A Framework for Secure Cloud Computing

Ahmed E. Youssef[1] and Manal Alageel[2]
[1] Dept. of Information Systems, King Saud University
Riyadh, 11543, KSA

[2] Dept. of Information Systems, King Saud University
Riyadh, 11543, KSA

Abstract
Cloud computing is one of the most discussed topics today in the field of information technology. It introduces a new Internet-based environment for on-demand, dynamic provision of reconfigurable computing resources. The biggest challenge in cloud computing is the security and privacy problems caused by its multi-tenancy nature and the outsourcing of infrastructure, sensitive data and critical applications. In this paper, we propose a framework that identifies security and privacy challenges in cloud computing. It highlights cloud-specific attacks and risks and clearly illustrates their mitigations and countermeasures. We also propose a generic cloud computing security model that helps satisfy security and privacy requirements in the clouds and protect them against various vulnerabilities. The purpose of this work is to advise on security and privacy considerations that should be taken and solutions that might be considered when using the cloud environment by individuals and organizations.
Keywords: *Cloud Computing; Utility Computing; Security and Privacy; Service Oriented Architecture.*

1. Introduction

Cloud computing is one of the most rapidly growing areas in information technology [3-5,7-13,18-20]. There are many definitions for cloud computing in the literature [2]. The definition provided by the National Institute of Standards and Technology (NIST) [14] appears to include key common elements widely used in the cloud computing community [36]: *"Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*.

Figure 1 below shows the NIST visual model for cloud computing. NIST defines four Cloud deployment models (*public, private, hybrid and community*) [1,12,19,22,36,65,70,79,88,95,99,106] which describe the scope of services offered to cloud customers. NIST also defines three service models, *Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (Iaas),* [1,2,12,13,18,19,22,36,60,65, 70,71,79,88,93,94,95,97,106] which are a Service-Oriented Architecture (SOA) that describes the type of services provided by the cloud at different levels of abstraction. In addition, NIST describes a number of essential cloud computing characteristics [1,19,36,55,64,79,85,95,100,106] which includes *on-demand self services, broad network access, resource pooling, rapid elasticity and measured services.*

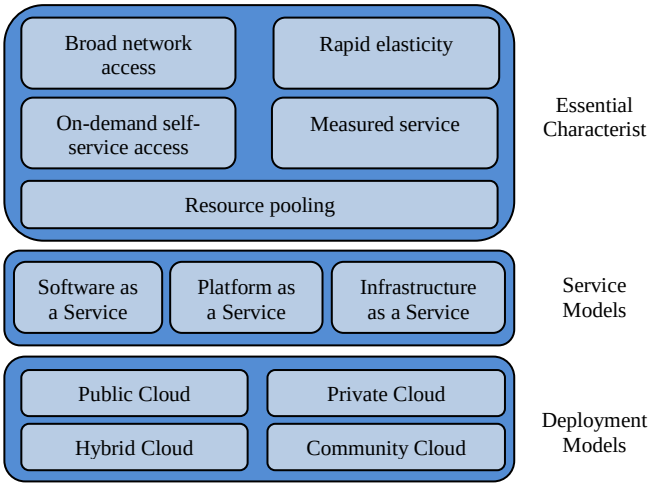

Fig. 1: NIST visual model for cloud computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

The biggest challenge in cloud computing is to successfully address the security and privacy issues associated with their deployment. During August 2009 the International Data Corporation (IDC) [37] conducted a survey to rank cloud computing challenges. The results of the survey illustrated that security is the biggest concern in cloud computing [6,19,22,75,104]. The security and privacy problems in cloud computing are mainly due to its multi-tenancy nature and the outsourcing of sensitive data, critical applications and infrastructure onto the cloud. There are many concerns from organizations and individuals about how security and privacy can be maintained in the new cloud environment. Moreover, organizations have strict constraints on putting their sensitive data and critical applications on public clouds. In order to alleviate these security concerns, efficient approaches should be employed to ensure that customers can continue to have the same security and privacy controls over their applications. Cloud Service Providers (CSPs) should be able to provide evidence to their customers that their

data and applications are secure and they can meet Service Level Agreements (SLA) [6].

In our preliminary work [106] we introduced a brief survey on security issues in cloud computing. In this paper we extend our previous work in the following aspects: First, we provide an extensive review for the most recent work in cloud computing since research is growing very rapidly in this area. Second, we provide a framework for security and privacy in cloud computing. The framework gives guidelines on most of the aspects of secure clouds including: security and privacy requirements, attacks and threats that clouds are vulnerable to and risks and concerns about cloud security. Third, we propose a generic security model for cloud computing that helps satisfy its security requirements and protect clouds against various malicious behaviors. The purpose of our work is to advise on security and privacy considerations that should be taken and solutions that might be considered when using the cloud environment by individuals and organizations.

The rest of this paper is organized as follows: in section 2, we provide an extensive review for the most recent work in cloud security. In section 3, we provide our framework for cloud security and privacy. In section 4, we propose our generic security model for cloud computing. Finally, in section 5 we give our concluding remarks and future work.

2. Related Work

Many researchers have conducted work related to the security and privacy problem in cloud computing [6, 22, 39-43, 55, 59-64]. We summarize this work here:

In [6] Popovic *et al.* presented some standards that can be used to address security issues in cloud computing such as: Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO 27001/27002) and Open Virtualization Format (OVF). In [22] Ramgovind *et al.* presented guidelines for managing cloud security which include: cloud governance, cloud transparency and cloud computing security impacts.

In [39] the authors proposed an Effective Privacy Protection Scheme (EPPS) to provide the appropriate privacy protection for cloud services. EPPS satisfies users' privacy requirements and maintains system performance simultaneously. First, they analyzed the privacy level users require and quantified the security degree and performance of encryption algorithms. Then, an appropriate security composition is derived by the results of analysis and quantified data. Their simulation results showed that the EPPS not only fulfils users' privacy requirements but also maintains the cloud system performance in different cloud environments. The execution results show that EPPS outperforms other security schemes by 35% to 50%.

In [40] in order to satisfy the assurances of cloud data integrity and availability and enforce the quality of cloud storage services for users, the authors proposed a highly efficient and flexible distributed storage verification scheme with two salient features. By utilizing a homomorphic token with distributed erasure-coded data, their scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior work, the new scheme further supports secure and efficient dynamic operations on outsourced data, including: block modification, deletion and appending. Extensive security and performance analysis showed that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attacks, and even server collusion attacks.

The work in [41] studied the problem of ensuring the integrity of data storage in Cloud Computing. In particular, the authors considered the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminated the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for cloud computing. They stated that a significant step toward practicality is the support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, since services in cloud computing are not limited to archive or backup data only. While prior work on ensuring remote data integrity often lacks support for either public auditability or dynamic data operations, this work achieves both. The authors showed how to construct an elegant verification scheme for the seamless integration of these two salient features in their protocol design. In particular, to achieve efficient data dynamics, they improved the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, they explored the technique of bilinear aggregate signature to extend their main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis showed that the proposed schemes are highly efficient and provably secure.

In [42] the authors proposed a generic security management framework allowing providers of cloud data management systems to define and enforce complex security policies. They designed the framework to detect and stop a large number of attacks defined through an expressive policy description language and to be easily interfaced with various data management systems. They showed that they can

efficiently protect a data storage system by evaluating their security framework on top of the BlobSeer data management platform. The benefits of preventing a DoS attack targeted towards BlobSeer were evaluated through experiments performed on the Grid5000 testbed.

