An Exploration on Cloud Computing Security Strategies and Issues

Amrita Raj and Rakesh Kumar

Abstract Cloud computing is revolutionizing many ecosystems by providing organization with computing resources that feature easy connectivity, deployment, automation, and scalability. In the recent past, the attractive features of cloud computing fuel the consolidation of cloud environment in the industry, which has been consequently motivating research on the related technologies by both the academia and industry. Regardless of its advantages, computing paradigm raises security concerns in transition phase, which have subjected several studies. Cloud computing tends to offer scalable on-demand services to the consumer with greater flexibility and lesser infrastructure investment. Since cloud services are delivered using classical network protocols and formats over the Internet, implicit vulnerabilities existing in these protocols as well as threats introduced by newer architectures have raised many security and privacy concerns. In this paper, we have focused on the data security issues found in the cloud computing. In addition to this, we discovered an appropriate solution and a private cloud domain.

Keywords Cloud computing on-demand services · Virtualization · Security · Data security · Threads · Attacks

1 Introduction

In the distributed computing framework implementation, the client has the features of high adaptability and quality [1]. The assets on the demand and the client do not know any information about the place of assets. Client can equip their application and information from an unspecified area. The distributed computing is considered as the valuable difference in data industry as well as a more effective improvement of

A. Raj (✉) · R. Kumar
Department of Computer Science and Engineering (CSE), M.M.M. University of Technology, Gorakhpur, U.P. 273010, India
e-mail: amritaraj4501@gmail.com

R. Kumar
e-mail: rkiitr@gmail.com

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 89,
https://doi.org/10.1007/978-981-15-0146-3_52

data technology for the general society. Most of the cloud computing framework now consists of reliable services which have been sent through information center built on the servers with various levels of virtualization technologies. The cloud computing is the outcome of various factors like conventional computing, communication technology, and business approach [2]. The cloud computing can ensure the information security and client will not secure the information without anyone else's input [3]. So the distributed computing will be the process for storing information in the cloud framework. Numerous organizations support the distributed computing stages, for example, IBM, Amazon, Microsoft, Google, VMware, and EMC which involves its common element that has been done by the cloud computing [4]. In spite of the fact that distributed computing and their advantages are huge, security and protection concerns are the essential obstructions toward their wide appropriation [5].

1.1 Measured Service

Although computing assets are combined and shared by more than one consumer (i.e., multi-tenancy), cloud framework is to utilizing a suitable system for measuring the usage of these assets for required person. The National Institute of Science and Technology (NIST) had defined cloud computing as "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." The services given by the cloud are very striking because of there intrinsic feature present in on-demand service. Due to this feature, the client is required to pay to remunerate for service that they have used [6].

1.2 On-Demand Self-service

Consumer can individually calculate computing skills, such as server time and network storage automatically, if needed, without the need for human communication with all the service providers [7].

1.3 Broad Network Access

Capabilities are accessible over the network and access through the standard component that promotes use by heterogeneous stages (e.g., cell phones, laptops, and PDAs).

1.4 Resource Pooling

In the attempt of using multiplex consumers or virtualization, the cloud service provider is pooled with computing resources; models are dynamically assigned with defibrillators, resources and redistributed the need of user demand. In this way, the motivation to establish a pool-based computing design is contained in the two-impact factor.

1.5 Economics of Scale an Expertise

The outcome of a pool-based model is that the physical computing resources become "invisible" to the customers, who do not normally have the information of controller on the place, formation, and ownership of these resources.

Example: Databases, Central Processing Unit etc. It is easy to access the information as it is stored in the cloud.

1.6 Rapid Elasticity

Computing resources for customers develop fast rather than constant: There is no upfront and agreement because they can increase them as much as they want and leave them after scaling them. Apart from this, the resources provision seems to be infinitely mated for them, and consumption can increase rapidly to complete the time-peak imports [9] (Table 1).

Table 1 Comparison of data processing centers

Parameter	Data processing center		
	Traditional	Virtual	Cloud based
On-demand service	No	No	Yes
Wide network access	Yes	Yes	Yes
Elasticity	No	Yes	Yes
Measured pooling	No	Yes	Yes
Resource pooling	Yes	Yes	Yes

2 Cloud Model Provides Three Types of Services

2.1 Software as a Service

The SaaS provides the customer a platform or application to manage a cloud infrastructure continuously. In general, SaaS allows to use software applications as a service to end users. Example: Google Applications.

