Modelling Threats with Security Requirements in Cloud Storage

Fara Yahya, Robert J. Walters, Gary B. Wills
Electronics and Computer Science
University of Southampton
United Kingdom

Abstract

Cloud storage is becoming an option for users in keeping their data online, but it comes with the security requirements and challenges of protecting their data from threats. Many security frameworks have been suggested by existing studies, governing bodies, industry standards etc. as guidelines to be implemented by cloud service providers (CSPs) but the complete set of controls cannot be fully implemented due to several challenges such as decreasing availability, less user convenience, need of a robust infrastructure etc. Therefore, there is a need to investigate the security requirements and threats which will enable efficient security protection to protect data in cloud storage. This paper will discuss security requirements and analyses existing cloud security threats. The threats will be modelled in a cloud storage scenario.

1. Introduction

In computer security, a threat is a risk of potential harm to a computer system. It may or may not happen but causes harm leading a vulnerability to breach security [1]. It is possible for these vulnerabilities to lead to attacks such as gaining unauthorised access to stored information, denial of service to the authorised users, or introduction of false information to mislead the users or to cause incorrect system behaviour (spoofing) [2]. Computer security means to protect information. It deals with the prevention and detection of unauthorised actions by users of a computer.

Lately computer security has been extended to include privacy, confidentiality, and integrity [1]. Threats in cloud include; interception, modification of data at rest and in transit, data interruption (deletion), data breach, impersonation, session hijacking, traffic flow analysis and exposure in network [3–7]. Consequently, with the emerging threats, research has focused on security frameworks in the cloud [8]. Each requirement refers to security objectives while security threats are specific to cloud storage. This paper will discuss the security requirements and security threats in cloud by analysing and modelling threats in the context of cloud storage and drawing some conclusions.

2. Security Requirements

With the utilisation of the cloud, users lose control over physical security. In fact in public cloud storage, users are sharing the computing resources with other users. In this section, a review of existing frameworks for security requirements and cloud security is discussed to obtain common security requirements. Table 1 and Table 2 show a summary of security requirements from existing studies and organisations on security frameworks.

2.1. Cloud Security Frameworks and Requirements

Firesmith [9] developed a detailed specification which attempts to provide a comprehensive security framework. It consists of nine layers: access control, attack harm detection, non-repudiation, integrity, security auditing, physical protection, privacy and confidentiality, recovery and prosecution. This framework provides a detailed analysis of the required functionality and therefore is able to serve as a reference model. This framework is applicable and widely adopted but it has not been addressed within the cloud context. It was created at a general level to provide an overview of security requirements in information systems.

Takabi, Joshi and Ahn [10] proposed a comprehensive SecureCloud framework that provides access to the data, but ensures only authorised entities have access to the data. The focus is to understand data protection and resources from a security breach in the cloud that provides shared platforms and services. Generally, a framework for cloud computing environments highlights the security challenges in cloud computing. The framework modules are: access control, policy integration, service management, heterogeneity management, authentication and identity management.

Brock and Goscinski [11] characterise security problems of clouds, evaluate security of current cloud environments, present current security countermeasures, and propose a Cloud Security Framework (CSF). This framework takes into consideration cloud infrastructure protection (access controls), communication and storage security

(encryption to handle active and passive attacks), authentication, and authorisation (only authenticated users can be provided with cloud services).

Zissis and Lekkas [5] recommended user-specific security requirements for end clients (a person or organisation who subscribes to a service offered by a cloud provider and is accountable for its use). A security requirement should have these six criteria: access control, communication protection, data protection from exposure (remnants), privacy in multitenant environment, service availability and software security [5]. All of these criteria are closely related to important security aspects; confidentiality, integrity and availability. Thus, the requirement is used as a building block in designing secure information systems.

Mapp et al [12] suggested a Security Framework using Capabilities that are required to provide the operational flexibility needed in cloud environments. The proposed functions in this framework are developed into mechanisms using a capability-based approach. The development is implemented for an eHealth system to monitor patients. The framework describes five layers: user, application, hypervisor, transport and storage and the method that happens in each layer. However, the framework is described as a process and does not specify security requirements for a cloud storage in general.

