focuses on application level issue. The service with utility relies on web services and technology. There are many lines of code in software application and many developing languages to create an interface, which can lead to many security vulnerabilities.

Data in rest or in communication has issues because of flaws in cryptographic techniques. Sometimes a problem arises from client experience its authentication policy of customer relationship management. Clustering issue also affects the cloud, some flaws in the physical cluster, and virtual cluster brings attack in the network cloud. There is much vulnerability in the operating system of desktops, network servers and smartphones that are open to some serious attacks.

2.1. Embedded security issues

Security in cloud computing environment is a crucial concern in these days. The security in embedded systems has several challenges that caused by the unique features of these systems. The advancement of embedded system is because of improved tools working with them. The simple way to debug an embedded device is to connect it to a local network. An embedded system related to the ubiquitous computing. The main security issues for cloud computing in embedded systems are caused by virtualizations (Zissis and Lekkas, 2012). Different areas of security issues in embedded systems are as following:

- *Virtual machine isolation:* The primary benefit of virtualization is isolation. If it does not deploy correctly then it can be a threat to the environment. The workload is separated amongst the VMs is one of the important issues in implementing the cloud. It can lead to data leakage and cross-VMs attack. So the isolation process should be configured carefully while deploying virtual machine in cloud infrastructure (Flavio and Pietro, 2011).
- *VM Monitoring:* In a virtual environment, the host machine considered as a control point and designed for monitoring the application running on the VMs. In general, all the traffic data is

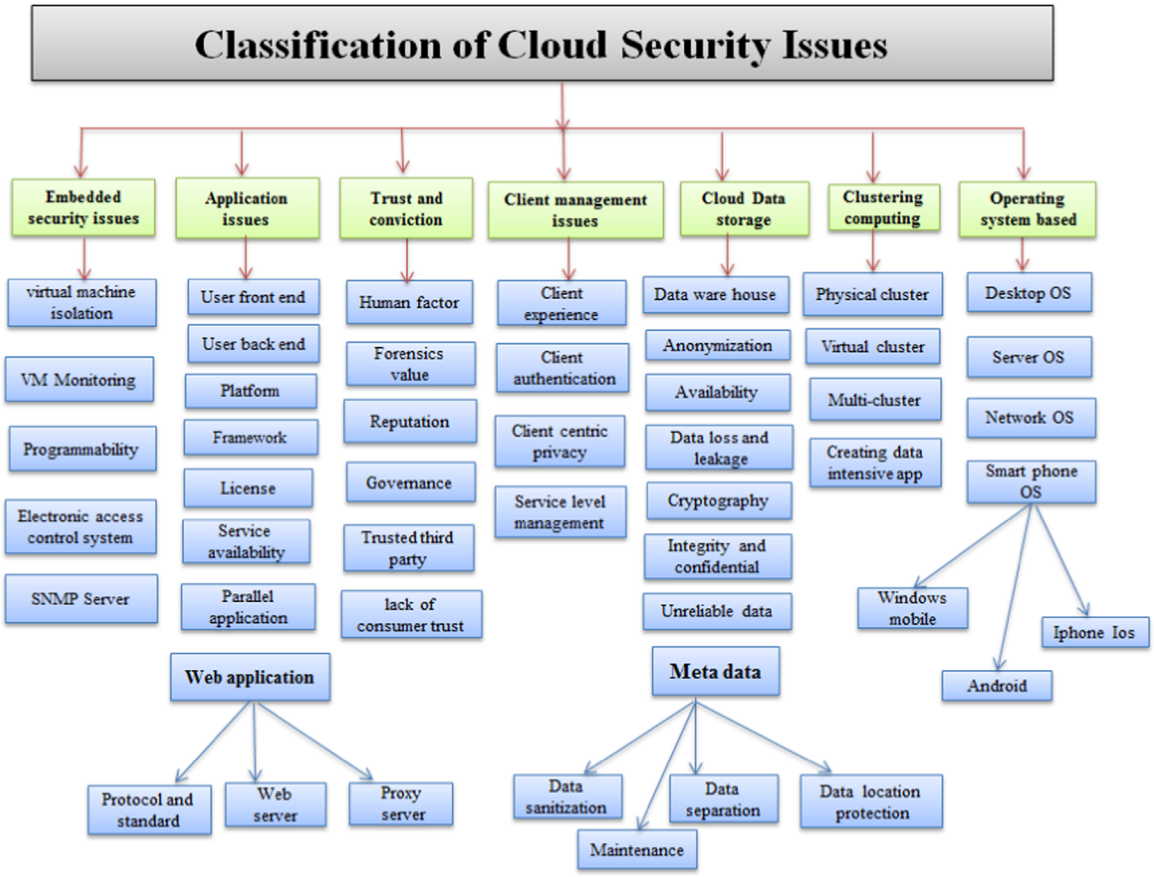

Fig. 3. Classification of cloud security issue.

passing through the monitor host. There are many techniques that influence the host monitor machine, for example, the host can restart or shutdown the VMs, it cannot monitor the traffic in this span of time. Another way is that the host itself can sniff, alter, change, copy or delete the resources that are available in VMs (Li et al., 2012).

- *Programmability:* In a cloud environment, commercial routers use advanced functionality (e.g., accounting, blocking, anomaly detection, etc.) for programmable processor packet on each port. The key challenge of using this device in network processor is to implement packet monitoring functionality for developing software. Many software environments in network processing use a low level of abstraction to achieve high throughput performance (Beloglazov, 2013).
- *Electronic access control system:* Information of client transmitted over the cloud network. EACS negotiates the authentication system and perimeter security by providing the support of Security Assertion Markup Language (SAML). It is a federation protocol, which contains authentication credentials (Artem et al., 2012). SAML used to exchange the information related to subject or authentication between the cooperating domains, and the request and response mapped in Simple Object Access Protocol (SOAP) relying on XML. However, by using signature-wrapping attack, it is possible to alter an eavesdropped message despite being it digitally signed. That means an attacker allowed to execute random machine act as legitimate users (Chen et al., 2011).
- *SNMP Server:* It is simple network management protocol, which designed to provide a low-overhead mechanism to collect the data from network devices. There are some concerns about the cryptographic part of SNMP when there is more variation in export control on cryptography software. SNMP is still a developing tool and it is easy for an attacker to breach the confidentiality in the virtual environment.

2.2. Application issues

Security in a software application is the most vulnerable area. Most of the applications have a front end, back end, different types of platforms, frameworks, parallelism, which have different types of vulnerabilities. The basic security issue in a software application is that it has a million lines of programming code (Ouedraogo et al., 2015). Different programmers in a different language write the software and many of the programming languages have vulnerabilities. In this section, we will discuss different varieties of application issues in cloud computing.

- *User front end:* The security of front end should be like an onion structure but there is the very high probability of an authorized access and deficient configuration in the software application. A programmer needs to know the security aspects of the web developing language like HTML/CSS/PHP/JS. Subashini and Kavitha (2011) stated that the isolation barrier can breach by loophole or injection masked code. Suppose that if an intruder has already compromised the database, there should be a proper front end to prevent the error.
- *User back end:* SQL injection attack takes advantage of backend application weaknesses. $<$script$>$alert(document.cookie)$<$/script$>$ and visit the post, we will find that the script gets injected and executed (Fernandes et al., 2014). OWASP project aimed for backend security and it focuses on three fields like development, hardening, and testing. However, in these three fields have already many security issues, which need to be concerned.
- *Platform:* It is important to discuss what kinds of security issues are present while deploying the platform as service model such as windows Azure. The shared environment includes some unique challenges involving authentication, authorization, and access control. Isolation, rapid elasticity, and resource accounting are also big challenges in a multi-tenant cloud environment (Chen et al., 2011). To isolate the running programs, java implements sandbox bytecode to check the integrity and cryptography for secure communication APIs. Still, this is not secure enough and it does not prevent information leakage.
- *Framework:* The major security issue in cloud computing is found on the framework. IBM cloud framework proposed the strength and weakness of security functionalities. IBM defined five functional security subsystems that are: audit & compliance, access control, flow control, identity management and solution integrity (Xing et al., 2013). The framework has designed in java and.net for isolation and resource accounting but they failed with thread termination. Multitasking Virtual Machine (MVM) provided generic API.
- *License:* While moving in the cloud, the major issue is the licensing of the applications. It is a very complex problem and vendors still have not found a proper solution. The Copy, Sell, Sharing or Distribution of software illegally is called software piracy. Dynamically change the number of servers hosting a variety of application demand uptime, elastic scaling, reliability, performance, and stability. Even today, in the world of personal computer users use 57% pirated software, this is a big issue from a security point of view. There are many possible attacks on this unauthorized pirated software (Bansidhar and Joshi, 2012).
- *Service Availability:* Technically, there are so many ways to achieve high availability in the cloud. Cloud services categorized as SaaS, PaaS, and IaaS. Because of the fluctuation in the cloud environment, application and infrastructure level need high availability and scalability. On the contrary, there is a chance of availability attack like DoS or Botnet DDoS (Kang et al., 2014). Subashini and Kavitha (2011) discussed multi-tier architecture to adopt and providing 'security as a service' framework.
- *Parallel application:* Parallel application improved the performance of the system, but there are some challenges while deploying it. While executing many applications parallel there is a problem of mutual authentication among them and due to this vulnerability some attacks are possible. Due to high non-uniform data distribution, the parallel algorithm is troubled by catastrophic load imbalances (Pal et al., 2011).

2.3. Web application

Hashizume et al. (2013) stated that the cloud computing influences many technologies like SOA, Virtualization, web 2.0 which also inherit the security issue and identify the vulnerabilities in this kind system. It may create the flaws in SaaS application; an attacker can compromise the slave computers and perform the malicious activities (Jansen, 2011). Web application issues are very much similar with the internet services security issues which have a lot of inherent problems like a man in the middle attack, port scanning, IP spoofing, social engineering injection flaws and much more.

- *Web server and technology*: Dhage and Meshram (2012) discussed that the biggest issue in web technology is attack on integrity. When a web server is compromised via eavesdropping, injecting and forged XML, which broke the authentication from the web server, is a big threat as for as cloud environment is concerned. As the increase of people connecting online via chat server and the devices on the web, the black hacker tries to focus on this attack vector. The common mistake is a direct object reference that means an internal object like the one a confidential file, database, or authorized signature key is

exposed to the user is a threat when an attacker can provide these references. The experienced hacker gets the privilege to access the database, operating system via breaching the service side scripting (Lee, 2012).

- *Protocol and standard:* The TCP/IP protocol model or Wireless Application Protocol (WAP) is the basis of only communicating over the internet and it has much vulnerability to be attacked. Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Wireless Markup Language (WML), Simple Mail Transfer Protocol (SMTP) is well known vulnerable protocols (Fernandes et al., 2014). Domain Name Server spoofing (DNS), DNS-cache poisoning, Address Resolution Protocol (ARP) attack that also based on cross multi-tenants attack.
- *Proxy server:* Security of proxy server is depends on the specific types of proxy attacks. One popular attacks is DoS, in which the slaves or compromised computer are used as a proxy. An attacker uses an open proxy for unauthorized access to cover their connection while injecting different sites. Some of the major security problems are created while using the proxies' X-Forward-For, rpaf, 400 error and Obfuscation (Jensen et al., 2009).

2.4. Trust and conviction

For considering trust, we measured it as the belief that utilizes the experience of the employer, which gives contribution in the trustworthy decision. In addition to cloud stakeholders, storage hardware, virtualization, web-based access, the computational algorithm related to trust. The evaluation of trust is a multi-phased and multifaceted phenomenon depends on the multidimensional factor. Chen and Zhao (2012) in security transparency the next frontier presented the TCP concepts, which aim to ensure the confidentiality and integrity of data undertaken by the service provider. Security program in TCP detects whether data has been altered or tampered or not.

- *Human factor:* To explain the role of the human in the context of security in the cloud, first it well known that human is the root of creating all problems as well as it can solve all the problems. We cannot judge or firewall the human nature. People from a different level of system access working in IT department, non-IT employee or customer, some of them are at administrator level can play a critical role in maintaining and damaging system security. Saving, remembering and encrypting the password on every single node might be hard or even impossible some cases (Sen, 2013). Moreover, another big problem is social engineering, which only executed by humans. Some of the social engineering attacks are pretexting, phishing, baiting, quid pro quo, tailgating.
- *Forensic value:* As the increasing use of online network application and the digital crime is also increasing in the same manner. Digital forensics plays a vital role in an organization and system. Digital forensics becomes more popular and important to investigate cyber crime and computer-assisted crime (Dykstra and Sherman, 2012). Forensic majorly concerns in the area of data seizing, locality of data, data disclosure and compromising confidential data. In addition, the Bring Your Own Device (BYOD) concept brings more difficulties to the investigator. Table 2 shows the security challenges involving in each phase of digital forensic cloud (Yu et al., 2012).
- *Reputation:* The rapid development of cloud computing has attracted a lot of attention. In cloud computing environment, several logical virtual machines installed on the same machine and they shares the same hardware. The customer behavior and activities affect each other known as reputation isolation, which is an issue. Some customer abusing the service such as SPAM, DDoS, and the customer regarding that service could prosecute through an investigation. User behavior keeps under control and mainly the customers of most companies, however, business interests and reputation may be affected within the cloud (Ouedraogo et al., 2015).
- *Governance:* The fact is that organizations building cloud environments don't understand about the governance in the new world of IaaS. This issue brings up of losing the administrative operational, and access and security control. Outsourcing the infrastructure of the inter-connected cloud may cause issues to data synchronization if we have improper governance. It affects the financial capabilities of the cloud provider, time management to recovery, disaster recovery, liabilities of data breaches, service termination, and business termination (Fernandes et al., 2014).
- *Trusted third party (TTP):* Cloud users are concerned about how their data is used as data center owners can abuse this data. TTP can authenticate, audit, authorized the confidential data, and it provides the reliability protection from unauthorized hackers. Anyhow, if the third party is compromised, there is a big threat to the cloud environment; many security attributes will be compromised. The user does not know the exact location of data and neither does not know the resource location from where the data is collectively stored. These data can find from public cloud services that have minimal security concerns. Ushadevi and Rajamani (2012) provided a private key mechanism on which trust overlay network over multiple data centers to establish trust and for this data coloring and watermarking technique used to protect shared data (Chen et al., 2011).
- *Lack of consumer trust:* A survey on European citizen about their attitude on data protection. In this survey less than one third phone companies, mobile companies and internet service providers (33%), only one-fifth percentage trust in internet search engine companies, email services, and social networking companies (22%). Furthermore, 70% of European citizen are concerned with their personal data, which is distributed over cloud industries. Recently one survey conducted on cloud industry, result how people trust in online providers—Reputation (28%), trusted a third party (26%), trial experience (21%), contractual (19%), others (6%) (Mansooreh and Sterkel, 2012; Lee, 2012).

