DOI: https://doi.org/10.24113/ijoscience.v7i8.402

A Review on Security Aspects and Countermeasures for Cloud Computing

Rajat Maheshwari
Department of CSE
India
rajat17.maheshwari@gmail.com

Abstract: **For large-scale companies or people that desire a range of system services at a cheap cost, cloud computing is now the most popular phenomena to use. Personal information is frequently kept in a public cloud that is open to the public. This fundamental raises a number of concerns about cloud providers' flexible services, including confidentiality, persistence, and endurance. The paper aims to better understand cloud components, security concerns, and dangers, as well as developing solutions that might help minimise cloud vulnerabilities. It is a well-known truth that the cloud has been a viable hosting platform since 2008; nevertheless, the view of cloud security is that it requires major changes in order to achieve higher rates of adaptability at the corporate scale. Many of the difficulties affecting cloud computing need to be rectified immediately. The industry has made tremendous progress in combating cloud computing risks, but there is still work to be done to reach the level of maturity that traditional/on-premise hosting has.**

Keywords: Cloud Computing, Security Issues, Privacy, Countermeasures.

I. INTRODUCTION

Each day, everybody is linked one way or another to this digital world and it is the major cause for the rise of IT. The key aspect is the user-friendly atmosphere, accessible from anywhere. The Internet allows a variety of organisations, such as businesses, researchers, students, etc. to finish their job by providing several alternatives to meet their objectives. Many customers access the web and use IT facilities to meet daily needs. When Digital demand increases, the service offered by the Internet, for example through software, platform, database services, storage services etc. Here are the essential phrases Cloud Computing that give its consumers with a large range of services. The basic customer may profit most from utilising this service at reduced costs since it offers 'Pay as you go'. Cloud is a computer system based on the Internet that provides clients, on request, with common resources such as programs, framework, space and data. Cloud Computing is an information exchange environment for hardware, software, programs and business systems. The virtual pool of computer resources is Cloud Computing. It supplies computer resources over the internet in pool users. As an evolving computer architecture, cloud computing seeks to openly share storage, computing and services across enormous users. The protection of user confidentiality is seriously restricted by Current Cloud computing platforms. As confidential user data has been sent to remote systems owned and controlled by third-party service providers in non-encrypted formats, there might be considerable potential for unauthorized user sensitive data exposure by services providers. Many measures are in place to secure users' data from external intruders. Approach to safeguarding the confidentiality of user information from service providers is described and assures that service providers cannot obtain sensitive user information when data is processed and stored in cloud computing systems. Many web- based data storage services and cloud computing platforms offer. Cloud computing has recently gained momentum as a new paradigm of distribution calculation for various applications, particularly for business applications together with the therapy growth of the Internet thanks to its many major benefits, including cost efficiencies and high extensibility. The growth of the "cloud computing" age continues to cause worries about "Internet security." How do "Cloud" clients know that they can share their data and secure and safe information?

Cloud computing offers its customers several advantages but, at the dark side of the computer, it suffers from many problems, including as integrity and storage correction. These problems make it relatively difficult for consumers to adopt the cloud environment. This requires a lot of study to establish confidence in cloud providers by cloud users.

II. OBJECTIVES

- A thorough examination of existing research on cloud computing security problems.
- To comprehend the security danger and to recognise the many security solutions offered by various researchers to minimise it in cloud computing.
- A thorough examination of all current approaches for improving the security and privacy of consumer data housed in cloud computing platforms.

III. LITERATURE SURVEY

There are numerous security mechanism that have been proposed by different researchers. In this section we will provide the literature survey of work done in this field.

Jan de Muijnck-Hughes presented a privacy approach called Transitive Dependent Cryptography in 2011. (PBE). PBE is a type of symmetric cryptography that has its roots in Specific Instance Cryptography [1]. This method combines Public Key Security Controls (ABAC) and encryption algorithm, allowing for the establishment of a new encryptor/multi gameshark atmosphere with a single plan. This Conditional Based Encryption works on both Cloud solution and Host

system implementations. This suggested fix also protects cloud permanent data from undesired access, leaking, and some other privacy violations.