Table 1. Summary of security requirements from existing studies

Author / Requirement	Firesmith (2004) [9]	Takabi, Joshi & Ahn (2010) [10]	Brock & Goscinski (2010) [11]	Zissis & Lekkas (2012) [5]	Mapp et al. (2014) [12]
Confidentiality	√	√			
Integrity	√				√
Availability	√	√	√	√	√
Non-repudiation	√				
Authenticity			√	√	√
Reliability			√	√	√

2.2. International and Industry Standards, Best Practice, and Guidelines

The interest in cloud computing has led an explicit and constant effort to assess the latest trends in security [13]. The interest in cloud computing has led an explicit and constant effort to assess the latest trends in security [13]. Effective governance in cloud computing environments follows from well-developed information security processes as part of the organisation's obligations [6], [14]. In this section, IT industry standards in relation to promoting security are reviewed.

When the cloud was first introduced, a non-profit organisation Cloud Security Alliance (CSA) developed cloud security best practices. Almost all major cloud providers (including Amazon, Oracle, RedHat, and Salesforce) are members of the CSA. Their efforts include identifying the top threats; CSA conducted a survey of industry experts to compile professional opinion of the vulnerabilities within cloud computing. Their efforts include identifying the top threats. CSA conducted a survey of industry experts to compile professional opinion of the vulnerabilities within cloud computing. In the latest edition, experts have identified data loss and breaches, and insecure APIs as the critical threats to cloud security [6], [15]. A compliance standard called cloud control matrix (CCM) was developed to provide standard security controls that can guide providers and help users in the assessment of the risks associated with a provider [16]. The CCM is specifically designed as a control framework with security concepts aligned to CSA guidance in 13 domains. It also describes the relationship with other industry-accepted security standards, regulations, and controls frameworks (such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP) [16].

The National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems and Organisations (NIST SP 800-53 Revision 4) was created to assist organisations in making the appropriate selection of security controls for information systems by introducing a security control baselines [17]. Security control baselines are used as a starting point for the security control selection process and are chosen based on the security category and associated impact level of information systems determined in accordance with FIPS Publication 199 and FIPS Publication 200 [18]. The baselines address the security needs of a comprehensive and various set of group, and are developed based on several assumptions, including common environmental, operational, and functional considerations. However, the baselines also assume typical threats facing common information systems [17] but not specifically in the context of a cloud or a cloud storage.

The European Network and Information Security Agency (ENISA) has developed an authoritative security reference that listed risks, vulnerabilities, and provides a survey of related research recommendations. It consists of a report and practical guides designed for managing security in the cloud. In the asset management section, security measures are highlighted that CSPs should review user data sensitivity. Providers are recommended to request information from users whether deploying

data in the cloud would require additional security protection if it is deemed as sensitive by users. CSPs are also encouraged to apply appropriate segregation between systems with different classifications [19]. The recommendation is only made in general and then only if there are sensitive data.

The United Kingdom Centre for the Protection of National Infrastructure (CPNI) has also provided critical security controls for cyber defence as baselines of high-priority information security measures and controls [20]. It can be applied across an organisation to improve its cyber defence. The Council on Cybersecurity is coordinating the development of these controls. In their guidelines, controls (and sub-controls) concentrate on technical measures and activities. The main goal is assisting organisations in prioritising efforts to secure against the current and most common attacks. Besides that, comprehensive security should take into account other areas of security; such as policy, organisational structure, and physical security. CPNI has added these in their latest guideline publication [21]. However, this guideline has not discussed cloud security in depth although some recommendation can also be applied in the cloud context.