2.2 Platform as a Service

It is the ability that has been given to a customer to deploy onto the cloud infrastructure his own applications without the need of installing any platform or tools on the local machine. PaaS states towards providing platform layer resources, in addition to it providing the operating system support and software development frameworks that can be deployed to craft higher-level services [10].

2.3 Infrastructure as a Service

It provides the customer with the ability to plan prepare, storage, network, or different basic computing assets, or all pass the customer to deploy and fast arbitrary, which can include software and applications. Furthermore, it enables the customer to send and run subjective programming, which can incorporate working framework and applications. Consumers have limited authorized over operating systems and applications, storage deployment applications, and potentially selected networking components [8]. Be that as it may, client can deal with his information put away on cloud and applications which he has sent. Gmail and Dropbox are a few uses of distributed computing administrations [11].

3 Attacks on Cloud Computing

3.1 Zombie Attacker

On the Internet, the aggressor challenges to increase the victim by transfer demands from the honest host on the system in this way and these hosts are known as zombie. In the cloud, the demand for virtual machines (VMs) is approachable by every client by the Internet. An aggressor zombie may flow largest multiple calls. Such attacker cloud software helps to improve the performance of the cloud.

In order to serve the large number of requests the cloud becomes overloaded and finally becomed exhausted causing the DoS (Denial of Service) or DDoS (Distributed Denial of Service) to the servers. The results of above becomes adverse as the cloud is not able to serve valid user's request due to the flooded attacker's requests. Thus better authentication and authorization & IDS/IPS can give better protection against such attacks. In case of flooding or zombie attack, the cloud provider provides more computing power to serve the huge number of requests (which includes zombie requests too). Attacker Service can become a lead offs insufficiency of the attack you are not able to do so, you cannot use any information about any service that is used in the search result [12]. With the gadgets, these methods enable an aggressor to screen the simple qualities of intensity supply and interface associations; along these lines, they can be utilized to get to the chip surface straightforwardly, so we can watch, control, and meddle with the gadget. Owing to these truths, employers are extra relying on cloud-based information processing to achieve a large information amount. The employers are ignorant of the strength data processing methods of the cloud-based features and want that the existing network is protected and reliable adequate to inhibit any unapproved approach to the information [8]. This type of attack is DDOS attack. Thus the existing network must be protected & reliable enough to prevent any unapproved accessing of the information [8] (Table 2).

3.2 Man-In-The-Middle Cryptographic Attack

This attack is complete when places himself between two clients. Whenever attackers put themself in the information way, there is the feasibility that they can interrupt changes information [13].

3.3 Side-Channel Attack

These methods enable an aggressor to screen the qualities of intensity supply and interface associations; along these lines, they can be utilized to get to the chip surface straightforwardly, so we can watch, control, and meddle.

3.4 Service Level Agreement

In numerous regards, cloud computing speaks to redistributing of calculation and capacity to outside specialists co-op. Such redistribution has been administered service level agreement (SLA) that indicates least dimensions of execution that the client can anticipate. Although, classically there exists 99.99% system availability per year yet SLA have not covered security aspects such as confidentiality and integrity.

Table 2 Analysis on security problem and solutions directive

Synopsis of threads into cloud and solution instruction			
Threads	Issues	Causes cloud services	Resolution instruction
Modification into economical class	Decline of modify over cloud database infrastructure framework	IaaS, PaaS, or SaaS	Access control or checking framework on offered administrations
Insulting utilization of Cloud computing	The intruder gives the signup or when due to the strong attackers the absence of approval, benefit minimum	PaaS and SaaS	Strong enrollment and verification of comprehensive monitoring of system traffic
Unsafe interfaces and APIS	Poses threads like clear-content validation, transformation to content: advance verification	SaaS, PaaS or IaaS	Establish secure verification as well as provide modify component among coded communication
Malicious insiders	Insider malicious movement debate from firewall and pass around protection model	PaaS, IaaS, or SaaS	Access clarity as security and management system, usage deference broadcasting as well as breath information
Shared technology problem	Allow one client to interface other client's services by compromise hypervisor	IaaS	For solid certification access control component and for managerial task. Inspection and vulnerability as well as structure
Information damage and leakage	Confidentiality information can be removed and modified	IaaS, PaaS, or SaaS	Uses protected APIs encrypting, keys, apply information detention, or substitute policy
Service hijacking	Customer file and service instances cases could thus make another new base for attacker	PaaS, IaaS, and SaaS	Uses security strategies, solid validation mechanism, or movement monitoring