2.5. Client management issue

In cloud computing, the management of client is one of the major concerns for the security point of view. In a simple way, it is

Table 2
Issues to digital forensics in cloud environments.

Phase	Action provides	Security issues
Identification	Identifying criminal event	Lack of agendas
Preservation	Software tools	Lack of specialist tools
	Sufficient storage capacity	Distributed, virtualized and volatile storage
	Legal authority	Data stored in multiple jurisdictions and limited access to physical media
	Data integrity	Write a blocking force or lack of persistence mechanism for cloud services and data
Analysis	Software tools and recovery of deleted data	Privacy regulations, Lack of tested, certified tools, and implementation mechanism
Presentation	Documentation of evidence	Integration of multiple evidence sources in record

as like as protecting the president in the crowd on street verses in president house, similarly data in public cloud verse data in client organization system. In this section, we will discuss the issues about the client experiences, its authentication system, identity, and centric-privacy, their service level management, contractor background (Attas and Batrafi, 2011).

- *Client experience (CX):* The experience of customer plays a vital role in a cloud. As time is going the cloud-based customer gets lots of growth in service market experience. In the recent, 74% of respondents said that improving cross-channel customer experience (http://customerthink.com/the-cloud-customer-experiences-saving-grace/). Some of the cloud provider companies are struggling because they have not yet deployed cloud-based solution as expected from the client side. Those customers who are lacking the experience in security areas will suffer to choose a secure cloud provider companies.
- *Client authentication:* A strong user authentication, which restricts the illegal access to the cloud services provider, is a paramount requirement to secure cloud. Sumitra et al. (2014) has discussed a variety of authentication attacks on a cloud in and provides the solution approaches. User prefers to access their application from a different location with different devices like cell phone, laptop, PDA, smartphones etc. It is mandatory to cloud service providers to ensure the only legitimate user can access their services (Fernandes et al., 2014). Some of the authentication attacks are Eavesdropping, password discovery attacks, wrapping attack, cookie poisoning, Man in the middle attacks and so many.
- *Client centric privacy:* Now a day's many organizations are moving to focus their business on the customer. A recent survey in 2015, an independent specialist in market research, 675 IT decision makers interviewed over five countries (UK, USA, Australia, Hong Kong, and Singapore) and the result is that they targeted to the customer-centric cloud. They are concerning their service requirements, security, privacy, trust and maintain CRM-Customer relationship management policy (Chen and Zhao, 2012).
- *Service level management:* It is the process of setting the benchmark for service level, measuring performance and compliance with our service goals and customer expectations. It manages analysis and report on performance metrics. Some questions are arriving in it- can security is adequately expressed in the context of service level agreement. Some security issues in service level management such as incorrect installed Windows NT, administrator unintentionally turnoff the auditing of security events, while monitoring of critical vendor sometimes the response alert may not occur (Fotiou et al., 2015).

2.6. Cloud data storage

Data storage is also one of the most important components of cloud computing. As the growing of many online application and internet devices, the storage of data and its security over the distributed computing is the big issue. In this section, we discuss the security issue regarding cloud storage such as the location of data warehouses, anonymity, availability, integrity management, data loss and leakage, cryptography, unreliable data, sanitization, maintenance, and location protection of metadata, etc. (Hussein et al., 2016).

- *Data warehouse:* Data warehouses are very large system and surveying different user communities along with their security needs. For the deploying of DWH, security is an important requirement for implementation and maintenance. Wang et al. (2009) said that storage security has always been an important aspect of the QoS (Quality of Service). Data warehouse pretenses the three basic securities issue i.e. confidentiality, integrity, and availability.
- *Anonymity:* A particular technique or process to obscure the published data and key information preventing the associated identity of the owner of data. In the cloud enterprises it is increasing to have anonymity without proper privacy measure which causes de-anonymity attack (Feng et al., 2011). Data anonymity has different vulnerability like hidden identity of adversary threats, loopholes in the procedure of re-identification or de-anonymity.
- *Availability:* The main goal of cloud service is also to provide high availability to the client. It focuses that user can get information anywhere anytime. Availability not only refers the software, data but it also provides hardware as demand from authorized users. In a multi-tier architecture, which is supported by load balancing and running on many servers will approach network based attack such as DoS or DDoS attack (Choi et al., 2013). Sometimes cloud storage lacks in availability attribute because of flooding attack in the network. Insider malicious in storage is also a big issue for it.
- *Data loss and leakage:* Data breaches are the result of is an intrusive action and data loss may occur when disk drive dies without creating any backup. It is the loss of privacy, trust and direct effect the SLA policy, which are the main concerns of cloud users. The data leakage affects the web application and attacker took advantage of configured permission in cloud implementations (Gupta and Kumar, 2013).
- *Cryptography:* Many times in cryptographic mechanisms seem to fail when the security measure applied. In cloud cryptography applied to overcome the loopholes in security areas but same time, it has many challenges still yet to overcome. Prime factorization of large numbers in RSA and discrete logarithmic problem in ECC failed for bad password and faulty implementation causes brute force attack. Poor key management, computation efficiency, verifiable data are also other issues related to cloud cryptography (Jamil and Zaki, 2011).
- *Integrity and confidentiality issues:* The three basic challenges for cloud storage are integrity, confidentiality, and availability (CIA), availability we discussed earlier, we discuss the issue related to integrity and confidentiality. As we know integrity is the most critical element in information system to protect the data from unauthorized modification, deletion or altering data (Tumpe Moyo and Bhogal, 2014). Cloud data should follow ACID property to ensure the integrity and confidentiality. The security issue arises when malicious incorrectly defined security parameter or incorrectly configured VMs and hypervisor. Because of multi-tenant nature of cloud may result in the violation of integrity and confidentiality, even the increasing the number of users may enhance the security risk (Thakur and Gupta, 2014). Man in the middle (MIM) attack, session hijacking, data diddling attack are a well-known attack in integrity and phishing, password, packet sniffing social engineering attacks affects the confidentiality of information (Wang et al., 2011).
- *Malware and worm*: Smart cybercriminal involves e-crime attack start to inject malware into cloud storage, turning them into 'zombies' aiming of adding larger network servers' computer called Botnets. According to the websense report (http://securityaffairs.co/wordpress/12703/cyber-crime/my-read-of-websense-2013-threat-report.html) in 2013 50% of malware download as droppers in the first 60s and it can disable the local security. In 2014 cyber, threats combined new technique with old resulting evasive attack and it is the age called malware-as-a-service. In 2014 99.3% malicious file with additional payload used command and control (CnC) to become the part of botnet (Khorshed et al., 2012a, 2012b).

- *Inference:* Inference is a database system technique used to attack databases where malicious users infer sensitive information from complex databases at a high level. In basic terms, inference is a data mining technique used to find information hidden from normal users.

An inference attack may endanger the integrity of an entire database. The more complex the database is, the greater the security implemented in association with it should be. If inference problems are not solved efficiently, sensitive information may be leaked to outsiders.

2.7. Metadata

Metadata means 'data about data', the security professional knows it contains confidential and sensitive information. It may extract by an attacker faulty accounting and implementation of metadata security. In Metadata, spoofing attack the adversary alters or modifies the service's Web Service Description Language (WSDL) (Ku and Chiu, 2013). The sensitive detail that is kept in Metadata from having unintended leakage can pose many risks to the organization. In this section, we discuss the issue related to metadata like data sanitization, its maintenance issue, Metadata separation, and location protection.

- *Data sanitization:* Sanitization is the irreversible process of deliberately cleaning, removing and destroying permanently the piece of data stored on hardware memory device such as hard disk drives, CDs, USB etc. The instance of data, which is under metadata, in Google while destructing metadata store in physically wreck hard drives, may result sometimes data loss and data disclosure because maybe it is not fully wiped out or other tenants might still use them. Therefore, the issue related with data sanitization is the deficient implementation of destruction policy, non-wiped, multitenant use the hard disk and irreversible resources (Ku and Chiu, 2013).
- *Data separation:* Due to multi-tenant nature of cloud, many users avoid public cloud so business address separation of data but not full, which it is a partial separation of data. Data separation ensures that user can access the data in his domain and it cannot see the data in other domain. During separation of data, there is leakage or loss of sensitive information is possible which increase high risk in security. In a physical separation, it increases the cost to purchase the storage arrays. The problem of geo-location of data increases complexity in the cloud. To solve the issues of we can use cryptographic separation of data and follow the policy of SLA (Kertész et al., 2014).
- *Data location:* Due to elastic and high mobility feature of cloud computing the VMs can be easily moved along with data from one location to another location, causes a high degree of mobility. The user does not know always the location of data and it is very difficult for copying and cloning of data repeatedly (Yu et al., 2012). Moving of sensitive data from metadata increases the error and loss of sensitive information. Multi-location of servers for backup of data is rather dangerous in the cloud. Some researchers reconnoitered the man-in-the-middle attack on VMware while mitigating the VMs online.
- *Data maintenance:* Maintaining the cloud metadata while enabling the rich application is a challenging task and risky also. Issue related to maintenance is not updating the software security patches. Sometimes the error is coming while updating, processing, and handling and transmission of metadata (Ali et al., 2015).

2.8. Clustering computing

Cluster computing utilizes many computers, virtual machine, servers and they set to be loosely or tightly connected that work together that they can view as a single system is called computer cluster. Basic use of clustering in the cloud is for implementing the parallel processing application in enterprises (Kim et al., 2013). But it brings many challenges while increasing the nodes per cluster for the system administrator. In this section, we discuss the different cluster security issues in physical, virtual, multi and hierarchal clusters.

- *Physical cluster:* cluster computing requires many virtual machines, servers, interconnected computers and servers to have a high bandwidth connection, extensive computational power, and massive storage capacity. Because of high bandwidth connection, a large data set transfer in and out of the cluster, which would be attractive to the attacker and it can leverage them for launching DoS attack. In the context of computational power, it involves dictionary type or brute force attack (Kim et al., 2013). Because of parallel computing, the traditional cracking tool of password is runs on the compromised cluster to decrypt the stolen password file. An attacker would be attracted towards massive cloud storage to attack for use in creating a repository of stolen copyrighted software and multimedia files (Panth et al., 2014).
- *Virtual cluster:* It can be either physical or virtual machine and runs on different operating system on the same physical node. Misconfiguring automatic physical server and managing firmware, online patches, and driver updates may be key to fixing Microsoft Hyper-V virtual machine (VMware and Citrix Xen server (Fernandes et al., 2014)) clustering problem (Xing et al., 2013).
- *Multi-cluster:* In the IBM knowledge center, we may not able to see the Platform Symphony Management Console (PMC) or multi-cluster Management Console in Microsoft Internet Explorer 10 because of the default setting in IE and some problem in the console. Sometime misconfiguration or disable the setting of active scripting creates the clustering issue in internet explorer version 10.
- *Data-intensive applications*: Data-intensive computing utilizes parallel computing and processes large volume of big data typically in terabytes or petabytes. It utilizes computing cluster to achieve high scalability availability and high performance. Challenges in big data analysis include data inconsistency, incompleteness, and timeliness. While utilizing parallel computing we encounter of mutual authentication problems and the possibility of brute force attacks.

2.9. Operating system

Cloud computing utilizes many virtual machines, different kind of servers in a different inter and intra network, different kind of operating system working together brought many security challenges. According to a survey of National Vulnerability Database (NVD) in 2014 an average 19 vulnerability per day were reported in this year (Artem et al., 2012). Much exploitation is available on Windows, Linux, BSD, iOS. Attacks on OS like stack buffer overflow attack, GNU Bash Common Vulnerability and Exposure CVE-2014-6271 with high severity and serious threat and this GNU Bash could be lead to code execution remotely. In this section, we discuss different security issue and vulnerability on different operating systems used in cloud computing (http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in).

- *Desktop OS:* On cloud computing environment, desktop virtualization is software that separates desktop environment and

associated application from a physical client. In the cloud, client/server computing is implemented by remote desktop virtualization. This approach involves multiple desktops operating systems is on a server hardware platform called VMM or hypervisor. In CVE-2014-6271 is remote code execution vulnerability, this bug allows a remote unauthenticated attacker to run an arbitrary code by sending RDP packets. The compromised OS can cause DoS attack. According to the NAD report in 2014 the total vulnerability found in Microsoft Windows7 was 36, in version 8 36, in 8.1 36, in the Linux kernel, 119 vulnerability found (https://www.cvedetails.com/vulnerability-list/vendor_-id-16/product_id-19/Cisco-IOS.html).

- *Server OS:* Recently Microsoft discloses a serious vulnerability (MS 15-034) on IIS web server that allows unauthenticated DoS attack on unpatched windows servers. Remote Code Execution (RCE) used to execute any command on the target machine for a remote location, bypassing security mechanism. There are many vulnerabilities in Red Hat Enterprise Linux Long Life 5.6 server, Sun Solaris 11, IBM HTTP Server 6.0.2, Cisco TelePresence Video Communication Server (VCS) 0. In CVE-2015-7031 Web Service component in Apple OS X Server before 5.0.15 omits an unspecified HTTP header configuration, which allows remote attackers to bypass envisioned access restrictions via anonymous vectors (https://msdn.microsoft.com/en-us/library/ff648651.aspx).

