Journal of Network and Computer Applications 74 (2016) 98–120

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

On cloud security attacks: A taxonomy and intrusion detection and prevention as a service

Salman Iqbal [a,*], Miss Laiha Mat Kiah [a,*], Babak Dhaghighi [a], Muzammil Hussain [a], Suleman Khan [a], Muhammad Khurram Khan [b], Kim-Kwang Raymond Choo [c,d,e]

[a] Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia
[b] Centerof Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia
[c] Department of Information Systems and Cyber Security, University of Texas at San Antonio, USA
[d] School of Information Technology & Mathematical Sciences, University of South Australia
[e] School of Computer Science, China University of Geosciences, Wuhan, China

ARTICLE INFO

Article history:
Received 31 May 2016
Received in revised form
19 July 2016
Accepted 15 August 2016
Available online 16 August 2016

Keywords:
Cloud computing
Taxonomy
Security attacks
Intrusion detection

ABSTRACT

Major provisioning of cloud computing is mainly delivered via Software as a Service, Platform as a Service and Infrastructure as a Service. However, these service delivery models are vulnerable to a range of security attacks, exploiting both cloud specific and existing web service vulnerabilities. Taxonomies are a useful tool for system designers as they provide a systematic way of understanding, identifying and addressing security risks. In this research work, Cloud based attacks and vulnerabilities are collected and classify with respect to their cloud models. We also present taxonomy of cloud security attacks and potential mitigation strategies with the aim of providing an in-depth understanding of security requirements in the cloud environment. We also highlight the importance of intrusion detection and prevention as a service.

Contents

* Corresponding authors.
E-mail address: raymond.choo@fulbrightmail.org (K.-K. Raymond Choo).

http://dx.doi.org/10.1016/j.jnca.2016.08.016
1084-8045/

1. Introduction

While Cloud Computing (CC) is not entirely new, it is still gaining traction among organizations and individual users. For example, Garner predicted that cloud adoption will continue to rise at a compound increase rate of 41.7% in 2016. However, transition to the cloud environment is not straightforward and there are a number of operational and security challenges. Ensuring the security of data outsourced to the cloud is increasingly important due to the trend of storing more data in the cloud (Duncan et al., 2013; Ristenpart et al., 2009).

The use of hypervisor and Virtual Machine (VM) technologies are also a security threat, as these hypervisor and VM technologies are vulnerable to VM level attacks. In reality, these systems consist of a number of on-site computer organizations which may have a large number of hardware and software systems. Vulnerabilities in VM infrastructure can be exploited by attackers to exfiltrate data or conduct attacks such as DDoS (Osanaiye et al., 2016; Gilad et al.). This is due to the inherent weaknesses in the TCP/IP stack. Additionally, several new attacks have appeared in recent times that make use of polymorphism and metamorphisms to evade detection. In an IaaS cloud environment, for example, information about victim's machines can easily be acquired and exploited; thus, facilitating attacks on VMs (Tupakula et al., 2011; Khan et al., 2014; Gani et al., 2014).

Attackers can inject kernel scripts to the host operating system (OS), and as all guest OS run their OS on this kernel, attackers can control all VMs. Furthermore, by successfully exploiting known or zero-day vulnerabilities in the hosted VM, the attackers can then gain access to the server's VMs since the hypervisor shares the hardware and software in the shared virtual environment (Ibrahim et al., 2011). Some hypervisors provide APIs which render the VM facility completely visible to network traffic. However, these APIs provide additional avenues for attackers to monitor and exploit the network communication (Scarfone, 2011). There are also other attacks such as data intrusion, data availability and data integrity targeting CC (AlZain et al., 2011).

The multi-cloud database model is an integral component in today's cloud infrastructure. Addressing the security in multi-cloud providers is a critical task. The challenge in deploying CC is to ensure the confidentiality and integrity of software applications running on a customer's VMs. Challenges arise when multiple VMs share the same hardware resources in the same physical host. Attackers can, for example, bypass the integrity measurement by reusing or duplicating the code pages of legitimate programs. The security architecture is probably dependent on the participants in the cloud ecosystem, namely: Cloud Service Providers (CSP), service instance and cloud service users (Xiao and Xiao, 2013).

In this paper, we systematically review the literature by locating published materials from Google Scholar and academic databases such as SpringerLink, ScienceDirect, IEEE eXplore, ACM Digital Library, Wiley Interscience, and Taylor & Francis Online, using keywords presented in Table 1.

The survey included both quantitative and qualitative research published in English between 2006 and April 2016. Slightly over 1440 research articles were located, and we eventually reduced to 738 research articles by reviewing their titles, 480 research articles by reviewing their abstracts and conclusion, and finally, 220 research articles by reviewing the full text. Eventually, only 105 research articles were included in this survey, due to thei relevancy.

Table 1
Systematical review methodology.

Sr. No.	Keywords	Years	Sources
1	Cloud computing	2006–2016	Journal, Conference, Workshop, Magazine, White paper And Transactions
2	Service deliver models		
3	Software as a Service		
4	Platform as a Service		
5	Infrastructure as a Service		
6	Security attacks		
7	Vulnerabilities		
8	Virtualization		
9	Privacy		
10	Quality of service		
11	Service level agreements		
12	Intrusion detection Systems		
13	Incident handling in the cloud		
14	Authentication methods		

We also located 16 surveys on this topic, as shown in Table 2.

In this research, we examine major attack vectors on CC service delivery models. It is important to understand these attack vectors because cloud offerings are relatively different from traditional web based environments (we refer the reader to (Prokhorenko et al., 2016) for a review of web application protection techniques). We also investigate the methods proposed to defend against these attacks in each cloud model. Lastly, the potential for Intrusion Detection and Prevention as a Service is explored.

The background and categories of CC security attacks are discussed in Section 2. The taxonomy is presented in Section 3. In Section 4, we present Intrusion Detection and Prevention as a Service. Open research challenges and issues are discussed in Section 5. Lastly, we conclude the paper.

2. Background

As more organizations adopt CC, this opens up new security risks that could impact on a wider user base. To-date, little effort has been devoted to addressing CC attacks and developing intrusion detection and prevention techniques for a cloud environment. Although existing studies such as (Subashini and Kavitha, 2011; Zissis and Lekkas, 2012; Takabi et al., 2010; Armbrust et al., 2010) investigate the potential of IDS in CC, these efforts do discuss the various security threats in each service delivery model. Evaluating IDS at the service delivery models is important (see Table 3), as it provides a detailed look into how we can secure the different CC service delivery models.

Major services include: virtualization resources, bandwidth and on-demand services to their customers. These services aim at reducing capital investment costs in such infrastructures, licensing and upgrades. The combination of HTTP and XML messages results in the HX-DoS attack, where messages are intentionally sent to the cloud service to break the communication channel in the CC model. The network based control are becoming less relevant as cloud services are delivered through the web browser, in new cloud based services model (Anitha and Malliga, 2013; Khan et al., 2015).

Malware can also affect the availability of Internet connections. Traditional mechanisms for detecting vulnerabilities and attacks on the traditional web applications do not scale well for CC where

Table 2
Existing surveys on cloud service models.

Papers	Description	Parameters	Year
(Juliadotter and Choo, 2015)	The authors provide a comprehensive study on taxonomies, and present different attacks against cloud services.	Attack taxonomy classifiers	2016
(Shameli-Sendi et al., 2015)	This research studies DDoS against CC as well as the mitigation strategies.	DDoS mitigation	2015
(Alizadeh et al., 2015)	The research defines the authentication methods and compares the mobile CC authentication methods by considering five evaluation metrics.	Cloud-side authentication methods, User-side authentication methods,	2015
(Shiraz et al., 2015)	The research investigates existing computational offloading methods and highlights technical issues such as resources intensive distributed platform, deployment of virtual mobile devices on cloud server node, accessibility of virtual mobile devices, and constraints on computing resources of the virtual mobile device.	Energy consumption and timing cost. Data transmission in computational offloading	2015
(Shaikh and Sasikumar, 2015)	This research presents the measurement to calculate the trust model. This trust model computes the trust value to strengthen the security.	Static and dynamic trust	2015
(Liu et al., 2015)	The authors present a thematic taxonomy for application partitioning algorithms in cloud computing.	Dynamic computational offloading	2015
(Ab Rahman and Choo, 2015)	The research surveys existing security incident handling and digital forensic in CC.	Digital forensic, incident handling, and Capability Maturity Model	2105
(Simou et al., 2014)	The paper presents CC forensic challenges.	Cloud Forensics, Cloud Forensics Process, Cloud Forensics Challenges, Digital Forensics	2014
(Toosi et al., 2014)	The survey paper discusses and categorizes possible cloud interoperability scenarios and architectures.	Cloud federation, Multi-cloud, Utility computing, Inter-cloud, cross-clouds	2014
(Whaiduzzaman et al., 2014)	The paper surveys vehicular CC issues.	Cloud formations, Key management, Inter cloud communication systems,	2014
(Manvi and Shyam, 2014)	This paper surveys resource management techniques in IaaS.	Resource provisioning, resource adaptation, resource allocation and resource mapping.	2014
(Patel et al., 2013)	The paper surveys and presents a conceptual Intrusion Detection and Prevention (IDP) architecture for CC.	Autonomic computing, risk management, ontology, and fuzzy theory	2013
(Grispos et al., 2013)	The paper presents the case study of Global Fortune 500 organizations and identifies the real world information security documentation issues.	Auditing policies, Standards and guidelines Applicable	2013
(Modi et al., 2013)	The paper surveys CC security issues.	Virtualization, Security, Privacy and Vulnerabilities	2013
(Sun et al., 2011)	The authors survey CC security, privacy and trust issues.	Presents the solution to analyze and eliminate potential privacy, security and trust threats.	2011
(Subashini and Kavitha, 2011)	The paper classifies CC security issues, focusing on Software as a Service.	SaaS	2011

Table 3
Different level of security issues in CC.

Security Issues	Attack vectors	Attacks Types	Impacts
Virtualization level Security Issues	• Social engineering • Storage vulnerabilities • Datacenter vulnerabilities and Network • VM vulnerabilities, etc.	• DoS and DDoS • VM Escape • Hypervisor Rootkit	• Software interruption and modification (deletion) • Programming flaws
Application level Security Issues	• Session management and broken authentication • Security misconfiguration, etc.	• SQL injection attacks • Cross Site scripting and • Other application based attacks.	• Modification of data at rest and in transit • Confidentiality • Session hijacking
Network level Security Issues	• Firewall misconfiguration, etc.	• DNS attacks • Sniffer attacks • Issues of reuse IP address • Network Sniffing, VoIP related attacks (e.g. VoIP phishing).	• Traffic flow analysis • Exposure in network
Physical level Security Issues	• Loss of Power and environmental control	• Phishing Attacks • Malware injection attack	• Limited access to data centers • Hardware modification and theft

services are distributed over multithreaded network infrastructures (Oliveira et al., 2008). For these reasons (Chen et al., 2013; Khan et al., 2014; Khan et al., 2016), Internet security problems remain the most common risks to CC. Internet threats include malware (including malicious mobile apps), spam, and phishing attacks. Botnets are probably the most well-known attacks on distributed network environment. A botnet attack typically consists of a huge number of bots which generate large volume of spam or launch DDoS attacks from compromised hosts. Other ways of attacking cloud services are through internet protocols such as man-in-the-middle attack, DNS poisoning, IP spoofing, RIP attacks, and flooding. Newer generations of botnet attacks have also seen (Khorshed et al., 2011).

2.1. Levels of attacks in CC

The following section defines the different types of attacks which occur in a CC environment. Each of these attacks is described as follows:

2.1.1. VM-to-VM attacks

Virtual machines are considered as a container which contains applications and guest operating systems. Cloud providers use hypervisor and VM technologies in cloud multi-tenant environment which consists of potential vulnerabilities. CC based on VM technology includes hypervisors such as VMWare vSphere, Microsoft Virtual PC, Xen etc. Attacks occurs due to the vulnerabilities in these technologies (Sabahi, 2011).

2.1.2. Client-to-client attacks

Client attacks on other client's machines by gaining the benefits of vulnerabilities in client applications which runs on a malicious server. As there is one physical server over several VMs, one malicious VM can infect all the other VMs working on the same physical machine as illustrated in Fig. 1. Here, the attack occurs on one client VM escapes to other client's VMs that are hosted over a single physical machine. As a result, the entire virtualize environment could become compromised and malicious clients can escape the hypervisor and can access the VM environment. As a result, the attackers can get the administrative privileges of the virtualized environment and can officially get access to all the VMs. Hence, the "client to client attacks" is a major security risk to the virtualized environment (Sabahi, 2011).

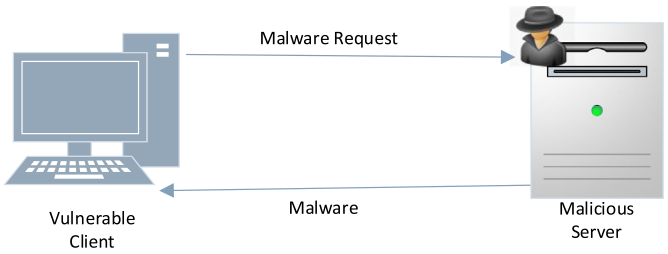

Fig. 1. Client to client attacks.

2.1.3. Guest-to-guest attack

To secure the host machine from attacks is an important factor because if an attacker gains administrative access to hardware, then most probably the attacker can break into the VMs. This scenario is called the guest-to-guest attacks which are illustrated in Fig. 2. As a result, the attackers can hop from one VM to another because the underlying security framework is compromised (Reuben, 2007).

2.2. Attack surface in CC

An attack surface includes all the points in the software environment through which an adversary or unauthorized users can try to gain access to a system and cause damage to the environment. In a cloud multi-tenant environment, resource sharing is one of the most critical issues creating new attack vectors.

There are differences between practice and theory. Large hypervisors may be seen to have relatively low surface attack vectors in theory, but there are a number of emerging real-world attacks targeting hypervisors (e.g. the use of rootkits and covert channel calls). Thus, virtualization is a new attack vector. A hypervisor compromised by a side-channel attack is likely to leak information

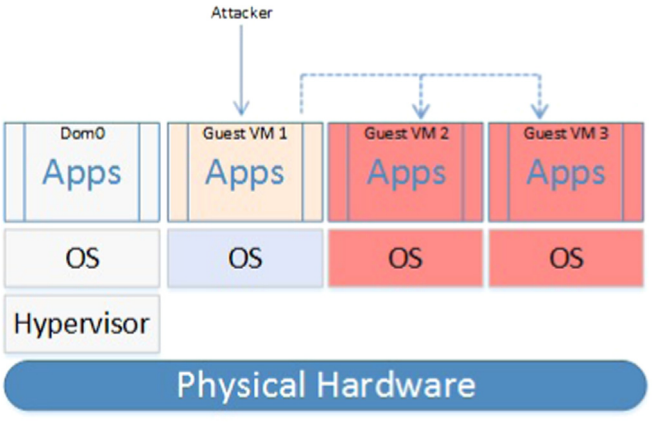

Fig. 2. VM to VM/ Guest to guest attacks.

outsourced to the cloud. Likewise, layer spoofing also has a new threat in the BluePill rootkit. Further, compromised hypervisor becomes the new attack vectors in a virtualized environment. Some potential attack vectors in CC are as follows (Turnbull and Shropshire, 2013) and a comparison of attack surface of each cloud service model is shown in Table 4:

- Redirecting Data Flows Using Firewall Ports
- API, Hooking System Calls and
- Hooking Library Calls

In some kind of virtualization systems, it is easy to share data between the systems, but sometimes, this feature can turn into an attack vector if not carefully controlled. It is important to identify the attack surface which is prone to security attacks (Scarfone, 2011). CC is based on the Internet and normally exposes its resources over the Internet. These resources can be categorized into three types (Bouayad et al., 2012):

- In SaaS model – web browser
- In PaaS model – Web services and APIs: SOAP, REST and RPC protocols
- In IaaS model- VMs and storage services: VPN and FTP

2.2.1. Attack surface in SaaS cloud layer

Web applications are called software and constitute a service in CC. These dynamic services pull data from various sources in a cloud distributed environment. Due to this feature, hackers sometimes insert text into the web page by using the comment which is called the script. When these scripts are executed on the browser they causes the unwanted behavior.

