Journal of Intelligent & Fuzzy Systems xx (20xx) x–xx
DOI:10.3233/JIFS-179539
IOS Press

Cloud computing and data security threats taxonomy: A review

Mohammed Farsi[a], Munwar Ali[b,*], Reehan Ali Shah[c], Asif Ali Wagan[d] and Radwan Kharabsheh[e]
[a]*College of Computer Science & Engineering at Yanbu, Taibah University, Yanbu, Saudi Arabia*
[b]*Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan*
[c]*Department of Computer Systems Engineering, Faculty of Engineering, The Islamia University Bahawalpur, Pakistan*
[d]*Department of Computer Science, SMIU, Karachi, Pakistan*
[e]*College of Administrative Sciences, Applied Science University, Bahrain*

Abstract. Cloud computing is considered as a new paradigm shift in distributed computing. Due to its increasing popularity, it has gotten increasing attention in the research community. In the last few years, the usage of cloud computing has increased because of its user-friendly services. However, as the number of users increases in the cloud, the service complexity and new security challenges take place. Data security is one of the major issues, which blocks users from adopting cloud. In this paper, we conducted a detailed literature review divided into two categories i.e. Single/multi-cloud data security issues and data security techniques used to secure the data in cloud virtual environment. We worked hard to find out the limitations of the existing data security solutions. This effort may help the research community to analyze single and multi-cloud in more details.

Keywords: Cloud computing, security threats, physical threats, virtual threats, security solution

1. Introduction

Cloud computing is an emerging area of research and has gotten greater attention in the research communities [1]. According to the National Institute of Science and Technology (NIST), cloud computing is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications and other services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3]. The European Network has also reported it and Information Security Agency (ENISA) that cloud computing provides on-demand services to users based on the distributed and virtualization technologies [2]. In general, cloud computing is a service provider to users through the Internet using virtualization. The infrastructure, services, and resource management of cloud computing are more efficient and powerful than a small and medium level organizations' personal services. Cloud computing increases the income of an organization by reducing software and hardware purchasing, management, implementation, and maintenance cost [2].

Cloud computing is classified into four models, i.e., public, private, community and hybrid clouds as shown in Fig. 1. These modes are also known as cloud deployment models [6]. The public cloud is basically used in a public domain and the private cloud is available for specific organizations [6]. The hybrid is a

[*]Corresponding author. Munwar Ali, Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan. E-mail: mazardari@gmail.com..

ISSN 1064-1246/19/$35.00 © 2019 – IOS Press and the authors. All rights reserved

combination of public and private clouds, whereas the community cloud is for groups of organizations. The cloud paradigm contains three services, i.e., infrastructure, platform, and application. The on-demand services of cloud computing can be obtained on a pay-per-use basis. These cloud services are available at any time and are accessible from anywhere [4], [7] and [8]. These services are well defined with clouds and their features are presented in Fig. 1.

1.1. Software-as-a-Service (SaaS)

The SaaS is a software implementation model also known as a software delivery model based on user-demand. The main SaaS service providers are salesforce.com, 3Tera and IBM Lotus Live [3]. The cloud service providers install and run the number of software in cloud servers and allow the users to access the software available in the cloud database through web browser software. The software is virtualized at the cloud server and can be accessed from anywhere and at any time. The users can customize the software according to their requirements [7].

1.2. Infrastructure-as-a-Service (IaaS)

Basically, the IaaS provides hardware services to users for virtualization, file systems, network resources, data storage and hardware components for rent. Users do not need to purchase the infrastructure such as servers, hardware, and software supporting tools to fulfill their requirements [8]. By that means, the purchasing cost of the infrastructure can be saved by the organization. The IaaS model assists in providing three main services such as Hardware as a Service, Storage as a Service and Database as a Service. The main IaaS service providers are MSSQL Azure, Oracle and Enterprise DB [9].

1.3. Platform-as-a-Service (PaaS)

The PaaS is also a service model that provides a software development environment. The users are