- *Network OS (NOS):* In cloud computing environment, NOS includes some special function to connect and operates the computer and devices (router, switches, firewall etc.) in a LAN, MAN, or WAN. The example of NOS is Artisoft's, LANtastic, Novell Netware, Cisco IOS, RouterOS, Microsoft Windows Server, ExtremeXOS, and Windows NT (https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-19/Cisco-IOS.html). The common vulnerability in NOS is weak default installation setting, unpatched devices. Wide open access control causes snipping, spoofing, session hijacking, DoS. In the given example, all NOS have vulnerability in a local network of cloud the Neighbor Discovery (ND) protocol implementation in IPv6 stack in Cisco IOS 15.3(3) S0.1 on ASR-5000 series devices mishandles internal tables, which allows remote attackers to cause a DoS (memory consumption or device crash) via flood of crafted ND messages, aka Bug ID CSCup28217 (http://searchsecurity.techtarget.com/feature/Longti me-Windows-vulnerabilities-fixed-in-Windows-10).
- *Smartphone OS:* The use of smartphones by cloud users with cloud application is exponentially increasing and it brings the high availability of application, games, vehicle guidance, and navigator. The increasing popularity of smartphone attracted the malware developers, increasing the attacks on its OS. However, many android malware apps have produced in these few years. The top-10 mobile vulnerabilities are listed in Open Web Application Security Project (OWASP) (https://nvd.nist.gov/). Some of the issues are insecure data storage, weak server side control, client side injection, broken cryptography, security decision via untrusted inputs This section discusses the different types of smartphone (e.g., windows, android, iPhone) based on their operating system and vulnerabilities in it.

a) *Windows mobile:* The latest Window Phone 8 runs on Windows NT Kernel. It has CVE-2008-4609 vulnerability in the TCP implementation in LINUX, BSD Unix, and Windows, and in cisco products allow a remote attacker to cause a DoS via multiple vectors which alter the TCP stable table (https://msdn.microsoft.com/en-us/library/ff648651.aspx).
b) Android smartphone has more than 80% of the total market share of smartphones and this has attracted the attraction of malware developers. Google Play Store have a million apps which are not manually checked either it is malicious apps or not. Some of the android malware threat perceptions are Trojan, Backdoor, Worm, Botnet, Spyware, Aggressive adware, Ransomware, which causes privilege escalation attack, colluding attack, DoS. The vulnerability CVE-2011-4276 (Wang et al., 2015) in which Bluetooth service of the mobile phone allows a remote attacker who is within the Bluetooth range to obtain the contact data. The information disclosure is present in the kernel with CVE number-2015-6642 with high severity (http://searchsecurity.techtarget.com/feature/Longti me-Windows-vulnerabilities-fixed-in-Windows-10).
c) *iPhone iOS:* iPhones have more vulnerability than windows and android phones. According to CVE data and NVD, the iOS have 210 vulnerabilities. In 2015, Apple iOS having severity and score is 10 CVE-2015-7113 allows an attacker to execute arbitrary code in privilege or cause of DoS attack in 2015 there is 222 vulnerabilities found (http://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49).

Table 3 summarizes the cloud security concerns at the different field of cloud environment. The issues and the works identified in the tables typically ordered according to the textual descriptions, to enable one to find the discussion on each one of the topics easily. Nevertheless, the issues are, grouped per study references, whenever applicable on a certain sub-category. The Table also includes studies of the academia, which discussed in the respective section.

3. Security threats in cloud computing

Many researchers have studied and discussed the security issues of cloud computing. Fernandes et al. (2014) suggested making comprehensive reviews on cloud security issue, it addresses many several key topics namely threats, vulnerability, attacks proposing and taxonomy for their classification. Ali et al. (2015) explained the security survey highlighted the communication, architectural, contractual and legal aspects. It also discussed the countermeasure for communication issues, it also surveyed on the vulnerability of virtual machine like VM migration, VM image, hypervisor, and discusses security in future direction. Flavio and Pietro (2011) gave the detailed knowledge on critical infrastructure for the secure cloud. Moreover, Subashini and Kavitha (2011) emanated the security issue in service delivery models of cloud computing system and provide solution to counter these issues.

Saripalli and Walters (2010) surveyed the most relevant privacy and trust issue and analyzing privacy, security and trust threats. The author provide solution in the paper to achieve a secure trustworthy and dependable cloud computing. This paper provides the security requirements for effective governance, personal requirements, some better encryption techniques, disaster and backup recovery management and scheme for secure virtualization in the cloud system.

3.1. Threats and compromised attribute

The cloud computing is the set of services and resources and it is viewed a "computing as utility". Even though cloud is becoming more ubiquitous in a commercial setting, there are still many misconceptions and myths that may cause confusion regarding security like all cloud app is created equal and we can rely on cloud service provider to protect our business that have strong authentication mechanism. This confusion help to attack developer to launch malicious activity on cloud system (Booth et al., 2013). There are several security risk is adopted by the new paradigm of cloud computing. To cops the risk challenges we have

Table 3
Summary of the cloud security issues and respective studies.

Category	Topic	Issues	References
Embedded security	Virtual machine isolation	Data leakage, cross VM-attack	(Hashizume et al., 2013; Xu et al., 2014; Wei et al., 2009)
	VM monitoring	Untrusted VMM, single point failure, configuration	(Muhammad et al., 2013; Flavio and Pietro, 2011)
	Programmability	Setting wrapping attack, identity, physical	(Beloglazov, 2013; Fernandes et al., 2014)
	Electronic access control	Confidentiality	(Artem et al., 2012)
	SNMP Server	Insecure setting, vendor patch	(Ali et al., 2015)
Application	User front end.	Masked Injection, reverse. engineering, loopholes, SQL	(Ouedraogo et al., 2015; Saripalli and Walters, 2010; Lagesse, 2011)
	User back end	injection, authentication,	(Lagesse, 2011)
	Platform	Access control,	(Choi et al., 2013; Chen et al., 2011)
	Framework	Flow control, thread termination,	(Xing et al., 2013)
	License	Pirated software,	(Bansidhar and Joshi, 2012),
	Service availability	Botnet DoS attack, mutual authentication, MIM,	(Zissis and Lekkas, 2012; Czarnowski, 2014; Kang et al., 2014)
	Parallel application	IP spoofing DNS spoofing, proxy injection,	(Pal et al., 2011)
	Web application	ARP attack, XSS attack	(Sharma et al., 2015; VivinSandar and Shenai, 2012; Jansen, 2011)
Trust and Conviction	Human factor	Password sharing, phishing, bating.	(Nabil, 2014; Behl and Behl, 2012; Sen, 2013)
	Forensic value	Data seizing, data disclosure, compromising data,	(Taylor et al., 2011; Dykstra and Sherman, 2012),
	Reputation	customer behavior and repudiation isolation.	(Modi et al., 2013; Subashini and Kavitha, 2011; Ouedraogo et al., 2015; Sumitra et al., 2014)
	Governance	Disaster recovery, service, vendor lock-in, price increases.	(Tan and Ai, 2011; Dzombeta et al., 2014; Panth et al., 2014)
	Trusted third party	Location of data, termination,	(Sun et al., 2011; Pearson, 2013; Ryan et al., 2011)
		Reliability protection.	(Wayne and Grance, 2011; Behl and Behl, 2012;
	Lack of consumer trust	data sharing,	Pearson and Benameur, 2010)
		trust, privacy	
Client management issue	Client experience	Identity, authentication, privacy.	(Attas and Batrafi, 2011)
	Client authentication	Cookie poisoning, eavesdropping.	(Te-Shun., 2013; Metzger et al., 2012; Fernandes et al., 2014)
	Client centric privacy	CRM policy, trust.	(Mowbray and Pearson, 2009)
	Service level management	Installation, auditing and monitoring failure.	(Subashini and Kavitha, 2011; Fotiou et al., 2015; Dykstra and Sherman, 2012)
Cloud data storage	Data ware house	Loss of control, data locality, authentication, de-	(Ahmed et al., 2012; Feng et al., 2010),
	Anonymity	anonymity attack, hidden identity.	(Choudhury et al., 2011)
	Availability	DoS/DDoS attack, flooding attack, cloud outages, multi-location.	(Choi et al., 2013; Feng et al., 2011),
	Cryptography	Poor key management, faulty crypto algorithm,	(Choi et al., 2013; Singh and Pandey, 2013; Te-Shun., 2013)
	Data loss and leakage	trust, privacy, disk drives die without backup	(Jamil and Zaki, 2011)
	Integrity and confidentiality	Session hijacking, phishing, data diddling attack,	(Chen and Liu, 2014; Wang et al., 2010)
	Management	packet sniffing.	
	Malware and worm	Malware botnet attack, signature-based malware, injection and side channel attack, authentication.	(Xia et al., 2014; Sachin Meena and Vasanthi, 2013; Dacosta et al., 2012; Attas and Batrafi, 2011)
		Wrongly implementation of destruction policy,	(Khorshed et al., 2012; Liu et al., 2014; Kumar et al., 2012)
	Metadata	non-wiped,	(Kebert et al., 2013)
		Data leakage, MIM	(Modi et al., 2013; Subashini and Kavitha, 2011; Ku and Chiu, 2013)
Clustering computing	Physical cluster	DoS attack, brute force.	(Kim et al., 2013)
	Virtual cluster	Misconfiguration, patch updating.	(Xing et al., 2013; Nassif and Hruschka, 2013),
	Multi-cluster	The default setting, parallel application.	(Wang et al., 2011)
	Data intensive app	Having mutual authentication issue.	(Popović, 2010)
Operating system	Desktop OS	Desktop virtualization, remote code execution.	(Xu et al., 2014; Artem et al., 2012)
	Server OS	Unpatched windows server, DoS/ DDoS attack, HTTP Header configuration,	(Perez-Botero et al., 2013; Fernandes et al., 2014),
	Network OS	Snipping, spoofing, unpatched network device, memory consumption or device crash,	(Bansidhar and Joshi, 2012; Wang et al., 2015; Te-Shun., 2013)
			(Dhage and Meshram, 2012; Singh and Pandey, 2013; Polze and Tröger, 2012),
		Protocol implementation in ipv6 stack.	(Xing et al., 2013; He et al., 2014)
	Smartphone OS	Weak server side control, client side injection, broken cryptography,	(Feng et al., 2011),
			(Yu et al., 2012)
		TCP implementation in windows mobile, android malware like trojan, backdoor, spyware	(Khan et al., 2014; Kebert et al., 2013; Singh et al., 2014)
			(Jamil and Zaki, 2011; Fernandes et al., 2014; Behl and Behl, 2012)

to classify the attack with security attribute means, which challenge or attack affecting which security attribute and what are the opinion of research work regarding that attack challenges.

According to the report of CSA, the top nine security threats in 2013 are arising from the sharing of common resources. In 2014 and 2015 there is a tremendous increase in threats activity such as data loss, DDoS, account hijacking, insecure interface, malicious insider and more (Bansidhar and Joshi, 2012).

This study aims to identify the popular security threats in cloud computing that will enable both end users and vendors to be

Table 4
Cloud computing threats, description, compromised attributes and related study.

Threats	Description	Compromised attributes	References
Elevation of Privilege	An attacker able to penetrates all system defenses to join the trusted system itself.	Confidentiality, Trust Authorization, Identity	(Yan et al., 2013; Factor et al., 2013; Singh and Pandey, 2013)
Repudiation	The risk of user performs a criminal operation in a system that lacks the ability to trace it.	Auditability, Trust Privacy, Cryptography	(Behl and Behl, 2012; Chen and Liu, 2014, Wang et al., 2011; Ryan et al., 2011a, 2011b; Sumitra et al., 2014)
Denial of Service	An adversary gains control of a tenant's VM, and makes another's web server inaccessible	Resource Availability, Privacy,	(Thakur and Gupta, 2014; Mansooreh and Sterkel, 2012; Behl and Behl, 2012; Sun et al., 2010, Wang et al., 2011; Al-Saffar, 2015; Xiao and Xiao, 2013; Sagar et al., 2013; Singh et al., 2014),
Injection and XSS Attack	To aim at injecting a malicious service implementation or virtual machine into the Cloud system.	Availability, Trust, Authentication	(Mansooreh and Sterkel, 2012; Kumar et al., 2012; Yu et al., 2012; Te-Shun., 2013; VivinSandar and Shenai, 2012; Kebert et al., 2013; Sharma et al., 2015)
Wrapping attack	The risk of by using XML Signature for authentication or integrity protection.	Integrity, Authentication	(Fotiou et al., 2015; Xu et al., 2014; Chen et al., 2011; Chen and Liu, 2014; Pearson, 2013; Dhage and Meshram, 2012; Somorovsky et al., 2011; Jamil and Zaki, 2011)
Self-adaptive storage resource management	Monitoring information in a dedicated circuit, to enable the automatic management and optimize the dynamic control for large-scale data transmission for the prediction performance of the remote storage service	Integrity, Confidentiality, Privacy	(Tan and Ai, 2011; Sun et al., 2010; Perez-Botero et al., 2013; Polze and Tröger, 2012; Metzger et al., 2012; Jiang et al., 2011, 2012; Kertész et al., 2014)
Weak Service Level Agreements (SLAs)	Consumers might face problems that occur from vendor lock-in, data unavailability, hidden costs, non-transparent infrastructure, and insufficient security measures.	Availability, Confidentiality, Deferment	(Hashizume et al., 2013; Chen et al., 2011; Kumar et al., 2012; Ouedraogo et al., 2015; Pearson, 2013; Taylor et al., 2011; Chaves et al., 2010; Pearson and Benameur, 2010; Buyya et al., 2009)
TCP/Session Hijacking	Attack computer is replaced by its IP address for the credit of the client and the server will continue to believe in communication with a trusted client, conversation.	Confidentiality, Trust, Integrity, Auditability, Accountability, Weak Registration system and Service availability	(Fan et al., 2015; Kumar et al., 2012; Tianfield, 2012; Wang et al., 2015; Dacosta et al., 2012; Gupta and Kumar, 2013; Khorshed et al., 2012a, 2012b; Ryan et al., 2011a, 2011b; Ahmed et al., 2012; Fung and Cheung, 2010; MacDermott et al., 2013)
Roll back attack	When the data owner updated the data to the new version malicious service provider provides a still earlier version to the user.	Availability, Usability, Integrity	(Xia et al., 2014; Wang et al., 2015; Feng et al., 2011; Khalil et al., 2014; Sachin Meena and Vasanthi, 2013; Bleikertz et al., 2012)
Data loss or Leakage	A provider may fraudulently retain additional copies of the data in order to retail it to interested third parties.	Privacy protection, Availability, System and Network auditing	(Ouedraogo et al., 2015; Tan and Ai, 2011; Popović, 2010; Feng et al., 2011, 2010; Gonzalez et al., 2012; Wang et al., 2010; Tripathi and Mishra, 2011; Mowbray and Pearson, 2009; Dahbur et al., 2011)
Data manipulation	This involves data insertion, modification and data deletion	Availability, Integrity, Auditability	(Lagesse, 2011; Attas and Batrafi, 2011; Wang et al., 2011; Zhu et al., 2011)
Backup	The vendor needs to ensure that all the sensitive enterprise data is regularly backed up to facilitate quick recovery in the case of disasters happening.	Availability, Reliability	(Hashizume et al., 2013; Beloglazov, 2013; Thanh Cuong et al., 2015; Mallikharjuna Rao et al., 2012; Yu et al., 2012; Pophale et al., 2015; Jain and Kaur, 2012)

aware of the significant security threats associated with cloud computing. Table 4 has summarized about the different challenges along with a description and compromised attribute. It contains many research work related to well-known threats.