2.2.2. Attack surface in the PaaS cloud layer

As the PaaS cloud layer is responsible to provide the software execution environment for their customers without buying servers, storage and networks, security is the most important part of PaaS services. The responsibility of PaaS providers is to implement strong encryption techniques to provide services to their customers without disruption. In this way, the responsibility of PaaS providers is to secure runtime engines from attackers which run the customers applications. The programming framework which is also provided by PaaS vendors should also be secure from malicious threats. Multi-Tenancy (Rodero-Merino et al., 2012) is another major attack vector in the PaaS cloud layer. As multi-tenancy is supported in many platforms (Operating system or Virtual Platform), the PaaS cloud must facilitate their users by providing a secure platform where they can run their application components. The PaaS model allows multiple users to access cloud services simultaneously; thus, a malicious user can have multiple ways of interfering and disrupting the normal execution of the PaaS container.

2.2.3. Attack surface in the IaaS cloud layer

In cloud virtualization technology the hypervisor or virtual machine monitor is the additional layer between the operating system and hardware. This technology is common to the IaaS cloud to support virtualization technologies. In addition, they are used to create APIs in order to perform administrative operations. This addition of hypervisor causes an increased attack surface. This is due to the fact that there are many additional methods such as APIs, channels like sockets and data items like input strings which can be exploited (Szefer et al., 2011).

3. Classification of security attacks on cloud computing

The key motivation of this research is to determine the potential attacks on the CC environment and their possible impact on cloud services. As there has been a paradigm shift to CC, new solutions are needed to support modern business functionality. However, this adaptation is not hazard free and poses new security threats to its adopters. To address these challenges new taxonomies and classifications are required. In this paper we present the new taxonomy which is based on service delivery model of CC as illustrated in Fig. 3. Cloud Security Alliance and Gartner have identified several potential threats that may be encountered in a CC environment. Security in CC environments needs a holistic approach.

3.1. Security attacks on SaaS cloud layer

According to Gartner, SaaS is the “software that's owned, delivered and managed remotely by one or more providers.” Moreover, Gartner (Council, 2006) estimates that more than 75% of companies' IT budgets is used to purchase, run and repair software systems and infrastructures. Many security considerations are similar in SaaS as in web services. Users obviate to use SaaS services due to cloud data security and confidentiality. Encryption can be done on outsourced data to achieve confidentiality and security. Potential problems with this service delivery model includes: data related security issues such as who owns the data, data backup, data access, data locality, data availability Identity Management and authentication etc. Mostly, the security attacks occur due to the behavior of legitimate users. According to Forrester's research report, 70% of security breaches are caused by internal sources. These security risks can be reduced significantly by imposing the security checks.

3.1.1. Denial of service (DoS) attacks

DoS attacks are the malicious attempt to render the system or network resources unavailable to users. CC infrastructures are shared by millions of users, making it more difficult to resolve this sort of attacks due to its potential to have much greater impact compared to single tenanted architectures. As in CC, new weaknesses have opened as the use of virtualized data centers and cloud services increasing (Khan et al., 2016). Modern attackers do not need to attack the full infrastructure. As such, the Botnets play a major role in spreading these attacks. The more resource-

Table 4
Attacks surfaces in the cloud service models.

Attack surface	Attack Vectors		
	SaaS	**PaaS**	**IaaS**
Application level	Input/output validation	Runtime engine that runs customer's applications	virtual workgroups
Data Segregation	Unauthorized Access of Data	Data Service Portal	Multi-Tenancy and Isolation
Data Availability	Hosted Virtual Server	Network traffic	Virtual Network
Secure Data Access	Encryption/ Decryption Keys	Third Party Components	Cloud Multi-tenant Architecture
Data Center Security	Server based Data Breaches	Datacenter Vulnerabilities	Virtual Domain Environments
Authentication/Authorization	ID and Password	Client API Password Reset Attack	Poor Quality Credentials

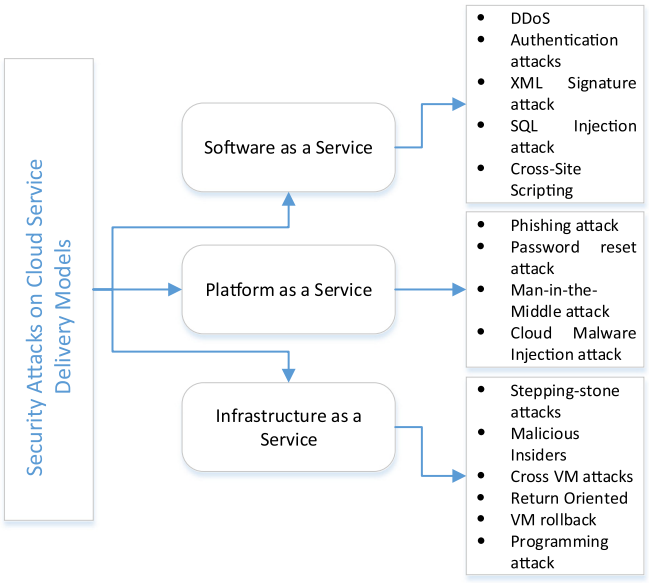

Fig. 3. Taxonomy of attacks along with their Cloud Service Delivery Models.

intensive applications running on the cloud with low bandwidth may attract attacks. An example is how Twitter was overwhelmed by DoS attacks in 2009.

SaaS provides the services to their customers, if the services become unavailable due to the DDoS attackers, the SaaS customers will not get their money's worth. Therefore, SaaS services become the attractive targets for the DDoS attackers. The DDoS scenario is shown in Fig. 4. This diagram aims to show the attacks scenario within a system. The handler is probably the most high volume server in which attack packets can be hides easily. Agents are the home users that are already infected. In this way it is very difficult to track down the attacker.

To address this issue (Szefer et al., 2011), a comprehensive analysis of the system should be undertaken to provide intrusion detection and prevention in order to defend against DDoS attacks. This mechanism takes a complete and concise study of the systems to prevent the systems from such attacks.

In OS level virtualization (Modi et al., 2013), several guest operating systems run on a single hosted OS and have a visibility and control on each guest's OS. In this way, the attackers can get the control of all guest machines by compromising the security of host machines. On the other hand, application based virtualization presents the top of host OS. This type of configuration allows each VM to have its own guest OS which is related to applications. In this case, the compromised hypervisor may compromise the entire guest OS. These vulnerabilities in virtualization or hypervisor level allow the attackers to launch the cross VM side channel and DoS attacks (Zhang et al., 2011).

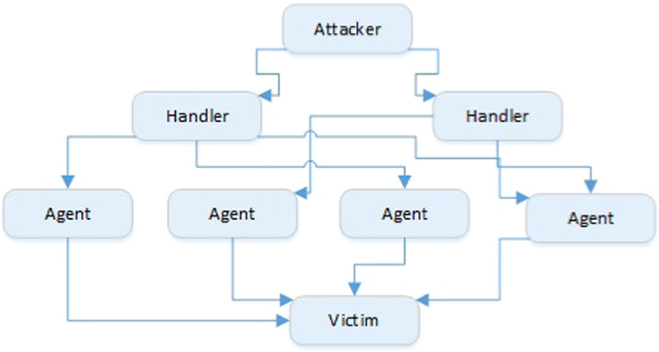

Fig. 4. A general diagram for distributed DoS.

Different scenarios of DoS attack.

- **SOAP:** SOAP allows communication between different web services. This protocol uses Hypertext Transport Protocol (HTTP) and Extensible Mark-up Language (XML). This implies that DDoS can bring down the web services by using HTTP or XML. This type of attack is called HX-DoS. As a result, the communication channel of the CSP is destroyed (Anitha and Malliga, 2013). DoS is easy to implement and is very effective. The technique such as SOA-Based Traceback Approach (Yang et al., 2012) is used to trace the source of these attacks by using SOA.
- **Timing:** sometimes the attackers choose the timing to launch attacks. The situation is called a flash crowd when a server would burden a large workload. In this situation when the attackers launch the attacks they may reach the attacks purpose. In this way the attack request may seem the same as flash crowd's request rate. Thus the detection algorithms should be able to detect the DDoS attack in time (Lin et al., 2010).
- **Isolation:** in a cloud-based platform, it is a difficult task for cloud providers to distribute the same set of network resources and isolation techniques to all tenants. This includes the isolation performance between tenant, minimizing disruptions and preventing DoS attacks. As a result, it is difficult for network administrators to efficiently allocate the network allocation and isolate techniques among all tenants. The vulnerability in DoS attacks results in the design of the bandwidth sharing mechanism.

There are many types of DoS attacks. However, cloud services are highly vulnerable to network based DoS attacks. Likewise network performance isolation is also an integral part of any virtual system as it minimizes the disruption from legitimate users as well as provides efficient protection against malicious tenants that launch DoS attacks. Similarly (Xiao and Xiao, 2013), cloud customers may also require physical isolation.

The authors in (Shea and Liu., 2012) investigate the impact of DoS attacks on hypervisor based systems. The authors state that even a small attack can affect the larger portion of VMs' systems and affects the memory access performance. Authors shows that virtualized network systems are more vulnerable compared to their non-virtualized counter parts. HX-DoS are a new type of attack that attacks compromised cloud providers. One approach is CLASSIE (Anitha and Malliga, 2013) which is a role set based detection in order to defend HX-DoS attacks. In this method, Reconstruct and Drop methods are used to decide which packet is affected and should be dropped. Other issues regarding these DDoS attacks are to differentiate the legitimate and illegitimate messages and users. Moreover, legitimate users also degrade the performance of the services. Meanwhile, Polymorphism (Hamdi, 2012) and evasion are probably the most technical issues regarding DDoS attacks. In this scenario, various attack vectors are sent to the victim's configuration in order to know the weaknesses in the infrastructure and to enhance the efficiency of the DoS attacks in terms of delay and probability. Some of the most common attack vectors for DoS attacks are:

- **HTTP** Get the flood attack: the attacker target the server under many requests and further target the URL to saturate the computing resources.
- **TCP** connection flood on port 80: resources of web application target on it.
- **SYN** flood attack: Sends the TCP connection request faster than a server can process them in order to target the server TCP/IP stack.
- **UDP** flood attack: bandwidth resources of the network has

targeted in these attacks.

As virtualization provides better resource utilization across multi-tenant cloud environments, thus virtualization layer can also help to defend against the DoS attacks. On the other hand, organizations are also realizing their responsibilities to prevent generating the DoS attack from their network. The anti DDoS can help prevent the DoS attacks in a standard way.

3.1.2. Authentication attack

It is important to authenticate for both users and CSP. The primary purpose of authentication is to allow only authorized persons to access the data processing system according to the cloud provider's policy. In essence, the mechanism and methods used to authenticate the system are frequent targets by attackers. For a certain class of cloud applications, many users are still using the simplest and unsophisticated mechanism of username and password to verify their account.

As an example, the LastPass (Barron et al., 2013) Company which stores and manages passwords in the CC environment stated that their systems were effected from a successful hack. Luckily no data was stolen but the company encouraged their customers to take measures to ensure that their data is secure. On the other hand, security experts discovered unusual behavior in their systems as there were more data going out as compared to incoming data. Due to these activities, the company assumed that this was a hacking activity related to siphoning stores sensitive user data and logging credentials. As a result, the company enhanced its encryption algorithms and introduced additional measures to protect sensitive data on its sever. The main authentication attacks include:

- Customer fraud, Insider attacks
- Key logger attacks
- Man-in-the-middle attacks
- Password discovery attacks, Phishing attacks
- Session hijacking attacks

It should be noted that identity is the core part of any virtualized CC system. It is used to identify the users, services, servers, clouds and other entities to be identified by the system in order to access that system. For this, the set of information is associated with a specific entity. CC providers should deliver a concise and consistent set of identity management systems. The existing standards (such as SPML, SAML, OAuth and XACML) are used to secure federated identities among different sets of entities and between different domains and cloud platforms (Bouayad et al., 2012).

Shared technology puts a heavy load on clients due to traditional authentication mechanism. To address this issue, the authors in (Kang and Zhang, 2010) propose the hierarchical Identity-Based Authentication (IBA) approach, which is a short key size and identity based to allow the encryption of files only once and storing of the corresponding cipher text in the cloud. The first cloud based RFID authentication protocol (Xie et al., 2013) was proposed to secure backend channels and offer readers with anonymous access to preserve the tag/ reader privacy to database keepers. Moreover the texture password authentication mechanism is more vulnerable to dictionary attacks (Dinesha and Agrawal, 2012).

Typically two kinds of authentication methods are offers by SaaS providers:

- A centralized authentication and
- Decentralized authentication systems

The authors in (Revar and Bhavsar, 2011) investigate existing authentication mechanisms such as SSO. The authentication of users through mechanisms such as cURL and SSL is very effective as it provides efficient solutions to protect users over insecure networks. As a result, the users can be protected from man-in-the-middle attacks by providing a set of cipher suites and server certificates that are verified and trusted. The encryption process is done through RSA algorithms when users create SSO agents and information is passed through http requests. However, the authors did not provide how the SSO can be access the cloud services from the mobile or other cloud compatible device.

On the other hand, (Sawesi et al., 2013) XML Digital signature based authentication could be the best option in order to protect the system from inherent weakness of online and web based authentication.

MiLAMoB (Lomotey and Deters., 2013) is an authentication mechanism which authenticates the users on behalf of customer's device. Authentication is the process to identify the legitimate users through some means such as ID and password. As CC is growing, there is the need for multiple authentications. In cloud SaaS increased users increases the number of identities and authentication mechanisms for users to log into the SaaS system. One way to protect the system from unauthorized use is to use multilevel authentication mechanisms. In reality, the multilevel authentication system (Dinesha and Agrawal, 2012; Yassin et al., 2012) requires alternative means of authentication besides providing the password and user name. Some approaches use digital signatures with fingerprint. However, these types of methods can be costly.

The authentication scenario of SaaS based applications is shown in Fig. 5 (Corporation, 2008):

- The user requires authenticating himself while accessing the information from SaaS provider. As the SaaS platform is web based therefore some sort of encryption done in the URL or a cookie.
- Through a direct web service call, the information is then authenticated against the customer's user directory.
- Customer's user directory replies back with some sort of authorization and authentication information.
- Finally, based on the scenario of authentication and authorization queries, the resulting request will be fulfilled or denied.

3.1.3. SQL injection attack

The two most common threats which are used to steel user information from the web application are SQL-injection and Cross Sit Scripting (XSS). These are used to steel user's data by inserting malicious code to inject into the web application as a user input. Consequently, when users return the data by using textbox in a web page the hackers add special characters in it. The malicious code is inserted into a standard SQL code that changes the nature

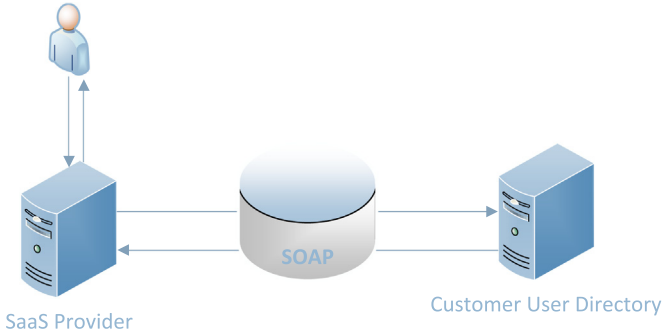

Fig. 5. Simple version of SSO.

of the query. As a result, the attackers gain access to a database and they run their own SQL command against the database so that it can be used to break into, alter, and delete the standard database design (Bhadauria et al., 2011). Eventually, the vast majority of SQL injection attacks have occurred through the user-submitted strings that have two parts. The first part contains the guess which contains the information to securely terminate the command which is performed by the code and second part is the hostile code which attackers wants to runs on the VPS. Moreover, the user input data, including the URL and AJAX interface etc. are also vulnerable. But amongst these the SQL query itself is more vulnerable for attackers. This is due to the reason that there are some basic commands or two to three different possible commands. There are several points where vulnerabilities could exist. In this way the attackers inserted the malicious code into the SQL code, as a result the attackers gain the unauthorized access to the data and become able to steel the important information. In some cases, the web servers misunderstood the hacker's data as the user's data. The attackers may get access to the SQL server and know the internal functioning of the web site and easily make changes into it (Bhadauria et al., 2011; Azeez et al., 2010).