Venkata Sravan and colleagues authored Safety Methods for Managing Data in Cloud in 2011. The goal of this work is to analyse safety issues in Cloud computing and to develop effective data encryption for mitigating them [2]. A total of 43 security issues and 43 security approaches were discovered in the study. Privacy (31%) is the most often tested trait, followed by Fidelity (24%), and Affordability (19%) [2].

In 2011, Ali Asghary Karahroudy published a study called Protection Research and Environment of Cloud Computing with Mostly Distributed Database Based on Parity. This study described a method known as the Mostly Distributed Database with Parity (PDFSP), which really is a mechanism based on the existing GFS/HDFS [3]. Group Policy Unit, User Open Robot, Cloud Management Engine, and Data Return Server are the four basic components of this PDFSP. All of these pieces assure that the data being transferred is not intercepted. Anonymity, Decency, and Allocation were the three aspects of security presented in this report.

In 2013, Nabil Giweli presented the Cloud Based Security strategy, which is a solution-based approach. This technique intends to provide data security by allowing data to self-describe, defend, and protect themselves throughout their lifecycle in cloud environments. This approach places the full burden of setting and managing data privacy and security safeguards on the data owner.This method is based on the Central Limit Theorem (CRT) and employs both symmetrical and asymmetrical data encryption. The suggested technique is shown to be highly efficient in this study since it does not require sophisticated public key methodologies and the file system is not encrypted twice [4].

Miao Zhou suggested five approaches for ensuring data integrity in cloud computing in 2013. Unique forest password control system, Security enhanced cloud data exporting, Protection protected security controls for cloud computing, Privacy enhanced keyword search in clouds, and General populace remote integrity check for personal data are some of the approaches used. This research used a Phrase Finding Mechanism, which makes it more effective multi-user keyword searches while concealing personal information in search queries [5]. To enable flexible and fine-grained access control in the cloud, an encryption technique for a two-tier system has been presented. The suggested technique is efficient, according to the test findings, particularly when the data file is big and the integrity check is performed often [5].

Sudhansu Ranjan Lenka and colleagues published a paper titled "Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm" in 2014. They implemented both the RSA and MD5 algorithms, as the title of the study indicates. The RSA Algorithm is utilised in this work for encrypted transmission and file encryption and decryption, while the MD5 Algorithm is used for digital signature and table protection from unauthorised users [6]. Confidentiality, Integrity, and Availability are the three (3) elements of security provided by the two algorithms described.

In 2014, Aastha Mishra presented a Key Management Scheme for Advanced Secret Sharing. The goal of this work is to offer a more reliable decentralised light weight key management approach for cloud systems that will improve data security and key management [7]. The suggested strategy preserves the security and privacy of user data by replicating key shares across several clouds utilising a secret sharing mechanism and a voting method to verify share integrity. The method proposed in this study also provides improved security against byzantine failure, server collusion, and data alteration attacks [7].

Nesrine Kaaniche published a study in 2014 called Cloud Data Storage Security based on Cryptosystem Mechanisms. ID-Based Cryptography (IBC) and CloudaSec are two (2) approaches presented by Nesrine in this article to protect data. The article proposes using ID-Based Cryptography to employ each client as a secret key creator, generating his own ID-Based Cryptographic Public Elements (IBC-PE). These IBC-PE are used to generate ID-based keys and encrypt data before it is stored and shared in the cloud [8]. CloudaSec enables scalable and flexible implementation of the system, as well as high security guarantees for outsourced data stored on cloud servers [8]. This study examines and explains why cryptographic activities on the client side are acceptable as compared to install operations and do not need extensive computing resources. For example, encoding a data set of 8*105 bytes takes only 0.1 second, but uploading it takes 10 seconds [8]. As a result, the encryption operations consume 1% of the Open - source upload overhead.

In his article Data Confidentiality and Risk Mitigation in Cloud Computing, published in 2014, Afnan Ullah Khan presented a system called as Access Control and Data Confidentiality (ACDC). The goal of the study was to create a new system for enforcing access control regulations in cloud computing environments [9]. He utilised a health emergency to come up with the following compostions: Data Owner (Medical Center), Data Consumers (Patients, Nurses, Doctors, etc.), Information Infrastructure, and Trusted Authority. The paper's deployment paradigm was Infrastructure as a Service, and the suggested technique was utilised to ensure data secrecy and authentication.

