A Review on Cloud Security

Duygu Sinanc
Gazi University
Faculty of Engineering
Department of Computer
Ankara, Turkey
duygusinanc@gazi.edu.tr

Seref Sagiroglu
Gazi University
Faculty of Engineering
Department of Computer
Ankara, Turkey
ss@gazi.edu.tr

ABSTRACT
This article presents a brief overview on cloud computing security in terms of security considerations, models, threats and precautions. The articles published in recent years were classified and they were then analyzed in terms of problems, solutions and challenges. It should be concluded that standards, measurements and metrics for evaluations of threats need to be initially discussed carefully and then applied to the real applications.

Categories and Subject Descriptors
C.2.0 [Computer-Communication Networks]: General - *Security and Protection.*. H.5.3 [Information Interfaces and Presentation]: Group and Organization Interfaces - *Web-based interaction.* K.6.5 [Management of Computing and Information Systems]: Security and Protection.

General Terms
Management, Design, Security, Human Factors, Theory

Keywords
Cloud security and protection, cloud privacy, cloud security models

1. INTRODUCTION
Technology changes our life and expectations. Cloud computing is recent technology to provide new benefits to users, companies and institutions. This is also a new era of future computing. It is a macrostructure distributed computing instance with minimal effort and cost in highly available and dynamically scalable computing resources [4]. Cloud computing allows customers to share data resources dynamically and charged based on usage [12]. This technology raises concerns about security requirements that are interest to customers and needed for cloud providers such as data prevention, web security, location, identity and access management, recovery, data loss prevention, web and e-mail security, security assessments, regulatory compliance, violation management, event management, encryption, data segregation, business continuity and disaster recovery [3,10]. The cloud computing model has three actors: cloud provider presents infrastructure to consumers, service provider uses infrastructure to present applications or services to end users, service consumer uses services on the infrastructure [11].

SIN '13, November 26 - 28 2013, Aksaray, Turkey

http://dx.doi.org/10.1145/2523514.2527013

According to National Institute of Standards and Technology (NIST), cloud model consists of five essential characteristics, three service models, and four deployment models [2,5,6,7,23]. These are summarized below.

Essential characteristics [2]:

1. On demand self service: Consumers can procure computing capabilities as needed automatically.
2. Broad network access: Abilities are available on network.
3. Resource pooling: Different physical and virtual resources dynamically assigned in provider's resource pool according to consumer demand.
4. Rapid elasticity: Abilities can be assigned for consumers in any amount at any time.
5. Measured Service: Both provider and consumer can monitor, control and report resource usage.

Service models [5,6,23]:

1. Software as a Service (SaaS): It is used by consumers to use provider's software and associated data running on a cloud infrastructure. Some examples are; Flickr, Siri, Google Docs, VMWare Cetas, Google BigQuery, Rackspace Hadoop and Windows Azure HDInsight.
2. Platform as a Service (PaaS): Consumer creates applications via this service using tools supported by providers like Force.com, Red Hat OpenShift, Google App Engine, Windows Azure and VMware Cloud Foundry.
3. Infrastructure as a Service (IaaS): Essential computing resources provided to consumers to deploy and run software. Some samples of IaaS solutions from providers are Amazon Web Services, Citrix CloudPlatform, Windows Azure, Microsoft System Center, OpenStack, Rackspace, Savvis and VMware vCloud Suite.

Deployment models [2,7]:

1. Private cloud: This infrastructure supplies exclusive use by a single organization including multiple consumers.
2. Community cloud: It is shared by determined

consumers from organizations that have same interests.
3. Public cloud: This infrastructure is for open use and allows users' access to the cloud via interfaces using web browsers.
4. Hybrid cloud: It is a composition of two or more distinct cloud deployment models.

Many companies provide the cloud computing platform such as Google, Microsoft and Amazon [5]. Google cloud computing system includes GFS (Google File System), MapReduce and BigTable. GFS is a distributed file system, MapReduce is not only a programming mode but also parallel task scheduling model and BigTable is a distributed and large scale storage system for managing structured data. Windows provides Azure operation system to create cloud computing platform. Amazon provides the EC2 (Elastic Compute Cloud) for application hosting and S3 (Simple Storage Service) for data storage.