(continued)

Table 2 (continued)

Synopsis of threads into cloud and solution instruction			
Risk profiling	Interior protection strategies, security compliance, structure, solidifying fixing inspecting or log might be ignored	SaaS, IaaS, or PaaS	Uncover incomplete logs, information and infrastructure detail. Use observing and alerting framework for information breaks

In a cloud computing seller market, it is sensible to expect that not all suppliers will be capable, or willing, to give some level of security to their customers.

Besides, a given cloud supplier may offer administrations with differing dimension of security relying upon how much the client will pay for the administration [14].

In spite of the fact that cloud consumer does not command over the fundamental computing assets, they do need to guarantee the assets when purchasers I have related their center business capacities onto their depended cloud. In other words, it is important for client to get provides on service delivery. Normally, these are given through service level agreement (SLA) consulted between suppliers and purchasers. The first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity is the tradeoffs between expressiveness and complicatedness such that they can cover most of the consumer desires and relatively simple to be verified and evaluated. Also the different cloud offerings (IaaS, PaaS, SaaS & DaaS) will certainly need to define different SLA meta-specifications.

This likewise raises various usage issues for the cloud provider. For instance, assets administrator needs to have exact and restored data on the assets use at specific time inside the cloud. By refreshed data, we mean any adjustment subscribed to by. The assets administrator is in continuous assessment and modification for SLA fulfillment. The assets administrator needs to utilize quick useful choice model and streamlining algorithm to do. SLAs cannot be completed when resource requests may be required to be dismissed. All of these need to be done complete "self- service" in the cloud computing. Apart from this, there is a need to consistently include user feedback and evaluation features in advanced SLA evaluation framework [9].

3.5 Application-Level Security

The application level security refers to the usage of software and hardware resources for providing security to the applications such that the attacker is not able to get the unauthorised access to the application and make the desirable changes to its format. Now, some day the attack begins and it tries to access as the trusted user and it easily allows the full access to the attacker and this makes the client suffer. The major reason behind this is; old network level security policies. With the latest technological

progress, it is quite possible to duplicate a trusted user and contaminate the entire data without seeing it. Subsequently, it is important to introduce large amount of security checks to limit these dangers.

Traditional ways to deal with increased security problem have been developed to develop a work-oriented ASIC device that can handle the specific work that provides higher level of security with greater performance. Be that as it may, with application-level dangers being dynamic these shut frameworks have been seen to case back in contrast with the open finished framework.

The abilities of a shut framework and additionally the flexibility of an open finished framework have been consolidated to build up the security stages dependent on Check Point Open Performance Architecture utilizing Quad-Core Intel Xeon processors. Indeed, even in the virtual condition, organizations like VMware and so forth are utilizing Intel Virtualization Technology for better execution and security base. It has been seen that all the more frequently sites are anchored at the system level and have solid safety efforts; however, there might be security provisos at the application level which may permit data access to unapproved clients. The dangers to application-level security incorporate XSS assaults, cookie poisoning, hidden field control, SQL infusion assaults, DoS assaults, backdoor and debug options, CAPTCHA breaking, and so forth coming about because of the unapproved utilization of the applications [12].

3.6 Data Security

Data Security is the prime concern for any technology, but it still remains as a major challenge when SaaS users have to depend upon their providers for proper security [15].

The organisational data is often processed in plaintext & stored in the cloud in SaaS. Moreover the data backup becomes a prime topmost aspect in order to carry out recovery in case of any disaster but this imparts security questions as well [16]. Rotating administration applications & databases having sensitive data about the Cloud Service Provider (CSP) which have no controller of their own information have various weaknesses [17]. Numerous clients have weaknesses in the information security model and this increases an unauthorized access to information. The following valuations validate the security of the enterprise that collects the information at the SaaS vendor [15]:

- Cross-site scripting [XSS].
- Access control weaknesses.
- OS and SQL injection flaws.
- Cross-site request forgery [CSRF].
- Cookie manipulation.
- Hidden field manipulation.
- Insecure storage.