3.2. Security concerns in private cloud providers

Popular service vendors for 2015 said that cloud security platform helps organizations mitigate the risk using cloud-based services. The group of vendors provides strong data protection, encryption, and good access management. Others have good monitor based cloud system for suspicious activity that provides reporting and alerting, and policy enforcement (Toosi et al., 2014). Mr. Gray Hall, the chairman, and CEO of Alert Logic is a SaaS-based platform organization that concerns about log management, vulnerability scanning, intrusion detection and monitoring via managed service provider partner. Many major vendors and small cloud providers have a private cloud offering that are available for on-premises deployment or available as a secure hosted offering (Subashini and Kavitha, 2011).

In this section, we will overview the security concerns in a private enterprise cloud computing service provider. Like as, the security of Amazon EC2 by configuring firewall setting which controls network access between users and amazon S3 is done with SSL encryption. Google app uses java virtual machine (JVM) combined with java bytecode and python interpreter in a secure "sandbox" to isolate the application and security. Microsoft Windows Azure adopts firewall, filtering routers, security patch management of software, physical security, cryptography algorithm for encryption of data, SSL-128 bit encryption. Force.com uses SAML for authentication on login, session security, and auditing. It also provides security at various levels like logical network, host security, database security, and communication security. Meanwhile Rackspace protects against spam and gives SSL security. Rightscale and Apple cloud have security monitoring technique and key chain technique for password and authentication respectively (Modi et al., 2013).

Table 5 summarizes the well-known service providers and offers the services in the different environment of cloud computing. The security is the biggest issue of these providers; this table also consists of some security concerns along with website address.

Table 5
Security concerns attribute of cloud service provider.

Service provider	Cloud offering	Security concerns attribute
Amazon web service [PaaS]	It provides half dozen service including amazon elastic compute cloud (amazon EC2/S3), amazon secure server, virtual computing environment and on-demand storage for the internet	Multifactor authentication, EC2 security, and networking, Secure fault tolerance design,
Google apps [PaaS], [SaaS]	Provides a set of online productivity tools including customer e-mail, clambering, web security services, Google app engine, Google docs	Browsing security, HTTPs availability, Digital certificate security, Usenix enigma focuses on security, privacy, electronic crime and novel attack
Microsoft azure/sky drive [Waas] [Saas]	Platform consisting of operating system, store organize, developer service to build and enhance web host application,	Identity and access, penetration testing, encryption key management AES-256, security center (MSRC, MMPC), monitoring, logging, reporting
Salesforce [PaaS]	It is enterprise cloud that is leading the social enterprise helping companies connect to the customer (CRM tools), including automation, marketing, and social network tools, building a web application and hosting on sales force infrastructure.	Two forms of user authentication delegated authentication and security assertion markup language (SAML), focus on session security data auditing, programmatic security like SOAP API, security token-using O- AUTH
Rackspace cloud [Iaas], [PaaS]	It also is known as "most" which consist of three service: a platform for building cloud website, cloud files a storage service and cloud servers that provide access to virtualized server instance.	Managed security, cloud threat protection, vulnerability assessment, reduce DoS attack, data protection solution and payment card industry data security standard
Right scale [SaaS]	It support to maintain choice of vendors, offers self-service provisioning, automate routine task, it helps customer builds and clone virtual servers for cloud	Security monitoring, multi-cloud identity management, employing security automation
Apple iCloud	Offers device cloud with device-centric cloud storage, it also offers iCloud drive, cloud photo library, icloud backup. It automatically and securely stores our content so it's always available to our iPhone, iPad, iPod touch, Mac or PC.	Secure boot chain, touch ID security, keychain and key bags data protection and access control. Security certification like FIPS 140-2, ISO 15408, app code signing

3.3. *Cloud service project used by public authorities*

Government cloud services strategy include cloud-based project management tools, which are popular with business enterprises. A non-profit industry has blazed a trail in cloud adoption, but the public sector is catching up fast. Since the Implementation of a "cloud first" migration strategy in 2010, the US government has already moved to a leading 50 world-class agency services to the cloud, and the cloud of the government sector, and save billions of dollars.

According to the NITS in 2015 GIDC (Government Integrated Data Center) announced 143 e- government system adopt cloud in this year. GIDC renovates its security system based on uncooperative cloud computing to all 143 e- government system up to the end of 2015 (Toosi et al., 2014). GIDC is the management in charge of 1312 units of 44 organization of Korean government system. Government cloud project expected to picking up of adopting the cloud project. In 2014, 260 e- government systems have adopted the cloud project concerning security also and in 2015, it increases up to 403. They are expecting it will increase to the extent of 760 by 2017. To gain the significant cost saving, the governments are planning to develop the cloud technology and increase the performance, quality, innovation and security

Table 6
Description of public cloud business project.

Public administration	Description
RESERVOIR	It is a European project of cloud computing, which is developing a breakthrough system and service technologies. This project serves as IaaS and talking about virtualization in order to allow efficient migration of resources, exploitation and minimizing their utilization costs. The goal of this project to support the development of Service-Oriented Computing (SOC) as a new computing paradigm
United States (federal cloud computing strategy)	This Federal Cloud Computing Strategy is designed to considerations, articulate the benefits, and trade-offs of cloud computing. The basic two points are as follow: – Highlight cloud computing implementation resources. – Provides a decision framework and case samples to support organizations in migrating towards cloud computing. The Federal Government, cloud computing holds tremendous potential to deliver public value by increasing operational efficiency and responds faster to constituent needs. An estimated $20 billion of the Federal Government's $80 billion in IT spending is a potential target for migration to cloud computing solutions.
Slovenia kc-class	The Slovenian Ministry of Higher Education has collaborated with the European Commission and industry to develop the KC Class program. KC Class brings together institutions that deal with cloud computing in the country and has broad industry support. It currently employs researchers and developers from six small businesses, four middle-sized enterprises, and seven research organizations, who work to develop local solutions, services, and products in the field of cloud computing.
Australian government cloud computing policy	The Australian Government Cloud Computing Policy Version 3.0 October 2014 (the Policy) supersedes all previous versions of the Australian Government Cloud Computing Policy. The Policy is mandatory for non-corporate commonwealth entities subject to the Public Governance, Performance, and Accountability Act 2013 (PGPA Act), and reflects The Coalition's Policy for E-Government and the Digital Economy to accelerate the adoption of cloud services. The Australian Government is looking to the benefits of cloud services as a way of reducing redundancy and duplication across agencies, and seeking to realize economic savings and improved business outcomes.
U cities' (South Korea)	In South Korea, the government is adopting cloud technology for the provision of government services, such as in the fields of tax payment, business licensing, vehicle registration and education. For example, in the field of education, it plans to develop a cloud-computing network, where students can store digital textbooks that they can access from their laptops or smartphones. One major part of the South Korean government's plans for the development of cloud computing in the public sector is its promotion of ubiquitous cities, or 'u-cities'. The city has recruited the help of Cisco and Korean Telecom to deliver cloud-based city services to mobile devices. These 'Smart+Connected Community' (S+CC) services, which will be covered areas such as urban mobility, energy management, distance learning, and security.

Table 7
Disaster recovery at different level.

DR level	Description
Data level	Security of application data
Application level	Application continuity
System level	Reducing recovery time as short as possible

considerations in the services they provide to the citizens. Some of the cloud projects of government are in Table 6.

4. Requirements and literature solutions

Cloud computing offers both unique advantage and challenges to private and government users. Advantages include greater efficiency, flexibility, and economy, which can help enterprises to meet rapidly changing computing needs, and cheaply while being environmentally friendly. Among the many challenges, security is the commonly cited concerns in moving mission-critical services or sensitive information to the cloud. Considering the security issues here in the chapter we discuss and provide various approaches proposed in the literature to counter the better security solution and to achieve efficient, secure, good privacy, trustworthy and cost effective cloud system (Wayne and Grance, 2011).

4.1. Personal security requirements

Organizations are able to manage dozens to thousands of employees and users who can access their cloud applications and services, each with varying roles and privileges. Cloud service providers must allow the cloud consumer to assign and manage the roles and allied levels of authorization for each of their users in accordance with their security policies. For example, a cloud consumer, according to our security policies, an employee whose role is to permit them to be to generate a purchase request, but in a different role and powers of the authority to approve the request of another employee is to be responsible for.

4.2. Effective governance and risk analysis

Most organizations, which have established security, compliance policies and procedures, protect their intellectual property and corporate assets used exclusively in IT space. These policies and procedures for the organization to consider the impact of these assets compromising on basis of risk analysis are developed. A controls framework and further procedures established to mitigate risk and serve as a standard for the execution and validation of compliance. These principles and policies, enterprise security planning improves the quality of the process surrounding enterprise security governance, risk management, and compliance represents models.

In Liu et al. (2014), a risk framework presents security risks in terms of six key categories for security objectives (i.e., confidentiality, integrity, audibility, multiparty trust, mutual auditability and usability) in a cloud platform. The advantage of this approach of risk assessment is that it allows customers, vendors, and regulation agencies to assess comparatively the relative robustness of different cloud vendors with their offerings in a defensible manner.

Khan et al. (2012) shows that the information security principles of integrity, confidentiality and availability are most relevant to the cloud related scenarios. The information risk ratings performed shows the loss of confidentiality rated as the highest level of risk followed by availability and integrity. For each of the threat categories the common research issues identified are:

- Scalable fine granular access control and data confidentiality in cloud computing scenarios.
- Using an intrusion detection system (Identification of user behavior) to prevent data leakage at infrastructure provider level.
- Detection of malware on virtual machines, from the hypervisor level by performing the static and dynamic analysis.
- Identification of vulnerabilities at the hypervisor when giving API level access to the introspective layer of the hypervisor to the programs.
- Security architecture for a hypervisor using the Usage control model.

4.3. Backup and disaster recovery management

Disaster recovery is a determined problem in IT platforms. This problem is more crucial in cloud computing because CSPs have to provide the services to their customers even though the data center is down, because of disaster. A disaster is an unpredicted event in a system lifetime. There are three types of DR levels described in Table 7. It can be made by nature (like the tsunami and earthquake), hardware/software failures (e.g., VMs' failure of Heroku hosted on Amazon EC2 on 2011) or even human (human error or sabotage). The approach of Cloud-based DR solution is an increasing development because of its ability to bear disasters and to achieve the reliability and fast availability.

For an efficient performance, DR mechanisms must follow the five basic requirements:

- Have to minimize RPO and RTO
- Have a minimal effect on the normal system operation
- Must be geographically separated
- Application must be restored to a consistent state
- Must guarantee privacy and confidentiality

In Nakajima et al. (2013), a management engine introduced for carrier networks. In the instance of a large-scale natural disaster (e.g., earthquakes), system uses a DR scenario by scrambling up resources for the high-priority services (e.g., voice communication) and scaling down allocated resources up to low-priority service (e.g., video-on-demand).

Khoshkholghi et al. (2014) aims to gain both the performance of an asynchronous replication and the consistency of sync replication. It is not possible to continue the processing in synchronization replication until replication is completely finished at the backup site. In contrast, in an asynchronous replication, the processing will start after storing data in the local storage. The result for the customer may ask, and then writes a backup site in age repeated. Pipelined replication and replication processes in parallel as in the following scenario. Secure-Distributed Data Backup (SDDB): It is an innovative technique presented in to protect data in the event of a disaster. The data protection technique has six stages:

- The data encryption: Data has to encrypt after receiving into a data center.
- Spatial scrambling: A spatial scrambling algorithm changes the order of data files.
- Fragmentation, duplication: According to the policy of SLAs, the data files that divided into some fragments must be follow the duplication process on the data.
- Encryption: A secret key encrypts the small fragments again.
- Shuffling & Distribution: At a very last stage, the fragments distributed using a shuffling method into unused memory capacities.

To Transfer the Metadata to a backup server it includes encryption keys, shuffling, fragmentation and distribute information is sent to a supervisory server. If a disaster occurs, the supervisory server will gather all the information from distributed devices and decryption (2nd), and sort and merge, inversion scrambling and decryption (1st) spatial respectively.

4.4. Exception handling and fault tolerance

The system determines that exception has occurred while the executing of distributed cloud application. The serial exception has occurred when a computer system determines the exception has occurred and translates during the execution of distributed environment.

Wen and Watson (2013) Proposed a technique to handle the dynamic exception for partitioned workflow on federated clouds. The technique handles when cloud fails and it selects the best way re-partitions the flow and to meet the security requirements. It evaluates the implementation utilizing a central tool for e-science: a portable, high-level clouds Platform workflow application creation and deployment of the set of Electronic Science and monitors the central instance. The state of each running instance of e-science center system they handle exceptions that occur at run time.

Patra et al. (2013) presents a better understanding of fault tolerance in cloud system and compares the existing model on various parameters. Fault tolerance caused by error processing having two phases first one is effective error processing which aimed to bring the error to the "latent state" and second aimed that the error does not become again effective.

4.5. Cryptographic algorithm

The popularity of cloud computing is exponential increasing in growing internet technology, resulting the threats developer attracted and causes many difficulties in the security areas of cloud. For countermeasure of these problems, one of the one of the common method is the cryptographic approach. Which types of encryption implemented in a cloud environment to ensure the security attributes and it should be cost effective? In this section, we recommend good cryptographic proposed scheme, which fulfills the flaws in cloud security. Table 8 summarizes the cryptographic proposed scheme along with basic theory and security attributes.

Cao et al. (2014) proposed a Multi-key word Ranked search Scheme over Encrypted (MRSE) cloud data to provide better privacy preserving. MRSE utilizes coordinating matching among various multi-key word semantics it again utilizes secure inner product computation and then give two significantly improve MRSE MRSE_I: Privacy-Preserving Scheme in Known Ciphertext Model and MRSE_II: Privacy-Preserving Scheme in Known Background Model to achieve various rigorous privacy requirements. This paper through analysis investigating privacy and efficiency guarantees the proposed scheme.