2. CLOUD SECURITY

For good measure the traditional data and communication security, cloud computing data brings on new security threats and precautions. This are discussed below.

2.1 Availability

Service Level Agreement (SLA) is a trust between provider and consumer to define maximum time for which resources or applications may unavailable for use [26,30,35]. Because this agreement formalizes the relationship between cloud users and cloud service provider, it must arrange very carefully. An ideal way to reduce unavailability of resources because of a breakdown or an attack is to have backup to protect critical information. In this way consumer's information is available offline [1]. Besides, provider should serve monitoring and notification systems to known instant by consumer.

2.2 Integrity

Protecting data from deletion, modification or production without permission is possible with incident response and remediation, fault tolerance, failure recovery and disaster recovery [6]. Furthermore, digital signature is able to data integrity testing and recovers from corruption [19].

2.3 Confidentiality

Claiming confidentiality of users' data, allows for security protocols and proper encryption techniques to be enforced at different layers of cloud applications. Also customers can encrypt their information prior to uploading to cloud [6]. Because confidentiality is correlated to authentication, protecting a user's account is the same as controlling access to cloud objects [25]. In addition, the biometric authentication features may connect to anti theft and identity protection features in cloud security.

2.4 Multi Tenancy

To deliver secure multi tenancy there should be isolation among tenant data as well as location transparency where tenants may not have location of data in order to avoid internal or external attacks [1,37].

2.5 Elasticity

For providers, scaling up and down of consumer's resources gives possibility to other consumers to use previously assigned resources and this may cause confidentiality issues [1]. As a solution of this issue, resources of consumers may place incorporate to avoid other consumers' requests on same resource.

2.6 Privacy

Privacy protection mechanisms must be embedded in all security solutions. For the use of encryption process, to store keys of on only either provider or consumer side enhances security, additively customer can encrypt their information prior to uploading to cloud [1,6]. Cloud presents lots of legal challenges towards privacy issues involved in data stored in multiple locations [4]. Because of the changing legal requirements according to country which is hosting servers, organizations should know where their data at all times [33]. Security management operations should involve all security requirements, feedback from environment, policies and standards like Electronic Communications Privacy Act (ECPA), Statement on Auditing Standards 70 (SAS 70), Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), ISO/IEC 27001 and 27002 Cloud Survey Report [12,19,28].

2.7 Audit

Auditing process contains analyzing authorization and authentication logs to check whether compliances with security standards and policies are guaranteed [6]. Three main attributes should be audited; events, logs and monitoring to provide that there are no security breaches in system [19]. Third party auditor (TPA) verifies integrity of data in cloud on behalf of cloud client and it provides users to ensure the correctness of data [21].

2.8 Trust

In cloud environment trust mostly depends on the selected deployment model according to audit of data and applications are outsourced [6,31]. Organizations must know how to act these situations: how to describe and improve it, how to handle malicious information, how to consider and ensure different security level of service according to the trust degree and how to manage trust degree change with interaction time and context [3,11]. Another situation, Trusted Third Party (TTP) relationships should rely upon for confidentiality, authentication and authorization [4].

2.9 Nonrepudiation

To prevent the issue of denial, cloud provider has to ensure nonrepudiation enabled protocol or handshake is implemented so connected parties cannot dismiss their participation in an argued transaction [2].

2.10 Data Leakage

When moving to a cloud, data will be stored away from the customer's local machine or data is moving from a single tenant to a multi tenant environment [32]. These changes can cause data loss or leakage. For decrease effects of such problem, Data Leakage Prevention (DLP) applications should be used to protect

sensitive data [5]. Moreover, using access controls with strong encryption to consumer data ensures security even if the data is detained.

2.11 Deployment Models

Because of additional charge of ensuring all applications, public clouds are less secure than the other cloud models. Private and community clouds can be more secure than public clouds due to specified internal usage. In addition hybrid clouds provide more control of data and applications security [16,27].