Table 2. Summary of security requirements from organisations

Organisation / Requirement	CSA (2013) [15]	NIST (2013) [17]	ENISA (2009) [19]	CPNI (2014) [21]	ASD (2014) [24]
Confidentiality	√	√	√	√	√
Integrity	√	√	√	√	√
Availability	√	√	√	√	√
Non-repudiation	√				
Authenticity	√		√	√	√
Reliability			√	√	√

In 2011, the Australian Signals Directorate (ASD) published best practices of 35 strategies to mitigate targeted cyber intrusions [22] but it was simplified into top four mitigation strategies in 2012 [23] focusing on application whitelisting, patching applications and operating systems, using the latest version, and minimising administrative privileges. The strategies are ranked in order of overall effectiveness and are developed based on ASD's analysis of reported security incidents and vulnerabilities. These are derived from ASD security testing and audits on Australian government networks. At the same time, the top four mitigation strategies are expected to effectively help in achieving a defence-in-depth ICT system. The combination of all four strategies, if correctly implemented, will protect an organisation from low to moderately sophisticated intrusion attempts.

Another important manual was published in 2014, the Australian Government Information Security Manual (ISM) which is the standard which governs the security of government ICT systems [24]. It has 15 security aspects including; physical and personnel security, communications security, information technology security, product security, media security, software security, email security, access control, secure administration, network security, cryptography, cross domain security, data transfers and content filtering and working off–site. The ISM comprises three documents targeting different levels within the organisation, making the ISM accessible to more users and promoting information security awareness in Australian government agencies.

3. Analysing Threats in Cloud Storage

Threats analysis techniques are introduced such as DREAD and STRIDE to consider threats and elicit security requirements that mitigates such threats [25]. A threat model allows security designers to accurately estimate the attacker's capabilities. It might be tempting to skip threat modelling and simply extract the system security requirements from industry's best practices or standards. However, these standards merely provide general security guidance.

The common standards almost always need some customisation for the target system and additional requirements need to be defined [26]. In this study, a three step threat modelling is used to identify the threats [26]:

1. Characterising the system,
2. Identifying assets and access points, and
3. Identifying threats.

The threat modelling process targets software applications as cloud storage provides software-as-a-service to users. Characterising the system involves understanding the system components and their interconnections, and creating a system model emphasizing its main characteristics. Then assets and access points of the system are identified. Identifying threats creates a threat profile of a system, describing all the potential attacks that need to be mitigated against or accepted as low risk. Although these three steps of threat modelling process are common to all type of systems, the actual execution steps differ depending on the type of the system. Next, each of these threat modelling steps are elaborated in the context of cloud storage.

4. Threat Modelling

At the start of the threat modelling process, the security designer needs to understand the system in question completely. This entails understanding every component and its interconnections, defining usage scenarios, and identifying assumptions and dependencies.

4.1. Characterising system with cloud storage scenario

A cloud scenario can be modelled with three participants: users, cloud instances, and cloud provider [27]. Every interaction in a cloud scenario can be addressed to two entities of these participant classes. For example, a user requesting a service or a service instance inquiring more storage from the cloud provider in Figure 1 and Figure 2. In the same way, every attack attempt in the cloud scenario can be detailed into a set of interactions within this model.

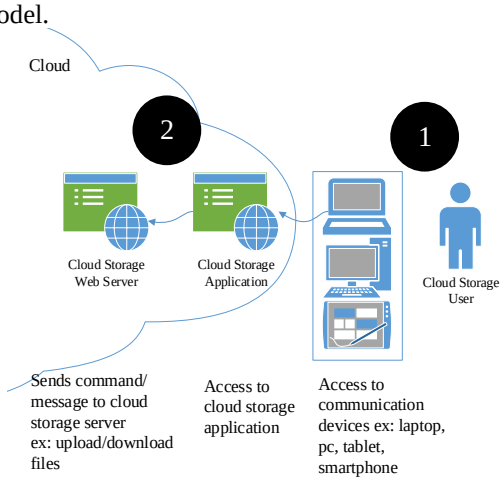

Figure 1. Cloud Storage Scenario (User to Application)