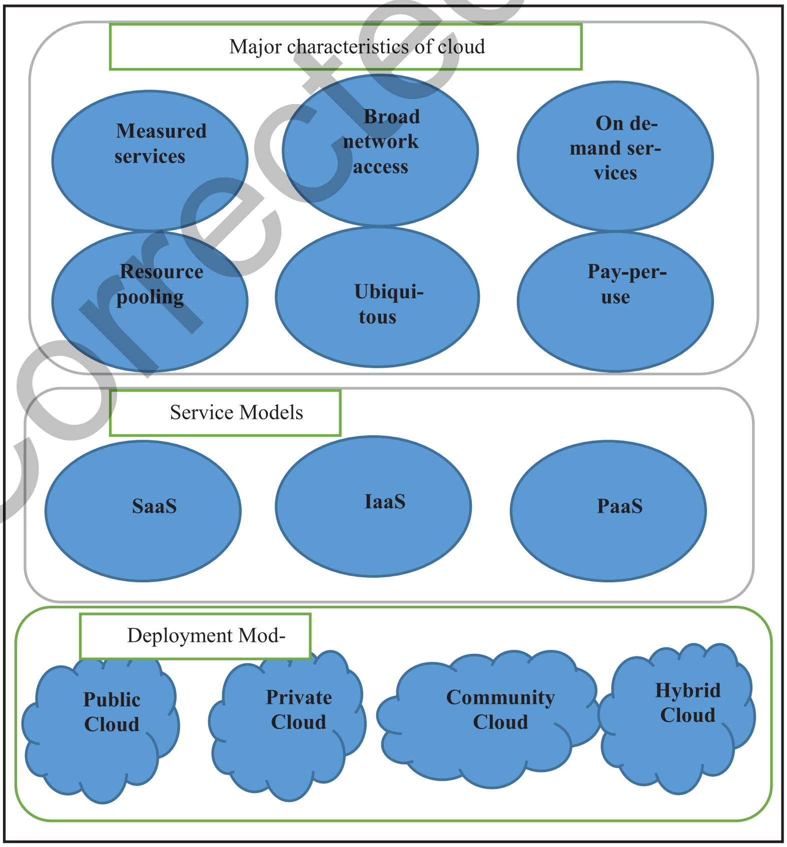

Fig. 1. Cloud models, services and characteristics.

able to deploy their own applications in the cloud servers using Application Programming Interface (APIs) frameworks. Using these facilities, users have full control of their deployed applications in the cloud. The best example of PaaS providers is the Google App Engine which is used to develop software and provides different APIs for software development [9].

The rest of the paper is organized as follows: Part 2 describes data security issues, part 3 is about taxonomy of security issues in cloud, part 4 describes solutions of security issues, and part 5 is the conclusion.

2. Data security issues in cloud computing

Despite the potential benefits of cloud computing, e.g., quick deployment, low cost, pay-per-use, scalability, ubiquitous, and on-demand services [6], it faces a number of challenging issues such as HPC, trust, reliability, efficiency, risk management, and many others. However, data security is one of the major challenging issues in cloud computing. It is still questionable as to how to keep data secure from malicious users. Every cloud deployment model has different levels of data confidentiality; the public cloud has low data confidentiality as compared to other clouds. The private cloud is more secure than the others, but it is more expensive. Obtaining the services of private clouds is difficult to afford for the low and middle-level organizations [10, 11]. The single public cloud suffers from data security, privacy, and availability issues [11]. Therefore, the notion of multi-clouds has been introduced [12, 18]. The multi-clouds provide more substantial security and availability of cloud services than a single cloud. These are also known as inner-clouds or clouds of the cloud. In multi-clouds, the cloud is divided into different clouds where data can be stored in different clouds in form of chunks [3, 12].

2.1. Major data security challenges

Cloud computing provides shared resources on the Internet using virtualization and distributed technology. The data storage service is one of the basic services provided by clouds. All services are openly available for all users. The different organizations and governments of different countries may also store their sensitive information on the cloud. The data can be stored at any location in the world. Instead of storing data in a company's server, the data is stored in a cloud's server which is shared and could be in Asia, Europe or anywhere in the world. Because of the shared centralized place, it is easy for malicious users to access sensitive data. Due to the increasing amount of user's data, security threats also increase [9]. According to the IDC survey, data security threat is rated as 87.5% [30]. The data in a cloud must be secure from insiders, outsiders, and an organization's employees.

2.1.1. Malicious insider

The insider malicious users are those who work in a cloud. The cloud employees can hack sensitive the data of an organization and may also provide access to competitors of the organization [12]. For this threat, the cloud provides only a post-action mechanism which is not acceptable for sensitive data. To avoid malicious insiders, the cloud must provide reliable a solution to the customer and there should be an accountability mechanism to check the activities of the cloud employees.

2.1.2. Malicious outsider

These malicious users are outsider hackers. It is known that different kinds of organizations store data, and also different departments of the USA and the EU are planning to store their sensitive information in clouds [12, 18]; as this environment provides information collectively of different countries and organizations, it may get the attention of outsider malicious users. Still, there is a lot of research required to fix this threat.

2.1.3. Malicious organization employees

Different organizations store data on clouds and may allow their employees to access the data. When different users of the same organization have the right to read and write data in the cloud, then they may edit, delete or hack data and leave the organization without informing the management. So, the employees of the organization must be treated carefully when data is outsourced on a cloud. Moreover, there should also be an accountability mechanism for checking the malicious organization employees' activities.

2.1.4. Data integrity

Data integrity is one of the most critical data security threats. It is easily achievable in a standalone system with a single database. It can be defined as "the data stored remotely or locally can only be changed by an authorized person" [63]. In cloud computing, data is stored remotely and can be stored at different locations. In such an environment, data integrity challenges take place. The data can be changed by malicious users by bypassing the authentication process.

2.1.5. Availability on demand

It is required that the services of a cloud be available twenty-four hours a day when users need them. The cloud must be available at the required time and the system must continue the functionality if there is any security threat or any user is misbehaving. This is a basic demand of the users but still a challenging issue in the cloud. The issue of availability in a single cloud is very critical as compared to the multi-clouds. The availability refers to hardware, software, servers, and other user required information technology services. According to a survey conducted by IDC, the availability-on-demand issue is rated as 83.3% [30].