Sarojini et al. proposed the Enhanced Mutual Trusted Access Control Algorithm in 2016. (EMTACA). To prevent security concerns in cloud computing, this method establishes mutual trust between cloud consumers and cloud service providers [10]. The goal of this work is to offer a system that includes the EMTACA algorithm to ensure increased confirmed, trusted, and reputation-based cloud services among cloud users [10]. The results of this article revealed that the three most essential aspects of data security, confidentially, quality, and availability, were all met.

Dimitra A. Geogiou published a paper in 2017 outlining security principles for cloud computing. The purpose of safety policies is to safeguard people and information, establish guidelines for expected user behaviour, reduce risks,

and track regulatory compliance [11]. The focus of the paper was on Software as a Service. The study provided a comprehensive overview and analysis of previous studies on cloud computing security. Dimitra concentrated his analysis of current threats on the ones that aren't relevant to traditional systems [11]. A technique for analysing distinct risks in the cloud was presented in order to be able to identify new rules that should be included into the cloud policy. This article examined the security needs of a cloud service provider using a case study of Europe's E-health system as a case study.

Ghallab presented a review article in 2021 that provides a high-level overview of existing data integrity and security problems in the distributed cloud computing environment. The article examined and contrasted eight alternative cloud traceability and security models[12]. It summarises the major schemes of private information public auditing, notably access management, attribute-based access control, and public key encryption, to showcase nearly solutions for some of the existing cloud security issues and difficulties. Furthermore, the study assigned extant data integrity and security models, methods, and techniques in the field of distributed cloud security.

Kanwal I in the year 2021. This article intends to cover all possible issues that have been under research and are opposing customers to move from old IT environment to growing trend of cloud computing which offers secure and dynamic system at low-cost. [13]

IV. Challenges Observed

The following are some of the problems and concerns that were discovered when reading and evaluating the research papers:

- Some of the research papers concentrated their implementation on Platform as a service and Software as a service, leaving Infrastructure as a service behind.
- Other studies focused on data confidentiality without considering integrity, non-repudiation, or authenticity.
- Only a few of the publications were theoretical in nature, implying that no practical implementation was carried out.
- In other studies, the proposed approach appears to be dependable, although it is strange, complex, and difficult to execute.

V. Cloud Services

Cloud offers four service kinds based on the customer needs indicated in the picture below.

Software as a Service (SaaS): Software as a service. Software companies provide various software in software as a service. This improves the use of our workplace in storage. Saas vendor offers the greatest software infrastructure for the industry development, such as software, network spaces and data centers. SaaS examples include:Salesforce.com, Google Apps.

Platform as a Service (PaaS): This is the method software services may be used, accessed, or not installed on local machines for just any client, if its provider or any end-user. Platform as a service (PaaS) For virtualized systems, it offers a high level of platform integration. If users cannot handle networks, servers, OS and data, they choose Platform as a service. Force.com, Google App Engine and Microsoft Azure are some instances of PaaS.

Infrastructure as a Service (IaaS): IAAS is a multi-physical resource network that is shared. IAAS' main objective is to ensure quick access by programs and OS to hosts, storage resources. Therefore, the Application Server is basic on-demand infrastructure (API). In the cloud infrastructure, the client doesn't really require main hardware management but may handle the server, application and OS. Amazon Elastic Cloud Computing (EC2) etc. are some instances of IaaS.

Database as a Service (DaaS): DaaS stores vital document files and other data to users. The facilities for the storage of huge volumes of files that may be mine to retrieve important information are also provided. It is also an important element of these services that share data relating to users such as personally identifiable information, credentials, etc.

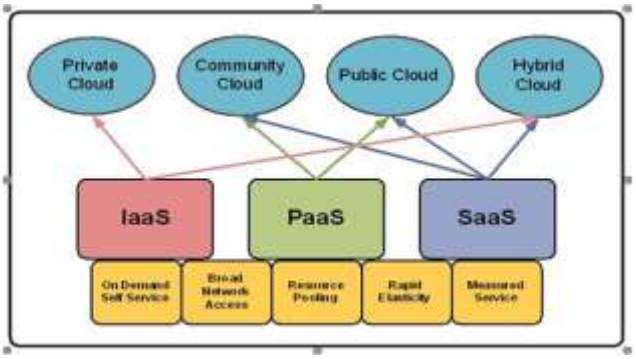

Fig. 1. Cloud service models; IAAS, PAAS and SAAS

VI. Cloud Models

Three models are provided by Cloud: Public cloud that is available to everyone; Private cloud that permits access just to users of that private area; Hybrid cloud that is a compromising task of both public and private cloud services. There are four models of deployment outlined below.