3.1.4. Cross-site scripting

As discussed above, Cross-site scripting (XSS) is one of the most common application layer hacking technique. These inject malicious scripts into web contents thus it is the type of injection attack (Rodero-Merino et al., 2012). As cloud provides shared environment, the attackers attempt to insert malicious script like JavaScript, HTML, and VBSCRIPT into dynamic web application in the form of browser side script in order to gather important information from different user's machine. Cross site scripting are very famous attacks on web 2.0. 64 million cyber-attacks blocked by secure cloud hosting company in 2012 (Bhadauria et al., 2011). In this attack scenario (Qaisar and Khawaja, 2012), sometimes users enter the right URL but attackers' hacks this URL and redirect them to their own site in order to hack their credentials. In this way the attacker hacks the user's web page to steel his important information. Likewise, XSS provides the way to buffer overflows and DOS attacks in order to steel user's credentials. In practice (Sun and He, 2012), the XSS such as JavaScript is probably the most commonly used language in network applications. In the same way the Cross-Site Scripting (XSS) is believed to be one of the common attacks on internet based applications, there are normally two ways the malicious scripts inserted into the web pages:

- Persistent XSS attacks
- Non-persistent XSS attacks

As cloud distributed infrastructure is used to provide multi-fold services to the users, these distributed cloud environments are affected by XSS attacks. As the cloud data is located at a cloud third party site, it is easy to insert malicious code through web pages or pop-ups, third party services insert themselves to steel user important information.

This paper (Sun and He, 2012) proposes the model checking method to defense against XSS. This method finds bugs in the e-commerce application and presents the counter examples to these attacks. An operational behavior of the web site is checked to detect and illegal behavior of the web site. This is the automatic modeling algorithm for the HTML.

Both Cross-Site Scripting and SQL Injection attacks are becoming serious threats. FireHost (FireHost, 2012) reportedly prevented over 64 million malicious cyber-attacks, and the most common attacks are cross-site scripting as reported in Fig. 6.

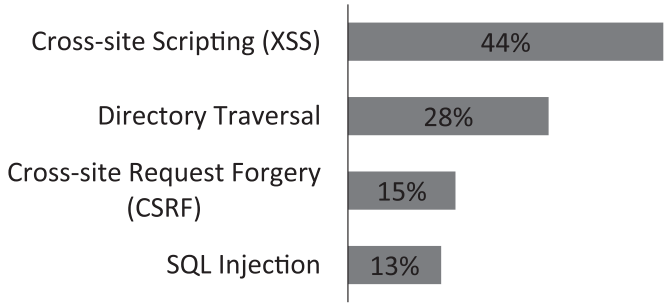

Fig. 6. Different Cyber-attacks blocked by secure cloud hosting.

3.1.5. XML signature wrapping attack

The SOAP messages become vulnerable to attacks. These are referred to as XML Signature Wrapping Attacks. In this scenario, the attackers can target the components through SOAP messages (Qaisar and Khawaja, 2012).

The SOAP message is generated by the server when the user sends a request through his VM browser. This message contains the structural information which is further used for communication between the client browser and server. In case of any flaw in the web server security protocol, attackers attack this protocol by using XML signature causing authenticating digitally signed SOAP message that has been change. Consequently, this task can be done by injecting the fake message into the SOAP message structure. In this way, an attacker has several arbitrary web service requests while authenticating him as a legitimate user.

UNWRAP (Nasridinov et al., 2012) is a way to present the wrapping attack of tolerant systems. In this way the authors first build the SOAP messages' header. SOAP messages elements structure has been build using ontology and attach it with SOAP message header. This way the attack is validated early in the validation process by validating ontology at the receiving end. This method also writes the SOAP messages as a log. In later stages if any security failure occurs, the log has checked and recovered from the effect of successful execution.

The attacks on protocols (Dawoud et al., 2010) by using XML Signature can also effect the CC services. The worst case scenario occurs when these attacks even break the security architecture between the browser and clouds. Consequently, the attacker can also exploit the important features of VMs like shared clipboard. Shared clipboard is the feature which allows data to be shared among VMs. The worst case occurs when the host machine is compromised. Due to this factor all the VMs are at risks.

In 2011 (Barron et al., 2013), researchers from the Ruhr-University Bochum found a security hole in the cryptography in Amazon's EC2 and S3 model. There is a flaw in the security protocol of web services that enable the attackers to bypass the security layer of digitally signed SOAP messages. The control interfaces that are used to manage the cloud resources are hijacked by the attackers. In this way the attackers would be able to create, modify, and delete the machine images and alter the administrative password.

The authors in (Sawesi et al., 2013) present an algorithms based on XML digital signature. The aim of this algorithm is to strengthen the mechanism against the XML wrapping and AML Namespace attacks. This approach aims to provide the digital signature instead of using traditional mechanism to authenticate the system. The XML scheme management includes the encryption and decryption mechanism which is used to defend against XML wrapping attack.

Cryptography, application credentials, external administration and multi-tenancy are vital features to secure SaaS based applications. One solution is to implement file and block level

Table 5
Summary of the approaches proposed to defense against attacks along with their pros and cons.

References	Method	Pros	Cons
(Garg and Saran, 2008)	Packet Filtering	Secure networked computers against DDoS attacks.	Although authors argues that their model is good for any virtualized environment, however this method is not proposed and implemented to be used in Cloud.
(Chen et al., 2011)	Packet Filtering	DDoS Attack Defense in Cloud Environment	The method does not have a strictly high accuracy because the use of CBF (Confidence-Based Filtering)
(Yang et al., 2012)	Trace Back methodology	CTB is based upon Deterministic Packet Marking (DPM) algorithm, which marks every incoming packet for tracing back attacker's true source IP address.	However, it may also make the cloud weak to DDoS attacks. If one server is suffering from a DDoS attack, it may spread the attack to other servers within the cloud system.
(Katkamwar et al., 2012)	Average Distance estimation	Detects DDoS attack in the cloud.	The proposed solution has high detection rate and low false positive rate but this is implemented on a simulator with 100 nodes not in the real cloud.
(Harnik et al., 2010)	Encryption / Dropbox protocol	Avoids deduplication of data	No practical evaluation of their attacks is given.
(Sun and He, 2012)	Model checking method	Defense against Cross-site scripting attacks	Not all types of cross-site scripting attacks detected.
(Saxena et al., 2013)	TRAP (Taint Removal and Analysis Platform)	Defense against SQLinjection attacks.	No implementation detail is provided.
(Chonka and Abawajy, 2012)	Decision Methods	Proposed a Defense method named ENDER which defense against HX-DoS	
(Karnwal et al., 2013)	Filter Tree Method	Defense XML DDoS and HTTP DDoS Attack	Not provide the hostile solution for complete cloud environment

encryption. Additionally, it is better to implement these encryption approaches at application layer level. Automated scanners (Brunette and Mogull, 2009) can also be used to detect most common vulnerabilities in addition with manual checking. In this case, multiple web application scanners are helpful to detect any vulnerability such as Cross Site Scripting (XSS) and Structured Query Language (SQL) injection attacks. Moreover, new approaches are necessary to completely overcome the web application malicious attacks from third party since the existing approaches not efficient to completely protect web applications flaws. Table 5 provides the comprehensive literature summary of approaches to defend against attacks along with their advantages and disadvantages.

3.2. Security attacks on PaaS cloud layer

In practice, the PaaS model relies on the Service-Oriented Architecture (SOA) model. In this model, there exists issues which can result in attacks targeting PaaS cloud and these attacks include DDoS, injection and input validation related, Man-in-the-middle, Replay and XML-related.

3.2.1. Phishing attacks/Social engineering attack

Phishing attacks are typically fraudulent email messages which directs to spoofed website. In PaaS cloud environment, these attacks affect both enterprise and users. This is a type of social engineering attack. These attackers convince the customers to reveal their most important data like password or other sensitive information by using bogus web pages, emails, or bloggers. Internet users suffer from phishing attacks (Li et al., 2011). These attacks affect both businesses and users of PaaS cloud model, and it may be easy to detect such attacks unless the victims realized that they are under attack unless their accounts have been compromised due to missing funds. Famous web browsers provide plug-ins to defend against these attacks but a complete client side solution is not being applied so far. Facebook users (Telegraph, 2009) are often targeted by phishing attack.

Mostly, phishing attacks target the vulnerabilities that occur due to the human factor. The users are normally the weakest element in the security domain because many attacks spread through exploiting the weaknesses in end users. There is no single approach which completely overcomes the problems of such attacks. In this way, multiple techniques can help to mitigate such issues. The paper (Khonji et al., 2013) investigates the mitigation techniques proposed and presents some high-level techniques such as: detection, offensive defense, correction and prevention. Likewise in August 2012 (Barron et al., 2013), attackers destroyed the digital library of technical writer Mat Honan by using social engineering attack through remotely deleting the data from his iPad, MacBook, and iPod. To provide strong authentication and authorization of customers IDs, Apple has temporarily disabled the customer's facility to change the password through phone. But customers can use the Apple's online “iForgot” system. Likewise the Amazon customer's service also terminates to change the credit card and email address through phone.

Phishing email is one of the challenging problems of today's world. These threats not only affect the users but also effect large organizations. Till now, these is no complete solution to address the problem of phishing attacks (Almomani et al., 2013). The Intelligent Cloud Based Email Encryption and Decryption System (ICLEEDS) (Ayodele and Adeegbe, 2013) is a new framework to improve the security of cloud based email messages. The focal point of the method is to encrypt the email message from user's mail box before sending it. This intelligent machine learning encryption system helps the systems to improve and protect users email from any attack such as phishing, spoofing, relaying of previous message etc. However, no detailed information on implementation in the real cloud environment is provided. For a cloud based environment, there is a need to propose self-adaptive, self-leaning encryption and decryption algorithms. The TLS configuration is going well for all types of web applications until the first phishing attacks detected in 2004 (Jensen et al., 2009).

The work in (Chen et al., 2013) design and implements a network based security forensic analysis has been conducted. The method uses the cloud storage to collect traffic data and process it in the CC platform to find malicious activity. For this purpose, they have used the phishing attack forensic analysis, store and process this to cloud platform to find any malicious activity.

3.2.2. Password reset attack

It is the process in which the attackers try every possible character combination to recover the password from data. The strong encryption process makes the content encrypt however, it does not means that it cannot be recovery again. It can be recovered to its own original content by applying more efforts through using high computational resources, tools, and

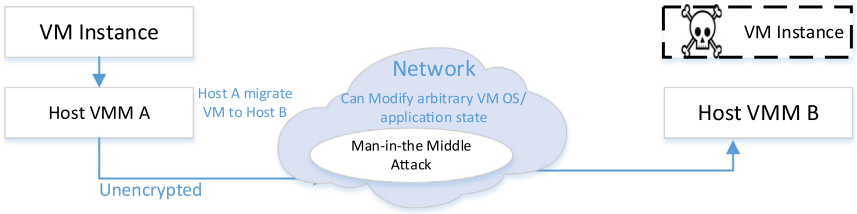

Fig. 7. VM migration attack scenario.

techniques. However, purchasing of high computing super-computers to decrypt encrypted information is not a wise decision which may work for specific task and is costly too in terms of financial burden. However, with CC, end-users have access to very powerful machines to execute their high computational task which is far better than the machines operating in the traditional infrastructure.

Account hijacking can be done through stolen credentials. Through stolen credentials, attackers can access to the important information. As an example, in July 2012 a group of hackers "UGNazi" exploited major flaws of Gmail's password recovery process and AT&T's voicemail systems. As a result they gained access to the personal Gmail account of the CEO of CloudDare's. Likewise, another case reported by Dropbox cloud storage service in July 2012 whereby hackers stolen the passwords and usernames from third party servers to access Dropbox users' accounts (Barron et al., 2013).

a) *Brute Force Attack*
   The attacks on web applications' log-in credential are the most common type of brute force attack. Users usually pick up the easy words or phrase as passwords. This makes it easy for brute force using the dictionary useful. These attacks attempt to log-in to the system by using a large list of words and phrases as a potential password. This method is called "word list attack" or a "dictionary attack"
b) *Brute Forcing Session Identifiers*

HTTP is a stateless protocol. To maintain the state the web application ensures that the session identifier has been sent by the browser with each request. This session identifier is most probably stored in the HTTP cookie or in URL. In brute attacks, the attacker attempts to guess the session identifier of another user.

In brute force, the attackers try single possible password until they find the correct password. To perform brute force attacks on a number of passwords there is a need of high performance computing power. Most people do not have such a performance system. But someone could go to amazon cloud to buy or rent a high magnitude machine to perform such attacks (Ristenpart et al., 2009).

3.2.3. Man-in-the-middle attack

This is the type of eavesdropping attack where the attackers intercept the communication between two parties. Here the attackers attempt to insert himself between two users (e.g. customers or verifier). They insert into the communication path and attempt to impose themselves as a customer to verifier and verifier to customers. In this way, they modify and intercept the communication. Network traffic normally travels between two computers that communicate with each other over the internet. During the transmission of messages between two computers, the attackers intercepts messages in a public key exchange and re-transmit this message by substituting his own public key in a way that original users still appear to be communicating with each another. Another popular example of this attack is when the client and server are communicating with each another in a http transaction, attacker splits this TCP connection into two new parts; one between client and attacker and other between attacker and server. Various tools have (Bhadauria and Sanyal, 2012) bene invented with strong encryption mechanism to defend against these types of attacks such as: Dsniff, Cain, Ettercap, Wsniff, Airjack etc.

By omitting the keys the attestation process would be open for man-in-the-middle attacks. As an example, the malicious users can wait for the attestation process to complete and then reboot a machine into the untrusted state without the knowledge of remote servers (Garfinkel et al., 2003).

The authors in (Zhang et al., 2008) proposed the scheme to secure the VM live migration. This method makes the VMM responsible for all processes needs for live migration such as locating and decrypting all source pages. First the method decrypts the keys and hash through public platform key of the source machine. After, it compares the hash values of the source pages before decryption. As a result this platform based session key based protocols aims to defend the man-in-middle attacks.

There are very less number of methods which are provides the security mechanism at network levels such as firewalls, encryption and network isolation. The need is to prevent the attacks like man-in-the-middle at network layer. These attacks can also be prevented by implying the conventional security measures secure APIs and taking frequent backups (Zhang et al., 2011). Moreover, in order to prevent unauthorized access, authentication and authorization of both personnel and trusted nodes are required.

If the migration protocol has encrypted during migration then it is susceptible to man-in-the-middle attack (Bryan Williams, 2010) which allows arbitrary state in VM to be modified as shown in Fig. 7.

3.2.4. Cloud malware-injection attack

In malware injection attacks, attackers insert or inject malicious code into a web page causing web pages to be infected by malware when internet users browse the page. It normally occurs by compromising FTP. It injects into the cloud server and may disturb the functionality of these services. When user sends their command to perform operation, attackers hacks it and inserts their own malicious command. In this case the code appears as a valid instance services running on the cloud.

In May 2009, the U.S. Treasury Department discovered that malicious code was present on their website and reportedly shut down four public-facing sites of the Bureau of Engraving and Printing. Subsequent investigations identified the cause due to a third party. Similarly, the chief research officer of Anti-Virus Guard (AVG) technologies discovered that affected pages are vulnerable to malicious code. Table 6 provides the comprehensive literature summary of approaches to defend against attacks along with their advantages and disadvantages.

3.3. Security attacks on IaaS cloud layer

On this layer, the attackers first hold the operations of hosted virtual machines opening the possibility to attack on other

Table 6
Summary of the approaches proposed to defense against attacks along with their pros and cons.