The work in [43] investigated the problem of assuring the customer of the integrity (i.e. correctness) of his data in the cloud. The cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised since the data is physically not accessible to the user. The authors provided a scheme which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the cloud provider and the customer and can be incorporated in the service level agreement. The authors suggested that this scheme ensures that the storage at the client side is minimal which will be beneficial for thin clients.

In [55] the author discussed some security and privacy issues in cloud computing and suggested four methods for cloud security and privacy including: 1) access control method which is an application of Role-Based Access Control (RBAC) [56] on cloud computing to produce one algorithm called cloud-based RBAC. The author defined the basic component in this method as: Cloud User, Access Permission, Role and Session. He stated that at the beginning of each session, Cloud Users can request to acquire some of the roles (permissions). If the Role is enabled, some sensitive requests are granted. In this way, the malicious attacks on user data can be prevented as for such activity a user cannot acquire the access permission, 2) policy integration method which is a dynamic policy control mechanism that handles the multi-policy problem and dynamically determines the dominant policy during certain data processing, 3) identity management method which is used to prevent the unauthorized secondary usage of data. In this method the author added the Cloud Privacy Label (CPL) to the user centric identity management [57] to get a mechanism to protect the cloud users' privacy, 4) user control method which is a method to solve the problem that the cloud users will lose control of their data as a result of virtualization. To address this problem the author introduced the Third Party Auditor (TPA) [58] to balance the power between cloud service providers and cloud users. The author concluded that his methods can only deal with one or two aspects of cloud security problems so some more methods have to be proposed in the future in order to provide a more secure cloud.

In [59] the authors discussed the main cloud computing security risks and focused on the data confidentiality problem in the context of e-commerce clouds. They identified the properties that must be fulfilled to conceal the data of legitimate users and proposed a data concealment component to protect legitimate data and its implementation. This security component is composed of three sub-components, they are: 1) the prediction sub-component which uses a basic but fast and efficient predictive model to define the number of artificial data vectors to insert in addition to the vector marked to conceal the real data, 2) the data generation sub-component which generates the number of artificial data vectors given by the predictive model, 3) the data marking sub-component which marks the data vector to insert. The authors evaluated the performance of their security component and found that it successfully conceals data of legitimate users to protect it against potential attackers. The authors concluded that although their security component is efficient, it is necessary to improve the data marking method to avoid concatenating the mark with the data, thus they are working on a marking method that uses the secret key principle but allows a reversible degradation of data in contrast to the existing water marking methods.

In [60] the author discussed some vital issues to ensure a secure cloud environment. This included a basic view of security policies (e.g., inside threats, access control and system portability), software security (e.g., virtualization technology, host operating system, guest operating system and data encryption) and hardware security (e.g., backup, server location and firewall). The author concluded that an important issue for the future of cloud security is the use of open standards to avoid problems such as vendor lock-in and incompatibility. Furthermore, the author believes that although there are no security standards specific to cloud computing, conventional security concepts can be usefully applied.

In [61] the authors introduced a new cloud security management framework based on aligning the FISMA standard to fit with the cloud computing model. The framework improves collaboration between cloud providers, service providers and consumers in managing cloud security. It consists of three main layers: a management layer, an enforcement layer and a feedback layer. Each layer is responsible for key security services. The authors stated that their framework can be used by cloud providers to manage their cloud platform security, cloud consumers to manage their cloud-hosted assets and as a security-as-a-service tool to help cloud consumers outsource their Security Management Process (SMP) to the cloud. They developed a proof of concept of their framework using .NET and deployed it on a testbed cloud platform. They evaluated their framework by managing some security multi-tenant SaaS applications.

In [62] the authors discussed the security issues in a cloud computing environment. They focused on technical security issues arising from the usage of cloud services. They discussed security threats presented in the cloud such as VM-Level attacks, isolation failure, management interface compromise and compliance risks and their mitigation. They also presented cloud

security architecture, using which; organizations can protect themselves against threats and attacks. According to the authors the key points for this architecture are: single-sign on, increased availability, defence in depth approach, single management console and Virtual Machine (VM) protection.

In [63] the authors tried to categorize the key concerns about cloud security and discussed the technical implications and research issues related to it. They identified four categories of common security issues around cloud computing, they are: cloud infrastructure, data, access and compliance. Additionally, the authors presented a few high-level steps towards a security assessment framework. They stated several observations related to the current status of cloud computing security including: the security standardization activities are fragmented among many industry forums, quick provisioning of users in the cloud has become complicated, more mainstream research is required in the area of data anonymization and privacy preserving techniques, adherence to compliance by cloud providers is essential for commercial success of cloud, and migrating generic in-house software to public clouds requires thorough understanding of potential security risks.

In [64] the authors analyzed vulnerabilities and security risks specific to cloud computing systems. They defined four indicators for cloud-specific vulnerability including: 1) it is intrinsic to or prevalent in core technology of cloud computing, 2) it has its root in one of NIST's essential cloud characteristics, 3) it is caused by cloud innovations making security controls hard to implement, 4) it is prevalent in established state-of-the-art cloud offerings. The authors were certain that additional cloud-specific vulnerabilities will be identified; others will become less of an issue as the field of cloud computing matures. However, they believe that using a precise definition of what constitutes vulnerability and the four indicators they identified will provide a level of precision and clarity that the current discourse about cloud computing security often lacks.

Many other works have been proposed in the literature discussing different issues in cloud computing security [30-34,38,65-90,92-105] and much of the ongoing work focuses on developing approaches that are able to address these issues. Examples of these approaches are [13]: The Cloud Security Alliance – Security Guidance for Critical Area of Focus in Cloud Computing, which identifies specific cloud security risks in different areas including architecture, governance and operational risks and provides recommendation for mapping them [47], The Jericho Forum Self Assessment Scheme, which defines crucial rules in the form of "commandments" which are mapped to accept/best practices that cloud's users can use to assess plans [48], The Shared Assessments questionnaires for vendor/service provider assessment, which allow the systematic evaluation of security and privacy control [49], The ENISA Cloud Computing Risk Assessment Report, which describes the primary information security benefits and risks for cloud computing as well as a set of practical recommendations [50] and The National Institute of Standard and Technology (NIST) which provides recommendations and guidelines for security and privacy in public cloud computing [14].

Most of the work mentioned above seem to focus on certain aspects of the security and privacy problem in cloud computing. In this work we provide a framework for security and privacy that serves as a comprehensive guidance for achieving higher security level in the clouds. The framework gives guidelines on most of the aspects of secure clouds including: security and privacy requirements, attacks and threats that clouds are vulnerable to and risks and concerns about cloud security. Moreover, we propose a generic security model for cloud computing that helps satisfy its security requirements and protect the clouds against various malicious behaviors.

3. A Framework for Secure Clouds

Figure 2 below shows our framework for secure cloud computing. It consists of three essential security components; each of them includes important challenges related to cloud security and privacy. These components are:

Security and privacy requirements: identifies security and privacy requirements for the cloud such as authentication, authorization, integrity, etc.

Attacks and threats: warns from different types of attacks and threats to which clouds are vulnerable.

Concerns and risks: pay attention to risks and concerns about cloud computing. We discuss each guideline in detail in the following sub-sections.