- Private Cloud: This is for each business whose employees utilize it internally. The Cloud infrastructure is often operated by a company itself or might be supported by any third party.
- Public Cloud: the cloud provider provides a platform for wide public access from all over the world who may access it and pay for it.
- Community Cloud: This cloud system is utilized jointly by the many communities in which all members have fair access to this resource.
- Hybrid Cloud: Two or more of the following cloud models offer effective customer services to a mixed infrastructure that can limit several of the technology for the wider population and those certain portions are accessible to everyone for access.

VII. Cloud Service Lifecycle

The Cloud service life cycle comprises the following steps:

- Request Formulation: The user sets the functional and non-functional SLA criteria for the Cloud service sought during the design process.
- Discovery and monitoring: discover candidate's SLA measurement and price information in various data repositories and save them.
- Deployment: Deploys the specified providers' system service elements.
- Matchmakers: Chooses the best clouds for the service to be provided to match the applicant compute and storage resources with the SLA criteria.
- Execution: the process carried out and the state of the service is constantly monitored.
- Completion: At customer choice the service may be ended. (e.g., in the event of SLA infringements offered)

VIII. Security Implications Based On Deployment And Delivery Models

The deployment and delivery models are the two most significant factors that define the amount of risk in a cloud computing platform. There are three deployment and delivery types that are widely used in the business. The security implications of each of these three deployment and delivery strategies are different. Each of these models and their security implications are briefly discussed in the sub-sections that follow.

A. Cloud Deployment Model

The three most common types of cloud deployment models are

Private Cloud : Positive security implications are relatively substantial, and the organisation has great influence over the participation in this study, procedures, and tools. High installation and administration costs, expertise requirements, and vulnerability management are among security issues. Cost and return on investment are major variables in this deployment strategy, and security implementation is generally dependent on risk assessment, thus security coverage is not complete.

Public Cloud: Because of the huge number of cloud customers and transaction volumes involved, there are positive security implications. The cloud service provider often has a sophisticated and layered security system that may possibly provide a high level of security owing to its install once and use numerous times approach, which minimizes the cost of security implementation for the customer. Because the resources are not dedicated but shared among multiple cloud consumers, security risks are increased. This not only adds to the effort of ensuring that all apps and data accessed on the public cloud are secure, but it also requires managing a plethora of external pressures such as legislative, regulatory, and other factors. Data protection etc.

Hybrid Cloud: Positive security implications include the ability to custom-build protection for identified weaknesses, intimidation, and dangers. As a result, it is both cost-effective and focused. Because the deployment architecture is complicated, with a docker container, numerous orchestration, and automation technologies, security issues are rather significant. This will add to the administrative burden, and any oversight will expose the company to substantial risk.

B. Cloud Delivery Model

The three cloud delivery models proposed by NIST and adapted by:

Infrastructure as a Service (IaaS): This is a fantastic concept in which the cloud user creates the application without having to worry about the infrastructure. The cloud service provider and the cloud user share security responsibilities equally. The risk is segmented and stacked in this paradigm. It's also a risk-sharing model.

Platform as a Service (PaaS): This is a suitable paradigm, in which the cloud consumer delivers application knowledge, as well as licenses, data, and facilities, to the platform shell and consumes it. Consumers that lack infrastructure expertise or wish to save money on the significant capital expenditure (capex) necessary to develop infrastructure utilise this approach. The security duty shifts more on the cloud provider in this delivery paradigm. This is a shared risk paradigm, similar to IaaS, except the service provider carries a larger risk than the user because the provider supports more levels.

Software as a Service (SaaS): When a cloud customer lacks the expertise, time, or resources to build up and manage an application ecosystem, this strategy is extremely successful. With minimal upfront capital expenditure, this approach also offers the highest commercial advantage. The cloud provider bears the brunt of the security liability. Client-side weaknesses are mostly the responsibility of the consumer. The service provider is the one who takes the biggest risks in this approach.