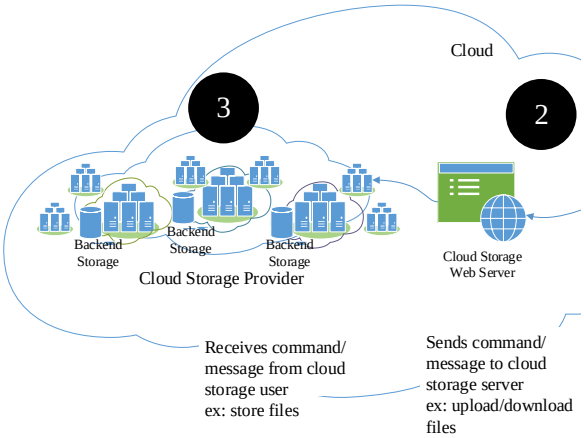

Figure 2. Cloud storage scenario (Application to Provider)

4.2. Identifying system assets and access points

To be more precise, each of the three participant roles provides a specific kind of interface to each other participant class. For instance, the cloud system provides every service instance with a specific interface (API depending on the service model type, IaaS, PaaS, or SaaS) that the service instance can use (i.e. run on).

In the same way, a service instance provides its service to a user with a dedicated interface (e.g. website, SSH connection, Web Service etc.). Thus, with three participants, there are six such interfaces to consider (as shown in Figure 3).

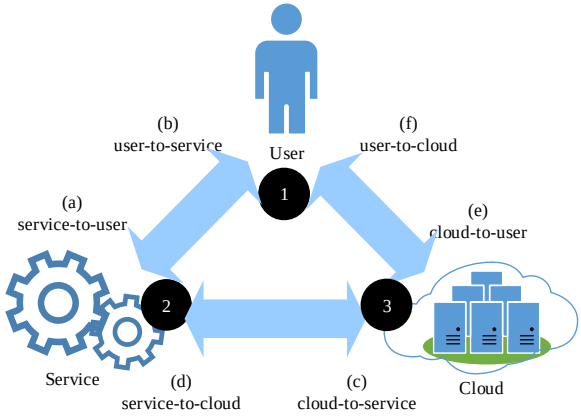

Figure 3. Cloud Computing Triangle Attacks Modified from Gruschka and Jensen [27]

Below are the descriptions involved in the triangle attacks:

(a) Service-to-user
The first and most prominent attack surface is a service instance towards a user (a). The common server-to-client interface is proving to be vulnerable to attacks that are possible in common client-server-architectures. This involves threats like account hijacking from SQL injection or privilege escalation [15].

(b) User-to-service
In the same way, the threats of service user provides towards the service (b) is the common environment a client program provides to a server, for an example, browser-based attacks for an HTML based service like SSL certificate spoofing [28], attacks on browser caches, or Malwares or Phishing attacks [15].

(c) Cloud-to-service
The interface between a service instance and a cloud system is a bit more complex. Here, the separation of service instance and cloud provider can be tricky, but in general the cloud system's attack surface

to the service instance includes all threats that a service instance can run against its hosting cloud system. An example would be resource exhaustion attacks, triggering the cloud provider to provide more resources or end up in a Denial-of-Service, or attacks on the cloud system hypervisor [15].

(d) Service-to-cloud
The other way around, the attack surface of a service instance against the cloud system is a very sensitive one. It incorporates all kinds of attacks a cloud provider can perform against a service running on it. This may start with availability reductions such as shut down service instances. It may also cover privacy related attacks (scanning a service instance's data in process) or even malicious interference (e.g. tampering with data in process, injecting additional operations to service instance executions; rootkit [29]).

(e) Cloud-to-user
The fifth attack surface of interest is that of the cloud system towards the user. This is hard to define since both usually do not have a real contact point; in common scenarios there always exists a service in between. However, the cloud system has to provide an interface for controlling its services. That interface, called cloud control, provides cloud users with the ability to add new services, require more storage, delete data in a cloud storage etc. As this is not a service instance, it is discussed as a separate attack, with threats being merely similar to the ones a common cloud service has to face from a user.

(f) User-to-cloud
The last attack surface is the one provided by a user towards the cloud provider. Considerable attacks may involve phishing-like attempts to trigger a user into manipulating its cloud-provided services, such as presenting the user a fake usage bill of the cloud provider. In general, this involves every kind of attack that targets a user and originates or spoofs to originate at the cloud system.

