An Overview of the State-of-the-Art of Cloud Computing Cyber-Security

H. Bennasar[1], A. Bendahmane[2], and M. Essaaidi[1](✉)

[1] ENSIAS, Mohammed V University in Rabat, Rabat, Morocco
essaaidi@ieee.org

[2] ENS, Abdelmalek Essaadi University, Tétouan, Morocco

Abstract. We presented an overview of the state-of-the-art of cloud computing security which covers its essential challenges through the main different cyber-security threats, the main different approaches, algorithms and techniques developed to address them, as well as the open problems which define the research directions in this area. The bottom line is that the state of maturity of cloud computing security is very promising and there are many research directions still open and which promise continued improvements of cloud security and privacy.

1 Introduction

Cloud computing is the use of computing resources that are delivered as a service via Internet [1] to provide a secure, and on demand network access to shared pool of configurable resources and different kind of services, such as, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a service (IaaS). During the last decade, there has been an increasing demand and adoption of cloud computing systems, technologies, applications and services. This is owing mainly to the many advantages this technology offers for businesses and organizations such as its high resources elasticity and scalability which provide important savings in terms of investment and manpower. However, Cyber-security is still considered among the most important issues and concerns limiting the widespread adoption of cloud computing. Among the major issues related with Cloud Computing security we can mention data security, intrusions attacks, confidentiality and data integrity Cloud computing provides several advantages allowing to have new business opportunities. However, it also involves potential cyber-security risks and vulnerabilities. For instance, storing data in the cloud may expose them to serious cyber-security attacks. The main objective of this paper is to present an up-to-date overview of cloud computing cyber-security issues. This will allow to identify the major research challenges in this increasingly important area. The remainder of this paper is organized as follows. In Sect. 2 we provide an overview of cloud computing, Sect. 3 is dedicated to the state of the art of cloud computing challenges, the current approaches used to circumvent them and a comparative study of related approaches.

S. El Hajji et al. (Eds.): C2SI 2017, LNCS 10194, pp. 56–67, 2017.
DOI: 10.1007/978-3-319-55589-8_4

2 Cloud Computing

A. Definition
According to the National Institute of Standards and Technology (NIST) [2]: "Cloud Computing is a model for enabling ubiquitous, 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.
B. Cloud Computing Characteristics
The main characteristics and features of Cloud Computing can be summarized in the following:

(1) Multi-Tenancy [3] which refers to having more than one occupants of the cloud, living and sharing other occupants of the provider's infrastructures, including computational resources, storage, services, and applications. By multi-tenancy, clouds provide simultaneous, secure hosting of services for various clients or customers using the same cloud infrastructure resources. It is an exclusive characteristic to resource sharing in clouds.
(2) Elasticity [4] is another important feature of cloud computing and it implies that the user is able to scale up or down resources assigned to services or resources based on the current demand. For providers, scaling up and down of a tenant's resources give a prospect to other tenants to use the tenant previously assigned resources.
(3) Availability of Information based on the Service level Agreement (SLA) [6] which is a trust bond between the cloud provider and the customer. This defines the maximum time for which the network resources or applications may not be available for the customer. Due to the complex nature of the customer demands, a simple measure and trigger process may not work for SLA enforcement.
(4) Multiple Stakeholder in the cloud Computing model means that there are different Stakeholders involved [5], such as the cloud provider (an entity that delivers infrastructures to the cloud's customers), the service provider (an entity that uses the cloud infrastructure to deliver applications/services to end users), and the customer (an entity that uses services hosted in the cloud infrastructure). Each stakeholder has its own security management systems/processes and its own requirements and capabilities distributed from/to other stakeholders.
(5) Third-Party Control [7] which is considered to be the major security challenge, that is, the owner of the data has no control on their processing. The biggest change for Information Technology (IT) department of an organization using cloud computing will be reduced control even as it is being tasked to tolerate increased responsibility for the confidentiality and compliance of computing practices in the organization.