References	Method	Pros	Cons
(Li et al., 2011)	Network traffic	LARX is an offline phishing detection system which can be scaled to large volume of trace data.	However their solution requires digital manual submitters, verifiers of suspicious URLs and required up-to date information.
(Ayodele and Adeegbe, 2013)	Machine learning encryption	The focal point of the method is to encrypt the email message from user's mail box before sending it.	No implementation detail is provided to implement their method in real cloud environment.
(Ferguson et al., 2012)	VMM	Phishing detection analysis from multiple cloud providers.	Heavy workload when implementing multiple cloud based platforms simultaneously.
(Zhang et al., 2008)	VMM	Session key based protocols aims to defend against several attacks such as man-in-middle attacks.	Cannot apply for other VMM-enforced process protection systems.
(Chen et al., 2013)	Forensic analysis	The work in design and implements a cloud based security center for network based security forensic analysis to detect malicious activities.	Only known attacks can be detected through this method.
(Volokyta et al., 2012)	VMM	Deals with various activities of guest VMs and monitor the inter-communication among different system's components.	No implementation detail is provided.

compromised hosted VMs or an attack on the hypervisor. As an example, the DKSM is an approach to bypass such security mechanisms which is dependent on the OS in order to solve the semantic gap. It introduces two attack models: one changes the semantics of the kernel structure and other changes the syntax. The same setup in the cloud such as virtualization technologies, vulnerable software and shared physical resources attracts attackers to attacks on multiple compromised VMs (Ibrahim et al., 2011).

As previously discussed, hypervisor is an attack vector that can be exploited as a launch pad for other attacks such as abuse of computing power (Turnbull and Shropshire, 2013). In this way, running the malicious VM is the same as moving the malicious code into the network system over a single physical machine and bypassing any intrusion detection system over the network infrastructure. The installed VM is logically connected to a virtual network to serve many users. Due to the shared environment of cloud infrastructure the attack models can be presented in the virtual network. Consequently, the migration of running data applications with their data and state are vulnerable to security breaches and attacks. Sometimes, the attackers subvert the page tables. As a result the attackers could misuse the existing code. The attackers can disturb and change the normal routine that handles the page table updates with malicious parameters. The VM image is rebuilt on the target machine, after an attacker has successfully received the memory pages. Consequently, this can be used to launch spoofing attacks by replacing the targeted content (Wang and Jiang, 2010).

There are two types of traffic among VMs:

- *Internal Traffic*: is communication in which VMs communicate in a user group. The internal traffic could contain any confidential information. Thus this information should be protected from malicious users and from malicious cloud ISPs. In this way, the security policy should be independent of the management of a cloud ISP and policy should be established and enforce by the user group. Likewise, the user group should take the responsibility of internal communication and is independent of ISP.
- *External Traffic*: in this mode of communication, the VM accesses other users groups which reside on the same cloud ISP or on the internet. This is the communication between user groups. The cloud ISP manages and controls the traffic between user groups. The security policy establishes and is enforced by the ISP, and is responsible for external traffic security problems.

Additionally, survey shows that security over virtual environment has been neglected. Major securities threats to the IaaS computing environment include the security concerns at virtualize level; hypervisor security, Virtual Network security, Virtual storage etc. some major security attacks on IaaS layer has described below.

3.3.1. *Malicious insiders*

Malicious Hypervisor, Malicious Clients, Malicious Cloud Provider/Broker etc. are all the other terms which can also be used as an alternative to malicious insiders. This kind of attack occurs from client to server when the person, employee or staffs who know how the system runs, can implant malicious codes to destroy everything in the cloud system.

The CC industry is well aware from the threat of insider attacks. This threat is much more dangerous in cloud environment because it may gain a lot of important information from the cloud data. It is also very important to know the scope of the insider attacks and their effect to better defend against such threats. We need to understand whether insiders exposed the important information from both actors and attack surface (Duncan et al., 2012).

Insider attacks remain a major threat. However, these kinds of threats not gain too much attention because companies normally focus on external threats instead of paying attention to insider threats. Insider attacks were generally planned in advance. For example, the study of Eric and Shaw reported that perpetrators of insider attacks have no common demographic and there were different risk indicators (Nkosi et al., 2013).

In the CC environment, the elastic nature of IaaS VMs enables the frequent reallocation with physical machines or with other virtual machines. While during this migration potential threats and vulnerabilities can also be introduced due to compromised hypervisors. These insider's activities can be detected inside the hypervisor and in guest operating system. The work in (Khorshed et al., 2011) uses the rule based learning, which successfully identified the insider's activities. They also argue that sometimes, perhaps, these insiders' activities become insider's malicious attacks so carefully observation of these attacks should be monitored. No practical implementation is provided to detect these threats in real world.

The paper (Nkosi et al., 2013) presents the approach to detect the malicious insiders in the cloud environment. Authors show that the malicious insiders can also be detected on the basis of their behavior pattern. Their model uses the sequential mapping approach in order to detect any malicious pattern activity for a particular profile. However this model does not provide complete security architecture for entire cloud environment. The system is implemented only for the SaaS environment and not for PaaS and IaaS.

The work investigates the malicious modification threats through insiders by observing the relational database. The effort has been made to observe the insiders modification by

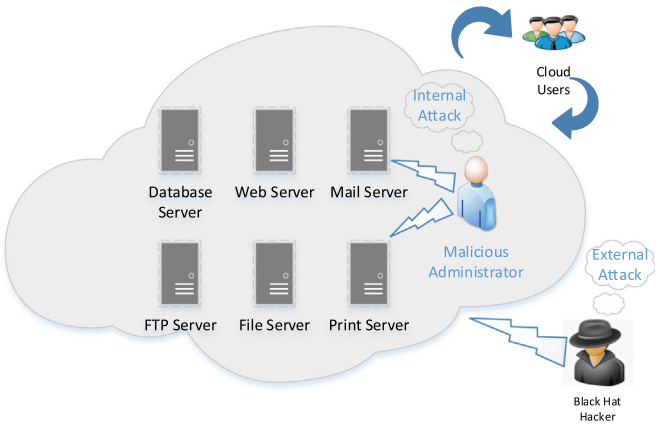

Fig. 8. An overview of internal and external attacks.

constructing insiders modification graph, through which the activities would be to observed that whether the data is authorize or unauthorized by which insider's attempts to make changes (Yaseen and Panda, 2010).

Furthermore, the current status of insider threats and their impact on the CC environment has been identified in (Duncan et al., 2012; Rocha et al., 2013). This work also investigates that due to the complex nature of insider threats which is very hard to detect by using current technologies. Normally there are two types of attacks faced by CC referred to as internal attacks and external attacks as shown in Fig. 8 (Oktay et al., 2013).

3.3.2. Cross VM attacks (Side channel attacks)

An often overlooked attack on cryptography software is the side channel attacks. Side channels attacks are based on "side channel information". This information is retrieved from the cryptographic software that is neither the plaintext nor the cipher text. The two main steps of side channel attacks are:

- Placement: attackers The malicious VM resides on the same physical machine and
- Extraction: confidential information, file and documents extracted after successfully placement of malicious code to target VM machine.

The Cross-VM can also exploit the nature of multi-tenancy. It enables the different customers from multiple VMs can co-reside on the same physical machine (Xiao and Xiao, 2013).

Side channel attacks are, probably, the one of the most challenging threats to address. For example, due to the shared cloud infrastructure, timing channels can be exited at any point in time and malicious users co-located on the same infrastructure can potentially steal sensitive data from other legitimate users.

VM techniques allow the attackers to exploits the underlying design of VM machines to allows attackers to perform cross-VM and timing attacks due to shared virtual and physical resources (Xiao and Xiao, 2013).

Recent work (Godfrey and Zulkernine, 2013) investigates the uncovered vulnerabilities in cloud systems. The most common vulnerability in a virtualized CC environment is the risk of information leaks through virtual machine isolation through side-channel. Side channel attacks are becoming significant threats to CC due to the resource sharing capability of CC. Among these the most common is the cache-based side channels attacks. As a result, the side channel threats effects both the host and guest machines. This leads the problem of better resource utilization (Yu et al., 2013). Due to the shared environment of CC, the malicious tenant wants to steal the important information of other tenants. In the encryption process, cache based side channel attacks are probably the most common threats in a virtualized cloud environment. Although cross VM side channel attack looks simple, there are some problems (Suzaki, 2012):

- 14KB Alignment problem: attacker must prepare exact same pages in order to guess victim's contents.
- Self-reflection problem: caused by redundant memory management on cache and heap. Attacker has a false-positive result.
- Run time modification problem: caused by swap-out, etc. Attacker has a false-negative result.

The work in (Shi et al., 2011) proposed the approach which considered dynamic cache coloring. In this way, the VMM is a point to migrate the data to a more safe and isolated line when doing security sensitive operations. However these solutions are not feasible for commercial cloud based applications and can create overhead. Moreover, the need is to validate their solutions in other virtualized environments such as extended page table or nested page table. SilverLine (Mundada et al., 2011) is a method to introduce the data and network isolation over a cloud hosting infrastructure. The goal of this approach is to audit and prevent any data leaks. The authors know the competence of existing information flow control techniques which results of misconfiguration and side channels attacks. While the focus of this approach is mainly on the server side protection without paying attention to the leakage from web browser.

The authors in (Zhang et al., 2012) extract the cryptography keys in order to infer cypher operation from cache timing observation and perform a cross-VM channel attack by using a combination of support vector machine and hidden Markov model (HMM). In (Potlapally et al., 2007), side channel attacks are modeled as a search problem. Their approach takes as input leaked information, which then uses Boolean reasoning attempting to extract the relevant secret key. However, it is not unclear if this approach is practical.

Another type of Cross-VM attack is memory disclosure (Xiao and Xiao, 2013). Virtualizes technologies allows to reduce the utilization of physical memory through memory deduplication. In this process, the memory pages are shared with same content. In a co-residing VM, the existence of an application or files can be detected by measuring the differences in write access time between reduplicated pages and regular pages (Harnik et al., 2010).

Moreover (Suzaki, 2012), memory deduplication is vulnerable for side channel attack. The vulnerability is caused by Copy-On-Write of memory deduplication. Copy-On-Write is a common technique to manage shared contents, but it became a Covert Channel for Information Leak. Memory deduplication is vulnerable for cross-VM side channel attack resulting Information leak. The main task to isolate among different physical machines and several users to avoid the threat of side channel attack. These attacks break the physical properties of hardware to break and take control of the information such as usage patterns for memory access, CPU and other resources (Scarfone, 2011).

3.3.3. VM rollback attack

VMs roll back to their previous state if an error occurs. Unfortunately, this factor can re-expose them to security vulnerabilities, and attackers can gain benefit to attack on this compromised hypervisor. It is important to protect the data during migration. In fact, this is the defending of data privacy and integrity from various network attacks during migration. The threats during migration include spoofing, replay and man-in-middle attack. To balance the security and functionality, (Xia et al., 2012) proposed a method where users securely logs to all suspend/ resume and migration operation inside the trusted computing domain. In this

way the users have a method to audit the log in order to check the malicious rollback and limit the operation on VMs. This approach provides the way to restrict the users from VMs. The important point is to protect the VMs from compromised hypervisors. In the old IaaS platform it is difficult to identify the normal resume/suspend and migration operations in old systems so as a result they are vulnerable to rollback attacks. Before, systems simply disable all these features or required continuous feedback from customers to defend against these attacks.

The research in (Fiebig et al., 2013) provides a way to detect the VM live migration. Their approach is based on the hybrid detection approach using delay measurement with ICMP ping and time-lag detection with network time protocol to detect VM live migration. However, they only provided the prototype and did not implement their solutions in real time cloud environments. The need is to test their prototype against different server's type's i.e. video servers or web shop servers to create more improved monitoring solutions. The secure counter which is always being incremented by time is greatly enhancing the functionalities of VM. This secure counter has the functionality to defend against file system rollback attacks.

3.3.4. Stepping-stone attack

CSP delivers VMs for users so that they can set up their own operating system and applications. There may be some flaws inside VMs due to smaller security patches. The attackers not attack from their own machine in stepping stone attack rather from intermediary hosts by using previously compromised VMs in the IaaS cloud. The attacks could happen when the VMs in the IaaS platform are compromised. In this way VMs are used to attack the host in the outside. In this scenario, the service providers are responsible and are victims at the same time, when the attacker uses the stepping stone attack against the host in the outside.

Stepping stone attacks through hosted VMs are critical in the IaaS infrastructure. These attacks use the compromised VMs to attack on outside hosts. In this way the IaaS service providers can also be considered as an attacker. To protect this scenario the IaaS cloud should provide an active response against these types of attacks. It is very difficult to protect against types of attacks through firewalls because firewalls only protect the information in network packets (Kourai et al., 2012).

Similarly, (Kourai et al., 2012) cloud providers should implement some type of control to detect botnet, prevent from them and trace the botmater. In this way, the work in (Lin and Lee, 2012) proposed the Pebble trace scheme which identifies the botmaster. This mechanism first identifies the cryptographic keys of botnet communication to configure botnet operation and then trace back to the botmaster. This unique approach identifies the botmaster without deploying any monitors, router updates, ISP support across stepping stone and multiple cloud platforms.

3.3.5. VM escape

In the cloud virtualization model there is normally a privilege VM and several unprivileged VMs. Privilege escalation attack is to escalate the privilege of unprivileged VM. In this mode, the Boolean value in the hypervisor controls whether the VM is privilege or not. After escalating the privilege of compromised VM the attacker can destroy the VM. In a virtualized environment the code reuse is called the Return-oriented Programming. This type of attack overwrites the stack with addresses that are pointing to the function in the standard library. But the functions of these attacks are restricted by the functions in libc (Ding et al., 2012).

In this type of attack the attackers attempt to break down the guest OS in order to access the hypervisor or to penetrate the functionalities of other guest OS and underlying host OS. This breaking of the guest OS is called as escape. If the attackers escapes the guest OS it may compromise the hypervisor and as a result it may control over the entire guest OS. In this way the security breach in single point in hypervisor may break down all the hypervisor (Scarfone, 2011). If the attacker controls the hypervisor, it can do anything to the VM on the host system. Likewise, “Escape the VM” is the malicious code which is another major issue at VM level and which can interfere the hypervisor or other guest VMs. Thus it is very important to investigate the effective way to defend against these types of attacks (You et al., 2012).

As we know, (Reuben, 2007) VM allows the sharing of resources over a host machines and provides the isolation between VMs and hosts. Therefore the VM is designed in a way that a program running on one VM cannot view or interferes another VM or with the program running on other host machines. But in reality the companies' compromises isolation and new software bugs introduce to compromise isolation. One such example of this type of attack is VM escape. This is the worst case attack which happens when the isolation between VM and between the hosts is compromised. In this type of attack, the program running on a VM completely bypasses the virtual layer (hypervisor layer) and gets the access to the host machine. Thus, the entire environment is compromised and results in a VM Escape problem. A mitigation strategy is proper configuration of the guest machines.

3.3.6. Return oriented programming attack

Successful attacks were launched when the attackers injects and execute their own code or modify the existing code. This may signify the adversary model when the attackers inject code, modify the existing one, or practice more sophisticated attacks such as return-oriented. In this scenario, instead of focusing subverting page tables, the attacker may attempt to modify and misuse the existing code, most commonly known as the return-oriented attacks (Wang and Jiang, 2010).

The authors in (Ding et al., 2012) launched the return-oriented programming attack. Instead of modifying any code in order to change the privileged field, this method has taken advantage of the existing hypervisor code. The adversary still maliciously alters the hypervisor's non-control data by taking advantages of return oriented programming techniques.

The paper presents a technique to investigate the security of Xen Hypervisor by using Return-Oriented Programming (ROP) and discovers the vulnerabilities points in the hypervisor. It controls the data on the Xen hypervisor to see whether the VM is privileged or not. This method bypasses the integrity measurement by using ROP technique to attacks without changing or modifying the existing code. However they did not present any preventive or defensive mechanism to defend against these types of attacks. Table 7 provides the comprehensive literature summary of approaches to defend against attacks along with their advantages and disadvantages.