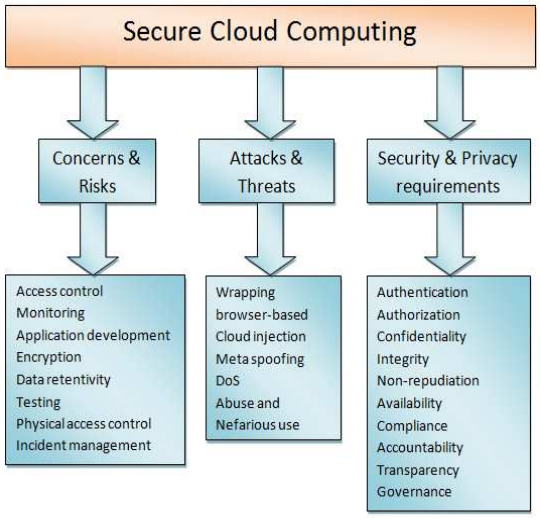

Fig. 2: A Framework for Secure Cloud Computing

3.1 Security and privacy requirements

Security concerns confidentiality, availability and integrity of data or information. It also includes Authentication, Authorization and Access control (AAA). On the other hand, privacy concerns the adherence to various legal and non legal norms. It includes: consent, purpose restriction and legitimacy which all ensure that a cloud deployment meets the requirements imposed by law. It may also include transparency, governance and compliance. The International Standards Organization (ISO), in ISO 7498-2 [21, 23], suggested a number of information security requirements, they are [22]:

Identification and Authentication management: user identification and authentication problem in the cloud environment results from its multitenancy feature which allows adversary of malicious users to utilize the cloud [55]. To mitigate this problem, CSPs are required to employ methods that help individually verify and validate cloud users when they logon to their accounts. Authentication and user identification are usually accomplished by employing usernames and passwords when using web browser to access the cloud. A more efficient way for authentication is to use an additional authentication factor outside the browser such as two factor authentication (2FA) [54, 98], but this limits cloud scalability and usability [60]. Authentication is important to prevent intruders from using the cloud and to protect cloud users' profiles.

Authorization and access control: in a cloud environment, especially public cloud, many users at different locations in the world access the cloud with different privileges. Users are granted privileges by CSPs based on their account type. The challenge here is how to control access priorities, permissions and resource ownerships of authenticated users on the cloud. Also, one of the most difficult problems is how to monitor and control the activities of those privileged users [96]. Moreover, some unauthorized users can have access to the cloud jeopardizing customers' data. Apple and Google attempt to resolve these problems through separation of duties, to ensure that activities of privileged customers are monitored by the staff, and gathering enough information on administrators who are allowed to access customers' information [96]. An important thing that helps resolve authorization issue in cloud environment is to establish a solid confidence between CSPs and customers who should both trust cloud administrators as well [60].

Confidentiality: due to the increased number of users and access points to the cloud, data is vulnerable to unauthorized access by unauthorized users. Confidentiality ensures that information is accessible only to those authorized to have access. Confidentiality becomes vital in public clouds due to its accessible nature. Data confidentiality could be threatened on the cloud due to multitenancy, data remanence, week user authentication and software applications [95]. Multitenancy allows for resource sharing among different cloud users which, if not controlled carefully, may permit a user to access other user's data since cloud resources are virtually separated but not physically. Data remanence refers to the residual representation of data that has been erased from the cloud which may lead to disclosure of private data. Lack of strong user authentication can also lead to unauthorized access to the data; users' account should be protected from theft on the cloud. CSPs should also ensure that software applications interacting with customer's data will not introduce additional confidentiality breaches and threats and will securely handle and maintain this data [95]. Encryption algorithms [44,45] and advanced electronic authentication methods such as 2FA [54,98] are common techniques to achieve confidentiality.

Integrity: refers to protecting cloud data and software from unauthorized deletion, modification, theft or fabrication [95], this ensures that data has not been tampered with or abused. Integrity includes data accuracy, completeness and ensures Atomicity, Consistency, Isolation and Durability (ACID). These properties should be robustly imposed across all cloud computing models [22,106]. CSPs should maintain data integrity by preventing unauthorized access. Hash function algorithms [46] are used widely to achieve data integrity. Hardware and network integrity is an additional issue that should be address by CSPs.

Non-repudiation: ensures that the sender of a message cannot deny the message was sent and that the recipient cannot deny the message was received. This can be achieved using techniques such as digital signatures, timestamps and confirmation receipt services [106].

Availability: refers to cloud data, software and also hardware being available, usable and accessible to authorized users upon demand. CSPs should be able to continue providing customers with services even in case of the existence of security breaches, malicious activities or system faults [95]. Availability is an important factor in choosing among various CSPs. It is also essential to ensure safety of enterprise data, minimal downtime, Business Continuity (BC) and Disaster Recovery (DR) [99]. Availability can be achieved using backup and recovery schemes, fault tolerance, and replication techniques.
Other security and privacy requirements are described in [13, 62, 96, 100] such as:

Compliance and Audit: compliance with regulations and laws is a necessary privacy requirement to ensure that the cloud deployment meets the requirements of general legislation, sector-specific rules and contractual obligations [13]. CSPs are required to comply with a set

of audits and with different standards such as SAS 70, ISO 27001, Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCIDSS) [96]. Cloud users should comply with the software licences of the applications they use and the regulations of data encryption when transmitting this data over public networks. Compliance with regulations is not an easy task since CSPs often do not know what data is being stored in their infrastructure or where it is located and may not be able to provide evidence of compliance to their customers. Customers may not be allowed to look at the cloud processes, procedures and practices and cannot be certain if they are in compliance with applicable laws [62, 96]. CSPs should implement strong internal and external audit on all cloud activities. They should permit customers to define their control requirements, understand internal monitoring process and analyse external audit report [100]. However, the huge amount of data in the cloud makes it difficult to audit all data processes and even to determine which data need to audit [55].

Transparency: the operation of the cloud should be sufficiently clear to users and CSPs. Users must be able to get a clear overview of where and how their data will be handled. They also must be able to determine who the cloud provider is and where his responsibility ends [13]. In [22] SLA was considered as one of the most important protocols to ensure transparency since it is the only legal agreement between CSPs and customers that contains guidelines to customers such as: service to be delivered, tracking and reporting, legal compliance, and security responsibility.

Governance: data on the cloud is vulnerable since it is processed and stored remotely. Customers have concerns about why their personal information is requested and who will use it. There are also threats associated with virtualization [15-17, 35] and resource sharing. Policies and procedures should be applied to protect the cloud from attacks, threats and data loss [13]. Governance ensures protecting data against various malicious activities and helps control cloud operations [22].

Accountability: implies that security and privacy gaps are correctly addressed [13]. Table 1 summarizes cloud security and privacy requirements and methods to achieve them based on our literature review.