Liu et al. (2014) proposed the time based proxy-re encryption for data sharing in a cloud environment. The aim of this scheme is to encrypt the data before outsourced it. Key generation, Proxy Re-Encryption (PRE), attribute-based encryption, the bilinear map is used to demonstrate to provide fine-grained access control on encrypted data, scalable user revocation, authentication and confidentiality of cloud data. To enhance the security mechanism of identity and access management in the cloud proposed in Abbas (2015). The author combines the Elliptical Curve Cryptography (ECC) technology for low-key size but high-security level with robust nature and Identity-Based Cryptography (IBC) to reduce key management complexity using trusted cloud. The enhance IAM mechanism provide a high level of authentication, robustness less

Table 8
Existing cryptographic techniques for cloud security.

Refs.	Existing scheme	Basic theory	Security attribute	Cost efficient	Other features
(Cao et al., 2014)	Privacy preserving multi-key word ranked search in cloud data	Multi-keyword semantics, coordinating matching	Privacy, integrity	Yes	Usability,
(Liu et al., 2014)	Time-based proxy re-encryption scheme	Key generation, proxy re-encryption, ABE, Bilinear map	Confidentiality, scalability, authentication	Yes	Big key size, correctness, no global time, Fined grained access control and data sharing
(Abbas, 2015)	Enhancing the security of IAM in cloud	IAM Lifecycle, ECC, trusted cloud, IBC, federated identities and single sign-on	Authentication, authorization, robustness, privacy	–	Access control, self-service, De-provisioning, security reporting
(Li et al., 2015)	Identity-based encryption with outsourced revocation in cloud	Public key infrastructure, key issue and update processing, PKG, bilinear and DBDH Problem	Authentication	Yes	Less time and cost, Efficient revocation management,
(Sood, 2012)	A combined approach to ensure data security in cloud computing	SSL 128 and 256-bit encryption, SSL certificate, MAC	Confidentiality, integrity, availability, authorization,	Yes	Provide user identity and password, keyword search,
(Rewagad and Pawar, 2013)	Digital signature and key exchange and AES encryption scheme	ECDH, AES, Trusted computing,	Confidentiality, authentication, integrity	–	Provide session encryption key,

cost and efficient revocation management. The ECC implemented with a 160-bit key size that offers same security level against 1024-bit key size of RSA cryptosystem that makes IAM more efficient.

Li et al. (2015) presented a technique of identity-based encryption that simplifies public key management and certificate in Public Key Infrastructure (PKI), which is alternative to public key encryption. The basic theory in this paper public key generator, key service procedure in which key issue and update processing technique were utilized and two cryptographic background techniques Bilinear map and decision bilinear Diffie-Hellman problem is proposed in IBE. The paper also provides the computational-experimental result to determine the cost and time efficiency of proposed model.

Sood (2012) gave the idea of combined approach to ensure the data security in the cloud that focuses on the basic security attribute such as confidentiality, integrity, availability, and authentication and provide user identity and password. The concept followed to secure the data 128-bit and 256-bit SSL encryption and MAC for integrity check and double authentication of user one by the owner of data and another is by cloud. This paper proposes model divided into two phases that deal with data transmission and secure data storage in the first phase. In the second phase provides the retrieval of data request of data access, double authentication, integrity check, and verification of digital signature and prevent data leakage for availability.

For the better enhancement for cloud data security using digital signature concept with Diffie-Hellman key exchange and AES encryption is proposed in Rewagad and Pawar (2013). The proposed architecture utilizes ECDH that generates the key for key exchange and then digital signature is used to authenticate the data after that AES algorithm is used for encryption/decryption by session key to avoiding MIM attack and maintain the integrity of data (Hussein et al., 2016).

4.6. Digital forensics tools and technique

As the increasing use of cloud application and devices, the digital crime is also increasing in the same manner. Digital forensics plays a vital role in an organization and system. The digital forensic toolkit helps to analyze the text indexing, file interpretation, and analysis of log records and network. Now a day's digital forensics becomes more popular and important to investigate cyber crime and computer-assisted crime. It is associated with people's mind primarily with the investigation of crime. In this section, we discuss the tools and techniques of digital forensics regarding each level of digital forensics lifecycle. It seems as the arrival of forensic community with several other devices for examining digital evidence barely Disk images, logs, a network capture, memory dumps, mobile phones and so on. Security based company likes access data and softer guidance with their own evidence storage format.

4.6.1. Description

Table 9 shows the digital forensic tool analysis with the different level of a framework like indexing, binary abstraction, File system consideration, Digital Log Analysis and Network analysis. Toolkit Encase is a popular multipurpose tool that covers several areas of digital forensics. This tool quickly gathers various data from various devices. It is very good in indexing and data abstraction. Whereas FTK, which is a commercial toolkit is also efficient in file system considerations and not so much fit for log and network analysis.

The Sleuthkit (2015) is exported the result to the browser interface (Autopsy) as HTML output. Cohen (2008) extended the functionality of Sleuthkit and developed the Pyflag framework that

Table 9
Comparative analysis of digital forensics toolkit.

Tools	Indexing and search	Binary intellection	File system consideration	Digital log analysis	Network analysis
Encase	Yes	Yes	No	No	Yes
FTK	Yes	Yes	Yes	No	No
Sleuthkit	Yes	Yes	Yes	No	No
PyFlag	Yes	Yes	Yes	Yes	Yes
OCFA	Yes	No	No	No	No

can operate on forensic images, memory dumps, logs and network captures. Open Computer Forensics Architecture (OCFA) is another most popular digital forensic tool, which built in Linux platform developed by Dutch National Policy Agency (DNPA).

The efficient scheme to check the integrity of hard disk in digital forensics proposes by author Fang et al. (2011). For this, it utilizes the efficient hashing with combinational group testing to calculate the hash value of all sector of the hard disk as an integrity proof. The proposed scheme carried out experimental result proves that scheme significantly decreases the hash value and execution time comparing to existing approach. It also decreases the storage overhead for example for 250 GB hard disk only 0.5 MB is required.

Qi et al. (2013) presented evidence protection model by utilizing the basic theory of batch verifying and public verifiability for the computer forensics. The author analyzes the relationship between digital evidence and intrusion process it defines the witness model and protects generated evidence on time by the two basic theories. It is three-party authenticated protocol which provides efficient integrity assurance and non-repudiation procedure in cloud forensics.

Dykstra and Sherman (2012) explored and evaluated the tool and techniques to acquire the digital forensic from IaaS cloud service provider. It explores the trust issue during acquiring forensic evidence in IaaS and analyzes some strategies for these challenges. For cloud forensic examination first proposes a model of a layer of trust for potential acquisition technique for each layer in the cloud and the second investigator chooses at what layer of cloud in the forensic process will be executed. Then discuss the acquisition tool including Guidance EnCase and Access Data FTK extracting from Amazon EC2. The author discusses the other solution for acquisition such as management plane, forensic-as-a service legal solution that has less trust but more cooperated with cloud service provider.

Lin et al. (2012) presented an improved novel scheme that makes sure the security for sealing and storing the digital evidence in the cloud. For privacy and verification of evidence it improved the security model and for better efficiency by applying RSA signature in our scheme and to reduce the overloading of computing cost. Nassif and Hruschka (2013) proposed document clustering for forensics analysis to improve the computer inspection. The proposed approach carrying out the extensive experimentation with good clustering algorithm like K-means, K-medois, and Single link, Complete Link, Average Link and CSPA applied to five real-world data sets obtained from a computer seized in real-world investigations. Table 10 is the summary of the recent existing research work on forensic.

4.7. Secures virtualization

In this section, we explain some efficient proposed scheme in virtualization as far as security is a concerned. Virtualization is the important key component of cloud technology. It makes more

Table 10
Existing schemes to provide better forensic level.

Refs.	Existing scheme	Basic theory	Integrity	Efficiency	Other features
(Fang et al., 2011)	A scheme for hard disk integrity checks in digital forensics	Hashing and combinatorial group testing	Yes	Yes	Low computational time, trust
(Qi et al., 2013)	Digital evidence protection model	Batch and public verifiability	Yes	Yes	Three parties authenticated, non-repudiation
(Lin et al., 2012)	Cloud-aided RSA Signature Scheme for sealing and storing digital evidence	Cryptography, RSA, signature algorithm	Yes	Yes	Privacy, low computational time
(Dykstra and Sherman, 2012)	Acquiring forensics evidence from IaaS	Packet capturing introspection, forensics tools	Yes	No	Trust, law enforcement, legal solution
(Nassif and Hruschka, 2013)	Document Clustering for Forensic Analysis	Portioning algorithm K-means and K-medoids	Yes	–	High computational cost, accurate

efficient the system for a user who is sitting at a remote location.

According to the CSA recommendations against the vulnerability in virtualization is as follow:

- Securing each virtualized OS running on guest VMs
- That Virtual machine which is at rest should be encrypted.
- Evaluating risk associated with virtual technologies
- Securing all element of the virtual machine and restrict and protect the administrator to the virtual machine.
- Awareness of security tools and techniques while deploying virtualization in cloud computing.
- Configuration, installation should be carefully planned while deploying it.
- Evaluate the hypervisor technologies and harden the hypervisor (VMM) and another component.
- Evaluate the virtual network security feature and recognize dynamic nature of VMs.

Gonzalez et al. (2012) considered the virtualization is the key element in future. The paper shows a lack of data control mechanism, hypervisor vulnerability, and the isolation solution virtual cloud environment. The author provides most popular isolated virtual machine is Xen, KVM, and VMware aiming to verify their security concern and availability solution.

The privacy, encryption, and integrity check has been used to provide secured VMS runtime environment in the cloud (Xia et al., 2013). The author proposed a scheme named a hardware-software framework in short Hyper Coffer which focuses integrity and privacy to tenant's VMs. Hyper Coffer retains the transparency between existing virtual machine and it can only trust the processor chip and assume no security in any external devices. Hyper Coffer architecture protects cache data, memory data, and CPU context when execution transfers from VM to the hypervisor. It also protects EPT-Extended page table of VMs and VM table for multiplexing. It introduces VM-Shim that runs between guest machine and hypervisor. For secure processor design, two techniques were reviewed AISE-based encryption and Bonsai Markely tree. Both used for encryption and integrity respectively.

Danev et al. (2011) considered the complications of enabling a secure VM-vTPM migration protocol in a private cloud. The author used trusted computing technology to secure intra-cloud migration of VMs. It ensures data integrity, privacy, the freshness of data and secure mitigating information to the communication channel. Virtual trusted platform module vTPM key structure combined with the virtual machine to certify the integrity of VMs. Literature implements to evaluate the feasibility of proposed scheme on Xen Hypervisor and it is successful and securely migrated to the existing hypervisor.

A novel security solution of virtualization, which provides a widespread protection to the virtual environment, proposed in Win et al. (2014). The author combines basically three technologies: first is Mandatory Acess Control (MAC)- access of resource is controlled and determined by administrator by the help of reference monitor, access enforcement hook, and access policy. Second one, Linux Security Module (LSM) – gives a function hooks which can place within kernel and run as kernel module without causing any compatibility issue with the main Linux kernel. The third one is SELinux developed by NSA and works alongside DAC to provide fine–grained access of resources. The proposed solution also protects against guest VMs and hypervisor attack.

Live migration is an indispensable feature of a virtual machine that allows the movement the VMs from one physical host to another without halting the VMs. A framework is proposed in (Anala et al. (2013) for secure live migration in virtualization in cloud computing. The approach uses four next doors level of privilege covers starting, stopping, pausing, executing, or getting information status information of VM. L4 defines end users who have no authority to access VMs command. The framework protects against unauthorized access, breach of confidentiality, the integrity of live migrated data and network attack. In Table 11, the proposed scheme provided with the basic theory and it summarizes the security attribute provided by the scheme.

Table 11
Existing scheme for secure virtualization.

Refs.	Existing scheme	Basic theory	integrity	privacy	Other feature
(Gonzalez et al., 2012)	Secure runtime environment for VM	Cryptography, Access control	Yes	Yes	Availability and low scalability
(Xia et al., 2013)	Hyper Coffer, Secure runtime environment for VM	Decoupling of security and VM management tasks, trusted computing, cryptography	Yes	Yes	Security against VM rollback
(Danev et al., 2011)	Protocol for vTPM based VM migration	Trusted computing, Remote-auditing, and tunneled communication channel	Yes	Yes	Data freshness
(Anala et al., 2013)	Framework for secure live VM migration	Trusted computing, role-based access control, cryptography	Yes	Yes	Security against VM hopping and Useless migrations
(Win et al., 2014)	Virtualization Security Combining Mandatory Access Control	Mandatory access control, SELinux architecture, Linux security model	Yes	No	Comprehensive protection and system security

5. Security suggestion and discussion

In this chapter, we suggest 3–tier security architecture as shown in Fig. 4, where security is interdependent on each other. The proposed security classification is consists of three levels: application level, cloud-service middle level, and infrastructure level. Organizations that are keen to use cloud computing to run their in-house applications need to review and potentially modify their software development approach. The organizations should concern about the key points that help to design programming standards, and adopt multi-tenancy and most important the security capabilities. Here we will discuss the security issues on each level of the cloud security architecture.

The organization is eager to move their in-house developed application of cloud to save money, increase efficiency and application level security, and counter the challenges in cloud environment. So a proper security methodology should be adopted. There are many application level threats such as SQL Injection attack, Cross-site scripting [XSS], Cookie Poisoning, Hidden field manipulation, Backdoor and debug options. To counter these threats we have to consider the following factors illustrated in section A.

In public cloud architecture, the data moves to or from the organization, and ensures confidentiality and integrity. In Middleware, tools can present huge vulnerabilities such as host vulnerability, object vulnerability issues in access control. The risks of the vulnerabilities are classified depending on what they affect: data confidentiality, availability or integrity. Because of these vulnerabilities, many security attacks on middleware level exist like Eavesdropping, side channel attack, cross-tenant side channel attack, attack on data sharing, and Man-in-the-middle attack. To deal with the challenges, attacks and threats, we should also consider the factors illustrated in section B.

The flexibility and scalability of cloud computing system can offer significant benefits to governments and the private industry. Until IaaS doesn't offer hardware roots of trust, it will remain challenging for organizations to ensure security within the equipment, networks and virtual machines against attacks. The difficulty comes from the limited visibility into these levels, making actual conditions hard to verify. The attacks at IaaS level are Software Define Networking (SDN) attack, VM attack through HV, VM migration attack, Disk injection to live VM attack. To counter these attacks and challenges, we should consider the factors illustrated in section C.