Techniques for detecting and preventing intrusions can be applied to different layers of cloud computing models. For example these techniques can be adapted from virtualization/network layer (IaaS) to the operating system layer (SaaS), or even application or middleware layers (PaaS). In the next section, we will see that how IDS techniques can assist CC environment to protect different service delivery models.

4. Intrusion detection and prevention as a service

In Section 3, we have thoroughly explored that each cloud layer suffered from certain vulnerabilities. These vulnerabilities are introduced by different programming and configuration errors of internet and web application, wireless communication networks of the user or the service providers. In this way, the Intrusion Detection System (IDS) is an essential component of a defensive

Table 7
Summary of the approaches proposed to defense against attacks along with their pros and cons.

References	Method	Pros	Cons
(Kourai et al., 2012)	Packet filtering	Can protect guest machines and cloud platform from stepping-stone attacks.	SMPT server which is used to block the SPAM attack can also block the legitimate users
(Godfrey and Zulkernine, 2013)	Hypervisor	It provides the server side solution to cache based side channel attacks in CC.	No practical implementation is given. Hard to implement.
(Yaseen and Panda, 2010)	Modification Graphs	The scheme proposed how to detect and prevent the malicious insider's attacks.	Experimental results are not conducted
(Khorshed et al., 2011)	Decision tree classifier	Monitoring of insider activities	Advanced practices should be provides for real-world activity classification problems.
(Oyama and Hoshi, 2011)		The framework for injecting effects of attacks against targeting guest VMs from PrivVM. This method involves by targeting specific processes or parts of processes.	However they do not consider the hypercall attacks and the attacks which targets VMMs in general.
(Nkosi et al., 2013)	Sequential rule mining	Detect malicious insiders	Not proposed for complete cloud environment.
(Shi et al., 2011)	Dynamic cache coloring	Detects the cache based side channel attacks in a virtualize cloud environment.	However these solutions are not feasible for commercial cloud based platform.
(Fiebig et al., 2013)	Hybrid detection	The authors provide the way to detect the VM live migration.	However, they only provide the prototype and not implemented their solutions into real time cloud environment.
(Xia et al., 2012)	Observation by the end users	Defend VM rollback attack	Creates the overhead and degrade the performance
(Potlapally et al., 2007)	Boolean reasoning technique	Side-channel attacks	No mathematical evaluation of the attacks has been done.
(Nkosi et al., 2013)	Sequential Rule Mining	Check the malicious behavior of insider's activities	However, one of the major threat is still the insider threats.
(Duncan et al., 2013)	Digital forensics	Detects Insider Attacks	More work needs to be done to form the effective attack vector from the extracted information.
(Lin and Lee, 2012)	Pebble trace scheme	Defense against Stepping stone attacks	However they not consider the asymmetric key identification for their method.
(Yu et al., 2013)	Pattern recognition technique	Detects the cache-based side channel attacks.	More experiments needs to be performed for dynamic cloud environment.

Table 8
Difference between IDS and Firewalls.

Intrusion detection system	Firewalls
Device or application	Device or application
Analyses whole packets	Analyses packet headers
Looking for known events	Enforces policies
Monitors traffic	Block traffic based on network information
An IDS monitors traffic	Screening network traffic
Monitors the system for unwanted entries	Monitors the system based on the rules

mechanism to protect network and computer systems against various attacks at different service models.

There is continuous evolvement in the current enterprise architecture. Therefore, traditional firewalls methods cannot provide good solution as the firewall rules need to be modified for each trivial update in enterprises. A comparison between IDS and firewall is shown in Table 8. Moreover, in this section we will define the IDS with CC perspective and investigates how intrusion detection is performed in cloud services models. Moreover the approaches so far proposed for IDS in cloud environment are also discussed (Fig. 9).

Intrusion detection system is the procedure which monitors network traffic to detect any vulnerability exploits against a target applications or system. Thus the main task of intrusion detection is to enhance the security in a computer network. Basically, the ID system is the whole compound that includes the components of ID. This IDS system contains variety of flavors and approaches to detect the suspicious traffic in different ways (Oktay et al., 2013; Araújo and Abdelouahab, 2012).

Numerous services are provided by the CC to the end users. Therefore, to provide safe and reliable services assurance is quiet important. The IDS is one of the practical approaches to defend these attacks and various types of vulnerabilities. The role of IDS in cloud environment is very important because it provides the additional layer to protect the attacks and other vulnerability against their malfunction behaviors. In the cloud multi-tenant environment, IDS provides the best way to defend against known and unknown attacks.

The attacker can attack by taking the advantage of

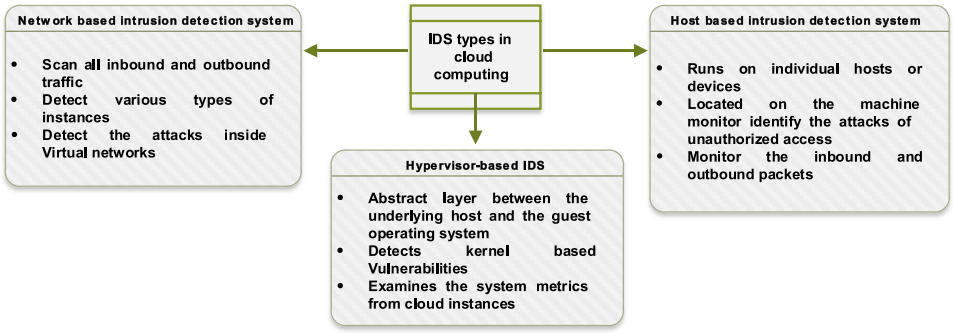

Fig. 9. Types of IDS in CC.

vulnerabilities in VM, and can sabotage the physical host and the virtual networks supported by them. But the things go even worst when attacker launches the attacks on multiple virtual hosts over one single physical machine. The IDS can help to reduce the risk of this type of attack. For the cloud environment the hypervisor based security solutions are effective to protect the virtualized environment. A comprehensive Table 9 is presented to show insight about different IDS techniques used in CC. Each of the techniques is compared based on Software, Platform and Infrastructure (SPI) layers, methods, types, pros and cons.

4.1. Intrusion detection approaches

The common types of IDS techniques are (Oktay and Sahingoz, 2013):

- Signature based detection
- Anomaly detection
- Artificial neural network (ANN) based IDS
- Fuzzy logic based IDS

4.1.1. Signature based

Signature based detection compares signature of files on a system which are known as a malicious files. In this way, the malicious packets are detected by searching through network traffic. The signature-based detection identified the packets on the network. The signature is formed by a set of rules and characterized the attackers, detects the threats and prevention of the occurrence of any false positive (Araújo and Abdelouahab, 2012). However this kind of IDS is not successful for new attacks (Oktay and Sahingoz, 2013).

4.1.2. Anomaly based

The anomaly detection technique lookup into the baseline to identify the network behavior. This baseline is specified by the network administrator. The network traffic has been monitored in anomaly based detection. This system detects abnormal system behavior, identifying suspicious activities, look up the ports and protocols used, and indicate any malicious activities in order to alert the administration about the detection of anomalies, or significantly different from the baseline (Araújo and Abdelouahab, 2012; Oktay and Sahingoz, 2013).

4.1.3. Artificial neural network (ANN) based IDS

In this type of IDS the program's internal states has been monitored in order to defeat the malicious files. It utilizes ANN (Artificial Neural Network) as a pattern recognition technique.

4.1.4. Fuzzy logic based IDS

This method based on rule based technique and detect the intrusion behavior of the network traffic. IDS based on fuzzy logic and data mining techniques.

4.2. Intrusion detection system types

There are some major types of IDS which are used in CC.

4.2.1. Network based intrusion detection system (NIDS)

NIDS observes, examines and analyzes the traffic to and from all the devices on the network. It can scan all inbound and outbound traffic and detect various types of instances. Once the attacks have been detected from this method the active system immediately takes necessary actions to tackle the attacks (Araújo and Abdelouahab, 2012; Oktay and Sahingoz, 2013).

The cloud provider's responsibility is to manage and deploy the NIDS in cloud environment. These types of NIDS can be useful to detect some kinds of attacks in VMs and hypervisor. However, NIDS cannot detect the attacks inside virtual networks. Moreover the network traffic within and outside of the cloud environment cannot be decrypted to analyze the network traffic.

4.2.2. Host based intrusion detection systems (HIDS)

This method runs on network of individual host or devices. Host machine can be analyzed and observe through HIDS. It could be located on the host machines which contains the important information. HIDS located on the machine monitor and identify the attacks and attempts of unauthorized access to the machines.

Inbound and outbound packets are monitor and alerts to the users or administrators about any suspicious activity. In cloud environment the HIDS can be applied either on the VM or on the host machines. The HIDS deployed on the VM can be monitored and managed by the customers. However, the HIDS deployed on the hypervisor is monitored by the cloud providers. It is the responsibility of the providers that they should ensure that they are providing adequate IDS in their sides (Araújo and Abdelouahab, 2012).

4.2.3. Hypervisor-based intrusion detection system

Hypervisor based or VMM implements the abstract layer between the underlying host and the guest operating system. This layer provides the security, so that the kernel becomes free of vulnerabilities In this way the HIDS examines the system metrics from cloud instances from the hypervisor and detect any potential misuse patterns.

In the cloud environment this type of intrusion detection runs inside the hypervisor. This detection method allows monitoring and analyzing the communication between VMs, hypervisors and inside the virtual networks. This approach can be effective in cloud environment, however as this method is new so it will take some time to mature and take some time to be fully adopted by the cloud providers and customers (Bharadwaja et al., 2011; Nikolai and Wang, 2014).

4.3. Intrusion detection in cloud computing service models

As every cloud service delivery model is different from others service models similarly, IDS techniques used for each cloud services models also differs.

Software as a Service: in SaaS users merely depend upon their providers to deploy their services. Therefore, it is also the responsibility of the SaaS cloud providers to develop IDS for the security. The users can have the option to get some logs and deploy some kind of customs monitoring and alerting however, CSP should be at lead to implement IDS in the CC environment.

Platform as a Service: in PaaS, IDS are merely deployed outside of the applications thus; most of the IDS in PaaS are deployed by the CSP. The users can configure their applications and platform to log onto a central location to monitor and alert about IDS. In this way, IDS can be deployed at the platform level.

Infrastructure as a Service: IaaS is considered a more flexible model for IDS. The users have more options to perform their IDS over this layer. Consequently, IDS can be executed several ways over the IaaS cloud layer such as:

- *Virtual machine:* deploying IDs in the virtual machines can allows you to monitor the systems and alert and detect any unusual behavior of the machines. In this way the customers themselves alert the administrators about any unusual behavior.
- *Hypervisor or host system*: As the hypervisor provides the abstract layer it allows monitoring the hypervisor itself and

Table 9
Summary of the approaches proposed for IDS along with their pros and cons.

References	Year	SPI Layer/ Platform	IDS Method	IDS Type	Pros	Cons
(Alqahtani et al., 2014)	2014	SaaS	Packets	NIDS	The DoS attacks can be detected.	More comprehensive solution consisting of qualitative and quantitative methods should be conducted.
(Nikolai and Wang, 2014)	2014	IaaS	Signature	Hypervisor based	DoS attacks can be detected from various sources	It Required continuously manually administrator's attention.
(Alqahtani et al., 2014)	2014	SaaS	Signature	Service-based intrusion prevention system	It detects the SQL injections attack.	Only known attacks can be detected.
(Oktay and Sahingoz, 2013)	2013	IaaS	Proxy based	NIDSs	This approach helps to locate the ideal location of the IDS in virtualize environment so that both providers and customers can be able to decide the location of defense mechanism.	The hardware usage percentage is get from network traffic which is non-realistic network traffic.
(Chung et al., 2013)	2013	IaaS	Attack-graph based IPS	NIDS	The attack graph is constructed to exploits the undesirable state of the systems i.e. an attacker gains the admin access of the machine.	The NICE framework did not detects the coordinated multi-step attacks across multiple servers.
(Mohamed et al., 2013)	2013	IaaS	Pattern matching detection and anomaly detection	Hybrid detection	It handles distributed attacks such as port scanning attacks.	Unknown attacks cannot be detected.
(Meng et al., 2013)	2013	–	Signature based	NIDS	This approach detects the network attacks.	Need to test their system in other cloud environment to validate the effectiveness of this approach.
(Oktay et al., 2013)	2013	Cloud Computing	–	Hybrid IDS	IDS model is proposed in order to protect the system from untrusted cloud providers.	The proposed approach must be tested for known attacks for improvement.
(VivinSandar and Shenai, 2012)	2012	Cloud Services	Signature based	NIDS	Block several attacks such as XML and DDoS attacks.	Unknown attacks cannot be detected in this method.
(Hamad and Al-Hoby, 2012)	2012	SaaS	Signature based Detection	NIDS	The known attacks can be detected on the user's running machine.	Unknown attacks cannot be detected in this approach.
(Bradai and Afifi, 2012)	2012	IaaS	Reputation of nodes	Trust based	This approach detects the attacks from user and cloud side.	Take heavy resources and computations overhead
(Khune and Thangakumar, 2012)	2012	PaaS	Memory scanners and system call anomaly detection	Mobile host agent	Detect any misbehaving in the network through forensic analysis in smart mobile phones.	However, the experimental results are not provided
(Yassin et al., 2012)	2012	SaaS	signatures	NIDS	Detect all possible threats in public and private Clouds.	It only sniffs packets at network level.
(Gupta et al., 2012)	2012	Cloud Computing	Anomaly	Hypervisor based	It detects the VM based attacks	Implementation in real time environment is not provided.
(Houmansadr et al., 2011)	2011	Smart phones	Anomaly detection	NIDS	Malicious behavior can be detected on smartphones.	The attack graph generated should be used to automatically decide upon response action in smartphone environment.
(Lee et al., 2011)	2011	Cloud Computing	Anomaly detection	HIDS	Fast detection mechanism to detect several types of attacks.	More resources consumed for high level users.
(Bharadwaja et al., 2011)	2011	IaaS	Anomaly detection	VMM	This ID method can do the dynamic filtering to detect malicious hyper-call attacks on VMM and host OS.	This method cannot detect the other types of attacks.
(Kwon et al., 2011)	2011	Cloud Computing	Anomaly detection	HIDS	It less system resources requires and can be calculated in real time.	This method works only for Windows system.
(Arshad et al., 2011)	2011	Cloud Computing	Signature based and anomaly detection	HIDS	It provides the fast method to have minimal time and human intervention.	There are not such experimental results evaluated.
(Jia and Wang, 2011)	2011	Cloud Computing	Anomaly prevention	HIPS	The intelligent IPS model with dynamic cloud firewall linkage can be used for real time interaction defense.	There are not experiments results are given.
(Tupakula et al., 2011)	2011	IaaS	Anomaly/signature based intrusion detection	VMM	Only Known attacks i.e. Zero Day Attack can be detected in this method.	It cannot detect unknown attacks.
(Vieira et al., 2010)	2010	Cloud and Grid computing	Signature and Anomaly detection	HIDS	The false rate for unknown attacks is lower.	However this method requires more training time and accuracy.
(Lo et al., 2010)	2010	Cloud Computing Networks	Signature based	Distributed	IDS launched in each cloud computing region and these IDS communicate with each other in order to protect from attacks such as DoS.	• It creates high computational overhead. • Unknown attacks cannot be detected.
(Bakshi and Yogesh, 2010)	2010	IaaS	Signature based	NIDS	The method secure VM from DoS attacks.	It Cannot detect unknown attacks.
(Mazzariello et al., 2010)	2010	IaaS	Signature based	NIDS	Distributed techniques can be used to detect and block attacks such as SIP flooding, or other malicious activities.	The unknown attacks cannot be detected.