Table 1: a summary for security and privacy requirements and how to achieve them

Security & privacy req.	**Achieved by**
Authentication	Username, Password, 2FA
Authorization and access control	Restrict cloud admins hiring process- Monitor activities of authorized users- Build trust between CSPs, cloud customers and admins.
Confidentiality	Employ strong authentication methods - Prevent unauthorized access-Use encryption techniques
Integrity	Use encryption and hash algorithms-Prevent unauthorized access
Non-repudiation	Digital signatures-Timestamps-Confirmation receipt services
Availability	Use backup and recovery schemes, fault tolerance and replication
Compliance and audit	Perform internal and external audits on a regular basis to monitor CSP's compliance to agreed terms, standards and regulations
Transparency	Provide customers with clear information on controls, security and operation of the cloud-Refer to SLA
Governance and accountability	Effective implementation and adherence of security policies and procedures to protect clouds from threats and data loss

3.2 Attacks and Threats

Before defining types of attacks in clouds, we must identify the attackers themselves and their impact on the security of cloud systems. Cloud attackers may be categorized as follows:

Random: the most common type of attackers uses simple techniques to randomly scan the internet in order to find vulnerable computers. They deploy well known tools that should be easily detected.

Weak: are semi-skilled attackers who target specific cloud providers by customizing publicly available tools for specific targets.

Strong: are organized, skilled and well financed groups of attackers who target particular applications and users of the cloud. Generally, they form criminal groups specialized in large scale attacks.

Substantial: are motivated, highly skilled attackers who can't be easily detected either by the organizations they attack or by the law enforcement and investigative organizations specializing in e-Crime or cyber security.

Attacks on cloud computing can be classified according to cloud service models and they are described below [24, 25,101]:

In SaaS the most common attacks are:

Wrapping attacks: these attacks occur between the web browser and the server by altering the Simple Object Access Protocol (SOAP) messages for two persons, the user and the attacker. When using XML signatures for authentication or integrity, the most well-known attack is XML Signature Element Wrapping.

Browser-based attacks: a browser attack alters the signature and encryption of SOAP messages. The security of Web browsers is defended against some types of attack such as phishing attack, SSL certificate spoofing, and attacks on browser caches.

In PaaS there are some types of attack such as:

Cloud injection attacks: attempt to create malicious service implementation modules or virtual machine instances for the opponent to be executed against intention. Examples for these modules are SQL injection, OS command injection and cross site scripting [64]. The threat occurs when considering the new instance to be a valid instance. To avoid this attack, a hashing algorithm should be used.

Metadata spoofing attacks: include reengineering Web Services' metadata descriptions. To defend against this threat, verification techniques should be used.

In IaaS, the most important attack is the flooding attack that is represented as:

Denial of service attacks: occur when an attacker sends a lot of malicious requests to the server and consumes its available resources, CPU and memory. When the server reaches its maximum capacity, it offloads the received requests to another server. In cloud computing, due to the large number of cloud users (multitenancy) who share the cloud infrastructure the problem of Distributed DoS (DDoS) attacks becomes of much greater impact than that in single tenant architecture. The problem is further magnified when the cloud has no sufficient resources to provide customers with services [65]. The cloud system works against the attacker by providing more computational power.

Buffer overflow attacks: when buffer overflow occurs, the attacker is able to overwrite data specialist in program execution to execute his malicious program.

Privilege escalation: utilizes a vulnerability that comes from any programming errors and aims to access the protected resources without permission.

In [64, 85] cloud-specific vulnerabilities are categorized into four categories, they are:

Vulnerabilities intrinsic core technology of cloud computing: these are vulnerabilities associated with virtualization, web applications and cryptography. Examples of these vulnerabilities are: virtual machine escape, session riding and session hijacking and insecure cryptography.

Vulnerability with root cause in essential cloud characteristics: these are vulnerabilities associated with the five NIST cloud characteristics. Examples of these vulnerabilities are: unauthorized access management interface which is caused by the first characteristic "on-demand self-service", Intranet protocol vulnerabilities caused by the second characteristic "broad network access", data recovery due to "pooling" and "elasticity" characteristics which makes it possible to a user to recover the data written by a previous user because of resource reallocation and belling evasion caused by the last characteristic "measured service".

Vulnerability caused by defects of known security controls in cloud setting: such as insufficient network-based control in virtualized network, poor key management procedure and security metrics not adapted to cloud infrastructure.

Vulnerability prevalent in state-of-the-art cloud offerings: such as insufficient or faulty authorization check, weak authentication schemes and injection vulnerabilities.

At the Black Hat USA 2010 Conference, the Cloud Security Alliance (CSA) [26,27], a non-profit organization formed to promote the use of best practices for providing security assurance within cloud computing, announced industry's first certification program on secure cloud computing. According to CSA the top seven threats in cloud computing are described as follows [28,100,106]:

Abuse and Nefarious Use of Cloud Computing: a cloud is a relatively open environment; consumers from everywhere can easily register to utilize its cost-effective services with simply a valid credit card. The easiness and the anonymity of registrations on the cloud have encouraged attackers to conduct their malicious activities. Attackers continue enhance their tools to improve the effectiveness of their attacks and to avoid detection. Examples of such attacks are password and key cracking, DDoS, launching dynamic attack points, hosting malicious data and botnet command and control. CSA suggested remedies to mitigate this threat such as: improving credit card fraud detection, applying strict registration and validation rules and performing extensive examination of network traffic.

Insecure Interfaces and APIs: cloud consumers interact with cloud through a set of user interfaces and APIs provided by CSPs. In order for the cloud to be secure, these interfaces should be designed to protect against unauthorized access, week authentication, data tampering and other malicious activities. Consumers should understand the security implications of these

interfaces and APIs. CSA suggested remedies to mitigate this threat such as: analysing the security model of the API, employing strong authentication, access control and encryption techniques and understanding the dependency chain of the API.

Malicious Insiders: this threat is caused by employees hired by CSPs. Those employees are granted a level of access that may allow them acquire confidential data and fully control cloud services without being detected. CSPs show little or no transparency on how they hire people, how they grant them access to cloud resources or how they monitor them. Malicious insiders can considerably influence financial impacts and productivity of organizations. CSA suggested remedies to mitigate this threat such as: requiring transparency in all information security issues, defining security breach notification processes and enforcing strict hiring requirements and human resource assessment.

Shared Technology Issues: sharing resources and multitenancy is one of the most important cloud characteristics. Although cloud customers are isolated from each other using virtualization technology, a customer can still have access to other customer's actual or residual data, network traffics, operations, etc. This is because cloud physical component are not designed to provide strong isolation properties for multitenant structure. Attackers may target shared computing resources such as CPU caches, GPUs and disk partitions. CSA suggested remedies to mitigate this threat such as: conducting vulnerability scanning and remediation, promoting strong authentication and monitoring unauthorized activities and implementing security best practice for installation and configuration.

Data Loss or Leakage: compromising data is an increasing problem in cloud computing due to its architectural and operational characteristics. It may occur in different way from deletion or modification without backup to loss of encoding key and for different reasons such as unauthorized access, insufficient authentication or inconsistent use of encryption keys. Data loss could significantly impact organizations' brand, business and reputation. CSA suggested remedies to mitigate this threat such as: implementing strong API access control, key generation and encryption techniques, providing backup and retention strategies and analysing data protection at both design and run time.

Account or Service Hijacking: there are several known methods for account hijacking such as phishing, fraud detection and man-in-the-middle attacks. Attackers can use stolen credentials or passwords to jeopardize the confidentiality, integrity and availability of cloud services. CSA suggested remedies to mitigate this threat such as: forbidding sharing of account credential between users, employing 2FA techniques and understanding CSPs security policies and SLAs.

Unknown Risk Profile: information on code updates, intrusion attempts, vulnerability profiles and security practice are not usually known to customers. CSPs do not often inform customers on how data and related logs are stored and who has access to them. This unknown risk profile may include serious threats. CSA suggested remedies to mitigate this threat such as: monitoring on necessary information and disclosure of applicable data, logs and infrastructure detail.