C. Vulnerabilities and Open Issues

Cloud is a collection of technology, processes, people, and business models. Cloud, like any other technology, method, person, or business creation, has flaws. The following are some of the cloud's weaknesses. Fig-2 shows some general type of security issues found on cloud computing. The following are some of the concerns and threats that require immediate attention:

Vulnerabilities in Shared Technology - greater resource leverage provides attackers a single point of attack, which can produce harm disproportional to its importance. A virtualization or cloud orchestration are examples of sharing technology.

Data Breach - As data protection moves from the cloud customer to the cloud service provider, the danger of a data

breach, whether unintentional, malicious, or purposeful, is increasing.

Account of Service traffic hijacking - one of the most appealing features of the cloud is Internet access, but this comes with the risk of account breach. Losing access to an advantaged account might result in service interruption.

DoS (Denial of Service) – any denial of service attack on the cloud provider can affect all of the principles.

Malicious Insider – a determined insider can find more ways to attack and cover the track in a cloud scenario.

Many inherent IP vulnerabilities, such as IP spoofing, ARP spoofing, and DNS poisoning, are genuine risks.

Vulnerabilities in the administration layer, such as SQL injection flaws, OS injection, and LDAP injection, can create severe difficulties across numerous cloud users.

Abusive usage - some cloud computing capabilities, such as the use of a trial period of use to conduct zombie or DDoS assaults, can be used for malevolent offensive goals.

Malicious Insider - a malicious insider is always a threat, but a malicious insider at a cloud provider may do considerable damage to a large number of customers.

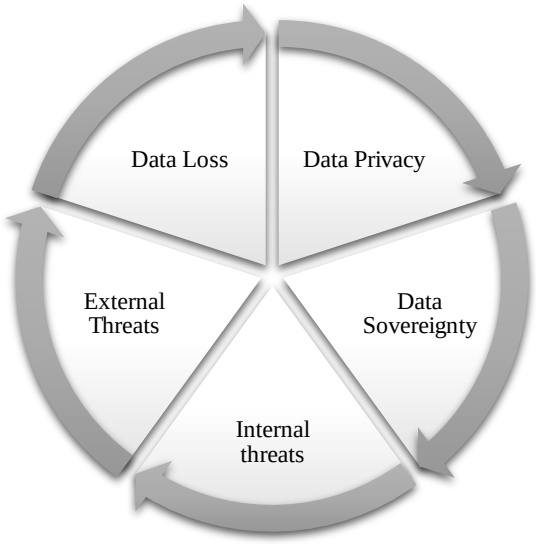

Fig. 2. Security Issues Related to Cloud

D. Counter Measures & Controls

The cloud's weaknesses and dangers are well-documented. Based on their evaluation, each cloud service provider and cloud user must design countermeasures and controls to reduce the risks. However, the following are some of the finest countermeasures and controls techniques to think about:

End-to-finish encryption — because data in a cloud delivery model may travel to several places, it is critical to encrypt the data from beginning to end.

End-to-end encryption, while strongly regarded, introduces new dangers because encryption key cannot be read by a Firewall or IDS. As a result, having adequate controls and countermeasures in place to reduce the risks of harmful software getting via encryption is critical..

Validation of cloud consumers - the cloud provider must take reasonable steps to screen cloud consumers in order to avoid critical cloud functionalities from being used for negative purposes.

Secure Interfaces and APIs — interfaces and APIs are critical for automating, orchestrating, and managing processes. Any vulnerabilities must be addressed by the cloud provider.

Insider assaults - cloud providers should do thorough background checks on employees and contractors, as well as enhance internal security mechanisms, to avoid insider attacks.

In a shared/multi-tenancy architecture, the cloud hosting has secure shared resources such a virtualization, orchestration, and analysis systems.

Business Continuity Plans – A disaster recovery plan is a procedure for documenting an organization's reaction to any occurrences that result in the complete or partial loss of a business-critical strategy.