Table 9 (*continued*)

References	Year	SPI Layer/ Platform	IDS Method	IDS Type	Pros	Cons
(Dastjerdi et al., 2009)	2009	IaaS	Anomaly detection	Distributed	Mobile agents' technology is used for cloud application for intrusion detection regardless of their locations.	Limited number of VMs visited in this approach.
(Roschke et al., 2009)	2009	Virtualization technology	Signature based detection	NIDS	Can meet the requirements of extensibility and secure VM based on user configuration	This approach only support minimum user mode Linux based features.
(Liu et al., 2009)	2009	Virtualization technology	Prevention	VMM	User configuration rules are used to prevent the attacks.	Unknown attacks cannot be prevented in this method.
(Guan and Bao, 2009)	2009	Cloud Computing	Anomaly detection		All types of attacks are detected.	The work not presents any experimental results.
(Oliveira et al., 2008)	2008	Virtualization technology	Signature based	VMM	Zero-day control-flow hijacking attacks and DDoS can be detected in this approach.	It cannot detect unknown attacks.
(Zhang et al., 2006)	2006	Virtualization technology	Storage-based IDS	VMM	File-aware block level storage method enables the virtual disk to detect the changes to file content online.	Works only for Windows system. This system based on hosted hypervisor therefore TCB becomes larger.
(Zhang et al., 2006)	2003	Virtualization technology	Anomaly detection	VMM	Adequate level of virtual machine monitor is provided to isolate the IDS from the monitored host to detect attacks on VMs.	It's a very complex method.

anything traveling between hypervisor and virtual machines, its acts like a central location for ID in IaaS environment.

- *Virtual Network*: in order to monitor the network traffic between VMs and host machine and between VMs itself.

5. Open research challenges and issues

This section highlights several open research challenges for different service models of CC. Each research challenge is described on the basis of key requirement parameters. Each of these requirements is important for the service models to deliver efficient services to the users. Table 10 presents to highlight different research challenges with respect to the significant security requirements of cloud service models.

5.1. Application security

Typically, cloud-based applications are delivered through internet to the users for fulfilling their requirements. Therefore, any vulnerability in traditional web application model is automatically inherited by the cloud applications. Cloud users can access their data through enterprise-distributed cloud applications.

The security and availability of these applications are highly depends on the behavior and quality of cloud services, therefore, this process should address the integrity and availability of data and software. One way is to encrypt the outsourced data confidentiality and security purposes. Moreover, the security of these applications also depends on APIs. These software interfaces or APIs provides security and availability of the cloud services. The existence of several virtualization technologies can also affect the security of these applications.

5.2. Data access security

Cloud vendors must always remain online because users can access the data at any time. In traditional enterprise applications, data owners and service providers are normally located at the same place; however, this scenario does not fit cloud computing. In cloud computing, customers and cloud-service providers may be located at two different locations. Moreover, cloud computing provides highly available services to different users on demand. During the processing, if one physical server fails, cloud servers migrate to another cloud server without experiencing an outage and affecting users work.

IaaS components mainly built on virtual platform environment enabling businesses to create their own virtual data centers. Surveys have shown that about 48% IT organizations report or doubting about unauthorized access of their data on virtual servers due to ignoring of data security (Modi et al., 2013). Cloud APIs play an integral role in cloud-based services through the provision of data storage (Stefanov and Shi, 2013), and database updates, among others. Service Level Agreement (SLA) documents can help customers assess their personal security needs. These assessment measures enable customers to monitor their set of standards regularly. Access control policies based on data attributes can also be combined with encryption. IaaS virtualization enables customers to access all resources to optimize confidentiality, integrity, and availability, among others. It is the hypervisor-based virtualization technology used to create virtual servers across the cluster of physical servers with resource sharing. The chances of mixing the data of several organizations over the cloud servers are very high. Data stored on a third-party server, including those belonging to a cloud service provider, can potentially be accessed without authorization by employees of the third-party organization. Additionally, customers need to know about what security measures

Table 10
Challenges in CC environment.

Challenges	Data integrity	Data Segregation	Availability	Confidentiality	API	Virtualization	SLA
Application-level Security	Δ, ¥	‡	Δ, ‡	Δ, ¥, ‡	¥	‡	Δ, ¥, ‡
Data Access Security	‡	Δ, ‡	Δ, ¥, ‡	Δ, ¥, ‡	¥	Δ, ‡	Δ, ¥, ‡
Data Center Security	‡	Δ, ¥, ‡	Δ, ‡	Δ, ‡	¥, ‡	‡	‡
Identity Management Control	Δ, ¥, ‡	Δ, ¥, ‡	¥	Δ	¥	Δ, ‡	Δ, ¥
Authentication	Δ, ¥	¥	Δ	Δ, ¥, ‡	Δ, ¥	Δ, ¥, ‡	Δ, ¥
Integration	Δ, ¥, ‡	Δ, ¥, ‡	Δ, ‡	Δ, ¥, ‡	Δ, ¥, ‡	Δ, ‡	Δ, ‡
Multi-tenancy	‡	Δ, ¥, ‡	‡			Δ, ‡	Δ
Development Life Cycle	¥	¥	Δ, ¥	Δ, ¥	¥	¥, ‡	Δ, ¥
Third-Party Services	Δ, ¥, ‡	Δ, ¥, ‡	‡	Δ, ¥, ‡	Δ, ¥, ‡	¥, ‡	Δ, ¥
Vendor Lock-in	Δ, ¥, ‡	Δ, ¥, ‡	Δ, ‡	Δ, ¥, ‡	Δ, ¥,	‡	¥, ‡
Encryption and Key management	Δ, ‡	‡	Δ, ‡	Δ, ¥, ‡	Δ, ¥,	‡	Δ, ¥, ‡
Access control	Δ, ‡	¥, ‡	Δ	¥, ‡	Δ, ¥, ‡	Δ, ¥, ‡	Δ, ¥, ‡

IaaS=‡, PaaS=¥, SaaS=Δ

are in place and how to protect against threats such as DDoS attacks that can prevent access to the cloud data and other cloud services. Potential problems with data related security issues are data backup, data access, data locality, data availability IDM & authentication etc.

5.3. Data center security

Cloud applications are generally located at the data center of the provider; therefore, maintaining and upgrading software is almost impossible for cloud users. Cloud users can only access software through an IaaS API. The cloud utilizes the IaaS layer via API to secure and to manage the infrastructure necessary for running the Cloud-based software and storing data. In the network management environment, however, storage virtualization enhances functionality, data protection, server configuration management, and space utilization. Data encryption can be applied before sending the data onto the cloud.

As network components in cloud computing are shared among several tenants resulting attacks on network layer. Some famous attacks on network layer are DNS attacks, Sniffer attacks, issues of reuse IP address, Network Sniffing VoIP free calls etc. In cloud data center, network security measures the control access to the operating system and other network systems. Consequently, many known vulnerabilities in traditional network environment also exists in cloud virtual network. Moreover, the cloud model is still having potential threats due to shared virtual resource infrastructures. The main threats come from hosted virtual machines. As there are number of hosted machines over single physical machine; host to host and host to guest machines attacks are famous threats.

Integrity can be broadly categorized into data integrity and computation integrity. The former implies that data should be stored on cloud servers, and any violations such as unauthorized access, loss or breaches, be detected and reported. The encryption, authentication, and backup are the most common way to secure data in virtualize data center. Virtualization technologies are becoming popular in cloud data centers (Qi et al., 2014). With virtualization, a single physical machine can be divided into several virtual machines over a dedicated network. In this way, it provides the better data segregation and safety against different attacks such as DoS. Physical security in cloud-based application is just as important. Physical security is outsourced to third part data center which restricts the physical access to the data center. These third party data center are mature enough to secure data into their side by that requires mandatory visitor registration, employee badge access, and biometric scanner for employee authentication.

5.4. Identity management control

IDM component provides identity services for users and organizations. A core component protects security and privacy to alleviate problems associated with cloud computing.

SLA documents provides helpful guidelines that can be established for security web services; these guidelines should define the standards on securing communication between applications by addressing integrity and confidentiality, as well as by improving authentications. Isolation over running services and APIs is also very important. SLA documents help define the rules regarding pieces of information that need to be migrated across different cloud platforms. Customers may lose confidence in the cloud service, due to non-availability of a particular service or the quality of service does not meet the SLA requirements.

5.5. Authentication

Authentication services are used to identify an individual; typically by entering an ID and a password. In a SaaS cloud, a web-based user should be authenticated without compromising usability and ubiquity. Multifactor authentication is increasingly popular in shared cloud environments because this process depends on multiple implementations of two or more classes of human authentication.

In reality, VM have same security and compliance concerns that physical machines have. Several types of security components and traffic encryption techniques can help to reduce the malicious threats over cloud network infrastructure. As these type of threats can bypass the integrity protection that base on code measurement which directly affect the virtualization layer. Implementing the key management for both clients and the cloud service providers is one of the ways to access monitoring to it. Moreover, there is the need to apply strong control to enforce policies over data segregation. The customer's responsibility includes checking the cloud vendor's architecture to ensure data segregation policies are in place. Consequently, confidentiality and integrity is an important aspect in cloud environment; which means that only authorize users can make authorize changes to the system. Moreover, DoS attacks can effects the network resources of cloud layer. The attacks on protocol are applied to web services using XML signature for authentication and integrity protection which also affects the performance of cloud services. The attackers on cloud virtualization layer first hold the operations of hosted virtual machines and then open the possibility to attack on other compromised hosted virtual machines or to attack hypervisor itself.

5.6. Integration

The integration of cloud-based services on heterogeneous multi-providers remains a challenging task for cloud providers. Developers who utilize PaaS can develop their own applications on local machines and deploy these applications on a cloud platform without possessing any specific system administrative skills. PaaS integration not only affects its business customers but also affects SaaS services. Hypervisor integration services must be enabled and installed properly.

Cloud providers must determine how to monitor a network and to maintain the integrity of the system. Well-defined APIs simplify data integration across multiple cloud platforms. Virtualization offers scalability, facilitates performance, improves resource management, and stores data efficiently.

The integration in cloud-based systems is easy if the applications run on the same cloud platform. However if these application runs on different cloud platforms, it would be more difficult to customize with different cloud platforms and their architecture. Likewise, the cloud systems may share with multiple users in different security domain, making it more vulnerable to security threats. Additionally, data integration is still an issue and is often ignored in cloud framework; need to be addressed thoroughly by cloud providers. Yu and Wen (2010) gives the solution of data security and argues that data security should be considered at data life cycle.

5.7. Multi-tenancy

Services and resources are shared among different users in multi-tenant cloud architecture. The data is shared between multiple customers and organizations. These results to imply that cloud providers must ensure the privacy, integrity, and consistency of data. Data should be isolated in the multi-tenant environment of cloud computing. Moreover, isolation should be considered over running services and APIs. Resources (such as tenants) should be segmented into isolated entities. Virtualization is a part of all private cloud strategies, and any attack on a VM should not affect any other VM on the server or host OS. The virtualization layer is used for good resource distribution and utilization because of the multitenant behavior of SaaS. In this mode, VLANs is designed to offers isolated segments in order to protect from external VMs threats (such as sniffing, spoofing etc.) by monitoring the internal traffic.

In addition, to separate the data of one customer to the data of another customer is called data segregation. As the resources are shared by multiple customers in cloud environment, this means the data for multiple customers may be stored or processed on the same physical machines. Furthermore, the service providers and other third party services may steal and view customer's important data. One of the key questions of this multi-tenant environment is how data is segregated from other shared environments? One way to handle this issue is to place individual customer's data in a segregated database which is completely tied to one customer. The vulnerabilities exists in the virtualize technology are the potential threats to multi-tenant cloud architecture. Vulnerabilities appeared in VMware, Xen, and Microsoft's Virtual PC and Virtual Server are big question marks to famous cloud providers companies.

5.8. Development life cycle

Main PaaS offering is System Development Life Cycle (SDLC), which is a framework that defines the tasks to be completed at each step of a software development process. Application developers need an accelerated development process. In addition, they face the complexities of building secure applications. Virtual network providers must follow the security requirements provided by SLA. Therefore, cloud SDLC should be adequately customized to address project requirements and integration of services. The PaaS model must also be incorporated into a novel SDLC that covers a cloud virtualized heterogeneous environment. SDLC directly impact on reliability, availability and serviceability requirements in cloud development framework. Cloud development model requires a quiet unique approach as compared with traditional software development lifecycle due to the complexity and management of cloud-based applications.

5.9. Third-party services

The cost, services, and framework of each cloud layer varies depending on the interface method applied. Currently, available PaaS platforms are relatively immature, and the infancy of the market enhances at the risk. In addition, the number and types of PaaS platforms and PaaS-resident applications available in the cloud environment are ambiguous.

However, major security issues are inevitably inherited when network, data, and integrity are used as third-party components. As in a third-party cloud environment, customers have no control over cloud infrastructure and the lack of transparency. Thus, PaaS users may experience security concerns with respect to both web-hosted development tools and third-party services. Security risks can be reduced by identifying and proactively addressing these third-party issues. Third-party add-ons such as code repository integration, caching services, logging services, and payment services are also offered by many PaaS service providers. Third-party service providers also do not recommend the use of their solutions with untrusted hosts. Thus, clients are increasingly concerned with data confidentiality. Moreover, API keys are used by cloud services to identify third-party applications. Several schemes have been established (i.e., SLA) to develop trust and privacy policies for cloud vendors and consumers.

5.10. Vendor lock-in

A lock-in issue has developed in PaaS due to the absence of SLA standards and formats. Thus, cloud consumers cannot migrate their enterprise applications to other cloud platforms. In some cases, the programming languages that are used to develop enterprise applications differ based on the application being migrated. This difference is caused by the variation in API providers. These firms face service lock-in problems in deploying/migrating their applications to different PaaS providers because the APIs used by each provider differ.

5.11. Encryption and key management

In cloud computing environment, the data locate outside the boundary of corporate firewalls raising security concerns. Most common way to secure data at cloud is to encrypt it. The strong encryption and key management techniques are used to minimize the risk of data loess. On the other hand, digital signature can also be used to secure client's data; it is a certain type of encryption mechanism to ensure authentication. Encryption, strong user authentication and backup are the most common way to secure data in virtualize data center. To encrypt all the data whether it is in transit or at rest and makes sure the strong encryption standards used to encrypt data. National Institute of Standards and Technology (NIST) introduces 256-bit Advance Encryption Standards (AES) SSL encryption technique for data in transit and 256 bit for data at rest. Moreover, cloud vendors must implement strong encryption techniques to optimize security solution. One way is to

use homomorphic token to provide holistic security solutions in data storage. This approach protects data modification as well as defends from byzantine cryptosystems.

5.12. Access control

Cloud data security means to protect data against scam and unauthorized access. The main focus behind data security is to protect personnel and enterprise data in Cloud model. The risk of loss of personnel, physical, and logical data is high as compare to traditional on premise applications. The reason is that, the data has located outside the boundary of enterprise organizations. In this way it increases the responsibility on Cloud vendors to secure data. As discussed above, Cloud computing provides multi-tenant architecture. Thus, data of various users in cloud is placed together at the same location, increasing the risks of unauthorized access of data. Furthermore, the service providers and other third party services may steal and view customer's important data. One of the key questions of this multi-tenant environment is how data is segregated from other shared environments? One way to handle this issue is to place individual customer's data in a segregated database which is completely tied to one customer.

6. Conclusion

Cloud computing (CC) is a trend that is unlikely to fade anytime soon, and considering the increasingly trend of storing data in one or more clouds (e.g. see cloud federation and fog computing (Bakshi and Yogesh, 2010; Nepal et al., 2015)), it is important to ensure the security and privacy of data outsourced to the cloud as well as the security of cloud services and cloud infrastructures. For SaaS, for example, the notion of security refers to data security on multi-tenant environments. PaaS is the abstraction layer below SaaS and above IaaS. PaaS cloud providers offers the intuitive programming environment to their customers. Correspondingly, IaaS cloud layer provides physical infrastructure (storage, network, and servers), virtualization infrastructure (hypervisors) and virtualized resource layers (e.g. VMs, virtual servers). However, all these layers resides on shared virtual machines, as a result malicious attacks can be injected on virtual machine software through other virtual machines. In this paper, we analyzed the wide range of potential attacks on CC based on the cloud service delivery models, and examined the potential of intrusion detection and prevention systems as a possible solution.