2.1.6. Data confidentiality

Confidentiality is the protection of data from unauthorized users [33]. Confidentiality threats increase due to the increasing number of users in cloud. When organizations allow multiple users to deal with data, it is difficult to maintain data confidentiality in a cloud [31]. In a cloud, data is outsourced; the user does not know the exact location and also does not have any idea who is accessing his/her data. For achieving data confidentiality, the traditional cryptography is widely used. The use of cryptography only for confidentiality is not enough; the cloud architecture model also plays an important role to enhance the confidentiality of data.

2.1.7. Trust

It is a psychological factor that the foundation of everything is established on trust. Trust is the believing in the security polices and the agreement between the cloud vendor and the user. It is considered that based on trust, both parties shall take care of the agreement [10]. The concept of trust is described as "An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required" [11]. Trust is also one of the main challenging issues in cloud computing. In a cloud, the user only has to trust whatever the cloud vendor says in the agreement. The user's trust becomes weak when the vendor provides insufficient information regarding cloud security.

2.1.8. Privacy

Cloud computing provides services such as SaaS, DaaS, PaaS, IPMaaS, and so on, these services are accessible through Internet connections. The secret information of the user is stored on a cloud, where many data files are stored by different users and all services are managed by the vendor of the cloud [31]. There is a risk of data theft from the cloud by malicious users. These malicious users can be insiders or outsiders and can also be employees of an organization [32]. Every user wants to keep his/her data private from the cloud vendor and unauthorized users.

2.1.9. Data classification

Data classification is not a new technique in the field of information technology. In cloud computing, it is very important to classify the data into different classes in order to know which data need to be secured, because some parts of the data (such as public data) may need only basic security, whereas, bank transaction data needs a high level of security. If this issue is ignored in cloud computing, the user may overvalue or undervalue his/her assets.

2.1.10. Data location

The data is stored in cloud servers which are away from the user's control. And the user does not know the location of the servers where the data is stored. In cloud computing, the data location plays the most basic role for data security because data, applications, and systems are hosted in data centers; these data centers are owned by the cloud computing server (third party). Most data centers are placed in more convenient places to decrease cost. These places can be in different counties and can be operated under the different laws of those countries. So, data security depends on the data location where it is stored. For example, the confidentiality of the accounts in a bank use of the data center located in the United States [33]. To solve this issue, some cloud computing vendors have considered the geographic location as a hosting parameter of the service level agreement with users. Figure 2 shows the major data security threats which need to be fixed to secure the data in cloud virtual environment.

3. Taxonomy of cloud security issues

Cloud security issues are further elaborated below in more details. In this paper except all cloud issues, we focus on only cloud security issues. Cloud security