4.3. Identifying threats

Specific threats related to cloud storage are identified after the previous steps have been completed. Threats may come from either inside or outside the system from authorised users or from others who masquerade as valid users or find ways to bypass security mechanisms [26]. Threats can also come from human errors. The goal of this step is to identify threats to the system from existing studies, published reports, and white papers. A list of known threats and vulnerabilities found in similar systems is often the step to start with threat modelling. System specific threats require deeper analysis of the unique qualities of the system being modelled. The identified threats in cloud storage are identified as [4], [7], [15], [27]–[29]:

- Data breach
- Data leakage and loss
- Insecure APIs
- Account hijacking
- Denial of service
- Malicious insiders
- Abuse of cloud service
- Inadequate cloud planning
- Cloud related malware
- Closure of cloud service
- Natural disaster
- Hardware failure
- Shared technology vulnerabilities
- Insufficient due diligence

5. STRIDE Threat Model

STRIDE is a classification system for describing known threats according to the type of exploits that are used. The STRIDE acronym is formed from the first letter of each of the following categories. In general, threats can be classified into six classes based on their effect [25]:

1. **S**poofing – Using someone else's credentials to gain access to otherwise inaccessible assets.
2. **T**ampering – Changing data to mount an attack.
3. **R**epudiation – A user denying performing an action, but the target of the action has no way to prove otherwise.
4. **I**nformation disclosure – The disclosure of information to a user who does not have permission to see it.
5. **D**enial of service – Reducing the ability of valid users to access resources.
6. **E**levation of privilege – When an unprivileged user gains privileged status

A security requirement can be mapped to security threats showing the effects of each threats to the security objectives a system is acquiring. Fig. 4 shows the security requirement and mapping to threats according to CSA Control Matrix [16]. Reliability was added as an additional requirement and also mapped with relevant threats. STRIDE was used in this study because it fits the output of threat identification. The output of a threat identification process is a threat profile for a system, describing all

the potential attacks, each of which needs to be mitigated or accepted. When defining a threat model, security designers are concerned with defining attacks and also prioritising it [26]. Risk assessment is performed to map each threat either into a mitigation mechanism or priority assumptions. The security requirements for the system can be defined clearly once the threats are identified.