In [62] Tripathi and Mishra mentioned some other cloud threats such as:

Loss of governance: refers to the loss of control by cloud customers on the services that is provided by CSPs which may cause security gaps in data availability, integrity and confidentiality. This risk can be mitigated by careful execution of SLA.

Lock-in: due to lack of standardization, cloud customers are unable to move their programs and data between CSPs. Standard cloud API should be used to achieve portability in cloud computing.

Lack of compliance: CSPs may not be able to provide evidence for compliance to their customers and may not permit them audit the cloud processes. Table 2 summarizes cloud attacks and threats and their mitigations based on our literature review.

Table 2: a summary for cloud attacks and their mitigations

Attacks and threats	**Mitigation**
Wrapping attacks	Increase security during message passing from the web server to the web browser by using the SOAP message
Cloud injection attacks	Use hash algorithms
Metadata spoofing attacks	Use verification techniques
Denial of Service (DoS)	Provide more computational power and resources
Abuse and Nefarious Use of Cloud Computing	Improve credit card fraud detection-Apply strict registration and validation rules-Perform extensive examination of network traffic
Insecure Interfaces	Analyse the security model of the API- Employ strong authentication, access control and encryption techniques- Understand the dependency chain of the API
Malicious Insiders	Require transparency in all information security issues- Define security breach notification processes- Enforce strict hiring requirements and HR assessment
Shared technology	Conduct vulnerability scanning

	and remediation- Promote strong authentication and monitor unauthorized activities- Implement security best practice for installation and configuration
Data Loss or Leakage	Implement strong API access control, key generation and encryption techniques- Provide backup and retention strategies- Analyse data protection at both design and run time.
Account or Service hijacking	Employ 2FA- Understand CSPs security policies and SLAs-Forbid sharing of account credential
Unknown Risk Profile	Monitor on necessary information, Disclose applicable data, logs and infrastructure detail
Lack of governance	Carefully execute SLAs
Lock-in	Use standard cloud API to achieve portability between CSPs
Lack of compliance	Perform regular audits for compliance-Let customers be aware of how CSPs adhere to laws and regulations.

3.3 Concerns and Risks

The literature noted a number of concerns about managing security and privacy in cloud computing [13, 63]. In [13] some concerns are:

Access control: how can cloud users govern access control risks when the levels and types of access control used by cloud providers are unknown?

Monitoring: how can accurate, timely and effective monitoring of security and privacy levels achieved in business-critical infrastructure when its providers are not prepared to share such information at SLA?

Applications development: how to accomplish application development and maintenance in the cloud when CSPs are responsible to?

Encryption: how can the cloud user manage encryption and assign responsibilities across the borders between the cloud service providers and his organization?

Data retentivity: how can the cloud user achieve appropriate confidence that the data have been actually and securely removed from the system by the cloud provider and are not merely made inaccessible to him?

Testing: how can consumers test the effectiveness of security control when these tests may not be made available by CSPs?

Physical access control: how can the cloud user achieve requirements for physical access when its measures are established and fully controlled by CSPs?

Incident management: how can the cloud user determine appropriate thresholds and criteria in order to respond to incident?

In [63] Sengupta et. al stated some concerns based on customers' responses such as:

- Is CSP's physical and software infrastructure secure? This includes concerns about security of datacenters, shard VM infrastructure, common software stacks, and the isolation in hybrid cloud.
- What happen to the data in the cloud? This includes concerns about data confidentiality, integrity, locking-in, data remanent and updates.
- Are users accessing the cloud authenticated and can authenticated users get secure accessibility? This includes concerns about authentication, authorization and access control (AAA).
- Are CSPs compliant with regulations? This requires regular internal and external audits for cloud processes.

Popovic et al. [6] listed some security concerns on cloud computing which we summarize below [106]:

- Does the CSP notify customers with privacy breaches and who is responsible for notification process?
- Company may disclose data to a foreign government.
- Customers may not be able to move data between different CSPs due to incompatible storage services
- Physical security of the cloud is lost because of sharing computing resources
- How is customers' personal information such as name, address and credit card number protected?
- Who controls the encryption/decryption keys?
- How is customers' sensitive information such as race, religion, health or financial information is protected?
- In case of payment information, data logs must be provided to security managers.
- How is information collected from computer devices such as smart phone, iPad or notebooks used?
- It may not be clear to individuals why their personal information is requested and how it will be used.
- Users must be updated by application improvements to be sure they are protected.
- Some governments have restrictions on what data may be stored about their citizens in the cloud and for how long. Some banks also do not want their customers' data to be located out of the country.
- Due to the dynamic and fluid nature of virtual machines, it is difficult to maintain the consistency of security.
- A common standard for ensuring data integrity does not exist yet.

The well-known Gartener: seven security risks [29] that customers should discuss with vendors before selecting

a cloud computing system are described in [6, 29, 65,96,106] as follows:

Privileged user access: ask your CSP to inform you about people who manage and access your data. Let him provide you with information on who hires administrators and how.

Regulatory compliance: make sure that your CSP undergoes external audits and security certification.

Data location: In cloud computing data may be hosted by another country, even without the end user necessarily being aware. Some countries have restrictions on transferring data outside the country. Moreover, virtualization technologies may make it harder to determine where data are located. Make sure that your CSP commits to obey local privacy requirements in data storing and processing on behalf of his customers.

Data segregation: refers to the separation of data to ensure that each cloud customer accesses his information only without affecting other customer's information. Make sure that your CSP uses encryption in data segregation or aggregation and tests the encryption schemes by security experts.

Data Recovery: ask your CSP about the ability to restore and recover data if a disaster occurred. Data replication and reliability of storage media should be considered by CSP to ensure adequate date recovery.

Investigative support: investigation of illegal activities is difficult in cloud computing because of its multitenancy nature. Customers and CSP should cooperate in the investigation process.

Long-term viability: CSP should convince customers that their data will remain available even if they went out of business.

In [88] Carrol *et. al* identified the following control objectives as important for the mitigation of cloud security risks: data security, administration and control, logical access, network security, physical security, compliance and virtualization and they described the risks associated with each objective and gave recommendations for possible mitigation as determined from the literature. In [74] Tanimto *et. al* used Risk Breakdown Structure (RBS) to extract most of the risks mentioned above. Furthermore, the extracted risks were analyzed and evaluated using the risk matrix method. In this method risks are classified according to generation frequency and degree of incidence and there are four countermeasures: risk avoidance by showing alternatives, risk mitigation by reducing its impact to an accepted level, risk transference to a third party and risk acceptance unconditionally.

In table 3 we summarize cloud computing risks and their countermeasure based on our literature review.