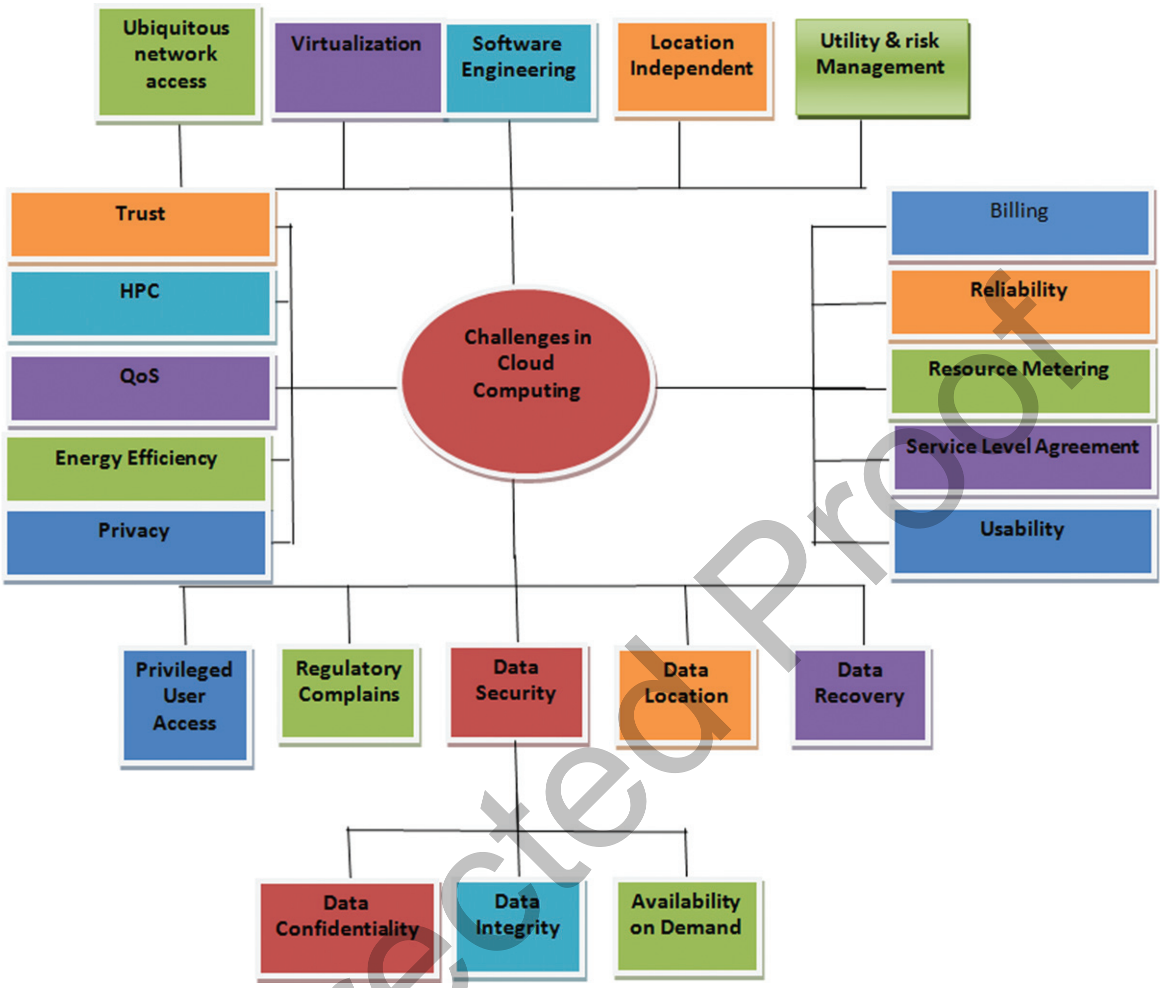

Fig. 2. Challenges in cloud computing.

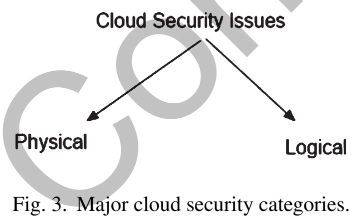

Fig. 3. Major cloud security categories.

issues are further divided into two subcategories i.e., physical and logical as shown in Fig. 3.

3.1. *Physical security issues*

The security threads which are physically associated with clouds are named physical security threats. The major physical security threats are a network security issue, security requirements, reliability, maintainability, environmental issues, physical access, audit and regional threat are shown in Fig. 4. Physical security threat is further divided into subthreats which are mobile platforms, circumference, denial of service, port scanning, dependency, botnets, spoofing attack. And environmental threat can be occurred due to disaster or heat issues.

3.2. *Virtual data security issues*

Majority cloud data security issues fall in this category. The discussion of each virtual data security issue is out of the scope of this paper. These are known as virtual threats because they occur through Internet without any physical interference. These issues are difficult to handle and predict. Almost all solutions are post-active means first threat will happen then it will control the threat. Robust solutions should be a pre-active solution. The pre-active solutions block the

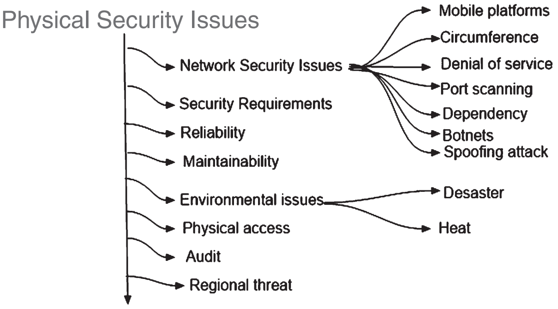

Fig. 4. Physical security issues.

threats. A detailed list of virtual data security issues is given in Fig. 5.

4. Solutions of data security issues

This section is divided into two sub-sections, i.e., cloud computing and data security techniques.

4.1. Multi-cloud as security solutions

In this section, we will discuss multi-cloud data security models. Recently different researchers have proposed many models. The DepSky and Multi-clouds Database (MCDB) models are models focused on in literature review.

4.1.1. DepSky model

The DepSky is a multi-clouds model consisting of four inner-clouds. The focus of this model is the confidentiality and availability of services at the required time. To achieve these objectives, the author designed and developed a model in which he proposed multi-clouds instead of a single cloud. There are three types of parties involved in this model such as writers, readers, and cloud storage service providers. The DepSky-AWrite and DepSky-ARead procedures provide the capability of reading and writing in the model. The DepSky-A algorithm improves the availability and integrity of the stored data using the quorum technique, secret sharing [18]. The DepSky model only works on data storage instead of using IaaS [12]; however, the collection of shared parts of keys stored in different cloud servers may be difficult when one or more cloud servers are not responding due to a technical fault.