- Insecure configuration.

In SaaS, organizational information is often managed in plaintext and stored in the cloud. The SaaS supplier is responsible for the security of the information in the way it is processed and stored. Additionally, data backup is very important feature for ceasing the recovery cause of disaster; however, it brings security burden as well [16].

3.7 Security Concerns with the Hypervisor

Distributed computing lays essentially on the idea of virtualization. In a virtualized world, the hypervisor is characterized as a controller prominently known as virtual machine director (VMM) that enables various working systems to be kept running on a system at any given moment, giving the assets to each working system to such an extent that they do not meddle with each other. As the digit of operating systems going on the hardware unit increases, however, the problem of security increases, the need to consider the new operating system. Since different working frameworks would keep running on a solitary equipment stage, it is beyond the realm of imagination to expect to monitor all, and consequently, keeping all the working frameworks secure is troublesome. It might happen that a visitor framework attempts to path a malignant encryption on the feaster framework and fetch the framework low or take complete control of the framework and square access to other company working frameworks.

It cannot be denied that there are dangers related with having the equivalent physical foundation among a lot of numerous employers; even one existence vindictive can make dangers the other utilizing the equivalent organization, and consequently, security as for hypervisor is of extraordinary worry as all the visitor frameworks are controlled by it. On the off chance that a programmer can deal with the hypervisor, he can make changes to any of the visitor working frameworks and oversee every one of the information going through the hypervisor.

Different kinds of attacks can be propelled by focusing on various parts of the hypervisor. In the hypervisor architecture, an advanced cloud security system can be developed on the basis of the behavior of different components, which monitors the interval between guest VM activities and various hybrids.

3.8 Virtualization Level Security Issues

Of cloud runs simultaneously on the host computer applying OSs in the virtualized (multi-inhabitant) condition. Actual weaknesses in a VM that are circulated all through the physical and simulated venture assets permit digital attacker, malware, or different dangers to remotely misuse.

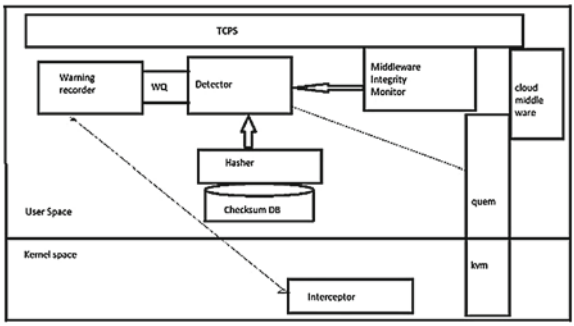

Fig. 1 Structure of TCPS

The security danger also increases with the help of VMS. As soon as the amount of visitor operating framework increases in the hypervisor, security concerns with that new visitor OS also increases. Since it is impossible to hope to screen all OSs, keeping up the security of those OSs is troublesome. There can be chances that a visitor framework attempt to execute harmful code upon the host structure as well as cleave lower hold the full control of a framework plus square approach to further visitor OSs. There are dangers related to having equivalent real framework among lot of various clients yet one being malevolent. On the off chance that a hacker can deal with hypervisor is that they can make changes to any of the visitor OSs and deal with every one of the information going through hypervisor. Isolation between two VMs is not completely adequate by current virtual machine monitors (VMMs). By compromising the lower layer hypervisor vulnerabilities, the attacker can get access over installed VMs. Example of some attacks include Blue pill, Subvert & DKSM on the virtual layer. This is still an open challenge to prevent such threats. Latest Generation of rootkits that benefit from the processor technology that allows an attacker to insert an additional hypervisor between the hardware and the software. The hypervisor takes control of the system & transforms the original OS into a virtual guest on the fly. As regards the software based virtualization is considered, this kind of hijacking does not require restart & this makes it all the way more difficult to detect the intrusion [11].