2.12 Service Models

According to NIST cloud model, consumer can have greater security control over more resources as one move from SaaS to PaaS and PaaS to laaS service model [18]. Virtual Machine(VM), VM images, VM boundaries, virtual network and hypervisor security for IaaS security; Service Oriented Architecture (SOA) and Application Programming Interface (API) security for PaaS security; Web application vulnerability and configuration for SaaS security must be procured [12].

2.13 Stakeholders

The importance rises about to enhance consumers' knowledge in cloud computing and awareness of security issues also increase providers' effort to make technologies secure and available [24]. Although, cloud providers cope with assuring long term secure operation, identify and block malicious customers and fight against numerous hackers; consumers confronted downtime of cloud computing environment, leak of commercial secrets and privilege management [9,22]. According to M.D. Ryan's proposed approaches' security level that they provide in descendent order is key translation in the browser, fully homomorphic encryption, CryptDB: a weaker attacker model and hardware anchored security. Additionally, authorities and limits are should be determined with the help of policies [13].

2.14 Attacks

If attacks are identified with existed signatures, Intrusion Prevention Systems (IPS) are effective but if there is legitimate content with bad intentions, they are inadequate [5]. If attackers access to credentials, they can eavesdrop on activities, manipulate data, return changed information and redirect clients to illegal sites [34]. By consuming inordinate amounts of system resources such as processor power, memory, disk space or network bandwidth, attackers cause an intolerable system slowdown. Even worse, since cloud providers bill clients based on their consume, attacker may cause to consume so much processing time that becomes too expensive and clients will be forced to shut down their services. If there is a flaw in one client's application or service, an attacker could access not only that client's data, but every other client's data as well. However, attackers might be able to crack an encryption key in minutes via array of cloud servers instead of using their own limited hardware or they might use cloud to stage other attacks, serve malware or distribute pirated software. So, cryptographic operations which are configured correctly reduce the impact of data breaches. In addition, consumers may implement Host Intrusion Prevention System (HIPS) at endpoints to protect DoS, DDoS, XSS, SQL injection phishing or zombie attacks [2,23].

3. CLOUD SECURITY MODELS

Cloud security models address security issues arising from the evolution of computing and cyber threats for service providers and customers to better structured cloud computing. In this section, some cloud security models discussed and demonstrated in Table I with their plus and minus.

Table 1: Comparison for Cloud Security Models

Name	Reference	Advantages	Disadvantages
ITU Security Model	[8]	Each layer and plane verify and validate end to end security communication	Not fully supporting verification and validation correctly to achieve secure communication
The Cloud Multiple Tenancy Model of NIST	[9]	Allows multiple applications of cloud service providers currently running in a physical server	Difficulties of data isolation, architecture extension, configuration and performance customization
Cloud Cube Model	[9]	To define the security requirements visually cause correct decisions	Accurate categorization is difficult
Sood's Combined Approach	[29]	Provides confidentiality, integrity, authorization, authentication, non-repudiation and prevents data leakage	Procure less security degree in MAC and classification of data process
CCMDSM	[20]	Provides privacy and safety advantages with three layer infrastructure	Block, chunk and matrix structures reduce performance

3.1 ITU Security Model

The International Telecommunications Union's (ITU) Data Networks and Open Communications Security Architecture for Systems Providing End to End Communications present telecommunications architecture as composed of three hierarchical layers which are infrastructure, services and applications [8]. ITU standard specifies that security be fully addressed at each layer with a distinction of processes for planes that exist at each layer which are management, traffic control and end user plane. Security modules targeted at each layer and plane must be designed verified and validated correctly to achieve secure communication.

3.1 The Cloud Multiple-Tenancy Model of NIST

Multiple-tenancy allows multiple applications of cloud service providers currently running in a physical server which partitions and processes different consumer demands with virtualization to offer cloud service for consumers [9]. Although virtualization enables to isolate fault, breach, virus, and malicious applications, this model includes technology difficulties of architecture broadening, data isolation, configuration and performance customization.