4.1.2. Multi-clouds database

The Multi-Clouds Database (MCDB) model uses multi-clouds with a database approach and ensures the security and privacy of the data using a distributed technique using DBMS. The MCDB is an advanced version of the DepSky model, which suggests a database instead of a data storage service of the cloud [12]. The MCDB generates random polynomial functions with the same degree. The polynomial function is applied on both numerical and non-numerical data and it is claimed by the author that the proposed model is different from Amazon's model. In the MCDB model, data is being secured using a technique like a substitution technique which is not secure in the field of cryptography and Shamir's secret sharing is used for the data distribution. However, it is not without its drawbacks; the most common limitation of Shamir's Secret Sharing Scheme is that at the time of the recovery of a few chunks of data, all the secret shares are combined including those which are not

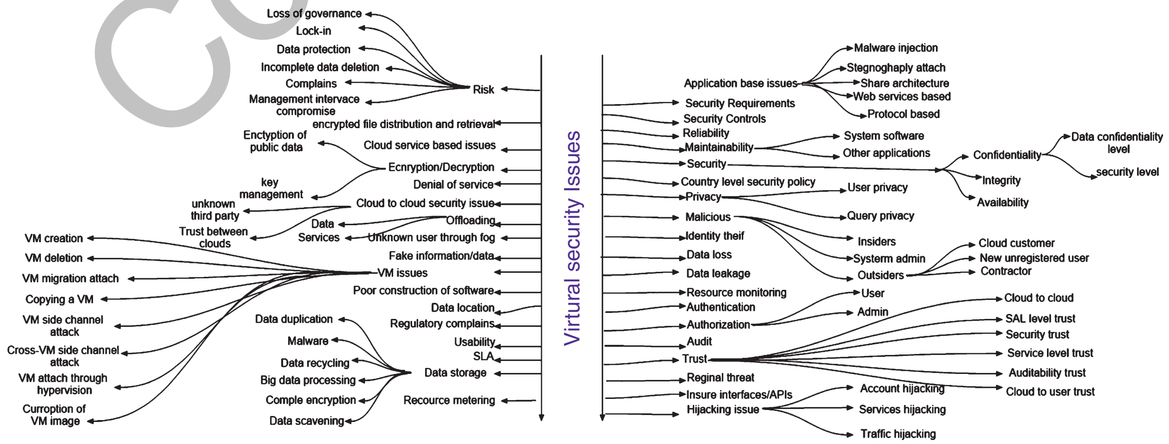

Fig. 5. Virtual security issues.

needed [17]. The MCDB model also does not provide any data encryption technique for security but only a substitution way of data security which is not a technique in the encryption field.

4.1.3. Hybrid multi-cloud data security model

A hybrid cloud model is proposed to secure the data in such a way that public clouds are used for storage purpose and private cloud is used to classify and split data into different chunks based on the classes [34]. A layering technique is used in HMCDS model. The first layer is the "cloud user" layer, the second layer is "cloud management" layer and the third layer is the "database" layer. This HMCDS model provides data security based on the class of the data and improves the process of data retrieval.

4.2. Other security solutions for single/multi-clouds

A standard organization ENISA published a cloud report in 2009 and revised version of that report was published 2012 to show the importance of security in cloud computing. The report "Cloud Computing: Benefits, risks, and recommendations for information security" from ENISA [2], discussed different benefits of cloud services for end-users and eight cloud risks were pointed out which were vital to being fixed [2]. Table 1 shows the detailed and critical summary of literature in the context of security issues and solutions in cloud.

4.2.1. Third-party and encryption based data security

In [10], B. Hayes proposed a new idea of using a third party for security, to keep an eye on the agreement signed between a cloud vendor and a user. If it finds something against the agreement it would inform the cloud vendor and the user. The solution provided by Hayes is an only agreement based but the most serious issues of security, privacy and data control are not solved practically; moreover, a private cloud is unaffordable for small and middle-level organizations. In 2009, the concepts of implicit security and shared key techniques were proposed in [7]. In the implicit technique, the data is partitioned into different chunks and stored in different cloud servers. The shared data can only be reconstructed when all partitions are combined together. Whereas in the shared key technique, data is encrypted by using an encryption technique and stored in a single cloud server; the key itself is divided into different chunks and stored on different servers [7]. This study has the limitations of using a single storage cloud for encrypted data and key distribution. If one of the cloud servers is not available at the required time, then the user cannot collect the distributed key parts stored in that particular cloud.

Another solution for security issues is the crypto co-processor. The crypto co-processor provides security as a service-on-demand [4] and controlled by a third party. The crypto co-processor allows users to select an encryption technique to encrypt the data in such a way that a hacker will not know which security technique is being used. But, it may be considered that the user may not be technically savvy enough regarding the selection of powerful encryption techniques. Moreover, cloud vendors may not allow or trust a third party. In the same year (2011), a new concept of inner-clouds was published by IBM to solve the security issues of a single cloud. The inner-clouds storage model hybridizes a digital signature with hash functions for the authentication and integrity of the data [14]. The key distribution technique is also applied in this model to make the key secure. This technique may lead to a serious key recollection issue when one cloud is not working properly due to a technical fault.