Table 3: a summary for cloud risks and their countermeasures

Risks	**Countermeasures**
Privileged user access	Monitor authorized users activities, restrict admin hiring.
Data location	Provide consumers with information about where their data stored and processed.
Data segregation	Use encryption and distributed storage to prevent data seize.
Data remanence	Ensure the deletion of data after use of cloud service.
Data recovery	Backup data at other data centres
Long term availability	Apply insurance when cloud service is no longer provided

4. Proposed Security Model

The framework discussed above has inspired us to propose a generic cloud computing security model that helps satisfy security and privacy requirements in clouds and protect them against various vulnerabilities. The model is shown in Fig. 3 and it consists of the following security units:

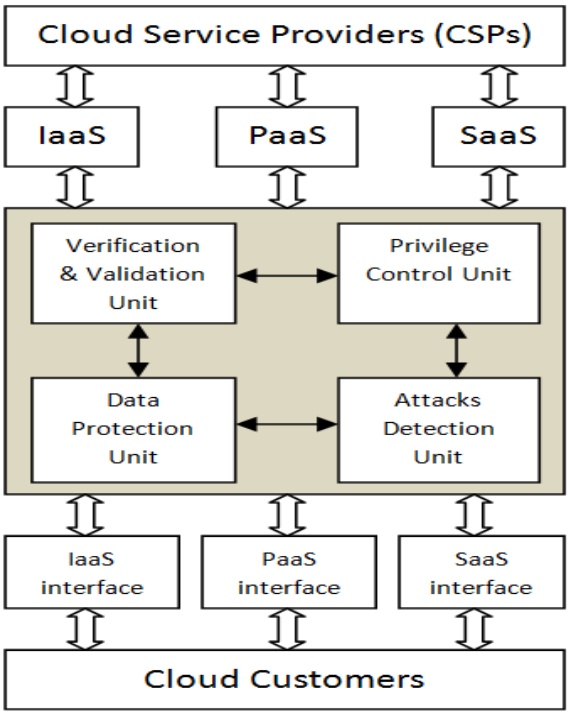

Figure 3: Cloud Computing Security Model

4.1 Verification and Validation (V&V) Unit

This unit is required in cloud computing not only to authenticate users but also to ensure the correctness of data and services on the cloud. The importance of this

security component is due to the fact that cloud computing environment is accessible by multiple consumers and providers who wanted to use or provide several services and applications. CSPs need to prove to the users that the services and data are valid using, for example, appropriate signature algorithms. Consequently, users will be able to verify the authenticity of the data and services made available to them through such type of digital signature. This security component can also employ techniques such as One Time Password (OTP) [53] and 2FA [54,98].

4.2 Privilege Control Unit

This security unit is necessary to control cloud usage by different individuals and organizations. It protects users' privacy and ensures data integrity and confidentiality by applying a collection of rules and policies that control *who* has the authority to do *what* on the cloud. Cloud users are granted different levels of access permissions and resource ownerships based on their account type. Only authorized users can access the authorized parts of the encrypted data through identity-based decryption algorithm. For example, in a healthcare cloud not all practitioners have the same privileges to access patients' data, this may depend on the degree to which a practitioner is involved/specialized in treatment; patients can also allow or deny sharing their information with other healthcare practitioners or hospitals [92]. Encryption/Decryption algorithms [52] such as AES [44,51] and RC4 [45] can be employed by this component to achieve confidentiality of information.

4.3 Data Protection Unit

Data stored in the cloud storage resources may be very sensitive and critical, for example, clouds may host electronic healthcare records (EHR) which contain patients' private information and their health history [91,92]. They may also store critical banking information (e.g., client account numbers, balances and transactions) or national security information. A cloud security model should protect these data from loss or damage by providing secure storage servers. These servers should also secure data retrieval and removal from the cloud. Securing data storage and processing is important since cloud users have no idea about data location. Techniques for data protection such as truncation, redaction, obfuscation, and others can be used in this security component. Encryption techniques can also be employed for data security. Hash functions and Message Authentication Code (MAC) can be employed in this unit to provide data integrity.

4.4 Attacks Detection/Prevention Unit

Clouds are vulnerable to many attacks and malicious behaviours that threaten both data and physical and virtual computing resources of the cloud. Basically, any set of actions that threaten the cloud security requirements (e.g., integrity, confidentiality, availability) are considered to be attacks. Attacks detection and prevention components should be installed within the cloud security system to protect cloud resources from various anomalies. For example, denial-of-service attacks should be reduced to the minimum to guarantee the maximum availability of business, governmental, health and other critical information and services. This can be achieved by deploying technologies that provide high availability such as dynamic server load balancing and active/active clustering [62]. Standard Distribution Denial of Services (DDoS) mitigation techniques such as synchronous cookies and connection limiting can also be used. Clouds should also be provided by the next generation of intrusion detection systems and firewalls in order to protect their resources from intruders, viruses and malware.

5. Conclusions and Future Work

In this paper, we reviewed the literature for security challenges in cloud computing and proposed a framework that identifies security and privacy requirements, attacks, threats, concerns and risks associated to the deployment of the clouds. Based on this framework we proposed a generic cloud security model that helps satisfy security and privacy requirements in clouds and protect them against various vulnerabilities. We believe that more effort should be exerted by both cloud vendors and organizations to provide a highly protected, safe and sound cloud computing environment. On the other hand, we suggest that future research should be directed towards the management of risks associated with cloud computing. Developing risk assessment helps organizations make an informed decision as to whether cloud computing is currently suitable to meet their business goals with an acceptable level of risks. However, managing risks in cloud computing is a challenging process that entails identifying and assessing risks, and taking steps to reduce it to an acceptable level. We plan to pursue research in finding methods for qualitative and quantitative risk analysis in cloud computing. These methods should enable organizations to balance the identified security risks against the expected benefits from cloud utilization.

References

[1] GTSI Group, "Cloud Computing - Building a Framework for Successful Transition," White Paper, GTSI Corporation, 2009.

[2] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Computer Communication Review, Volume 39 Issue 1, pages 50-55, January 2009.

[3] M. Boroujerdi and S. Nazem, "Cloud Computing: Changing Cogitation about Computing," World Academy of Science, Engineering and Technology, 2009.

[4] Michael Miller, "Cloud Computing Pros and Cons for End Users", microsoftpartnercommunity.co.uk, 2009.

[5] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009.

[6] Kresimir Popvoic and Zeljko Hocenski, "Cloud Computing Security Issues and Challenges" MIPRO, Opatijia, Croatia, May 24-28, 2010.

[7] Radu Prodan and Simon Ostermann, "A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers", 10th IEEE/ACM International Conference on Grid Computing, 2009

[8] http://en.wikipedia.org/wiki/Cloud_computing

[9] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing" Communication of the ACM, Vol. 53, No. 4, April 2010.

[10] K. Chard, S. Caton, O. Rana and K. Bubendorfer, "Social Cloud: Cloud Computing in Social Networks" 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA, July 5-10,2010.

[11] L. Tang, J. Dong, Y. Zhao and L. Zhang "Enterprise Cloud Service Architecture" 3rd IEEE International Conference on Cloud Computing,Miami, FL, USA, July 5-10,2010.

[12] W. Jansen and T.Grance "Guidelines on Security and Privacy in Public Cloud Computing", NIST Draft Special Publication 800-144, 2011. http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

[13] N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux, S. Creese and P. Hopkins, "The Cloud: Understanding the Security, Privacy and Trust Challenges", RAND Corporation, 2010. http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf

[14] NIST, http://www.nist.gov/itl/cloud/index.cfm

[15] CloudComputingvs.Virtualization http://www.learncomputer.com/cloud-computing-vs-virtualization/

[16] Wikipedia , http://en.wikipedia.org/wiki/Virtualization

[17] Y. Luo,"Network I/O Virtualization for Cloud Computing",IEEE Computer Society,Oct. 2010.