3.2 Cloud Cube Model

Cloud Cube Model by Jericho is a figuration description of security with feature of internal/external, proprietary/open,

perimeterised/deperimeterised and insourced/outsourced. If providers define clearly security controls and implements for consumer, consumer knows security requirements visually, correct decisions and outcomes acquired [9].

3.3 Sood's Combined Approach

A framework proposed that consists of different procedures and techniques to protect data by Sood [29]. Confidentiality, availability and integrity parameters for cryptography plus Message Authentication Code (MAC) for checking data integrity is used in this process. The technique provides confidentiality, integrity, authorization, authentication, non-repudiation and prevents data leakage. The security degree that they provide in ascending order is MAC, classification of data and implementation of index and encryption technique.

3.4 CCMDSM

Cloud Computing Multi-dimension Data Security Model (CCMDSM) involves three layers with blocks, chunks and matrix structures [20]. First layer manages users' authentication and permission. Second layer protects users' data via encryption and last layer regenerates data. Notwithstanding its performance, privacy and safety advantages, this solution is not widely accepted.

4. EVALUATION & FUTURE DIRECTION

In recent years, the usage of the cloud computing applications and services are becoming progressively common. As the interactions increases with the cloud, the advantages and disadvantages of the cloud are become more clearly observable. To determine the usage and needs of the cloud computing trends will provide to develop more accurate and efficient researches and the systems. In this article we revised 40 papers to determine research trends in the literature recent years in terms of article types and security issues were considered in this revision. According to the revision about cloud computing security, initially 40 articles were classified as shown in Fig.1. Academics mostly emphasize security challenges (23.14%) and solutions (22.31%). The authors who are prepared survey (9.92%) and offered the model or architecture (10.74%) were found to be approximately equal. Finally 22.31% of papers are focused on security metrics and 14.05% of papers are included security strategies.

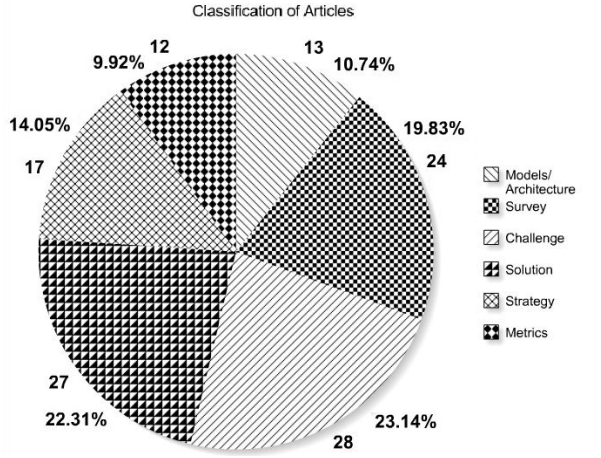

Fig. 1. Classification of articles in the literature last four years

Knowing security threats which are much highlighted in literature make easy to take specific measures and increase security on that subjects. According to the other comparison as seen in Fig.2 often mentioned security problems in descending order are privacy, availability, confidentiality, stakeholders, integrity, attacks, trust, data leakage, service models, multi tenancy, audit, repudiation, elasticity and deployment models. While obtained numerous articles on the cloud security issues in 2009, 2010 and 2011 higher values gained than in 2012 and 2013.