F. Hu conducted another review study on "design challenges in architectures and security". Security can also be enhanced by appending false data into original data and then dividing the data into different chunks and sending the chunks of data to different clouds [21]. This technique is the same as substitution which is considered an insecure technique. To overcome security threats, an integrated security framework is required for data security in cloud computing [6]. Trust is believing in the security policies and agreement between the cloud vendor and the customer. The contracted trust agreement binds the cloud vendor and the customer on the basis of trust. Therefore, they trust each other. The agreement fixes the critical data handling, multiple stakeholders and open space security issues [13]. However, a few studies have suggested that agreement trust only is not enough for a cloud environment which contains a huge amount of data from different organizations. P. Srivastava designed a proactive model for security based on policy. The policy is signed by the cloud vendor and the customer and it is managed by a private cloud, which continuously gives feedback to the cloud vendor and the customer about the policy [10].

In cloud computing, key management is still a challenging issue for cloud vendors and customers. Guojun, Qin, and Wu in their study [22] tried to

Table 1
Summary of cloud computing literature review

Reference	Year	Single cloud	Inner-clouds	Privacy/Security Mechanism/ others	Limitation(s)
[15]	2008	√	X	The idea of a third party and it is responsible to keep a watch over the agreement signed between cloud vendor and user	• Third-party may not be trusted, • Cloud vendors may not want to interact with the third party
[16]	2009	√	X	Dynamic Infrastructure Security Model	• Data storage confidentiality
[7]	2009	√	X	Implicit security by data partitions	• No encryption technique for data confidentiality is used
[2]	2009	√	X	Benefits of cloud and discussed 8 risks in cloud computing	–
[4]	2010	√	X	Third-party, Encryption Technique (based on user selection)	• User does not know about security protocols
[20]	2011	√	X	Hash Tree, (for Block tag Authentication), Bilinear aggregate signature (multi-user setting)	• Third-Party Auditor (TPA)
[13]	2010	√	X	Trust agreement between organization and Cloud	• Only contract-based agreement
[10]	2011	√	X	Hierarchical Attribute-Based Encryption (HABE)	• User traffic increase • Key management issue
[22]	2011	√	X	A pro-active policy-based model is defined	• The user only depends on the security policy of cloud
[23]	2011	√	X	Trusted Cloud model	• Verified & tested only by the numerical value
[6]	2011	√	X	Survey	
[23]	2011	√	X	Double authentication and hybrid obfuscation technique	• Unavailability of services
[25]	2012	√	X	Identified number of security gaps in cloud computing	–
[11]	2012	√	X	Discussed security challenges in public cloud	–
[26]	2012	√	X	Tree-based key management to allow multiple users to access data	• Traffic issue • Confidentiality and privacy issues will increase
[24]	2012	X	X	Full Disk Encryption+Fully Homomorphic Encryption	• Complex & expensive
[14]	2010	X	√	Hashing, signature	• The recollection of shared parts of the key, sometimes one or more servers do not respond
[12]	2011	X	√	Shamir Secret Sharing Algorithm and substitution encryption method	• Appending technique
[18]	2011	X	√	Byzantine, Secret Sharing	• Key distributed on all servers • Data storage in cloud via replication
[19]	2011	√	√	Review	–
[21]	2011	—	—	Review	–
[34]	2013	X	√	Data split into the multi-cloud model	Not practically performed
[35]	2016			Classification of data in to confidential and non-confidential classes	–
[36]	2018			Classification of data using E-KNN to understand the security requirements of the data.	Public data is also encrypted using AES algorithm but public data does not need any security.
[37]	2017	√	X	Secure classification of data by meta-classification	Selection of encryption algorithm is manual.

solve this issue. Every employee of the organization is assigned a key for data decryption. These keys are generated using the Hierarchical Attribute-based encryption (HABE) technique. When multiple users (employees of an organization) are allowed to access the organizational data, then security threats increase in such an environment. These users can change the keys or can be malicious users and the efficiency of the cloud can be affected due to increasing traffic. An efficient cloud storage model was proposed by Wang and tested on numerical values. The model was divided into three layers: a storage layer, basic management layer, and application interface layer [2].

A review study conducted in the context of security observed that recent a study failed to provide security [19]. In 2012, another review study was conducted by M.A. Alzain and Ben Soh. They determined that 74 % of users avoid cloud computing due to security, availability, and the integrity of the data. The multi-clouds with a shared database can be a good approach to avoid these threats [3]. In the same year (2012), the integrated Data Protection as a Service (DPaaS) model was proposed in [24]. The DPaaS model integrates information flow checking, encryption, and application installation in cloud computing using the hybridizing approach of the Full Disk Encryption (FDE) and Fully Homomorphic Encryption (FHME). The computation of the encrypted data is a very difficult task in cloud computing; HME provides computation over outsourced data but it is not practically implementable due to its complexity. So, there is still a lot of research needed on the security of public cloud computing [11].

An extensive survey study was conducted on security gaps in cloud computing. There are many security gaps in a cloud computing environment such as trust, threats, and risks. These gaps are detected by a threat detection model which focuses on attack detection. When an attack occurs it generates information about the attack and sends an alert to the user and the cloud about the threat [25]. However, the model is all about post-active, there is a need for a pre-active model for threats. These threats can also be fixed using a Trusted Third Party (TTP). It provides the certification of communication between cloud services and customers to communicate with each other on a certificate agreement basis [9]. But the question is whether cloud vendors will allow the third party or is third party reliable? Still answers are required for these questions.