3.9 Sharing of VM images in Cloud Introduces Security Risk

The proprietor of a picture is worried about privacy (e.g., unapproved access to the picture). The client of picture is worried about privacy, for example, a malignant picture that is able to debasing or theft the clients own individual information. For sample, instances working on Amazon's EC2 platform simply compromise by performing different attack, related the mark wrapping attack short scripting (XSS) attack, or DOS attack. This enables attackers to make, modify, and erase VM pictures and change administrative passwords and settings that are put into setting with EC2 for S3 get to. This is a threat of infringement (e.g., working unrestricted software

and programming with expired licenses). The manager of cloud is worried about the security and consistency of the cloud all in all and the trustworthiness of the pictures. There is a danger of harms caused by malware contained in any picture put away in the repository.

There ought to be standard machine for finding out integrity of visitor VMs for effective capability or avoid interface of computing, information damage, and abuse of assets.

Figure 1 depicts Manager based clear cloud protection system (TCPS) that screens honesty of cloud parts. TCPS is put among visitor's OS and the virtualization layers, which screens visitor VMs and secures them opposite to interlopers and assaults. It also addresses clear issues in the cloud [11].

4 Cloud Security Problems

The cloud framework is functioning in online network, and the security issues in online network also can be detected in the cloud classification. The cloud structure is not different from the traditional structure in the PC, and it can fit other important and unique security issues. The large outfit around cloud computing remains security and privacy [18]. The information resources the cloud classification. The cloud requirement provides information control framework for the employer. The information security analysis too may be deployed in the cloud system. The cloud framework can deploy in various cloud bud. The different area has various rules, so the security managing can face the rule problem. Distributed computing service is necessary to enhance permissible security [19]. It has appeared as a major issue for online network clients, and they have to face the problem of managing large multiple of records and identification, which helps the clients using password and identification management scheme that decreases security of their personal information. Besides, Web site-driven web experience issues in managing Internet client record and individual content allocation [18, 19].

For large and fast processing of the information, a CSP may utilize assets that are accessible around the activity. This factor reveals the client information over whole net which may result in major security menace. To fix this problem, an intrusion finding system (IDS) component is mostly in the cloud paradigm [20].

4.1 Trust Chain in Clouds

Trust has a significant influence in pulling in more customer by depending on cloud players, due to loss of control (as discussed earlier) cloud costumers depend upon the cloud providers using trust system as on alternate into giving customers transparent power their information and cloud resources (Fig. 2).

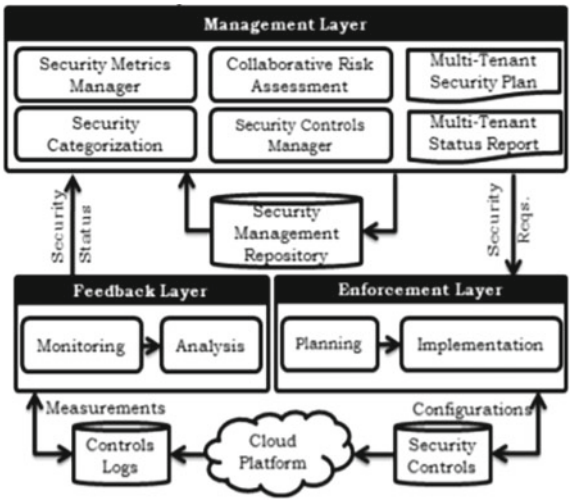

Fig. 2 Management layer

Therefore, the cloud provider assures the client that the operation of the provider is following organizational safety measures and standards.

Concern of identification management includes various measurements; amid others, they consist of clients having to share their characteristics to many service providers, dealing with individual data of the client being conciliated while executing a federated identity. Rodriguez et al. exhibited Federated Identity Architecture (FIA) as a method for resolving weakness and there are three designs for enforcing security problem in FIA including WS-Federation, Shibboleth, and Liberty Alliance [21]. Other than attack, permissible compliance and protection guaranty are other softy matter in federated identity. The recent FIA has no decent way to protect client's data. Stage for Privacy Perform.33 acnes Project or P3P (founded by W3C) has been introduced as a standard and an assignment for developing FIA, by integrating P3P into the FIA [22]. Network to human resources (HR) is hard because HR is the only master source for team identification. Ability to succeed federated identities does not exist in maximum administrations. There are no authoritative data sources to find identities in partner associations. Most associations have no capability to convey with individuals directly in extra institution. These problems and the need of provisioning standards emphasize the importance for decent and comprehensive method to manage how identity properties, accounts, and development management system of all entity-types will take action in the cloud co-framework [23] (Fig. 3).