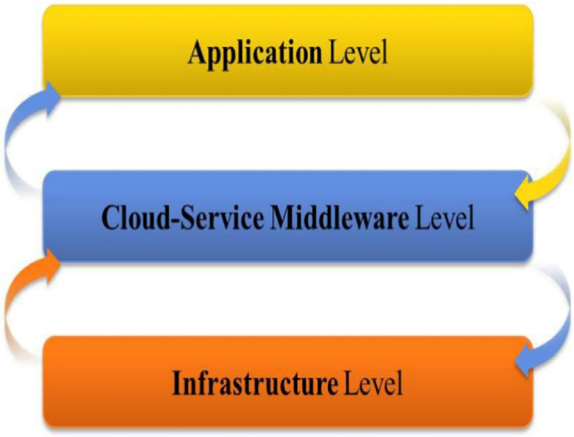

Fig. 4. 3-Tire security level architecture.

Fig. 5. Factors affecting on application level.

5.1. Application level

It resides on the top level where it directly delivers the outsourced software to the client. Customers don't need to expend the money to install software, only they have to pay for their usages. The security concerns for this level is end- to-end. Concern examples include client side scripting like XSS attack, API security, monitoring of data in the network, user authentication, some exception handling, interface cryptography and reputation of the service provider and authentication of the broker, as shown in Fig. 5.

Application level is also concerned with the need of an end-to-end security of data. Cloud systems need to have common security to achieve an end-to-end visibility and control over data, identities and application in cloud system. Intel and MacAfee enable end-to-end visibility to reduce the complexity of security and administration. However, in application level, enterprises data, along with another organization data, is stored at the SaaS provider data center. In addition, the cloud providers might be replicating the data across multiple locations in the world to maintain high availability. Cloud vendors such as Google App, Amazon and Elastic Compute Cloud (EC2) require administrators to use their individual cryptographic algorithm with strong Secure Shell (SSH) to access the hosts. A malicious programmer can exploit the vulnerabilities in data security model for unauthorized access. The assessments on application level like cookie manipulation, access control weakness, broker authentication, failure to restrict URL access, and insecure configuration.

5.2. Service middleware level

From the database servers, computer software provides services to application software. Middleware can be described as glue software that makes it easier to the software developer to perform communication in a cloud environment. Nowadays, as the importance of middleware increases, the security challenges also increase. Some of the issues include protocol standard security, user authentication and conceptualization, middleware trust, service credibility and regulations, cryptographic solution, spam snooping and sniffing as shown in Fig. 6.

To secure our cloud system, we use one of the best anti-spam sniffing tools, Heluna plus and Heluna standard, which block 99% of spam message with approximately zero false positive rates. We also use a protocol and standard called Cloud Trust Protocol (CTP) for establishing digital trust between end-users and providers. User and service authentication is verified through the login process. The cloud customers of USA or Canada follow the service regulations very securely and trustful to follow the confidential property. Legal requirements and regulations create a new

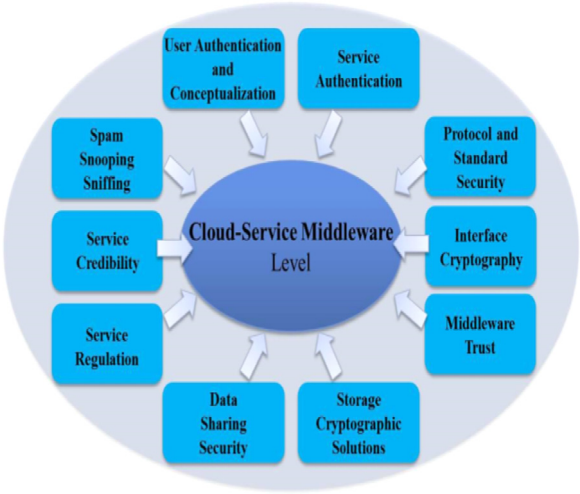

Fig. 6. Factors affecting on middleware level.

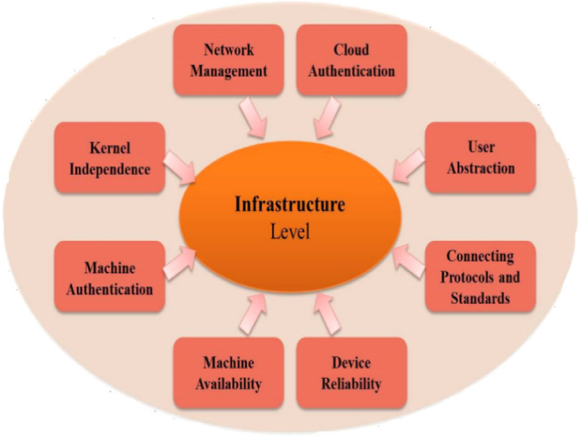

Fig. 7. Factors affecting on infrastructure level.

relationship between information of the organization and the third party, which describe how the information needs to be handled and stored by the cloud providers. For the middleware trust and service credibility, many approaches have been recently proposed. These approaches provide the trust management in cloud environments; still, not much attention has been given to determine the credibility of trust feedbacks. Credibility service checking is responsible for user credibility verification. It authorizes a device by providing a user interface that is the only single legal entry point.

Regarding protocol standards, the TCP/IP protocol model or WAP (Wireless Application Protocol) are the most common ways of communication over the internet. Nevertheless, they have much vulnerability to be exploited. Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Wireless Markup Language (WML), and Simple Mail Transfer Protocol (SMTP) are well-known vulnerable protocols also used in the cloud. Therefore, the security of protocols is necessary to secure Middleware level. In addition to the cryptographic solution we already discussed in chapter IV, to secure middleware level we should develop good authentication scheme between user and middleware, improve data sharing security and improve better spam management.

5.3. Infrastructure level

Cloud infrastructure abstracts the hardware (virtual machines, server, network components, and storage system) into a pool of computing. It provides a standard virtualized server to the consumer to take responsibility for configuration of the guest operating system. Cloud infrastructure can manage the computer capabilities such as performance, bandwidth and storage access. In this section, we consider the security concerns in infrastructure levels like kernel independence, network management, cloud authentication, connecting protocol and standard, device reliability, and machine availability/authentication.

Cloud service provider, in that data integrity, commonly uses security in web service. The confidentiality is fulfilled by XML encryption that endorses X.509 certificate and Kerberos. At the infrastructure level, the kernel acts as timer and system lock handling, descriptor and process manager. It also supports the network communication. In file system level, the kernel handles file blocking, I/O buffer management and pathname directories. Therefore, we need to isolate and make the OS kernel independent to avoid interferences on it. A secure and efficient Cloud authentication process and user abstraction should be provided in infrastructure level. All virtual machines working together should be mutually authenticated and good machine availability management should also be available, as shown in Fig. 7. The security risks to the cloud systems while facilitating Virtual Private Network (VPN) are on-demand resource availability and machine-to-machine performance monitoring.

5.4. Open issues and discussion

The adoption of cloud computing to provision the platform, infrastructure, and services for multitenant is growing exponentially during these years. In previous chapters, we have discussed in detail security issues and covered all important security aspects. In our paper, all the issues arise in the application level, Embedded, clustering computing, enterprises, data warehouse, kernel level are novel issue. However, orthodox issues become more critical and sensitive, for example, dealing with data without any administration management or configuring of a virtual machine without any hypervisor. Despite global and widespread adoption of cloud technology, researchers and analysts have been continuously reporting about the challenges and issues of the cloud. Summary Table 3 of chapter II has shown the academia and research work about novel security issues on factor affecting the cloud deploying elements. When writing a paper, researchers need to consider what security issues and interests have not been reviewed on the past five years. The following discussion will focus on a brief summary of all section learned from this work and provide some trustworthy and comprehensive security solutions.

The security attacks on cloud computing are obvious as their popularity keep increasing. Table 4 summarizes important attacks such as elevation of privilege, repudiation, wrapping attack, session hijacking, rollback attack etc., it also includes compromised security attributes, and related research works. Still there are some attacks on trust like social engineering; some insider attack in cloud storage like losing control over servers, lack of auditing management, misconfiguration of a security tool; compromised guest operating systems are also creating issues.

Logon Abuse, for example, refers to authorized users accessing a higher level of security that would normally be restricted to them. Similar to network intrusion, this type of abuse focuses primarily on legitimate user of different systems who have a lower security access.

Cloud service providers adopt good security measures and cover the security attributes according to the demand of the multitenant users. The government cloud projects developed their modules according to the situation of infrastructure needed like smart city, smart home, IoT etc. Moreover, only a few cloud

projects act as mediator between other cloud environments and technologies because of interoperability issues. Avoidance of vendor lock-in is the most common motivation for inter-cloud projects because the users are vulnerable to rises in prices.

The legal challenges the cloud computing industry is facing are not specific to the online world. Many of the issues are similar to any outsourcing service, in particular to cross-border outsourcing. This means that the challenges arising from the development of cloud computing can be tackled by laying a sound legal foundation to protect privacy and data.

Many security solutions and research techniques have been discussed in chapter 4 consider personal security, cryptography techniques, disaster recovery management, vitalization solutions, digital forensics tools and technique for the forensic cloud. Virtualization needs more attention for effective and comprehensive strategy because VMMs are large and complex system. This complexity comes from VMMs having thousands of lines of code that may include vulnerabilities. VMMs should isolate the running components to achieve good efficiency and throughput, by defining the virtualized network and providing a route to the virtual device.

Multi-tenancy is the essential characteristic of the cloud and it is applied for the utilization of resources; however it poses many threats. Trust, security and privacy for the multitenant user are great challenges in the cloud. Currently, there is not much work for solving security in multi-tenancy. But some work is been done to try to develop security solutions to deal with such challenges. To avoid unauthorized access to the shared pool resources, a trustworthy access control system is required. Because of the dynamic nature of the resources and the heterogeneity nature of the services, developing an access control is complex task. For the Future effort to integrate and mitigate the assurance and auditing tools to ensure the policy of involving entities needed directly.

Legal issues in the cloud should be surveyed and focus on laws and regulations across different regions and jurisdictions. Policies on how data is stored, processed and used should be surveyed too. In addition, various regulations in the disclosure of general specific data like financial data, health insurance records need to be examined. As used in the context the clouds, it is a particular problem with the new domain to the use of such a high-speed rail service cloud. Clouds spread system when integrated with sensor networks and grid-computing Furthermore, research on cloud privacy and security is a highlighted issue.

At last, it is a fortune to mention the security solution and proposing security module to cover all remains points provide the advantage to user and providers. The efficiency, cost overhead, and time management are also introduced. The inherent business model allows the organization to utilize their business process in a cost effective manner. We hope our work helps the user to analyze, quantify, and make a better decision of this research work.

6. Conclusion

The hype of cloud paradigm is changing the IT industry; it brings many benefits to companies, organizations and even countries. Despite bringing several advantages, the cloud still is vulnerable to many security challenges. This is why security is the major challenge in the adoption of the cloud. The customer and vendors are well aware of security threats.

This research attempted to show various security challenges, vulnerabilities, attacks and threats that hamper the adoption of cloud computing. Our paper provided a state-of–art survey on cloud security issues and challenges that arise from unique characteristics of the cloud like the sharing and virtualization of resources, resource pooling and the public nature of the cloud. We explored various cloud services and what they provide as well as analyzed the security concern on each provider. In addition, governments are also planning to develop the cloud technology to increase the performance, quality, innovation and security in the services they provide to the citizens. Subsequently, we have surveyed existing schemes that counter the security issues in an efficient, and cost saving manner. We have proposed the 3-tier security architecture for better security enhancement of cloud security. The model discussed the three level of cloud service system and important security considerations of each level. To conclude, we also discussed open issues and suggested future work.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea government (MSIP), Korea (No. 2016R1A2B4011069).

References

Abbas, Salim Ali, 2015. Enhancing the security of identity and access management in cloud computing using elliptic curve cryptography. Int. J. Emerg. Res. Manag. Technol. 4 (7).

Ahmed, Amjed Sid, Hassan, Rohayanti, Ali, Z.M., 2012. Eliminate spoofing threat in IPv6 tunnel. In: Proceedings of the 8th International Conference on Information Science and Digital Content Technology (ICIDT), IEEE, Vol. 1, pp. 218–222.

Ali, Mazhar, Khan, Samee U., Vasilakos, Athanasios V., 2015. Security in cloud computing: Opportunities and challenges. Inf. Sci. 305, 357–383.

Al-Saffar, Ali Mohammed Hameed, 2015. Identity based approach for cloud data integrity in multi-cloud environment. Identity 4 (8).

Anala, M.R., Shetty, Jyoti, Shobha, G., 2013. A framework for secure live migration of virtual machines. In: Proceedings of International Conference on, Advances in Computing, Communications and Informatics (ICACCI). IEEE, pp. 243–248.

Attas, Dalia, Batrafi, Omar, 2011. Efficient integrity checking technique for securing client data in cloud computing. Int. J. Electr. Comput. Sci. 11, 6105.

Behl, Akhil, Behl, Kanika, 2012. Security paradigms for cloud computing. In: Proceedngs of Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN). IEEE, pp. 200–205.

Behl, Aseem, Behl, Kanika, 2012. An analysis of cloud computing security issues. In: Proceedings of World Congress on Information and Communication Technologies (WICT). IEEE, pp. 109–114.

Beloglazov, Anton, 2013. Energy-efficient Management of Virtual Machines in Data Centers for Cloud Computing.

Bleikertz, Sören, Kurmus, Anil, Nagy, Zoltán A., Schunter, Matthias, Secure cloud maintenance: protecting workloads against insider attacks. In: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, pp. 83–84.

Booth, Gehana, Soknacki, Andrew, Somayaji, Anil, 2013. "Cloud Security: Attacks and Current defenses. In: Proceedings of the Annual Symposium on Information Assurance (ASIA'13), pp. 56.

Buyya, Rajkumar, Yeo, Chee Shin, Venugopal, Srikumar, Broberg, James, Brandic, Ivona, 2009. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Gener. Comput. Syst. 25 (6), 599–616.

Cao, Ning, Wang, Cong, Li, Ming, Ren, Kui, Lou, Wenjing, 2014. Privacy-preserving multi-keyword ranked search over encrypted cloud data. In: Proceedings of IEEE Transactions on Parallel and Distributed Systems, Vol. 25, Issue 1, pp. 222–233.

Chang, Victor, Kuo, Yen-Hung, Ramachandran, Muthu, 2016. Cloud computing adoption framework: a security framework for business clouds. Future Gener. Comput. Syst. 57, 24–44.