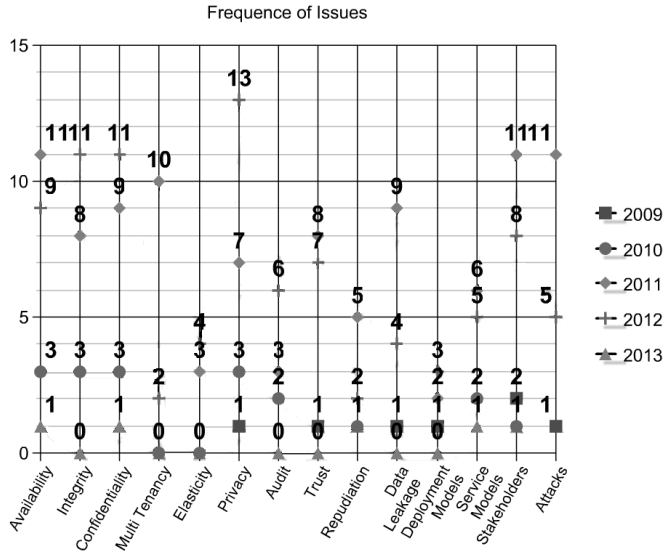

Fig. 2. Cloud security issues frequently examined in the literature

5. CONCLUSION

The cloud computing became a hot topic in industry, academia and government services with the development of technology. In this paper we discussed cloud computing properties, security issues and security models. By focusing more on security, privacy and policies cloud computing can be best applicable information technology solution. The risks and challenges in cloud computing can be easily overcome with making clear agreement between stakeholders and taking precautions before using a cloud computing solution. Finally we analyzed literature in terms of the popular cloud security subjects. Because, knowing cloud users' and reviewers' relevance will ensure to develop more available and manageable cloud security systems.

The articles in the literature about cloud computing security are examined from different perspectives and assumptions or proposed new security models. However, the academic literature and the business environment need to real life implemented applications or systems and their security analysis. As a subsequent work, we plan to compose a more elaborate survey supported by tools.

6. REFERENCES

[1] A. Behl, K.Behl, “An Analysis of The Cloud Computing Security Issues”, Information and Communication Technologies (WICT), Trivandrum, 109-114, 2012

[2] A. Behl, K.Behl, "Security Paradigms for Cloud Computing”, Computational Intelligence, Communication Systems and Networks (CICSyN), Phuket, 200-205, 2012

[3] D.Sun, G. Chang, L. Sun, X. Wang, “Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments”, Procedia Engineering, 15, 2852 – 2856, 2011

[4] D. Zissis, D. Lekkas, “Addressing cloud computing security issues”, Future Generation Computer Systems, 28, 583–592, 2012

[5] F.Sabahi, "Cloud Computing Security Threats and Responses", Communication Software and Networks (ICCSN), Xi'an, 245-249, 2011

[6] H.Tianfield, “Security Issues In Cloud Computing”, IEEE International Conference on Systems, Man, and Cybernetics, COEX, Seoul, 2012

[7] Intel Solution Brief, “Big Data in the Cloud: Converging Technologies”, 2013, Available on: http://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/big-data-cloud-technologies-brief.pdf

[8] J. Bayuk, “Cloud Security Metrics”, System of Systems Engineering (SoSE), Albuquerque, New Mexico, 341-345, 2011

[9] J. Che, Y. Duan, T. Zhang, J. Fan, “Study on the security models and strategies of cloud computing”, Procedia Engineering, 23, 586–593, 2011

[10] L. Badger, T. Grance, R. P.Corner, J. Voas, “Cloud Computing Synopsis and Recommendations”, National Institute of Standards and Technology, 2012, Available on: http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

[11] L. Xiao-hui, S. Xin-fang, “Analysis on Cloud Computing and its Security”, The 8th International Conference on Computer Science & Education (ICCSE 2013), Colombo, Sri Lanka, 839-842, 2013

[12] M.A. Morsy, J.Grundy, I.Müller, “An Analysis of The Cloud Computing Security Problem”, In Proceedings of APSEC Cloud Workshop, Sydney, Australia, 2010

[13] M.D. Ryan, “Cloud computing security: The scientific challenge, and a survey of solutions”, The Journal of Systems and Software, 2013

[14] M.Z. Meetei, A.Goel, “Security Issues in Cloud Computing”, Biomedical Engineering and Informatics (BMEI), Chongqing, China, 1321-1325, 2012

[15] M.Zhou, R.Zhang, W.Xie, W. Qian, A.Zhou, “Security and Privacy in Cloud Computing: A Survey”, Semantics Knowledge and Grid (SKG), Beijing, 105-112, 2010

[16] S. Subashini V. Kaitha, “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications 34, 1–11,2011

[17] S. Ramgovind, M.M. Eloff, E. Smith, “The Management of Security in Cloud Computing”, Information Security for South Africa (ISSA), Sandton, Johannesburg, 1-7, 2010