Very little effort has been made to explore security paradigms at service delivery levels of CC. We believe that each cloud layer has its own potential risks. We have also covered major attacks that pose a serious risk to cloud systems. Indeed, several of these attacks belong to web services. However, as these web services' technologies are also used in CC, these attacks also affect the CC services' security. One of the biggest challenges is to identify the attacks from normal VM operations in cloud virtual environment. Typical approaches to protect user's data are to adopt end-point encryption, firewalls and antivirus solutions. However, with the advent of new technologies from traditional to cloud technologies, the targets of attackers have shifted from the network layer to the application layer. Therefore, the paper also presents the alternative options to incorporate intrusion detection techniques into the cloud computing model. We have also explored the locations in cloud service delivery models where these IDS can be deployed for efficient detection and prevention. In the future work, we will develop an in-depth, advanced protection system to monitor the activities of different layers of cloud computing, to ensure integrity and confidentiality, and to offer end-to-end IDS support for cloud services.

Acknowledgment

This work is funded by Science Fund Research Project 01-01-03-SF0786 MOSTI, Malaysia. The work is also funded by the Deanship of Scientific Research at King Saud University Research Group (PRG-1436-16).

References

Ab Rahman, N.H., Choo, K.-K.R., 2015. A survey of information security incident handling in the cloud. Comput. Secur. 49, 45–69.
Alizadeh, M., et al., 2015. Authentication in mobile cloud computing: a survey. J. Netw. Comput. Appl.
Almomani, A., et al., 2013. A survey of phishing email filtering techniques. Commun. Surv. Tutor. IEEE 15 (4), 2070–2090.
Alqahtani, S.M., Balushi, M.A. and John, R., 2014. An intelligent intrusion detection system for cloud computing (SIDSCC). In: Proceedings of the 2014 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE.
Alqahtani, S.M., Balushi, M.A. John, R., 2014. An intelligent intrusion prevention system for cloud computing (SIPSCC). In: Proceedings of the 2014 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE.
AlZain, M.A., Soh, B., Pardede, E., 2011. MCDB: Using Multi-clouds to Ensure Security in Cloud Computing. In: Proceedings of the 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), IEEE.
Anitha, E., Malliga, S., 2013. A packet marking approach to protect cloud environment against DDoS attacks. In: Proceedings of the 2013 International Conference on Information Communication and Embedded Systems (ICICES), IEEE.
Araújo, J.D., Abdelouahab, Z., 2012. Virtualization in intrusion detection systems: a study on different approaches for cloud computing environments. IJCSNS 12 (11), 10.
Armbrust, M., et al., 2010. A view of cloud computing. Commun. ACM 53 (4), 50–58.
Arshad, J., Townend, P., Xu, J., 2011. An abstract model for integrated intrusion detection and severity analysis for clouds. Int. J. Cloud Appl. Comput. (IJCAC) 1 (1), 1–16.
Ayodele, T. and Adeegbe, D., 2013. Cloud based emails boundaries and vulnerabilities. In: Proceedings of the Science and Information Conference (SAI), 2013. IEEE.
Azeez, A., et al., 2010 Multi-tenant SOA middleware for cloud computing. In: Proceedings of the Cloud Computing (Cloud), 2010 IEEE 3rd International Conference on, 2010. IEEE.
Bakshi, A., Yogesh, B., 2010. Securing cloud from ddos attacks using intrusion detection system in virtual machine. In: Proceedings of the Communication Software and Networks, 2010. ICCSN'10. Second International Conference on, 2010. IEEE.
Barron, C., H., Yu, Zhan, J., 2012. Cloud computing security case studies and research. In: Proceedings of the World Congress on Engineering. 2013.
Bhadauria, R., et al., 2011. A survey on security issues in cloud computing. arXiv preprint arXiv:1109.5388, 2011.
Bhadauria, R., Sanyal, S., 2012. Survey on security issues in cloud computing and associated mitigation techniques. arXiv preprint arXiv:1204.0764, 2012.
Bharadwaja, S., et al., 2011. Collabra: a xen hypervisor based collaborative intrusion detection system. In: Proceedings of the Information Technology: New Generations (ITNG), 2011 Eighth International Conference on, 2011. IEEE.
Bouayad, A., et al., 2012. Cloud computing: security challenges. In: Proceedings of the Information Science and Technology (CIST), 2012 Colloquium in. 2012. IEEE.
Bradai, A., Afifi, H., Enforcing trust-based intrusion detection in cloud computing using algebraic methods. In: Proceedings of the Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference on. 2012. IEEE.
Brunette, G., Mogull, R., 2009. Security guidance for critical areas of focus in cloud computing v2.1. Cloud Secur. Alliance, 1–76.
Bryan Williams, T.C., 2010. Virtualization System Security. IBM.
Chen, Z., et al., 2013. Cloud computing-based forensic analysis for collaborative network security management system. Tsinghua Sci. Technol. 18 (1), 40–50.
Chen, Q., et al., 2011. CBF: A packet filtering method for DDoS attack defense in cloud environment. In: Proceedings of the Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on, 2011. IEEE.
Chonka, A., Abawajy, J., 2012. Detecting and mitigating HX-DoS attacks against cloud web services. In: Proceedings of the Network-Based Information Systems (NBiS), 2012 15th International Conference on, 2012. IEEE.
Chung, C.-J., et al., 2013. NICE: Network intrusion detection and countermeasure selection in virtual network systems. IEEE Trans. Dependable Secur. Comput., 1.
Corporation, P.S., 2008. SaaS Security and privacy.
Council, S.-a.-a.-S.E., 2006. Software-as-a-Service; A Comprehensive Look at the Total Cost of Ownership of Software Applications.
Dastjerdi, A.V., Bakar, K.A., Tabatabaei, S.G.H., 2009. Distributed intrusion detection in clouds using mobile agents. In: Proceedings of the Advanced Engineering Computing and Applications in Sciences, 2009. ADVCOMP'09. Third International Conference on, 2009. IEEE.

Dawoud, W., TakounaI., I., Meinel, C., 2010. Infrastructure as a service security: Challenges and, solutions. In: Proceedings of the Informatics and Systems (INFOS), 2010 The 7th International Conference on. 2010. IEEE.
Dinesha, H., Agrawal, V., 2012. Multi-level authentication technique for accessing cloud services. In: Proceedings of the Computing, Communication and Applications (ICCCA), 2012 International Conference on, 2012. IEEE.
Ding, B., et al., 2012. Return-oriented programming attack on the Xen hypervisor. In: Proceedings of the Availability, Reliability and Security (ARES), 2012 Seventh International Conference on, 2012. IEEE.
Duncan, A., et al., 2013. Cloud Computing: Insider Attacks on Virtual Machines during Migration. In: Proceedings of the Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, 2013. IEEE.
Duncan, A.J., Creese, S., Goldsmith, M., 2012. Insider attacks in cloud computing. In: Proceedings of the Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. 2012. IEEE.
Ferguson, E., Weber, J., Hasan, R., 2012. Cloud based content fetching: Using cloud infrastructure to obfuscate phishing scam analysis. In: Proceedings of the Services (SERVICES), 2012 IEEE Eighth World Congress on. 2012. IEEE.
FireHost, 2012. Cross-Site Scripting Attacks Up 160% in Final Quarter of 2012; Available from: ⟨http://www.firehost.com/company/newsroom/web-application-attack-report-fourth-quarter-2012⟩.
Gani, A., et al., 2014. A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing. J. Netw. Comput. Appl. 43, 84–102.
Garfinkel, T., et al., 2003. Terra: A Virtual Machine-based Platform For Trusted Computing, ACM SIGOPS Operating Systems Review. ACM,.
Garg, S., Saran, H., 2008. Anti-DDoS Virtualized Operating System. In: Proceedings of the Availability, Reliability and Security, 2008. ARES 08. Third International Conference on, 2008. IEEE.
Godfrey, M. and Zulkernine, M., 2013. A Server-Side Solution to Cache-Based Side-Channel Attacks in the Cloud. In: Proceedings of the Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on, 2013. IEEE.
Grispos, G., Glisson, W.B., Storer T., 2013. Cloud security challenges: Investigating policies, standards, and guidelines in a fortune 500 organization. arXiv preprint arXiv:1306.2477, 2013.
Guan, Y. and Bao, J., 2009. A CP intrusion detection strategy on cloud computing. In: Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09). 2009.
Gupta, S., et al., 2012. A fingerprinting system calls approach for intrusion detection in a cloud environment. In: CASoN.
Hamad, H., Al-Hoby, M., 2012. Managing intrusion detection as a service in cloud networks. Int. J. Comput. Appl. 41 (1), 35–40.
Hamdi, M., 2012. Security of cloud computing, storage, and networking. In: Proceedings of the Collaboration Technologies and Systems (CTS), 2012 International Conference on, 2012. IEEE.
Harnik, D., Pinkas, B., Shulman-Peleg, A., 2010. Side channels in cloud services: deduplication in cloud storage. Secur. Priv. IEEE 8 (6), 40–47.
Houmansadr, A., Zonouz, S.A., Berthier, R., 2011. A cloud-based intrusion detection and response system for mobile phones. In: Proceedings of the Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on, 2011. IEEE.
Ibrahim, A.S., et al., 2011. Cloudsec: a security monitoring appliance for virtual machines in the iaas cloud model. In: Proceedings of the Network and System Security (NSS), 2011 5th International Conference on. 2011. IEEE.
Jensen, M., et al., 2009. On technical security issues in cloud computing. In: Proceedings of the Cloud Computing, 2009. CLOUD'09. IEEE International Conference on, 2009. IEEE.
Jia, T., Wang, X., 2011. The research and design of intelligent IPS model based on dynamic cloud firewall linkage. Int. J. Digit. Content Technol. Appl. 5 (3), 304–309.
Juliadotter, N.V., Choo, K.-K.R., Chapter 3 - CATRA: Conceptual cloud attack taxonomy and risk assessment framework, in The Cloud Security Ecosystem. 2015, Syngress: Boston. pp. 37–81.
Kang, L., Zhang, X., 2010. Identity-based authentication in cloud storage sharing. In: Proceedings of the Multimedia Information Networking and Security (MINES), 2010 International Conference on, 2010. IEEE.
Karnwal, T., Thandapanii, S., Gnanasekaran, A., 2013. A Filter tree approach to protect cloud computing against XML DDoS and HTTP DDoS attack, Intelligent Informatics. Springer,, pp. 459–469.
Katkamwar, N.S., Puranik, A.G., Deshpande, P., 2012. Securing cloud servers against flooding based DDoS attacks. Int. J. Appl. Innov. Eng. Manag. (IJAIEM) 1 (3), 50–55.
Khan, S., et al., 2014. A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing. Sci. World J., 2014
Khan, S., et al., 2016. Network forensics: review, taxonomy, and open challenges. J. Netw. Comput. Appl. 66, 214–235.
Khan, S., et al., 2016. Cloud log forensics: foundations, state of the art, and future directions. ACM Comput. Surv. (CSUR) 49 (1), 7.
Khan, S., et al. Forensic challenges in mobile cloud computing. In: Proceedings of the Computer, Communications, and Control Technology (I4CT), 2014 International Conference on. 2014. IEEE.
Khan, S., et al., 2015. SIDNFF: Source identification network forensics framework for cloud computing. In: Proceedings of the Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE International Conference on, 2015. IEEE.
Khonji, M., Iraqi, Y., Jones, A., 2013. Phishing detection: a literature survey. Commun. Surv. Tutor. IEEE 15 (4), 2091–2121.
Khorshed, M.T., Ali, A.S. Wasimi, S.A., 2011. Monitoring insiders activities in cloud computing using rule based learning. In: Proceedings of the Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on. 2011. IEEE.
Khune, R., Thangakumar, J., 2012. A cloud-based intrusion detection system for Android smartphones. In: Proceedings of the International conference on radar, communication and computing, India. 2012.
Kourai, K., Azumi, T., Chiba, S., 2012. A self-protection mechanism against stepping-stone attacks, for IaaS clouds. In: Proceedings of the Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on. 2012. IEEE.
Kwon, H., et al., 2011. Self-similarity based lightweight intrusion detection method for cloud computing, Intelligent Information and Database Systems. Springer,, pp. 353–362.
Lee, J.-H., et al., 2011. Multi-level intrusion detection system and log management in cloud computing. In: Proceedings of the Advanced Communication Technology (ICACT), 2011 13th International Conference on, 2011. IEEE.
Li, T., et al., 2011. LARX: Large-scale anti-phishing by retrospective data-exploring based on a cloud computing platform. In: Proceedings of the Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on, 2011. IEEE.
Lin, C.-H., et al., 2010. A detection scheme for flooding attack on application layer based on semantic concept. In: Proceedings of the Computer Symposium (ICS), 2010 International. 2010. IEEE.
Lin, W. and Lee, D., 2012. Traceback Attacks in Cloud–Pebbletrace Botnet. In: Proceedings of the Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on. 2012. IEEE.
Liu, J., et al., 2015. Application partitioning algorithms in mobile cloud computing: taxonomy, review and future directions. J. Netw. Comput. Appl. 48, 99–117.
Liu, F., et al., 2009. The design and application of Xen-based host system firewall and its extension. In: Proceedings of the Electronic Computer Technology, 2009 International Conference on. 2009. IEEE.
Lo, C.-C., Huang, C.-C., Ku., J. A cooperative intrusion detection system framework for cloud computing networks. In: Proceedings of the Parallel Processing Workshops (ICPPW), 2010 39th International Conference on. 2010. IEEE.
Lomotey, R.K., Deters, R., 2013. SaaS Authentication Middleware for Mobile Consumers of IaaS Cloud. in Services (SERVICES), 203 IEEE Ninth World Congress on, 2013. IEEE.
Manvi, S.S., Shyam, G.K., 2014. Resource management for Infrastructure as a Service (IaaS) in cloud computing: a survey. J. Netw. Comput. Appl. 41, 424–440.
Mazzariello, C., Bifulco, R., Canonico, R., 2010. Integrating a network ids into an open source cloud computing environment. In: Proceedings of the Information Assurance and Security (IAS), 2010 Sixth International Conference on. 2010. IEEE.
Meng, Y., Li, W., Kwok, L.-F., 2013. Design of cloud-based parallel exclusive signature matching model in intrusion detection. In: Proceedings of the High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on. 2013. IEEE.
Modi, C., et al., 2013. A survey on security issues and solutions at different layers of cloud computing. J. Supercomput. 63 (2), 561–592.
Mohamed, H., et al., 2013. A collaborative intrusion detection and prevention system in cloud computing. In: Proceedings of the AFRICON, 2013. 2013. IEEE.
Mundada, Y., Ramachandran, A., Feamster, N., 2011. Silverline: data and network isolation for cloud services. Proc HotCloud.
Nasridinov, A., Byun, J.-Y., Park, Y.-H., 2012. UNWRAP: An approach on wrapping-attack tolerant SOAP messages. In: Proceedings of the Cloud and Green Computing (CGC), 2012 Second International Conference on. 2012. IEEE.
Nepal, S., Ranjan, R., Choo, K.-K.R., 2015. Trustworthy processing of healthcare big data in hybrid clouds. Cloud Comput. IEEE 2 (2), 78–84.
Nikolai, J., Wang, Y., 2014. Hypervisor-based cloud intrusion detection system. In: Proceedings of the Computing, Networking and Communications (ICNC), 2014 International Conference on. 2014. IEEE.
Nkosi, L., Tarwireyi, P., Adigun, M.O., 2013. Detecting a malicious insider in the cloud environment using sequential rule mining. In: Proceedings of the Adaptive Science and Technology (ICAST), 2013 International Conference on. 2013. IEEE.
Nkosi, L., Tarwireyi, P., Adigun, M.O., 2013. Insider threat detection model for the cloud. In: Proceedings of the Information Security for South Africa, 2013. IEEE.
Oktay, U., Aydin, M.A., Sahingoz, O.K., 2013. A circular chain intrusion detection for cloud computing based on improved AdjointVM approach. In: Proceedings of the Computational Intelligence and Informatics (CINTI), 2013 IEEE 14th International Symposium on. 2013. IEEE.
Oktay, U., Sahingoz, O., 2013. Proxy Network Intrusion Detection System for cloud computing. In: Proceedings of the Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013 International Conference on. 2013. IEEE.
Oliveira, D., et al., 2008. Bezoar: Automated virtual machine-based full-system recovery from control-flow hijacking attacks. In: Proceedings of the Network Operations and Management Symposium, 2008. NOMS 2008. IEEE. 2008. IEEE.
Osanaiye, O., Choo, K.-K.R., Dlodlo, M., 2016. Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud ddos mitigation framework. J. Netw. Comput. Appl.
Oyama, Y., Hoshi, Y., 2011. A hypervisor for injecting scenario-based attack effects. In: Proceedings of the Computer Software and Applications Conference