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

Chen, Fei, Liu, Alex X., 2014. Privacy and integrity preserving multi-dimensional range queries for cloud computing. In: Proceedings of IFIP Networking Conference. IEEE, pp. 1–9.

Chen, Yizeng, Li, Xingui, Chen, Fangning, 2011. Overview and analysis of cloud computing research and application. In: Proceedings of International Conference on E-Business and E-Government (ICEE). IEEE, pp. 1–4.

Choi, Junho, Choi, Chang, Ko, Byeongkyu, Choi, Dongjin, Kim, Pankoo, 2013. Detecting web based DDoS attack using MapReduce operations in cloud computing environment. J. Internet Serv. Inf. Secur. 3 (Issue ¾), 28–37.

Choudhury, Amlan Jyoti, Kumar, Pardeep, Sain, Mangal, Lim, Hyotaek, Jae-Lee, Hoon, 2011. A strong user authentication framework for cloud computing. In: Proceedings of 2011 IEEE Asia-Pacific Services Computing Conference (APSCC), pp. 110–115.

Cohen, M.I., 2008. PyFlag–An advanced network forensic framework. J. Digit. Investig. 5, S112–S120.
Czarnowski, Aleksander P., 2014. Service availability (in the clouds). In: AVET INS Euro Cloud Polska, Warsaw. pp. 3–9.
Dacosta, Italo, Chakradeo, Saurabh, Ahamad, Mustaque, Traynor, Patrick, 2012. One-time cookies: preventing session hijacking attacks with stateless authentication tokens. ACM Trans. Internet Technol. 12 (1), 1.
Dahbur, Kamal, Mohammad, Bassil, Tarakji, Ahmad Bisher, 2011. A survey of risks, threats and vulnerabilities in cloud computing. In: Proceedings of the International Conference on Intelligent Semantic Web-Services and Applications. ACM, p. 12, April 2011.
Danev, Boris, Masti, Ramya Jayaram, Karame, Ghassan O., Capkun, Srdjan, 2011. Enabling secure VM-vTPM migration in private clouds. In: Proceedings of the 27th Annual Computer Security Applications Conference. ACM, pp.187–196.
de Chaves, Shirlei Aparecida, Westphall, Carlos Becker, Lamin, Flavio Rodrigo, SLA perspective in security management for cloud computing. In: Proceedings of the 2010 Sixth International Conference on Networking and Services (ICNS). IEEE, pp. 212–217.
Dhage, Sudhir N., Meshram, B.B., 2012. Intrusion detection system in cloud computing environment. Int. J. Cloud Comput. 1 (2–3), 261–282.
Dykstra, Josiah, Sherman, Alan T., 2012. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. Digit. Investig. 9, S90–S98.
Dzombeta, Srdan, Stantchev, Vladimir, Colomo-Palacios, Ricardo, Brandis, Knud, Haufe, Knut, 2014. Governance of cloud computing services for the life sciences. IT Prof. 16 (4), 30–37.
Factor, Michael, Hadas, David, Hamama, Aner, Har'El, Nadav, Kolodner, Elliot K., Kurmus, Anil, Shulman-Peleg, Alexandra, Sorniotti, Alessandro, 2013. Secure logical isolation for multi-tenancy in cloud storage. In: Proceedings of IEEE 29th Symposium on in Mass Storage Systems and Technologies (MSST), pp. 1–5.
Fan, Haolong, Hussain, Farookh Khadeer, Younas, Muhammad, Hussain, Omar Khadeer, 2015. An integrated personalization framework for SaaS-based cloud services. Future Gener. Comput. Syst. 53, 157–173.
Fang, Junbin, Jiang, Zoe L., Yiu, S.M., Hui, Lucas C.K., 2011. An efficient scheme for hard disk integrity check in digital forensics by hashing with combinatorial group testing. Int. J. Digit. Content Technol. Appl. 5 (2), 300–308.
Feng, Jun, Chen, Yu, Ku, Wei-Shinn, Liu, Pu, 2010. Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms. In: Proceedings of the 2010 39th International Conference in Parallel Processing Workshops (ICPPW). IEEE, pp. 251–258.
Feng, Jun, Chen, Yu, Summerville, Douglas, Ku, Wei-Shinn, Su, Zhou, 2011. Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol. In: Proceedings of 2011 IEEE Consumer Communications and Networking Conference (CCNC), pp. 521–522.
Fernandes, Diogo A.B., Soares, Liliana F.B., Gomes, João V., Freire, M.ário M., Inácio, Pedro R.M., 2014. Security issues in cloud environments: a survey. Int. J. Inf. Secur. 13 (2), 113–170.
Flavio, Lombardi, Pietro, Roberto Di, 2011. Secure virtualization for cloud computing. J. Netw. Comput. Appl. 34 (4), 1113–1122.
Fotiou, Nikos, Machas, Apostolis, Polyzos, George C., Xylomenos, George, 2015. Access control as a service for the Cloud. J. Internet Serv. Appl., ISSN 1869-0238
Fung, Adonis P.H., Cheung, K.W., 2010. SSLock: sustaining the trust on entities brought by SSL. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 204–213.
Gonzalez, Nelson, Miers, Charles, Redigolo, Fernando, Simplicio, Marcos, Carvalho, Tereza, Näslund, Mats, Pourzandi, Makan, 2012. A quantitative analysis of current security concerns and solutions for cloud computing. J. Cloud Comput. 1 (1), 1–18.
Gupta, Sanchika, Kumar, Padam, 2013. Taxonomy of cloud security. Int. J. Comput. Sci. Eng. Appl. 3 (5).
Hashizume, Keiko, Rosado, David G., Fernández-Medina, Eduardo, Fernandez, Eduardo B., 2013. An analysis of security issues for cloud computing. J. Internet Serv. Appl. 4 (1), 1–13.
He, Xiangjian, Chomsiri, Thawatchai, Nanda, Priyadarsi, Tan, Zhiyuan, 2014. Improving cloud network security using the Tree-Rule firewall. Future Gener. Comput. Syst. 30, 116–126.
⟨http://searchsecurity.techtarget.com/feature/Longti%20me-Windows-vulnerabilities-fixed-in-Windows-10⟩. Available online, 2015.
⟨http://securityaffairs.co/wordpress/12703/cyber-crime/my-read-of-websense-2013-threat-report.html⟩. Available online, 2015.
⟨http://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49⟩. Available online, 2015.
⟨http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in⟩. Available online, 2015.
⟨https://msdn.microsoft.com/en-us/library/ff648651.aspx⟩. Chapter 15, Securing Your Network Available online, 2015.
⟨https://nvd.nist.gov/⟩. Available online, 2015.
⟨https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-19/Cisco-IOS.html⟩. Available online, 2015.
⟨http://customerthink.com/the-cloud-customer-experiences-saving-grace⟩. Available online, 2015.
Hussein, Nidal Hassan, Khalid, Ahmed, Khanfar, Khalid, 2016. A Survey of Cryptography Cloud Storage Techniques.
Jain, Neha, Kaur, Gurpreet, 2012. Implementing DES algorithm in cloud for data security. VSRD Int. J. Comput. Sci. Inf. Technol. 2 (4), 316–321.
Jamil, Danish, Zaki, Hassan, 2011. Security issues in cloud computing and countermeasures. Int. J. Eng. Sci. Technol. 3 (4), 2672–2676.
Jansen, Wayne, 2011. Cloud hooks: security and privacy issues in cloud computing. In: Proceedings of the 2011 44th Hawaii International Conference on System Sciences. HICSS. IEEE, pp. 1–10.
Jensen, Meiko, Schwenk, Jörg, Gruschka, Nils, Lacono, Luigi Lo, 2009. On technical security issues in cloud computing. In: Proceedings of the IEEE International Conference on Cloud Computing. CLOUD'09. IEEE, pp.109–116.
Jiang, Yexi, Perng, Chang-shing, Li, Tao, Chang, Rong, 2011. Asap: a self-adaptive prediction system for instant cloud resource demand provisioning. In: Proceedings of the IEEE 11th International Conference on Data Mining (ICDM), pp. 1104–1109.
Jiang, Yexi, Perng, Chang-shing, Li, Tao, Chang, Rong, 2012. Self-adaptive cloud capacity planning. In: Proceedings of the 2012 IEEE Ninth International Conference on Services Computing (SCC). IEEE, pp. 73–80.
Joshi, Bansidhar, Joshi, Bineet Kumar, 2012. Securing cloud computing environment against DDoS attacks. In: Proceedings of the International Conference on Computer Communication and Informatics. ICCCI. IEEE, pp. 1–5.
Kang, Seungmin, Veeravalli, Bharadwaj, Aung, Khin Mi Mi, Jin, Chao, 2014. An efficient scheme to ensure data availability for a cloud service provider. In: Proceedings of IEEE International Conference on in Big Data, pp. 15–20.
Kebert, Alan, Banerjee, Bikramjit, George, Glover, Solano, Juan, Solano, Wanda, 2013. Detecting distributed SQL injection attacks in a Eucalyptus cloud environment. In: Proceedings of the 12th International Conference on Security and Management (SAM-13), Las Vegas, NV.
Kertész, Attila, Kecskemeti, Gabor, Brandic, Ivona, 2014. An interoperable and self-adaptive approach for SLA-based service virtualization in heterogeneous Cloud environments. Future Gener. Comput. Syst. 32, 54–68.
Khalil, Issa M., Khreishah, Abdallah, Azeem, Muhammad, 2014. Cloud computing security: a survey. Computers 3 (1), 1–35.
Khan, Rouf Ab, Othman, Marini, Madani, Sajjad Ahmad, Khan, Samee U., 2014. A survey of mobile cloud computing application models. IEEE Commun. Surv. Tutor. 16 (1), 393–413.
Khan, Anwar Ulla, Oriol, Manuel, Kiran, Mariam, Jiang, Ming, Djemame, Karim, 2012. Security risks and their management in cloud computing. In: Proceedings of IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom). pp. 121–128.
Khorshed, Md. Tanzim, Ali, A.B.M. Shawkat, Wasimi, Saleh A., 2012a. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener. Comput. Syst. 28 (6), 833–851.
Khorshed, Md. Tanzim, Ali, A.B.M. Shawkat, Wasimi, Saleh A., 2012b. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener. Comput. Syst. 28 (6), 833–885.
Khoshkholghi, Mohammad Ali, Abdullah, Azizol, Latip, Rohaya, Subramaniam, Shamala, Othman, Mohamed, 2014. Disaster recovery in cloud computing: a survey. Comput. Inf. Sci. 7 (4), 39.
Kim, Jin-Mook, Moon, Jeong-Kyung, Hong, Bong-Hwa, 2013. An Effective Resource Management for Cloud Services using Clustering Schemes.
Ku, Cheng-Yuan, Chiu, Yu-Siang, 2013. A Novel Infrastructure for Data Sanitization in Cloud Computing. In: Diversity, Technology, and Innovation for Operational Competitiveness: Proceedings of the 2013 International Conference on Technology Innovation and Industrial Management. pp. S3_25–28.
Kumar, Arjun, Lee, Byung Gook, Lee, Hoon Jae, Kumari, Anu, 2012. Secure storage and access of data in cloud computing. In: Proceedings of 2012 International Conference on ICT Convergence (ICTC). IEEE, pp. 336–339.
Lagesse, Brent, 2011. Challenges in securing the interface between the cloud and pervasive systems. In: Proceedings of International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). IEEE, pp. 106–110.
Laura, Savu, 2011. Cloud computing: deployment models, delivery models, risks and research challenges. In: Proceedings of International Conference on Computer and Management (CAMAN).
Lee, Kangchan, 2012. Security threats in cloud computing environments. Int. J. Secur. Appl. 6 (4), 25–32.
Li, Jianxin, Li, Bo, Wo, Tianyu, Hu, Chunming, Huai, Jinpeng, Liu, Lu, Lam, K.P., 2012. CyberGuarder: a virtualization security assurance architecture for green cloud computing. Future Gener. Comput. Syst. 28 (2), 379–390.
Li, Jin, Li, Jingwei, Chen, Xiaofeng, Jia, Chunfu, Lou, Wenjing, 2015. Identity-based encryption with outsourced revocation in cloud computing. IEEE Trans. Comput. 64 (2), 425–437.
Lin, Chu-Hsing, Lee, Chen-Yu, Wu, Tang-Wei, 2012. A cloud-aided RSA signature scheme for sealing and storing the digital evidences in computer forensics. Int. J. Secur. Appl. 6 (2), 241–244.
Liu, Bingwei, Chen, Yu, Hadiks, Ari, Blasch, Erik, Aved, Alex, Shen, Dan, Chen, Genshe, 2014. Information fusion in a cloud computing era: a systems-level perspective. IEEE Aerosp. Electron. Syst. Mag. 29 (10), 16–24.
Liu, Qin, Wang, Guojun, Wu, Jie, 2014. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Inf. Sci. 258, 355–370.
Liu, Yuhong, Sun, Yan Lindsay, Ryoo, Jungwoo, Rizvi, Syed, Vasilakos, Athanasios V., 2015. A survey of security and privacy challenges in cloud computing: solutions and future directions. J. Comput. Sci. Eng. 9 (3), 119–133.
MacDermott, Áine, Shi, Qi, Merabti, Madjid, Kifayat, Kashif, 2013. Detecting Intrusions in the Cloud Environment. In: Proceedings of the 14th Annual Postgraduate Symposium on Convergence of Telecommunications, Networking and Broadcasting (PGNet 2013).
Mansooreh, Moghadam, Sterkel, Wendy, 2012. Cloud Computing vs Traditional Internet Setting: Which One is More Secure, Cameron University Spring.
Meena, Sachin, Daniel, Esther, Vasanthi, N.A., 2013. Survey on various data integrity