Privacy is another main concern in cloud computing because many organizations store their data in clouds and employees of each organization have access rights to the data. In such an environment, damage to privacy and authentication has a greater chance of occurring [26]. The browser software plug-in provides double authentication and obfuscation in cloud computing. For security, the data and keys are stored on separate clouds [23] but these plug-ins do not work when one of the clouds is unable to provide service [23]. According to senior researchers and analysts, the traditional way of authentication must be changed into a new way of authentication [28].

Recently, quantum is also used in security applications. In [38] authors suggested the quantum key distribution cryptography technique to reduce the time using key distribution mechanism. The proposed technique is based Deutsch-Jozsa algorithm which is highly efficient and secure as compare the traditional quantum techniques. In [39] a security scheme is proposed to provide secure communication between one sender and multiple receivers. The proposed scheme is based on traditional symmetric and key distribution principles. The proposed scheme main objective to overcome security issues such as key generation and key distribution in multicast scenario. Similar in [40] author has suggested authentication method for direct communication based on quantum cryptosystem. The proposed authentication method is performed between multiple users and quantum servers where validation is achieved by EPR entangled pairing. This authentication method is performed better under various type of security attack.

4.2.2. Data classification based models

Data security based on classification is a new technique to secure the data in cloud [35]. This technique is confidentiality based data classification using data mining algorithm. The data is classified into confidential and non-confidential classes based on the different data security rules and regulations defined by standard organizations. It practically helps to understand the importance of the data and encrypt only that data which has high confidentiality level and save the confidential data at more secure place in cloud. This process can save processing time and improve the security level by understanding the data. In another study, the data is classified into normal/public, sensitive and high sensitive classes using Enhanced-KNN [36]. Another confidentiality based classification approach is proposed in [37]. This new approach used Naïve Bayes and decision table is combined to make meta classifier. The data was classified into base, confidential and high confidential classes and encryption algorithms are used based on the class of the data. But this approach has limitation in the manual selection of encryption algorithm for the appropriate class.

5. Conclusion

Cloud computing will be a large and complex paradigm in the future. In this paper, we conducted a comprehensive and critical literature review on security threats, cloud models and also security techniques used in cloud computing. We also tried to find out the limitations of the existing work in cloud computing. Detailed data security techniques such as encryption and other techniques (which are used to provide security in the cloud) are critically reviewed by their founder authors papers. This effort may open a new door for research in cloud field.

References

[1] P. Jain, D. Rane and S. Patidar, “A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment,’’ *2011 World Congress on Information and Communication Technologies*, 2011, pp. 456–461.

[2] D. Catteddu and G. Hogben, “Cloud Computing: Benefits, risks and recommendations for information security’’, ENISA, 2009.

[3] M.A. AlZain, E. Pardede, B. Soh and J.a. Thom, “Cloud Computing Security: From Single to Multi-clouds,’’ *2012 45th Hawaii International Conference on System Sciences*, Jan. 2012, pp. 5490–5499.

[4] C.P. Ram and G. Sreenivaasan, “Security as a Service (SasS): Securing user data by coprocessor and distributing the data,’’ *Trendz in Information Sciences & Computing(TISC2010)*, Dec. 2010, pp. 152–155.

[5] R. Choubey, R. Dubey and J. Bhattacharjee, “A Survey on Cloud Computing Security, Challenges and Threats,’’ **3**(3) (2011), 1227–1231.

[6] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,’’ *Journal of Network and Computer Applications* **34**(1) (2011), 1–11.

[7] A. Parakh and S. Kak, “Online data storage using implicit security,’’ *Information Sciences* **179**(19) (2011), 3323–333.

[8] B. Training, “Cloud computing: A records and information management perspective,’’ *IEEE Computer and Reliability Societies*, December 2011.

[9] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,’’ *Future Generation Computer Systems* **28**(3) (2012) 583–592.

[10] P. Srivastava et al., “An architecture based on proactive model for security in cloud computing,’’ *IEEE International Conference on Recent Trends in Information Technology*, 2011, pp. 661–666.

[11] K. Ren, C. Wang and Q. Wang, “Security for the public cloud,’’ *IEEE Internet Computing* **16**(01) (2012) 69–73.

[12] M.a. Alzain, B. Soh and E. Pardede, “MCDB: Using multi-clouds to ensure security in cloud computing,’’ *IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, Dec. 2011, pp. 784–791.

[13] H. Sato, A. Kanai and S. Tanimoto, “A cloud trust model in a security aware cloud,’’ *10th IEEE/IPSJ International Symposium on Applications and the Internet*, 2010, pp. 121–124.

[14] C. Cachin and R. Haas, “Dependable Storage in the Intercloud,’’ *IBM Research Report RZ 3783*, 2010.