C. Service Models
Cloud Computing offers services that can be grouped into three categories, as shown in Fig. 1

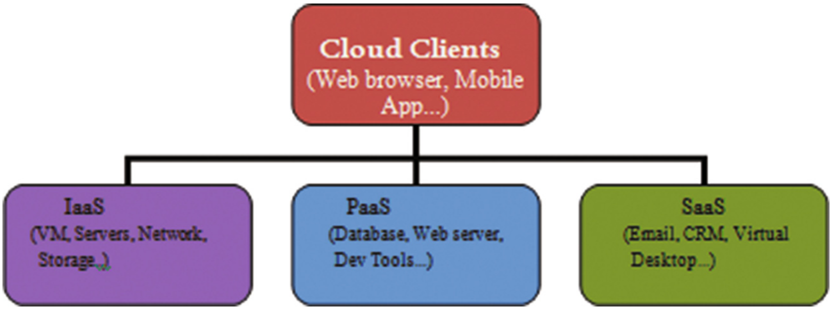

Cloud Clients
(Web browser, Mobile App...)
IaaS
(VM, Servers, Network, Storage...)
PaaS
(Database, Web server, Dev Tools...)
SaaS
(Email, CRM, Virtual Desktop...)

Fig. 1. Cloud computing service model

(1) Infrastructure-as-a-Service (IaaS) [1] through which the cloud providers deliver computation, storage and network resources. In this model, customers do not need to maintain huge servers; they just need to choose their required infrastructure using a web browser and they will be provided with all sorts of hardware infrastructure by the cloud service provider (CSP). As an examples of IaaS vendors, we can cite Citrix, 3tera, VMware, HP, and Dell.

(2) Platform-as-a-service (PaaS) [1] for which Cloud providers deliver platform, tools and business services to develop, deploy and manage their applications. PaaS facilitates the customer organization in developing software applications, without investing huge amounts of money on infrastructure, which will be delivered to the users over Internet on-demand and rent basis (i.e. pay-as-you-use). Web servers, application servers, development environment, and runtime environment are some example components with respect to PaaS. In this model, customers need not maintain underlying infrastructure including servers, cooling, operating systems, storage, etc. As examples of PaaS vendors, we can mention Google AppEngine, force.com, Microsoft Windows.

(3) Software-as-a-Service (SaaS) [1] for which Cloud computing providers offer applications hosted in the cloud infrastructures for application implementation. Example components for SaaS are office suites (docs), online games, email applications, online readers, online movie players, etc. In this model, customers need not maintain heavy investment on system configuration to run all these applications; they just require Internet access and a web browser. Salesforce.com, Amazon, Zoho, Microsoft Dynamics CRM, and Google are some examples of SaaS vendors.

D. Service Deployement

A cloud deployment model means a specific type of cloud computing environment, characterized by several features such as ownership, size, and access mode. As shown in Fig. 2, there are three common cloud deployment models, namely, private cloud, public cloud, and hybrid cloud.

(1) *Private cloud* [1] is for the only use of a single company/organization and its customers. This setup may reside inside or outside the customer's premises.

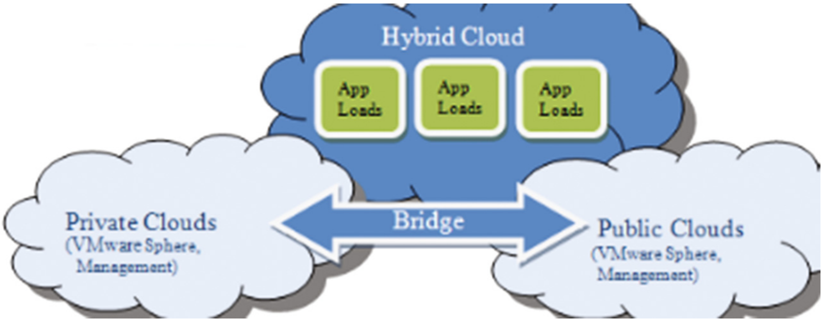


Fig. 2. Cloud computing deployment models

This cloud setup could be controlled, maintained or maneuvered by a third party or the organization itself or a combination of them.

(2) *Public cloud* [1] is for open use by the general public i.e. individuals or organizations. It resides on the premises of the CSP. This cloud setup could be controlled, maintained or maneuvered by different government organizations, corporate organizations, academic institutions or a combination of them to the extent permitted by the CSP.

(3) *Hybrid cloud* [1] is a combination of two or more distinct and unique cloud setups (private, community, or public) which are tied together by standardized or registered technology that ensures and allows data and application portability.

E. Cloud Actors

There are five cloud actors which are concisely explained below.