[18] W. Tsai, X. Sun, J. Balasooriya, "Service-Oriented Cloud Computing Architecture" 7th IEEE International Conference on Information Technology, 2010.

[19] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Appications, 2010.

[20] Introduction to Cloud Computing, White Paper,Dialogic Corporation, 2010.

[21] ISO, http://www.iso.org/iso/home.htm

[22] Ramgovind S, Eloff MM and Smith E. "The Management of Security in Cloud Computing" Information Security for South Africa (ISSA), Sandton, Johannesburg, 2-4 Aug, 2010.

[23] ISO. ISO 7498-21989. "Information Processing Systems-Open Systems Interconnection. ISO 7498-2.

[24] N. Gruschka and M. Jensen, "Attack Surface: A Taxonomy for Attacks on Cloud Services", 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA, July 5-10,2010.

[25] K. Zunnurhain and S. Vrbsky, "Security Attacks and Solutions in Clouds", 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, USA, Nov. 30- Dec. 3,2010.

[26] http://www.cloudsecurityalliance.org/

[27] SecureCloud 2010, http://www.cloudsecurityalliance.org/sc2010.html

[28] Cloud Security Alliance "Top Threats toCloud Computing V1.0", March 2010.

[29] J. Bordkin, "Gartner:Seven Cloud-Computing Security Risks", 2008.

[30] M. Yildiz, J. Abawajy, T. Ercan and A. Bernoth," A Layered Security Approaches for Cloud Computing Infrastrucure", 10th International Symposium on Pervasive Systems, Algorithms, and Networks,2009.

[31] CSA, "Security Guidance for Critical Areas of Focus on Cloud Computing V2.1", 2009.

[32] A.Albeshri and W.Caelli, "Mutual Protection in a Cloud Computing Environment", IEEE 12th International Conference on High Performance Computing and Communications (HPCC), Melbourne, 1-3 September 2010.

[33] Q. Tong and Z. Shen," The security of Cloud Computing System

Enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems (ICSPS),2010.

[34] J. Yang and W. Huang, "New network security based on Cloud Computing", Education Technology and Computer Science (ETCS), 2010.

[35] V. Sarathy, P. Narayan, and R. Mikkilineni, "Next generation Cloud Computing Architecture" 2nd International IEEE Workshop On collaboration & Cloud Computing, 2010.

[36] P. Mell and T. Grance, "The NIST Definition of Cloud Computing" Recommendation of NIST, Special Publication 800-145, 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[37] http://www.idc.com.

[38] "Cloud Computing Security Considerations", Cyber Security Operation Cenetre, Technical report, 2011.

[39] I. Chuang, S. Li, K. Huang, and Y. Kuo, "An effective privacy protection scheme for cloud computing", In Proceeding of the 13th International Conference on Advanced Communication Technology (ICACT), 2011

[40] C. Wang, Q. Wang, K. Ren, and W .Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Services Computing, Issue:99 , 2011.

[41] Q. Wang, C. Wang, K. Ren W. Lou, and J. Li, " Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE Transactions on Parallel and Distributed Systems, Volume : 22 , Issue:5, 2011.

[42] C. Băsescu, A. Carpen-Amarie, C.Leordeanu, A. Costan, and G. Antoniu, "Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies", In proceeding of IEEE International Conference on Advanced Information Networking and Applications (AINA), 2011

[43] R. Sravan Kumar and A. Saxena, "Data integrity proofs in cloud storage", Third International Conference on Communication Systems and Networks (COMSNETS), 2011.

[44] Federal Information Processing Standards Publication 197,"Specification for the Advanced Encryption Standards (AES)", 2001.

[45] S. Fluhrer, I. Mantin, and A. Shamir, "Weakness in the Key schedualing algorithm of RC4", 8th Annual International Workshop on Selected Areas in Cryptography, Springer-Verlag London, UK, 2001.

[46] http://en.wikipedia.org/wiki/Cryptographic_hash_function

[47] https://cloudsecurityalliance.org/research/initiatives/security-guidance/

[48] http://www.opengroup.org/jericho/

[49] http://www.sharedassessments.org/value/

[50] http://www.enisa.europa.eu/

[51] http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html

[52] Shucheng Yu, Cong Wang,KuiRen and Wenjing Lou, " Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", 2010

[53] M. Johnsson and A. Azam, "Mobile One Time Passwords and RC4 Encryption for Cloud Computing", Technical report, IDE1108, March 2011.

[54] http://en.wikipedia.org/wiki/Two-factor_authentication

[55] Z. Wang, "Security and Privacy Issues Within Cloud Computing" IEEE Int. conference on computational and Finformation sciences, Chengdu, China, Oct. 2011.

[56] James B.D. Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor, "A Generalized Temporal Role-Based Access Control Model",IEEE Computer Society, 2005.

[57] Moonam Ko, Gail-joon Ahn, Mohamed Shehab, "Privacy enhanced User-Centric Identity Management", IEEE International Conference on Communications, 2009

[58] Cong Wang, Qian Wang, Kui Ren, Wenjing Luo, "Privacy preserving public audting for data storage security in Cloud Computing", IEEE Communication Society, 2010

[59] C. Deletre, K. Boudaoud and M. Riveill, "Cloud computing security and data concealment" IEEE symposium on computers and communications (ISCC), Greece, June 28-July 1, 2011

[60] E. Mathisen, "Security Challenges and Solutions in Cloud Computing" 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), , Daejeon, Korea, 31 May -3 June 2011

[61] Almorsy, M. Grundy, J. Ibrahim, A.S., "Collaboration-Based Cloud Computing Security Management Framework" IEEE Int. confernce on cloud computing (CLOUD), 4-9 July 2011.

[62] A. Tripathi and A. Mishra, "Cloud computing security considerations" IEEE Int. conference on signalprocessing, communication and computing (ICSPCC), 14-16 Sept., Xi'an, Shaanxi, China, 2011

[63] Shubhashis Sengupta, Vikrant Kaulgud and Vibhu Saujanya Sharma, "Cloud Computing Security - Trends and Research Directions" IEEE World Congress on Services, 4-9 July 2011

[64] Vadym Mukhin, Artem Volokyta, "Security Risk Analysis for Cloud Computing Systems" The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Prague, Czech Republic, 15-17 September 2011

[65] Sabahi, F., "Cloud computing security threats and responses", IEEE 3rd International Conference on Communication Software and Networks (ICCSN), , 27-29 May 2011

[66] Gul, I. , ur Rehman, A. and Islam, M.H. , "Cloud computing security auditing", The 2nd International Conference on Next Generation Information Technology (ICNIT), 21-23 June 2011

[67] Ko, R.K.L., Kirchberg, M. and Bu Sung Lee, "From system-centric to data-centric logging - Accountability, trust & security in cloud computing", Defense Science Research Conference and Expo (DSR), 3-5 Aug. 2011

[68] Cheung, D.W., "Security on cloud computing, query computation and data mining on encrypted database" IEEE Technology Time Machine Symposium on Technologies Beyond 2020 (TTM), 1-3 June 2011

[69] Srivastava, P. , Singh, S. , Pinto, A.A. , Verma, S. , Chaurasiya, V.K. and Gupta, R., "An architecture based on proactive model for security in cloud computing" International Conference on Recent Trends in Information Technology (ICRTIT), 3-5 June 2011

[70] Jun-jie Wang and Sen Mu, "Security issues and countermeasures in cloud computing" IEEE International Conference on Grey Systems and Intelligent Services (GSIS), 15-18 Sept. 2011

[71] Zech, P., "Risk-Based Security Testing in Cloud Computing Environments", IEEE Fourth International Conference on Software Testing, Verification and Validation (ICST), 21-25 March 2011

[72] Jansen, W.A., "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii International Conference on System Sciences (HICSS), 4-7 Jan 2011

[73] Haoyong Lv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy" International Conference on Intelligence Science and Information Engineering (ISIE), 20-21 Aug. 2011

[74] Tanimoto, S. , Hiramoto, M., Iwashita, M., Sato, H. and Kanai, A., "Risk Management on the Security Problem in Cloud Computing" First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI), 2011

[75] Xuan Zhang, Nattapong Wuwong, Hao Li, and Xuejie Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments", 10th IEEE Int. Conf. on Computer and Information Technology (CTI 2010).