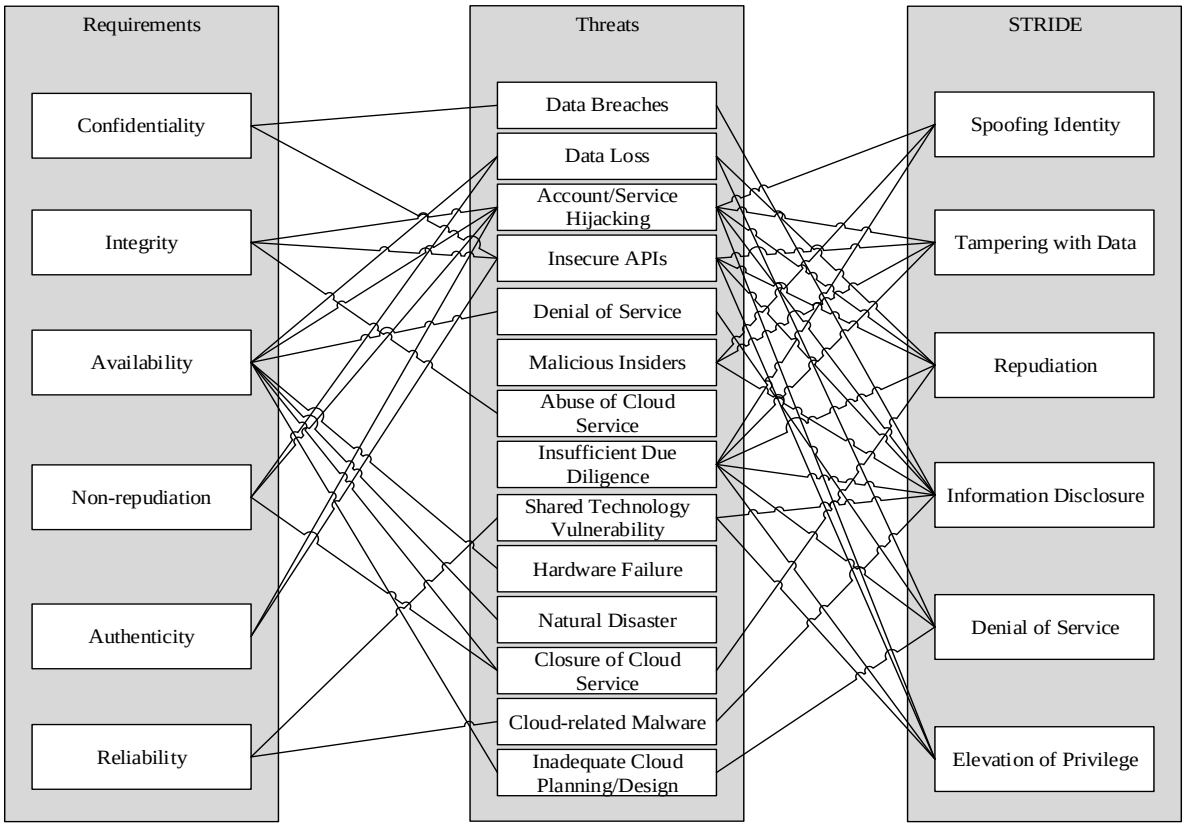

Figure 4. Identified threats mapped with security requirements and STRIDE

6. Conclusion

With the rise of cloud computing, security issues in the cloud have surrounded users, practitioners and providers. With threats to data in the cloud, existing studies were undertaken in the area of cloud security; this involved developing requirements to guide users and CSPs. This has encouraged governing bodies and agencies to publish standards, best practice and guidelines that can be used as references by those adopting cloud computing. CSA in particular has been actively developing guidelines and the CCM is among the important ones that map the controls to other standards protection domains.

Esisting research has shown that organisations and CSPs have implemented many controls to ensure security and data protection. However, some measures involve many controls that most CSPs are reluctant to impose, as it is likely to decrease the efficiency of accessing the cloud. Applying controls based on security requirements and threats is proposed here to protect data efficiently in the cloud.

A threat identification approach is chosen to explore threats in cloud storage. A scenario is used to characterise the system and system specific threats in cloud storage are analysed. Some of the threats identified are data breach, data leakage and loss, insecure APIs, account hijacking, denial of service, malicious insiders, abuse of cloud service, inadequate cloud planning, cloud related malware, closure of cloud service, natural disaster, hardware failure, shared technology vulnerabilities, and insufficient due diligence.

This study discusses threat analysis in the cloud. A risk assessment tool, STRIDE is also used to assess the identified threats. The identified threats are also mapped with security requirements objectives to make emphasis on its importance affecting the security of a system.

7. Acknowledgement

We acknowledge the award of Malaysian Public Service Department Training (HLP) scholarship to Fara Yahya allowing the research to be undertaken.

8. References

[1] Microsoft, "Security Threats," Microsoft Developer Network (MSDN), 2015. [Online]. Available: https://msdn.microsoft.com/en-us/library/cc723507.aspx. [Accessed: 22-Apr-2015].

[2] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," IEEE Netw., vol. 24, no. 4, pp. 19–24, 2010.

[3] F. Sabahi, "Cloud computing security threats and responses," 2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, pp. 245–249, May 2011.

[4] F. B. Shaikh and S. Haider, "Security Threats in Cloud Computing," 6th Int. Conf. Internet Technol. Secur. Trans. Abu Dhabi, UAE, no. December, pp. 11–14, 2011.

[5] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, Mar. 2012.

[6] CSA, "Cloud Computing Vulnerability Incidents : A Statistical Overview Report," Cloud Security Alliance (CSA), 2013. [Online]. Available: https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/. [Accessed: 22-Aug-2014].

[7] GTISC and GTRI, "Emerging Cyber Threats Report 2014," Georgia Tech Information Security Center (GTISC) and Georgia Tech Research Institute (GTRI), Georgia Tech Cyber Security Summit 2013, 2013. [Online]. Available: https://www.gtisc.gatech.edu/pdf/Threats_Report_2014.pdf. [Accessed: 22-Aug-2014].