(1) *Cloud consumer* [8] is a person or an organization that maintains a business relationship with the cloud providers and uses their services.

(2) *Cloud provider* [8] is a person or an organization that is in charge for making a service available to other parties.

(3) *Cloud auditor* [8] is a party that performs independent evaluation of cloud services, information system operations, performance, and security.

(4) *Cloud broker* [8] is an entity that supervises the use, performance, and delivery of cloud services and which negotiates the relationships between cloud providers and cloud consumers.

(5) *Cloud carrier* [8] is an intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers.

3 Cloud Computing Cyber-Security

Cloud computing attracts different users owing to its high resources elasticity and scalability which provide important savings in terms of investment and manpower. Cloud minimizes the need for user involvement by masking technical details such as software upgrades, licenses, and maintenance from its customers. However, the new concepts introduced by cloud computing, such as computation outsourcing, resource sharing, and external data warehousing, increase security and privacy concerns and create new security challenges. This section gives a thorough presentation and discussion of cloud computing cyber-security challenges, a review of security threats, and a comparative study of the latest different approaches and techniques used against them.

A. Cyber-security challenges

(1) *Data Security:* Ensuring data security and privacy in the cloud means the ability to ensure the principle key features of security, namely, confidentiality, integrity and availability. The main requirements for information security is data integrity that refers to the guarantee that users' data are not modified without authorization [10,13], in other words, data can be modified only by authorized users. In order to provide data integrity from both the provider and subscriber perspectives, secure encryption algorithms are generally used. However, encryption alone does not guarantee that data are not maliciously modified [12]. Due to the dynamic, shared and distributed nature of the cloud there is another important challenge for cloud users, namely, confidentiality. This refers to data privacy and accuracy which allows protecting private and sensitive data. To provide data confidentiality, one simple approach consists to save encrypted data in the cloud servers. As regards data availability, it refers to the ability of cloud users to access and use data any time and from anywhere. This means that the cloud system should be accessible and useful to authorized users anytime and anywhere [12,13]. There are several cyber-security threats that may face the cloud services availability. These are network based attacks such as Distributed Denial of Service (DDoS) attacks [10]. To ensure the safety and the availability of data, cloud providers should maintain an appropriate action plan for risk management to deal efficiently with these threats and to guarantee the cloud based services continuity [9].

(2) *Cloud Network Infrastructure Security:* A cloud service provider should be able to accept trustful network traffic, and to block malicious network traffic [9]. The cloud network infrastructure security should be able to block and protect against Denial of Service (DoS) attacks, to detect and prevent intrusions and to allow logging and notification. DoS defenses are based on network security, which should effectively filter queries and identify invaders to prevent malicious attacks [14]. The IDS/IPS systems detect or block known malware attacks, virus signatures and spam signatures but are also subject to false positives. Logging and notification allows cloud users to have some insight into the network's cyber-security health [9].

(3) *Cloud Applications Security:* Businesses and organizations should protect their cloud based applications from all sorts of cyber-security threats. Moreover, cloud applications security is similar to web applications security when hosted in data centers. Many organizations propose single sign on (SSO) as a solution to allow users to access multiple individual cloud services [14].

However, it is hard to implement SSO solutions correctly. In addition, many authentication methods require a secure software layer. To ensure cloud applications (APIs) security, there are different action items proposed in [9], namely:

- A design phase is used to carefully plan how the components of the cloud service will interact. Determine if the APIs can be restricted so that only trusted hosts can call them. Ensure that inter-service communication is securely authenticated.
- Ensure that the tools used are appropriate for APIs and can target the deployed technologies.
- Use testing to validate security monitoring and alerting capabilities. Ensure that any successfully exploited vulnerability was logged and appropriate alerting occurred.

B. Cyber-security threats

In this section, a classification of cloud computing cyber-security threats are detailed. In 2013, cloud security Alliance organized a panel of industry experts in order to present the Nine Cloud Computing Top Threats. Table presents a summary of Cloud security threats, proposed approaches to circumvent them, and a comparison with other approaches.

C. Cloud Cyber-security Techniques

In this section, we are going to make a zoom on some of the cloud cyber-security techniques presented in Table 1 above. These techniques may be classified into three categories:

- Data Integrity
- Authentication & Authorization
- Denial Of Service

Data Integrity (Data Loss & Data Breaches): In Table 1 above, several techniques have been proposed in order to deal with data integrity threats. These techniques use data encryption algorithms to give the data owner verifiable guarantees that their data remain trustful.