[76] Wang, Jen-Sheng, Liu, Che-Hung and Lin, Grace TR, "How to manage information security in cloud computing", IEEE International Conf. on Systems, Man, and Cybernetics (SMC), 9-12 Oct. 2011

[77] Bao Rong Chang, Hsiu Fen Tsai, Zih-Yao Lin and Chi-Ming Chen, "Access Security on Cloud Computing Implemented in Hadoop System", Fifth International Conference on Genetic and Evolutionary Computing (ICGEC), Aug. 29-Sept. 1 2011

[78] Xiaodong Sun, Guiran Chang and Fengyun Li, "A Trust Management Model to Enhance Security of Cloud Computing Environments" Second International Conference on Networking and Distributed Computing (ICNDC), 21-24 Sept. 2011

[79] Mahmood, Zaigham "Data Location and Security Issues in Cloud Computing" International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), 7-9 Sept. 2011

[80] Minrui Jia "Cloud Security of Cloud Computing Application" International Conference on Control, Automation and Systems Engineering (CASE), 30-31 July 2011

[81] Xue Jing and Zhang Jian-jung, "A Brief Survey on the Security Model of Cloud Computing", 9th Int. Symposium on Distributed Computing and Applications to Business, Engineering and Science, 2010.

[82] Hay, B., Nance, K. and Bishop, M., "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" 44th Hawaii International Conference on System Sciences (HICSS), 4-7 Jan. 2011

[83] Mana, A., Munoz, A. and Gonzalez, J., "Dynamic security monitoring for Virtualized Environments in Cloud computing", 1st International Workshop on Securing Services on the Cloud (IWSSC), 6-8 Sept. 2011

[84] Huang, Chun-Ting, Qin, Zhongyuan and Kuo, C.-C. Jay, "Multimedia storage security in cloud computing: An overview", IEEE 13th International Workshop on Multimedia Signal Processing (MMSP), 17-19 Oct. 2011

[85] Grobauer, B., Walloschek, T. and Stocker, E., "Understanding Cloud Computing Vulnerabilities" IEEE Security & Privacy March-April 2011

[86] Hemant, P., Chawande, N.P., Sonule, A. and Wani, H., "Development of servers in cloud computing to solve issues related to security and backup" IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), 15-17 Sept. 2011

[87] Achemlal, M., Gharout, S. and Gaber, C., "Trusted Platform Module as an Enabler for Security in Cloud Computing" Conference on Network and Information Systems Security (SAR-SSI), 18-21 May 2011

[88] Carroll, M., van der Merwe, A. and Kotze, P., "Secure cloud computing: Benefits, risks and controls", Information Security South Africa (ISSA), 15-17 Aug. 2011

[89] Mondol, J.-A.M. "Cloud security solutions using FPGA", IEEE Pacific Rim Conference on Communications, Computers and Signal Processing , 23-26 Aug. 2011

[90] Muller, I., Jun Han, Schneider, J.-G. and Versteeg, S., "Tackling the Loss of Control: Standards-Based Conjoint Management of Security Requirements for Cloud Services", IEEE International Conference on Cloud Computing (CLOUD), 4-9 July 2011

[91] D.C. Leonard, Alexander P. Pons, and Shihab S Asfour, "Realization of Universal Patient Identifier for Electronic Records Through Biometric Technology", IEEE Trans. On Information Technology in Biomedicine, Vol. 13, No. 14, July 2009.

[92] Rui Zhang and Ling Liu, "Security Models and Requirements for Healthcare Application Clouds", IEEE 3rd International Conference on Cloud Conputing, 2010.

[93] Andrew Joint and Edwin Baker, "Knowing the past to understand the present- issues in the contracting for cloud based services", Computer Law and Security Review 27, pp 407-415, 2011.

[94] Vania Goncalves and Pieter Ballon, "Adding value to the network: Mobile operators' experiments with Software-as-a-Service and Patform-as-a-Service models", Telematics and Informatics 28, pp 12-21, 2011.

[95] Dimitrios Zissis and Dimitrios Lekkas, "Addressing cloud computing security issues", Future Geberation Computer Systems 28, pp. 583-592, 2012.

[96] David Teneyuca, "Internet cloud security: The illusion of inclision", Information Security Technical Report, pp. 1-6, 2011.

[97] Rajnish Choubey, Rajshree Dubey and Joy Bhattacharjee, " A Survey on Cloud Computing Security, Callenges and Threats", International Journal on Computer Science and Engineering (IJCSE), vol. 3, No. 3, 2011.

[98] Dave Abraham,"Why 2FA in the cloud", Network Security, Vol. 2009, Issue 9, Pages 4-5, September 2009.

[99] S. Subashini and V. Kavitha, " A survey on security issues in service delivery models of cloud computing", Journal odf Networ and Computer Applications 34, pp. 1-11, 2011.

[100] S. Srinivasamurthy and David Liu, "Survey on Cloud Computing Security" http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_67.pdf

[101]Zaheer ahmad, Keith Mayes, Song Dong and Kostas Markantonakis, "Considerations for mobile authentication in the cloud", Information Security Technical Report, pp.1-8, 2011.

[102] Piers Wilson, "Positive perspectives on cloud security", Information Technology Technical Report, pp.1-5,2011.

[103] P.G. Dorey and A. Leite, "Commentary: Cloud computing-A security problem or solution", Information Technology Technical Report, pp. 1-8, 2011

[104] Minqi Zhou, Rong Zhang, Wei Fie, Weining Qian and Aoying Zhou, "Security and Privacy in Cloud Computing: A survey", 6th Int. Conf. on Semantics, knowledge and Grids, 2010.

[105] R. OalsonKennedy and T.V. Gopal, "Assessing the Risk and Opportuinties of Cloud Compiting-Defining Identity Management Systems and Maturity Models", Trends in Information Sciences & Computing (TISC), 2010

[106] Ahmed Youssef and Manal Alageel "Security Issues in Cloud Computing" in the GSTF International Journal on Computing , Vol.1 No. 3, 2011.

Ahmed E. Youssef: is an assistant professor at college of computer and information sciences, King Saud University. He obtained his Ph.D. and M.Sc. in computer science and engineering from university of Connecticut, USA. He also obtained his M.Sc and B.Sc in electronics and communications engineering from Helawn University, Egypt. His research interest includes cloud computing, mobile computing, data mining and information security.

Manal Alageel: is a TA at college of computer and information sciences, King Saud University. She obtained her M.Sc. in information systems from KSU. Her research interest includes cloud computing and information assurance.