attacks in cloud environment and the solutions. In: Proceedings of International Conference on Circuits, Power and Computing Technologies (ICCPCT). IEEE, pp. 1076–1081.
Metzger, Andreas, Pohl, Klaus, Papazoglou, Mike, Di Nitto, Elisabetta, Marconi, Annapaola, Karastoyanova, Dimka, Agarwal, Sudhir, 2012. Research challenges on adaptive software and services in the future internet: towards an s-cube research roadmap. In: Proceedings of the First International Workshop on European Software Services and Systems Research: Results and Challenges, IEEE Press, pp. 1–7.
Modi, Chirag, Patel, Dhiren, Borisaniya, Bhavesh, Patel, Avi, Rajarajan, Muttukrishnan, 2013. A survey on security issues and solutions at different layers of cloud computing. J. Supercomput. 63 (2), 561–592.
Mowbray, Miranda, Pearson, Siani, 2009. A client-based privacy manager for cloud computing. In: Proceedings of the fourth International ICST Conference on Communication System Software and Middleware. ACM, p. 5.
Moyo, Tumpe, Bhogal, Jagdev, 2014. Investigating security issues in cloud computing. In: 2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), pp. 141–146. IEEE.
Muhammad, Shiraz, Abolfazli, Saeid, Sanaei, Zohreh, Gani, Abdullah, 2013. A study on virtual machine deployment for application outsourcing in mobile cloud computing. J. Supercomput. 63 (3), 946–964.
Nabil, Sultan, 2014. Making use of cloud computing for healthcare provision: opportunities and challenges. Int. J. Inf. Manag. 34 (2), 177–184.
Nakajima, Yoshiki, Masutani, Hitoshi, Shen, Wei, Tanaka, Hiroya, Kamatani, Osamu, Shimano, Katsuhiro, Fukui, Masaki, Kawamura, Ryutaro, 2013. Design and implementation of virtualized ICT resource management system for carrier network services toward cloud computing era. In: Proceedings of ITU Kaleidoscope: Building Sustainable Communities (K-2013). IEEE, pp. 1–8.
Nassif, Luís Filipe da Cruz, Hruschka, Eduardo Raul, 2013. Document clustering for forensic analysis: an approach for improving computer inspection. IEEE Trans. Inf. Forensics Secur. 8 (1), 46–54.
Ouedraogo, Moussa, Mignon, Severine, Cholez, Herve, Furnell, Steven, Dubois, Eric, 2015. Security transparency: the next frontier for security research in the cloud. J. Cloud Comput. 4 (1), 1–14.
Pal, Shantanu, Khatua, Sunirmal, Chaki, Nabendu, Sanyal, Sugata, 2011. A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security. arXiv preprint arXiv:1108.4100.
Panth, Deepak, Mehta, Dhananjay, Shelgaonkar, Rituparna, 2014. A survey on security mechanisms of leading cloud service providers. Int. J. Comput. Appl. 98 (1).
Patra, Prasenjit Kumar, Singh, Harshpreet, Singh, Gurpreet, 2013. Fault tolerance techniques and comparative implementation in cloud computing. Int. J. Comput. Appl. 64 (14), 1–6.
Pearson, Siani, 2013. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing Springer, London, pp. 3–42.
Pearson, Siani, Benameur, Azzedine, 2010. Privacy, security and trust issues arising from cloud computing. In: Proceedings of IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), pp. 693–702.
Perez-Botero, Diego, Szefer, Jakub, Lee, Ruby B., 2013. Characterizing hypervisor vulnerabilities in cloud computing servers. In: Proceedings of the 2013 International Workshop on Security in Cloud Computing. ACM, pp. 3–10.
Polze, Andreas, Tröger, Peter, 2012. Trends and challenges in operating systems—from parallel computing to cloud computing. Concurr. Comput. Pract. Exp. 24 (7), 676–686.
Pophale, Kailas, Patil, Priyanka, Shelake, Rahul, Sapkal, Swapnil, 2015. Seed Block Algorithm: Remote Smart Data-Backup Technique for Cloud Computing. Vol. 4, Issue 3.
Popović, Krešimir, 2010. Cloud computing security issues and challenges. In: Proceedings of the 33rd International Convention MIPRO. IEEE, pp. 344–349.
Qi, Zhao-Hui, Gao, Zhan-Feng, Shen, Ying-Ming, Han, Bing-Xin, 2013. Digital evidence protection model with batch-verifying and public verifiability for computer forensics. In: Proceedings of International Conference on Intelligence Computation and Evolutionary Computation. Springer Berlin Heidelberg, pp. 237–242.
Rao, N. Mallikharjuna, Sasidhar, C., Kumar, V. Sathyendra, 2012. Cloud computing through mobile-learning. arXiv preprint arXiv: 1204, 1594.
Rewagad, Prashant, Pawar, Yogita, 2013. Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. In: Proceedings of International Conference on Communication Systems and Network Technologies (CSNT). IEEE, pp. 437–439.
Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee, 2011a. Towards achieving accountability, auditability and trust in cloud computing. In: Advances in Computing and Communications, Springer Berlin Heidelberg, pp. 432–444.
Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee, 2011b. TrustCloud: a framework for accountability and trust in cloud computing. In: Proceedings of IEEE World Congress on Services (SERVICES), pp. 584–588.
Sagar, Aman, Joshi, Bineet Kumar, Mathur, Nishant, 2013. A study of distributed denial of service attack in cloud computing (DDoS). Edition on Cloud and Distributed Computing: Advances and Applications, Vol. 2.
Saripalli, Prasad, Walters, Ben, 2010. Quirc: a quantitative impact and risk assessment framework for cloud security. In: Proceedings of the 3rd International Conference on Cloud Computing (CLOUD). IEEE, pp. 280–288.
Sen, Jaydip, 2013. Security and privacy issues in cloud computing. Archit. Protoc. Secur. Inf. Technol. Infrastruct., 1–45.
Sharma, Neeta, Alam, Mahtab, Singh, Mayank, 2015. Web based XSS and SQL attacks on cloud and mitigation. J. Comput. Sci. Eng. Softw. Test. 1 (2).
Singh, Shikha, Pandey, Binay Kumar, Srivastava, Ratnesh, Rawat, Neha, Rawat, Poonam, Awantika, 2014. Cloud Computing Attacks: A Discussion With Solutions. Open J. Mob. Comput. Cloud Comput. 1 (1).
Singh, Vaishali, Pandey, S.K., 2013. Cloud security related threats. Int. J. Sci. Eng. Res. 4 (9), 2571.
Sleuthkit, 2015. ⟨http://www.sleuthkit.org/sleuthkit/⟩. Accessed 2015.
Somorovsky, Juraj, Heiderich, Mario, Jensen, Meiko, Schwenk, Jörg, Gruschka, Nils, Lacono, Luigi Lo, 2011. All your clouds are belong to us: security analysis of cloud management interfaces. In: Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, pp. 3–14.
Sood, Sandeep K., 2012. A combined approach to ensure data security in cloud computing. J. Netw. Comput. Appl. 35 (6), 1831–1838.
Subashini, Subashini, Kavitha, Veeraruna, 2011. A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. 34 (1), 1–11.
Sumitra, B., Pethuru, C.R., Misbahuddin, M., 2014. A survey of cloud authentication attacks and solution approaches. Int. J. Innov. Res. Comput. Commun. Eng. 2 (10).
Sun, Dawei, Chang, Guiran, Sun, Lina, Wang, Xingwei, 2011. Surveying and analyzing security, privacy and trust issues in cloud computing environments. Procedia Eng. 15, 2852–2856.
Sun, Dawei, Chang, Guiran, Guo, Qiang, Wang, Chuan, Wang, Xingwei, 2010. A dependability model to enhance the security of cloud environment using system-level virtualization techniques. In: Proceedings of the First International Conference on Pervasive Computing Signal Processing and Applications (PCSPA). IEEE, pp. 305–310.
Tan, Xiang, Ai, Bo, 2011. The issues of cloud computing security in high-speed railway. In: Proceedings of IEEE International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), Vol. 8, pp. 4358–4363.
Taylor, Mark, Haggerty, John, Gresty, David, Lamb, David, 2011. Forensic investigation of cloud computing systems. Netw. Secur. (3), 4–10.
Te-Shun, Chou, 2013. Security threats on cloud computing vulnerabilities. Int. J. Comput. Sci. Inf. Technol. 5 (3), 79–88.
Thakur, Anandita Singh, Gupta, P.K., 2014. Framework to improve data integrity in multi cloud environment. Int. J. Comput. Appl. 87 (10).
Thanh Cuong Nguyen, Wenfeng Shen, Zhaokai Luo, Zhou Lei, Weimin Xu, 2015. Novel data integrity verification schemes in cloud storage. In: Computer and Information Science, Springer International Publishing, pp. 115–125.
Tianfield, Huaglory, 2012. Security issues in cloud computing. In: Proceedings of IEEE International Conference on Systems, Man, and Cybernetics. SMC. pp. 1082–1089.
Toosi, Adel Nadjaran, Calheiros, Rodrigo N., Buyya, Rajkumar, 2014. Interconnected cloud computing environments: challenges, taxonomy, and survey. ACM Comput. Surv. 47 (1), 7.
Tripathi, Alok, Mishra, Abhinav, 2011. Cloud computing security considerations. In: Proceedings of IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), pp. 1–5.
Ushadevi, R., Rajamani, V., 2012. A modified trusted cloud computing architecture based on third party auditor (TPA) private key mechanism. Int. J. Comput. Appl. 58 (22), 1–9.
Ussath, Martin, Jaeger, David, Cheng, Feng, Meinel, Christoph, 2016. Advanced persistent threats: behind the scenes. In: Proceedings of IEEE, Annual Conference on Information Science and Systems (CISS), pp. 181–186.
VivinSandar, S., Shenai, Sudhir, 2012. Economic denial of sustainability (edos) in cloud services using http and xml based DDoS attacks. Int. J. Comput. Appl. 41 (20), 11–16.
Volokyta, Artem, Igor, Kokhanevych, Ivanov, Dmytro, 2012. Secure Virtualization in Cloud Computing.
Wang, Bin, Qi, Zhengwei, Ma, Ruhui, Guan, Haibing, Vasilakos, Athanasios V., 2015. A survey on data center networking for cloud computing. Comput. Netw. 91, 528–547.
Wang, Bing, Zheng, Yao, Lou, Wenjing, Hou, Y. Thomas, 2015. DDoS attack protection in the era of cloud computing and software-defined networking. Comput. Netw. 81, 308–319.
Wang, Qian, Wang, Cong, Ren, Kui, Lou, Wenjing, Li, Jin, 2011. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Trans. Parallel Distrib. Syst. 22 (5), 847–859.
Wang, Qian, Wang, Cong, Ren, Kui, Lou, Wenjing, Li, Jin, 2011. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Trans. Parallel Distrib. Syst. 22 (5), 847–859.
Wang, Cong, Wang, Qian, Ren, Kui, Lou, Wenjing, 2009. Ensuring data storage security in cloud computing. In: 17th International Workshop on Quality of Service (IWQoS). IEEE, pp.1–9.
Wang, Cong, Wang, Qian, Ren, Kui, Lou, Wenjing, 2010. Privacy-preserving public auditing for data storage security in cloud computing. In: INFOCOM, 2010 Proceedings IEEE, pp.1–9.
Wayne, Jansen, Grance, Timothy, 2011. Guidelines on security and privacy in public cloud computing. NIST Spec. Publ. 800, 144.
Wei, Jinpeng, Zhang, Xiaolan, Ammons, Glenn, Bala, Vasanth, Ning, Peng, 2009. Managing security of virtual machine images in a cloud environment. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, pp. 91–96.
Wen, Zhenyu, Watson, Paul, 2013. Dynamic exception handling for partitioned workflow on federated clouds. In: Proceedings of the 2013 IEEE 5th

International Conference on in Cloud Computing Technology and Science (CloudCom). IEEE, Vol. 1, pp. 198–205.
Win, Thu Yein, Tianfield, Huaglory, Mair, Quentin, 2014. Virtualization security combining mandatory access control and virtual machine introspection. In: Proceedings of the IEEE/ACM 7th International Conference on Utility and Cloud Computing, pp. 1004–1009.
Wu, Hanqian, Ding, Yi, Winer, Chuck, Yao, Li, 2010. Network security for virtual machine in cloud computing. In: Proceedings of the 2010 5th International Conference on IEEE Conference in Computer Sciences and Convergence Information Technology (ICCIT), pp. 18–21.
Xia, Yingjie, Xia, Fubiao, Liu, Xuejiao, Sun, Xin, Liu, Yuncai, Ge, Yi, 2014. An improved privacy preserving construction for data integrity verification in cloud storage. KSII Trans. Internet Inf. Syst. 8 (10), 3607–3623.
Xia, Yubin, Liu, Yutao, Chen, Haibo, 2013. Architecture support for guest-transparent vm protection from untrusted hypervisor and physical attacks. In: Proceedings of the 19th International Symposium on High Performance Computer Architecture (HPCA). IEEE, pp. 246–257.
Xiao, Zhifeng, Xiao, Yang, 2013. Security and privacy in cloud computing. IEEE Commun. Surv. Tutor. 15 (2), 843–859.
Xing, Tianyi, Huang, Dijiang, Xu, Le, Chung, Chun-Jen, Khatkar, Pankaj, 2013. Snortflow: a openflow-based intrusion prevention system in cloud environment. In: Proceedings of IEEE Research and Educational Experiment Workshop (GREE), pp. 89–92.
Xu, Le, Huang, Dijiang, Tsai, Wei-Tek, 2014. Cloud-based virtual laboratory for network security education. IEEE Trans. Educ. 57 (3), 145–150.
Yan, Gongjun, Wen, Ding, Olariu, Stephan, Weigle, Michele C., 2013. Security challenges in vehicular cloud computing. IEEE Trans. Intell. Transp. Syst. 14 (1), 284–294.
Younis, Younis A., Merabti, Madjid, Kifaya, Kashif, 2013. Secure Cloud Computing for Critical Infrastructure: A Survey, Liverpool John Moores University, United Kingdom, Tech. Rep.
Yu, Huiming, Powell, Nakia, Stembridge, Dexter, Yuan, Xiaohong, 2012. Cloud computing and security challenges. In: Proceedings of the 50th Annual Southeast Regional Conference. ACM, pp. 298–302.
Zhaolong Gou, Shingo Yamaguchi and B. B. Gupta, 2016. Analysis of various security issues and challenges in cloud computing environment: a survey. In: Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, pp. 393–419.
Zhifeng, Xiao, Xiao, Yang, 2013. Security and privacy in cloud computing. IEEE Commun. Surv. Tutor. 15 (2), 843–859.
Zhu, Yan, Wang, Huaixi, Hu, Zexing, Ahn, Gail-Joon, Hu, Hongxin, Yau Stephen S., 2011. Dynamic audit services for integrity verification of outsourced storages in clouds. In: Proceedings of the ACM Symposium on Applied Computing, pp.1550–1557.
Zissis, Dimitrios, Lekkas, Dimitrios, 2012. Addressing cloud computing security issues. Future Gener. Comput. Syst. 28 (3), 583–592.