(1) Encryption algorithms: Plain RSA, AES, FDE, and Fully Homomorphic encryption (FHE).

(a) *Fully Homomorphic Encryption is* the most widely used encryption technique [22] in the literature. It means that the cloud provider can run the corresponding code a client requests, while not obtaining access neither to the argument data nor to the result data. Homomorphic encryption is an encryption algorithm proposing cloud computing data security scheme based on cloud data security problem. This encryption scheme includes four algorithms, namely, key generation algorithm, encryption algorithm, decryption algorithm and Additional Evaluation algorithm. The main idea behind this encryption scheme is the conversion of data into cipher-text that can be analyzed and worked with as if it were still in its original form [23]. FHE ensures the transmission of data between the cloud and the user safely, while the data stored in the cloud is still protected. However, FHE suffers so far from a problem related with huge computation requirements. This is still an open problem.

(b) *Field Programmable Gate Array (FPGA) [24]:* This is another approach which can also be used to ensure data integrity. FPGA is an integrated circuit designed to be configured by a customer or a designer after manufacturing - hence "field-programmable". J. M. Mondol proved that with the use of FPGA, four different types of solutions are given to ensure user authentication and user data security [25], namely:

- Trusted cloud computing platform ensuring computational trust.
- User enabled security groups for data collaboration.
- Data Security.
- Verifiable Attestation.

All these solutions guarantee that cyber-security is enabled by the Client who is the owner of the data. However, FPGA suffers from huge implementation complexity.

(2) Authentication and Authorization: Account hijacking, malicious intruders, and insecure Applications, are all threats resulting from authentication and authorization problems in cloud computing. *As solutions to these cyber-security threats, we present in* Table 1 *above the approaches and algorithms, such as Message Authentication code (MAC), key-hashed Message Authentication code (HMAC), Federated identity management (FIDM), Kerberos, Transport Layer Security (TLS), Trusted Third Party, Service Level Agreement (SLA) and cloud Security Management Framework. All these solutions could mitigate cloud computing security threats.*

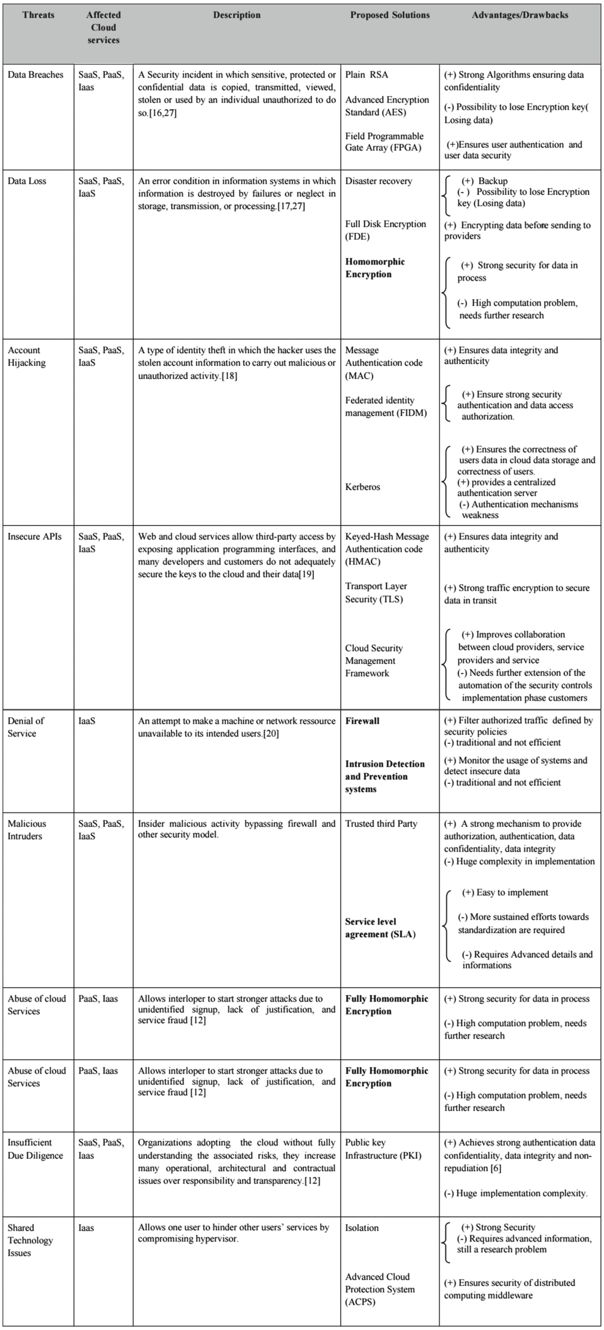
The most widely used approaches, namely, Kerberos and the Service Level Agreement are explained below