[8] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc., 2009.

[9] D. Firesmith, "Specifying reusable security requirements," J. Object Technol., vol. 3, no. 1, pp. 61–75, 2004.

[10] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "SecureCloud: Towards a comprehensive security framework for cloud computing environments," in Proceedings - International Computer Software and Applications Conference, 2010, pp. 393–398.

[11] M. Brock and A. Goscinski, "Toward a Framework for Cloud Security," in Lecture Notes in Computer Science, vol. 6082, Springer Berlin Heidelberg, 2010, pp. 254–263.

[12] G. Mapp, M. Aiash, B. Ondiege, and M. Clarke, "Exploring a New Security Framework for Cloud Storage Using Capabilities," Proc. - IEEE 8th Int. Symp. Serv. Oriented Syst. Eng., pp. 484–489, 2014.

[13] P. Honer, "Cloud computing Security Requirements and Solutions: A Systematic Literature Review," 19th Twente Student Conf. IT, Enshede, Netherlands, 2013.

[14] M. K. Srinivasan and P. Rodrigues, "State-of-the-art Cloud Computing Security Taxonomies - A classification of security challenges in the present cloud," in ICACCI '12, 2012, pp. 470–476.

[15] CSA, "The Notorious Nine: Cloud Computing Top Threats in 2013 Report," Cloud Security Alliance (CSA), 2013. [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf. [Accessed: 22-Aug-2014].

[16] CSA, "The Cloud Control Matrix V3.0.1 White Paper," Cloud Security Alliance (CSA), 2013. [Online]. Available: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1. [Accessed: 22-Aug-2014].

[17] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," Natl. Inst. Stand. Technol. Spec. Publ. 800-53 Revis. 4, 2013.

[18] NIST, "Standards for Security Categorization of Federal Information and Information Systems," National Institute of Standards and Technology (NIST) Special Publication FIPS 199, 2004. .

[19] D. Catteddu and G. Hogben, Cloud Computing: Benefits, Risks and Recommendations for Information Security White Paper. European Network and Information Security Agency (ENISA), 2009.

[20] CPNI, "The Critical Security Controls for Effective Cyber Defense V5.0 Report," Centre for the Protection of National Infrastructure (CPNI), 2014. [Online]. Available: http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-critical-security-controls.pdf?epslanguage=en-gb. [Accessed: 22-Aug-2014].

[21] CPNI, "Reducing the Cyber Risk in 10 Critical Areas White Paper," Centre for the Protection of National Infrastructure (CPNI), 2014. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf. [Accessed: 22-Aug-2014].

[22] ASD, "Strategies to Mitigate Targeted Cyber Intrusions - Mitigation Details," Australian Signals Directorate (ASD), 2014. [Online]. Available: www.asd.gov.au/publications/Mitigation_Strategies_2011.pdf. [Accessed: 16-Aug-2014].

[23] ASD, "Top four mitigation strategies to protect your ICT system," Australian Signals Directorate (ASD), 2012. [Online]. Available: http://www.asd.gov.au/publications/protect/Top_4_Mitigations.pdf. [Accessed: 22-Aug-2014].

[24] ASD, "Australian Government Information Security Manual Controls," Australian Signals Directorate (ASD), 2014. [Online]. Available: http://www.asd.gov.au/publications/Information_Security_Manual_2014_Principles.pdf. [Accessed: 12-Oct-2014].

[25] F. Swiderski and W. Snyder, Threat Modeling. Microsoft Press, 2004.

[26] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat Modeling as a Basis for Security Requirements," Proc. 2005 ACM Work. Storage Secur. Surviv. (StorageSS '05), pp. 94–102, 2005.

[27] N. Gruschka and M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services," 2010 IEEE 3rd Int. Conf. Cloud Comput., pp. 276–279, Jul. 2010.

[28] M. Marlinspike, "More Tricks For Defeating SSL In Practice," Black Hat USA, 2009.

[29] D. Brumley, "Invisible Intruders: Rootkits in Practice," Intrusion Detection Special Issue, p. 9, 1999.