[15] B. Hayes, “Cloud Computing’’, *Communications of the ACM* **51**(7) (2008), 9–11.

[16] M. Yildiz, J. Abawajy, T. Ercan and A. Bernoth, “A layered security approach for cloud computing infrastructure,’’ *10th International Symposium on Pervasive Systems, Algorithms, and Networks*, 2009, pp. 763–767.

[17] R. Steinfeld, J. Pieprzyk and H. Wang, “Lattice-Based Threshold-Changeability for Standard Shamir,’’ *Springer Verlag Berlin Heidelberg*, 2004, pp. 1–28.

[18] M. Correia and F. Andr, “D EP S KY: Dependable and Secure Storage in a Cloud-of-Clouds,’’ *6th ACM SIGOPS/EuroSys European Systems Conference*, 2010.

[19] F. Rocha and M. Cerreia, “Lucy in the Sky without Diamonds: Stealing Confidential Data in the cloud,’’, *1st International Workshop on Dependability of Clouds, Data Centres and Virtual Computing Environments, Hong Kong*, 2011.

[20] Q. Wang, S. Member, C. Wang and K. Ren, “Enabling public auditability and data dynamics for storagesecurity in cloud computing,’’ **22**(5) (2011), 847–859.

[21] F. Hu et al., “A Review on Cloud Computing: Design Challenges in Architecture and Security,’’ *JCIT* **19** (2011), 25–55.

[22] G. Wang, Q. Liu, J. Wu and M. Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers,’’ *Computers & Security* **30**(5) (2011), 320–331.

[23] P.V.G.D. Prasadreddy, T.S. Rao and S.P. Venkat, “A threat free architecture for privacy assurance in cloud computing,’’ *IEEE World Congress on Services*, 2011, pp. 564–568.

[24] D. Song, E. Shi, I. Fischer and U. Shankar, “Cloud Data Protection for the Masses,” *IEEE Computer Society*, 2012, pp. 39–45.

[25] M.T. Khorshed, A.B.M.S. Ali and S.a. Wasimi, “A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing,’’ *Future Generation Computer Systems* **28**(6) (2012), 833–851.

[26] M. Zhou, Y. Mu, W. Susilo, J. Yan and L. Dong, “Privacy enhanced data outsourcing in the cloud,’’ *Journal of Network and Computer Applications* **35**(4) (2012), 1367–1373.

[27] F.-C. Cheng and W.-H. Lai, “The impact of cloud computing technology on legal infrastructure within internet—focusing on the protection of information privacy,” *Procedia Engineering* **29** (2012), 241–251.

[28] D.B. Google, M.J. Paypal, S.K. Oneid and S.M. Cigital, “The future of authentication,’’ *IEEE: Computer and Reliability Societies*, 2012.

[29] W. Diffie and M. Hellman, “New directions in cryptography,’’ *IEEE Transactions on Information Theory* **22**(6) (1976), 644–654.

[30] IDC Enterprise Panel. Source: http://www.idc.com/about/about.jsp?t=1341555988277.

[31] M. Ahmed, Y. Xiang and S. Ali, “Above the trust and security in cloud computing: A notion towards innovation,’’ *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, 2010, pp. 723–730.

[32] M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, “Security and privacy in cloud computing: A survey,’’ *2010 Sixth International Conference on Semantics, Knowledge and Grids*, 2010, pp. 105–112.

[33] C. Vecchiola, S. Pandey and R. Buyya, “High-performance cloud computing: A view of scientific applications,” *2009 10th International Symposium on pervasive system algorithm and Networks*, 2000, pp. 4–16.

[34] Munwar Ali Zardari, Low Tang Jung and Muhamed Nording B Zakaria, “Hybrid Multi-cloud Data Security (HMCDS) Model and Data Classification’’, International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2013, pp. 166–171.

[35] Munwar Ali Zardari and Low Tang Jung, “Data security rules/regulations based classification of file data using TsF-kNN algorithm’’, Cluster Computing **19**(1), (2016), 349–368.

[36] Deepika Tripathi and Sudheer Kumar, “A cryptographic approach for information distribution by utilizing E-KNN in cloud environment’’, *International Journal of Research in Engineering, IT and Social Sciences* **08** (2018), 25–34.

[37] Tamanna and Rajeev Kumar, “Secure cloud model using classification and cryptography’’, *International Journal of Computer Applications* **159**(6) (2017), 08–13.

[38] K. Nagata, T. Nakamura and A. Farouk, “Quantum cryptography based on the Deutsch-Jozsa algorithm’’, *International Journal of Theoretical Physics* **56**(9) (2017), 2887–2897.

[39] A. Farouk, M. Rashad, F. Omara and A.A. Megahed, “Architecture of multicast centralized key management scheme using quantum key distribution and classical symmetric encryption’’, *The European Physical Journal Special Topics* **223**(8) (2014), 1711–1728.

[40] A. Farouk, M. Zakaria, A., Megahed and F.A. Omara, “A generalized architecture of quantum secure direct communication for N disjointed users with authentication’’, *Scientific Reports* **5** (2015) 16080.