(a) *Service Level Agreement (SLA)* [21] is a document that identifies the terms, conditions and it is able to create negotiations between the user and the provider. SLA is characterized by the following features.

- Minimum of performance level that the provider should provide
- Counteractive actions
- Consequences in case of breach of the agreement between user and provider.

The users have to be very obvious about security requirements for their property and all the requirement should be methodically agreed upon in the SLA. In case of doubts, it is harder to declare the defeat at a provider. In order to manage SLAs in a cloud computing environment, references [30,32] suggest

Table 1. Summary of threats to cloud and solution directions



Threats	Affected Cloud services	Description	Proposed Solutions	Advantages/Drawbacks
Data Breaches	SaaS, PaaS, Iaas	A Security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.[16,27]	Plain RSA Advanced Encryption Standard (AES) Field Programmable Gate Array (FPGA)	(+) Strong Algorithms ensuring data confidentiality (-) Possibility to lose Encryption key(Losing data) (+)Ensures user authentication and user data security
Data Loss	SaaS, PaaS, IaaS	An error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing.[17,27]	Disaster recovery Full Disk Encryption (FDE) **Homomorphic Encryption**	(+) Backup (-) Possibility to lose Encryption key (Losing data) (+) Encrypting data before sending to providers (+) Strong security for data in process (-) High computation problem, needs further research
Account Hijacking	SaaS, PaaS, IaaS	A type of identity theft in which the hacker uses the stolen account information to carry out malicious or unauthorized activity.[18]	Message Authentication code (MAC) Federated identity management (FIDM) Kerberos	(+) Ensures data integrity and authenticity (+) Ensure strong security authentication and data access authorization. (+) Ensures the correctness of users data in cloud data storage and correctness of users. (+) provides a centralized authentication server (-) Authentication mechanisms weakness
Insecure APIs	SaaS, PaaS, IaaS	Web and cloud services allow third-party access by exposing application programming interfaces, and many developers and customers do not adequately secure the keys to the cloud and their data[19]	Keyed-Hash Message Authentication code (HMAC) Transport Layer Security (TLS) Cloud Security Management Framework	(+) Ensures data integrity and authenticity (+) Strong traffic encryption to secure data in transit (+) Improves collaboration between cloud providers, service providers and service (-) Needs further extension of the automation of the security controls implementation phase customers
Denial of Service	IaaS	An attempt to make a machine or network ressource unavailable to its intended users.[20]	**Firewall** **Intrusion Detection and Prevention systems**	(+) Filter authorized traffic defined by security policies (-) traditional and not efficient (+) Monitor the usage of systems and detect insecure data (-) traditional and not efficient
Malicious Intruders	SaaS, PaaS, IaaS	Insider malicious activity bypassing firewall and other security model.	Trusted third Party **Service level agreement (SLA)**	(+) A strong mechanism to provide authorization, authentication, data confidentiality, data integrity (-) Huge complexity in implementation (+) Easy to implement (-) More sustained efforts towards standardization are required (-) Requires Advanced details and informations
Abuse of cloud Services	PaaS, Iaas	Allows interloper to start stronger attacks due to unidentified signup, lack of justification, and service fraud [12]	**Fully Homomorphic Encryption**	(+) Strong security for data in process (-) High computation problem, needs further research
Abuse of cloud Services	PaaS, Iaas	Allows interloper to start stronger attacks due to unidentified signup, lack of justification, and service fraud [12]	**Fully Homomorphic Encryption**	(+) Strong security for data in process (-) High computation problem, needs further research
Insufficient Due Diligence	SaaS, PaaS, Iaas	Organizations adopting the cloud without fully understanding the associated risks, they increase many operational, architectural and contractual issues over responsibility and transparency.[12]	Public key Infrastructure (PKI)	(+) Achieves strong authentication data confidentiality, data integrity and non-repudiation [6] (-) Huge implementation complexity.
Shared Technology Issues	Iaas	Allows one user to hinder other users' services by compromising hypervisor.	Isolation Advanced Cloud Protection System (ACPS)	(+) Strong Security (-) Requires advanced information, still a research problem (+) Ensures security of distributed computing middleware