[18] T. Francis, S.Vadivel, “Cloud Computing Security: Concerns, Strategies and Best Practices”, Cloud Computing Technologies, Applications and Management (ICCCTAM), Dubai, 205-207, 2012

[19] W. Liu, “Research on Cloud Computing Security Problem and Strategy”, Consumer Electronics, Communications and Networks (CECNet), Yichang, 1216-1219, 2012

[20] Z. Xin, L. Song-qing, L. Nai-wen, "Research on Cloud Computing Data Security Model Based on Multi-dimension", Information Technology in Medicine and Education (ITME), Hokodate, Hokkaido, 289-900, 2012

[21] I. Gul, M.H. Islam, “Cloud Computing Security Auditing”, Next Generation Information Technology (ICNIT), Gyeongju, 143-148, 2011

[22] M. Jia, “Cloud Security of Cloud Computing Application”, Control, Automation and Systems Engineering (CASE), Singapore, 1-4, 2011

[23] M. Hamdi, “Security of Cloud Computing, Storage, and Networking”, Collaboration Technologies and Systems (CTS), Denver, 1-5 2012

[24] A. Abuhussein, “Evaluating Security and Privacy in Cloud Computing Services: A Stakeholder's Perspective”, Internet Technology And Secured Transactions, London, 388-395, 2012

[25] A. Bhardwaj, V. Kumar, “Cloud Security Assessment and Identity Management”, Computer and Information Technology (ICCIT), 387 – 392, Dhaka, 2011

[26] F.B. Shaikh, S. Haider, “Security Threats in Cloud Computing”, Internet Technology and Secured Transactions, Abu Dhabi, 214-219, 2011

[27] S. Carlin, K.Curran, “Cloud Computing Security”, International Journal of Ambient Computing and Intelligence, 3(1), 14-19, 2011

[28] S. Sengupta, V. Kaulgud, V. S. Sharma, “Cloud Computing Security - Trends and Research Directions”, Services (SERVICES), Washington, 524 – 531, 2011

[29] S.K. Sood, “A combined approach to ensure data security in cloud computing”, Journal of Network and Computer Applications, 35 (6), 1831-1838, 2012

[30] Y. Demchenko, T.W. Wlodarczyk, W. Ziegler, “Security Infrastructure for On-demand Provisioned Cloud Infrastructure Services”, Cloud Computing Technology and Science, Athens, 255 – 263, 2011

[31] M. Mackay, T. Baker, A.Yasiri, “Security-oriented cloud computing platform for critical infrastructures”, Computer Law & Security Review, 28, 679-686, 2012

[32] A. Tripathi, A. Mishra, “Cloud Computing Security Considerations”, Signal Processing, Communications and Computing (ICSPCC), Xi'an, 1-5, 2011

[33] N.J. King, V.T. Raja, “Protecting the privacy and security of sensitive customer data in the cloud”, Computer Law & Security Review, 28, 308-319, 2012

[34] I. Muttik, C. Barton, “Cloud security technologies”, Information Security Technical Report, 14,1-6, 2009

[35] B.R. Kandukuri, R.V. Paturi, A. Rakshit, “Cloud Security Issues”, Services Computing, Bangalore, 517-520, 2009

[36] P. Prasad, B. Ojha, R. Ranjan, R. Lal, “3 Dimensional Security in Cloud Computing”, Computer Research and Development (ICCRD), Shanghai, 198-201, 2011

[37] A. Behl, “Emerging Security Challenges in Cloud Computing An insight to Cloud security challenges and their mitigation”, Information and Communication Technologies (WICT), Mumbai, 217-222, 2011

[38] K. Karnad, S. Nagenthram, “Cloud Security Can the cloud be secured?”, Internet Technology And Secured Transactions, London, 208-210, 2012

[39] P.G. Dorey, A. Leite, “Commentary: Cloud computing e A security problem or solution ?”, Information Security Technical Report, 16, 89-96, 2011

[40] G. Kulkarni, J. Gambhir, T. Patil, A. Dongare, “A Security Aspects in Cloud Computing”, Software Engineering and Service Science (ICSESS), Beijing, 547-550, 2012