(COMPSAC), 2011 IEEE 35th Annual. 2011. IEEE.
Patel, A., et al., 2013. An intrusion detection and prevention system in cloud computing: a systematic review. J. Netw. Comput. Appl. 36 (1), 25–41.
Potlapally, N.R., et al., 2007. Aiding side-channel attacks on cryptographic software with satisfiability-based analysis. Very Large Scale Integr (VLSI) Syst, IEEE Transactions on 15, 4, pp. 465–470.
Prokhorenko, V., Choo, K.-K.R., Ashman, H., 2016. Web application protection techniques: a taxonomy. J. Netw. Comput. Appl. 60, 95–112.
Qaisar, S., Khawaja, K.F., 2012. Cloud computing: network/security threats and countermeasures. Interdiscip. J. Contemp. Res. Bus. 3 (9), 1323–1329.
Qi, H., et al., 2014. Sierpinski triangle based data center architecture in cloud computing. J. Supercomput. 69 (2), 887–907.
Reuben, J.S., 2007. A Survey on Virtual Machine Security. Helsinki University of Technology,.
Revar, A.G., Bhavsar, M.D., 2011. Securing user authentication using single sign-on in Cloud Computing. In: Proceedings of the Engineering (NUiCONE), 2011 Nirma University International Conference on. 2011. IEEE.
Ristenpart, T., et al., 2009. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the Proceedings of the 16th ACM conference on Computer and communications security. 2009. ACM.
Rocha, F., Gross, T., van Moorsel, A., 2013. Defense-in-depth against malicious insiders in the cloud. In: Proceedings of the Cloud Engineering (IC2E), 2013 IEEE International Conference on. 2013. IEEE.
Rodero-Merino, L., et al., 2012. Building safe PaaS clouds: a survey on security in multitenant software platforms. Comput. Secur. 31 (1), 96–108.
Roschke, S., Cheng, F., Meinel, C., 2009. An extensible and virtualization-compatible IDS management architecture. In: Proceedings of the Information Assurance and Security, 2009. IAS'09. Fifth International Conference on. 2009. IEEE.
S., Fiebig, et al., 2013. Detecting VM Live Migration using a Hybrid External Approach. In: CLOSER. 2013.
Sabahi, F., 2011. Virtualization-level security in cloud computing. In: Proceedings of the Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. 2011. IEEE.
Sawesi, K.G.A., Saudi, M.M., Jali, M.Z., 2013. Designing a new E-Commerce authentication framework for a cloud-based environment. In: Proceedings of the Control and System Graduate Research Colloquium (ICSGRC), 2013 IEEE 4th. IEEE.
Saxena, A., et al., 2013. Detecting SOQL-injection vulnerabilities in sales force applications. In: Proceedings of the Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on. 2013. IEEE.
Scarfone, K., 2011. Guide to Security For Full Virtualization Technologies. DIANE Publishing.
Shaikh, R., Sasikumar, M., 2015. Trust model for measuring security strength of cloud computing service. Procedia Comput. Sci. 45, 380–389.
Shameli-Sendi, A., et al., 2015. Taxonomy of distributed denial of service mitigation approaches for cloud computing. J. Netw. Comput. Appl. 58, 165–179.
Shea, R., Liu, J., 2012. Understanding the impact of denial of service attacks on virtual machines. In: Proceedings of the 2012 IEEE 20th International Workshop on Quality of Service 2012 IEEE Press.
Shi, J., et al., 2011. Limiting cache-based side-channel in multi-tenant cloud using dynamic page coloring. In: Proceedings of the Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on. 2011. IEEE.
Shiraz, M., et al., 2015. A study on the critical analysis of computational offloading frameworks for mobile cloud computing. J. Netw. Comput. Appl. 47, 47–60.
Simou, S., et al., 2014. Cloud forensics: identifying the major issues and challenges, Advanced Information Systems Engineering. Springer.
Stefanov, E., Shi, E., 2013. Oblivistore: high performance oblivious cloud storage. In: Proceedings of the Security and Privacy (SP), 2013 IEEE Symposium on. 2013. IEEE.
Subashini, S., Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. 34 (1), 1–11.
Sun, D., et al., 2011. Surveying and analyzing security, privacy and trust issues in cloud computing environments. Procedia Eng. 15, 2852–2856.
Sun, Y., He., D., 2012. Model checking for the defense against cross-site scripting attacks. In: Proceedings of the Computer Science & Service System (CSSS), 2012 International Conference on. 2012. IEEE.
Suzaki, K., 2012. Security on cloud storage and IaaS, in Taiwan-Japan Workshop 2012/Nov/272012.
Szefer, J., et al. Eliminating the hypervisor attack surface for a more secure cloud. In: Proceedings of the Proceedings of the 18th ACM conference on Computer and communications security. 2011. ACM.
Takabi, H., Joshi, J.B., Ahn, G.-J., 2010. Security and privacy challenges in cloud computing environments. IEEE Secur. Priv. 6, 24–31.
Telegraph, T., 2009. Facebook users targeted by hackers in successful phishing attack, Available from: ⟨http://www.telegraph.co.uk/technology/facebook/5326971/Facebook-users-targeted-by-hackers-in-successful-phishing-attack.html⟩.
Toosi, A.N., Calheiros, R.N., Buyya, R., 2014. Interconnected cloud computing environments: Challenges, taxonomy, and survey. ACM Comput. Surv. (CSUR) 47 (1), 7.
Tupakula, U., Varadharajan, V., AkkuN., 2011. Intrusion detection techniques for infrastructure as a service cloud. In: Proceedings of the Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on. 2011. IEEE.
Turnbull, L., Shropshire, J., 2013. Breakpoints: an analysis of potential hypervisor attack vectors. In: Proceedings of the Southeastcon, IEEE. 2013. IEEE.
Vieira, K., et al., 2010. Intrusion detection for grid and cloud computing. IT Prof. 12 (4), 38–43.
VivinSandar, S., Shenai, S., 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, A., Kokhanevych, I., Ivanov, D., 2012. Secure virtualization in cloud computing.
Wang, Z., Jiang, X., 2010. Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity. In: Proceedings of the Security and Privacy (SP), 2010 IEEE Symposium on. 2010. IEEE.
Whaiduzzaman, M., et al., 2014. A survey on vehicular cloud computing. J. Netw. Comput. Appl. 40, 325–344.
Xia, Y., et al., 2012. Defending against VM rollback attack. In: Proceedings of the Dependable Systems and Networks Workshops (DSN-W), 2012 IEEE/IFIP 42nd International Conference on. 2012. IEEE.
Xiao, Z., Xiao, Y., 2013. Security and privacy in cloud computing. Commun. Surv. Tutor. IEEE 15 (2), 843–859.
Xie, W., et al., 2013. Cloud-based RFID authentication. In: Proceedings of the RFID (RFID), 2013 IEEE International Conference on. 2013. IEEE.
Y., Gilad, et al., CDN-on-Demand: An Affordable DDoS Defense via Untrusted Clouds.
Yang, L., et al., 2012. Defense of DDoS attack for cloud computing. In: Proceedings of the Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on. 2012. IEEE.
Yaseen, Q., Panda, B., 2010. Malicious modification attacks by insiders in relational databases: prediction and prevention. In: Proceedings of the Social Computing (SocialCom), 2010 IEEE Second International Conference on. 2010. IEEE.
Yassin, A.A., et al., 2012. Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing. In: Proceedings of the Cloud and Green Computing (CGC), 2012 s International Conference on. 2012. IEEE.
Yassin, W., et al., 2012. A cloud-based intrusion detection service framework. In: Proceedings of the Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on. 2012. IEEE.
You, P., et al., 2012. Security issues and solutions in cloud computing. In: Proceedings of the Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on. 2012. IEEE.
Yu, S., Gui, X., Lin, J., 2013. An approach with two-stage mode to detect cache-based side channel attacks. In: Proceedings of the Information Networking (ICOIN), 2013 International Conference on. 2013. IEEE.
Yu, X., Wen, Q., 2010. A view about cloud data security from data life cycle. In: Proceedings of the Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on. 2010. IEEE.
Zhang, F., et al., 2008. PALM: security preserving VM live migration for systems with VMM-enforced protection. In: Proceedings of the Trusted Infrastructure Technologies Conference, 2008. APTC'08. Third Asia-Pacific. 2008. IEEE.
Zhang, Y., et al., 2006. Virtual-machine-based intrusion detection on file-aware block level storage. In: Proceedings of the Computer Architecture and High Performance Computing, 2006. SBAC-PAD'06. 18th International Symposium on. 2006. IEEE.
Zhang, Y., et al., 2011. Homealone: Co-residency detection in the cloud via side-channel analysis. In: Proceedings of the security and Privacy (SP), 2011 IEEE Symposium on. 2011. IEEE.
Zhang, Y., et al., 2012. Cross-VM side channels and their use to extract private keys. In: Proceedings of the 2012 ACM conference on Computer and communications security. 2012. ACM.
Zissis, D., Lekkas, D., 2012. Addressing cloud computing security issues. Futur. Gener. Comput. Syst. 28 (3), 583–592.

Salman Iqbal received the BSCS From Islamia University of Bahawalpur and M.S(CS) degrees from the COMSATS Institute of Information Technology, Lahore in 2007 and 2009 respectively. Currently, he is pursuing his pH.D from the University of Malaya, Malaysia. His research interests are in various aspects of network security and distributed computing.

PROF. DR. Miss Laiha Binti Mat Kiah Department of Computer System & Technology, Faculty of Computer Science & Information Technology. B.Sc. Comp. Sc. (Hons) (Malaya), M.Sc. (London) pH. D. (London), joined the Faculty of Computer Science & Information Technology, University of Malaya, Malaysia as a tutor in 1997. She was appointed as a lecturer in 2001. She received her B.Sc. (Hons) in Computer Science from the University of Malaya in 1997, a M.Sc. from Royal Holloway, University of London UK in 1998 and a pH. D. also from Royal Holloway, University of London in 2007. Between 1999 and 2003 before pursuing her study, she was primarily involved in academic teaching and

research in University of Malaya. She was appointed as a senior lecturer in 2008 and currently she is a full professor of Computer Systems and Technology Department. Her current research interests include key management, secure group communication and wireless mobile security. She is also interested in routing protocols and ad-hoc networks.

Babak Daghighi received his B.Sc. in Computer Science from Azad University (Tehran branch), Iran, and M.Sc. from University of Malaya (UM), Malaysia. He is now pursuing his pH. D study in Computer Science from University of Malaya. His research interests include group key management, network security, mobile computing, and Internet of Things.

Muzammil Hussain received his B.S. (Computer Science) in 2013 from COMSATS Institute of Information Technology Sahiwal, Pakistan. Currently, he is pursuing his pH.D. in Computer Science at University of Malaya, Kuala Lumpur, Malaysia. He has published 6 international journal papers. His current research interests include Android Security, Operating System Security, mHealth Security, Cloud Computing, Mobile Security, Sensors Threats, and Telemedicine Security.

Suleman khan is currently a PhD student under Bright Spark Scholarship, University of Malaya, Malaysia since October 2013. He has completed several Master degrees including M.Sc-CS, MBA, MS-CS from University of Peshawar, IM-Sciences Peshawar, and Comsats Abbottabad in 2006, 2008, and 2011 respectively. He has published more than 20 research peer review articles in different journals and international conferences while having research interest of wireless sensor networks, software defined Networks, network forensics, and cloud computing security.

Muhammad Khurram Khan is currently working as a Full Professor at the Center of Excellence in Information Assurance (CoEIA), King Saud University, Kingdom of Saudi Arabia. He is one of the founding members of CoEIA and has served as the Manager R&D from March 2009 to March 2012. He developed and successfully managed the research program of CoEIA, which transformed the center as one of the best centers of research excellence in Saudi Arabia as well as in the region.

Prof. Muhammad Khurram Khan is the Editor-in-Chief of a well-esteemed ISI-indexed international journal 'Telecommunication Systems' published by Springer-Verlag since 1993 with an impact factor of 1.163 (JCR 2013). Furthermore, he is the full-time Editor/Associate Editor of several ISI-indexed international journals/magazines, including IEEE Communications Magazine, Journal of Network & Computer Applications (Elsevier), IEEE Access Journal, Security & Communication Networks (Wiley), IEEE Consumer Electronics Magazine, PLOS ONE (USA), IET Wireless Sensor Systems, Electronic Commerce Research (Springer), Journal of Information Hiding and Multimedia Signal Processing (JIHMSP), International Journal of Biometrics (Inderscience), Journal of Physical & Information Sciences, and Journal of Independent Studies and Research-Computing (JISR), etc.

He has also played role of the guest editor of several international ISI-indexed journals of Springer-Verlag and Elsevier Science, etc. Moreover, he is one of the organizing chair of more than 5 dozen international conferences and member of technical committees of more than 10 dozen international conferences. In addition, he is an active reviewer of many international journals.

Prof. Khurram is an adjunct professor at Fujian University of Technology, China and an honorary Professor at IIIRC, Shenzhen Graduate School, Harbin Institute of Technology, China. He has secured an outstanding leadership award at IEEE international conference on Networks and Systems Security 2009, Australia. He has been included in the Marquis Who's Who in the World 2010 edition. Besides, he has received certificate of appreciation for outstanding contributions in 'Biometrics & Information Security Research' at AIT international Conference, June 2010 at Japan.

He has been awarded a Gold Medal for the 'Best Invention & Innovation Award' at 10th Malaysian Technology Expo 2011, Malaysia. Moreover, his invention recently got a Bronze Medal at '41st International Exhibition of Inventions' at Geneva, Switzerland in April 2013. In addition, he was awarded best paper award from the Journal of Network & Computer Applications (Elsevier) in Dec. 2015.

Prof. Khurram is the recipient of King Saud University Award for Scientific Excellence (Research Productivity) in May 2015. He is also a recipient of King Saud University Award for Scientific Excellence (Inventions, Innovations, and Technology Licensing) in May 2016.

Prof. Khurram has published over 260 research papers in the journals and conferences of international repute. In addition, he is an inventor of 10 US/PCT patents. He has edited 7 books/proceedings published by Springer-Verlag and IEEE. He has secured several national and international research grants in the domain of information security. His research areas of interest are Cybersecurity, digital authentication, biometrics, multimedia security, and technological innovation management. Prof. Khurram has recently played a leading role in developing 'BS Cybersecurity Degree Program' and 'Higher Diploma in Cybersecurity' at King Saud University.

He is a Fellow of the IET (UK), Fellow of the BCS (UK), Fellow of the FTRA (Korea), senior member of the IEEE (USA), a member of the IEEE Technical Committee on Security & Privacy, and a member of the IEEE Cybersecurity community.

Kim-Kwang Raymond Choo received the PhD in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio, and is an associate professor at University of South Australia, and a guest professor at China University of Geosciences, Wuhan. He is the recipient of various awards including ESORICS 2015 Best Paper Award, Winning Team of the Germany's University of Erlangen-Nuremberg (FAU) Digital Forensics Research Challenge 2015, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is a Fellow of the Australian Computer Society and Senior Member of IEEE. He can be contacted at raymond.choo@fulbrightmail.org