Web Service Level Agreement (WSLA), a very flexible architecture for managing SLAs between providers and users. WSLA is designed to capture service level agreements in a formal way, but it suffers from some computation problems which need more investigations. The other approach used to provide Authentication and Authorization security is Kerberos [28].

(b) *Kerberos* is a computer network protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Cloud data storage security and user's data management in the cloud based upon Kerberos authentication service is proposed in [29]. In order to ensure the correctness of users' data in cloud, data storage and the users who can access the Cloud server, an effective and flexible distributed scheme with explicit dynamic data support, including Kerberos authentication service and third party, was proposed. Kerberos provides a centralized authentication server whose function is to authenticate the user to the cloud server and the cloud server to the user. To access the cloud server, all users should make the profile and set a password, then they can use the cloud server with some restrictions imposed by kerberos.

(3) Denial of Service: There are two main approaches proposed to deal with this cyber-security threat, namely, Firewalls and Intrusion detection Systems (IDPS).

(a) Firewalls [31] are utilized to reject or permit protocols, ports or IP addresses. Since firewalls detect the network packets at the limit of a network, intruders' attacks cannot be detected by traditional firewalls. Only some DoS or Distributed DOS (DDoS) attacks are also too complex to detect using traditional firewalls. For instance, if there is an attack on port 80 (web service), firewalls cannot distinguish good traffic from DoS attack traffic. Another solution is to add in IDS or IPS to the Cloud.
(b) *IDPS* [26,31] provides a real-time intrusion detection method and system. The IDS automatically and dynamically builds user profile data (known as a signature) for each user (or alternatively, a class of users) that can be used to determine normal actions for each user to reduce the occurrence of false alarms and to improve detection. The user profile data (signature) is saved and updated every time the user logs on and off Intrusion Prevention system [31] with the help of IDS, monitors network traffic and system activities to detect possible intrusions and dynamically responds to intrusions by blocking the traffic or quarantine it.
(c) *Intrusion Detection and Prevention Systems [31]:* Having their own strengths and weaknesses, individual IDS and IPS are not able to provide efficient security. It is very effective to use a combination of IDS and IPS, which is called IDPS. Apart from identifying possible intrusions, IDPS stops and reports them to security administrators. Proper configuration and management of IDS and IPS combination can improve Cloud security. NIST explained how intrusion detection and prevention can be used together to

strengthen security, and it also proposed different ways to design, configure, and manage IDPS. However, IDPS drawbacks are still an open problem.

(d) Reputation-Based Voting (RBV) approach [33] for tolerating collusive computing resources in large-scale grid computing systems, which can be seen as a cloud computing service, which is used for business development has a strong potential for other Cloud computing services. To overcome the high overhead and the performance degradation by replication with voting mechanisms in the presence of collusion attacks, the voting method has been improved by combining it with reputation system. The voting decision of the task is generated based on the reputation value of the computing resources that participate in the computation of such task. This approach can provide a lower error rate with better performance in terms of overhead compared to the m-first voting and credibility-based voting techniques. This tolerance scheme for detecting collusive computing resources is more accurate and more reliable. Therefore, this approach can help improve the efficiency of voting-based techniques, to tolerate collusive computing resources, and to increase the security level of cloud computing. However, this approach considers only the case of an attacks model which represents a single group of collusive computing resources distributed in several Virtual Organizations (VOs). Such resources always return the same wrong results with a fixed collusion probability.

4 Conclusions

In this chapter, we presented an overview of the state-of-the-art of cloud computing security which covers its essential challenges through the main different cyber-security threats, the main different approaches, algorithms and techniques developed to address them, as well as the open problems which define the research directions in this area. The bottom line is that the state of maturity of cloud computing security is very promising and there are many research directions still open and which promise continued improvements of cloud security and privacy.