5 Conclusion Direction

This paper explains the security problem of the cloud computing such as low-cost, platform, independent scalability, elasticity, as well as reliability. The security cloud

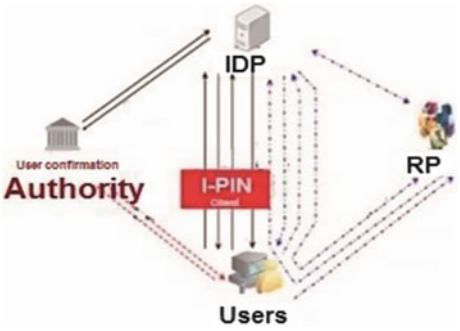

Fig. 3 You and Jun proposed mode [23]

computing manages various field of information management along with its services. The problems included data security in cloud problem also discuss problems in the cloud system are discussed. The cloud computing are on the accelerated pace in their development which have good prospect along with great potential. In this script presented the number of attacks cloud authentication although our main in used to magnified the theft concern because some of the issues are partially solved but identity theft requires further thought. The various customers which degrade mistrust as well as privacy of cloud computing which do not want to move the data into Cloud computing. The various method which are used to protect the security in order to make it effectively or solved this problem are issues are check by the cloud computing provide. Developing the cloud computing as well as security issues is the core problem.

References

1. AmazonElastic Compute Cloud, http://www.amazon.com/ec2/ National Institute of Standards and Technology. The NIST definition of cloud computing; 2011. [retrieved 14.04.11]
2. Google App Engine, http://appengine.google.com Google AppEngine, http://appengine.google.com
3. Microsoft, http://www.microsoft.com/
4. Ren K, Wang C, Wang Q (2012) Security challenges for the public cloud. IEEE Internet Comput 16(1):69–73
5. Vieira K, Schulter A, Westphall C, Westphall C (1989) Intrusion detection techniques for Grid and Cloud computing environment. IT Professional 12(4):38–43. Young M (1989) The technical writer's handbook. University Science, Mill Valley, CA
6. Mell P, Grance T (2011) The NIST definition of cloud computing
7. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Fut Gener Comput Syst 28(3):583–592
8. Dillon T, Wu C, Chang E (2010) Cloud computing: issues and challenges. In: 2010 24th IEEE international conference on advanced information networking and applications (AINA). IEEE, pp 27–33
9. Hashizume K, Rosado DG, Fernández-Medina, E, Fernandez EB An analysis of security issues for cloud
10. Veeramachaneni VK (2015) Security issues and countermeasures in cloud computing environment. Int J Eng Sci Innovative Technol 4(5)

11. Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M (2013) A survey on security issues and solutions at different layers of Cloud computing. J Super Comput 63(2):561–592
12. Singh A, Shrivastava DM (2012) Overview of attacks on cloud computing. Int J Eng Innovative Technol (IJEIT) 1(4)
13. Rong C, Nguyen ST, Jaatun MG (2013) Beyond lightning: a survey on security challenges in cloud computing. Comput Electr Eng 39(1):47–54
14. Bhadauria R, Chaki R, Chaki N, Sanyal S (2011) A survey on security issues in cloud computing. arXiv preprint arXiv:1109.5388
15. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB (2013) An analysis of security issues for cloud computing. J Internet Serv Appl 4(1):5
16. Kumar SN, Vajpayee A (2016) A survey on secure cloud: security and privacy in cloud computing. Am J Syst Software 4(1):14–26
17. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11
18. Cloud Securit Alliance: http://www.cloudsecurityalliance.org/
19. Dean J, Ghemawat S (2008) MapReduce: simplified data processing on large clusters. Commun ACM 51(1):107–113
20. Sun ST, Pospisil E, Muslukhov I, Dindar N, Hawkey K, Beznosov K (2011) What makes users refuse web single sign-on?: an empirical investigation of OpenID, p. 4
21. Gharooni M, Zamani M, Mansourizadeh M, Abdullah S (2011) A confidential RFID model to prevent unauthorized access. pp 1–5
22. Rodriguez UF, Laurent-Maknavicius M, Incera-Dieguez J (2006) Federated identity architectures
23. Archer DCJ, Puhlmann N, Boehme A, Kurtz P, Reavis J (2011) Security guidance for critical areas of focus in cloud computing v3.0. Cloud Secur Alliance