IX. Conclusion

Cloud computing security is growing in lockstep with dangers, which are sometimes detected too late to avoid catastrophes. Cloud computing poses a unique and serious danger to all parties owing to its disruptive nature, complicated design, and leveraged resources. Understanding the risk and appropriately mitigating it is critical for all stakeholders and actors. To properly reduce the risk, security must be incorporated into every tier of a cloud-computing platform by combining best practices and developing technology. Consumers, providers, brokers, carriers, auditors, and everyone else in the cloud must take the required measures against hazards in order to fully protect the cloud computing platform, or face considerable and sometimes business-critical risk. Security engineering offers quality practices, methodologies, and techniques for building systems and services that are built for security, sustainable development, and resiliency, according to a recent survey. It's critical to continue this study so that best practices may be applied to more applications and use cases. Further study in the systems development life cycle (SDLC) for cloud customers is also required in order to combine diverse development and technological advancement models, as well as container systems like Docker, to increase security at a fundamental level. Furthermore, there is relatively little study on the influence of training and personnel on security. Understanding the problems, requirements, and effects of good security training for customers and other providers may be done.

REFERENCES

[1] Muijnck-Hughes Jan de (2011) Data Protection in the Cloud, 12 Jan, 2019 [Online], Available: http://www.ru.nl/ds

[2] Venkata S. et.al (2011) Security Techniques for Protecting Data in Cloud Computing, 12 Jan, 2019 [Online] Available: https://www.bth.se/com
[3] Ali Asghary K. (2011) Security Analysis and Framework of Cloud Computing with Parity-Based Partially Distributed File System, 26, Jan, 2019 [Online] Available; https://www.academia.edu/27767213/security_Analysis_and_Framework_of_cloud_computing_with_Parity_Based_Partially_Distributed_File_System
[4] Nabil Giweli (2013) Enhancing Cloud Computing Security and Privacy, 20, Jan, 2019 [Online]Available:https://www.researchdirect.westernsydney.edu.au/islandora/object/uws%3AI7310/.../view
[5] Zhou Miao (2013) Data Security and Integrity in cloud computing, Doctor of Philosophy thesis, School of Computer Science and Software Engineering, University of Wollongong. http://www.ro.uow.edu.au/thesis/3990
[6] Sudhansu R. L. et.al Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2, Issue 3, June 2014
[7] Aastha Mishra (2014) Data Security in Cloud Computing Based on Advanced Secret Sharing Key Management System, 20 Jan, 2019 [Online] Available: https://www.ethesis.nitrkl.ac.in/5845/1/212CS2110.pdf
[8] Nesrine Kaaniche (2014) Cloud Data Security based on Cryptographic Mechanisms, 26 Jan, 2019 [Online] Available: https://www.tel.archives-ouvertes.fr/tel-01146029/document
[9] Afnan U.K. (2014) Data Confidentiality and Risk Management in Cloud Computing 2 Feb, 2019 [Online] Available: https://www.ethesis.whiterose.ac.uk/13677/1/Thesis_Final_Afnan _27072016_ EngD.pdf
[10] Sarojini G. et.al (2016) Trusted and Reputed Services using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud, 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016). www.sciencedirect.com
[11] Dimitra A. G. (2017) Security Policies for Cloud Computing, 26 Jan, 2019 [Online] Available: https://www.dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11007/Georgiou_Dimitra.pdf
[12] Ghallab A., Saif M.H., Mohsen A. (2021) Data Integrity and Security in Distributed Cloud Computing—A Review. In: Gunjan V.K., Zurada J.M. (eds) Proceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications. Advances in Intelligent Systems and Computing, vol 1245. Springer, Singapore. https://doi.org/10.1007/978-981-15-7234-0_73
[13] Kanwal I., Shafi H., Memon S., Shah M.H. (2021) Cloud Computing Security Challenges: A Review. In: Jahankhani H., Jamal A., Lawson S. (eds) Cybersecurity, Privacy and Freedom Protection in the Connected World. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-68534-8_29
[14] Varghese B, Buyya R (2018) Next generation cloud computing: new trends and research directions. Future Gener Comput Syst 79(September):849–861
[15] Birje MN, Challagidad PS, Goudar RH, Tapale MT (2017) Cloud computing review: concepts, technology, challenges and security. Int J Cloud Comput 6(1):32–57
[16] Li J, Zhang Y, Chen X, Xiang Y (2018) Secure attribute-based data sharing for resource-limited users in cloud computing. Comput Secur 72:1–12