References

1. Armbrust, M., et al.: Above the clouds: a Berkeley view of cloud computing. UC Berkeley Technical Report (2009)
2. Mell, P.: The NIST Definition of Cloud, Reports on Computer Systems Technology, p. 7, September 2011
3. Microsoft multi tenant data architecture. http://msdn.microsoft.com/en-us/library/aa479016.aspx
4. Sosinsky, B.: Cloud Computing Bible (2015)
5. Tianfield, H.: Security issues in cloud computing school of engineering and built environment. Glasgow Caledonian University, United Kingdom (2012)
6. Service Level Agreement and Master Service Agreement. http://www.softlayer.com/sla.html. Accessed 05 Apr 2009

7. Kandukuri, B.R., Ramakrishna Paturi, V., Rakshit, A.: Cloud security issues. In: 2009 IEEE International Conference on Services Computing. Advanced Software Technologies International Institute of Information Technology (2009)
8. Karajeh, H., Maqableh, M., Masa'deh, R.: Security of Cloud Computing Environment (2014)
9. Security for cloud computation: Ten steps to ensure success, version 2, March 2015
10. Rabai, L.B.A., Jouini, M., Aissa, A.B., Mili, A.: A cyber security model in cloud computing environments. J. King Saud Univ. Comput. Inf. Sci. **25**, 63–75 (2013)
11. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Generation Comput. Syst. **21**, 513–592 (2012)
12. Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., Vasilakos, A.V.: Security and privacy for storage and computation in cloud computing. Inf. Sci. **258**(10), 371–386 (2014)
13. Turban, E., King, D.: Electronic Commerce, Global edn. Person, Upper Saddle River (2012)
14. Sullivan, B., Tabet, S.: Practices for Secure Development of Cloud Applications (2013)
15. Scarfone, K., Mell, P.: Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology (2007)
16. Security Breach - Explore the Internet - urlfo.com, dreached while scanning argument. www.urlfo.com/phrase/security-breach
17. Data loss - Wikipedia, the free encyclopedia. en.wikipedia.org/wiki/Data_loss
18. Claburn, T.: Google Study Finds Widespread Account Hijacking, February 2014
19. InsecureAPImplementationT. http://www.darkreading.com/cloud/insecure-api-implementations-threaten-cloud/d/d-id/1137550?
20. Ali, M., Khan, S.U.: Security in cloud computing approaches and solutions (2015)
21. Balachandra, K.R., Ramakrishna, V.P., Rakshit, A.: Cloud security issues. In: Proceedings of the IEEE International Conference on Services Computing, SCC 2009, pp. 517–520 (2009)
22. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: STOC 2009, pp. 169–178. Association for Computing Machinery, New York (2009)
23. Ryan, M.D.: Cloud computing security: the scientific challenge, and a survey of solutions. J. Syst. Softw. **86**, 2263–2268 (2013)
24. http://en.wikipedia.org/wiki/Field-programmable_gate_array
25. Mondol, J.-A.M., IEEE Member: Cloud security using Solutions using FPGA (2012)
26. Leu, F.Y., Lin, J.C., Li, M.C., Yang, C.T., Shih, P.C.: Integrating grid with intrusion detection. In: Proceedings of the 19th International Conference on Advanced Information Networking and Applications, AINA 2005, vol. 1, pp. 304–309 (2005)
27. Lin, D., Squicciarini, A.: Data protection models for service provisioning in the cloud. In: Proceeding of the ACM Symposium on Access Control Models and Technologies, SACMAT 2010 (2010)
28. http://en.wikipedia.org/wiki/Kerberos_(protocol)
29. Hojabri, M., Venkat Rao, K.: Innovation in cloud computing: implementation of Kerberos version5 in cloud computing in order to enhance the security issues
30. Ludwig, H., Keller, A., Dan, A., King, R., Franck, R.: Web Service Level Agreement (WSLA) language specification. IBM Corporation (2003)
31. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., Rajarajan, M.: A survey of intrusion detection techniques in cloud. J. Netw. Comput. Appl. **36**, 42–57 (2013)

32. Patel, P., Ranabahu, A.H., Sheth, A.P.: Service Level Agreement in Cloud Computing (2008)
33. Bendahman, A., Essaaidi, M., El Moussoaui, A.: The effectiveness of reputation-based voting for collusion tolerance in large-scale grids. IEEE Trans. Dependable Secure Comput. **12**(6), 665–674 (2015)