IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN (P): 2347-4599; ISSN (E): 2321-8843
Vol. 5, Issue 8, Aug 2017, 51-60

A QUANTITATIVE ANALYSIS OF SECURITY ISSUES IN CLOUD COMPUTING

JAYALAKSHMI K, UMA K M, VEENA A & LAVANYA SANTHOSH

Assistant Professor, Department of Computer Science and Engineering,

Dr. Ambedkar Institute of Technology, Bengaluru, India

ABSTRACT

In cloud computing technology, user can store large amount of data on storage provided by cloud and make use of resources as and when required, due to which, it becomes very significant. As a result, cloud computing technology has recently become a new model, by which we can host and deliver services over the internet. In cloud computing, resources are shared between different computers and other devices by means of the internet. There are so many issues, which have been observed in a cloud computing environment that need to be addressed. These issues can be categorized as: Security, Protection, Identity Management, Management of resources, Management of Power and Energy, Data Isolation, Availability of resources and Heterogeneity of resources. The first point of security, where, cryptography can facilitate cloud computing is secure storage, but the major disadvantages of secure storage is that we cannot perform processing on encrypted data. This paper presents the challenges and issues of security aspects in cloud computing method. We first look into the impacts of the distinctive characteristics of cloud computing, namely, multi-tenancy, elasticity and third party control, upon the security requirements. Then, we analyze the cloud security requirements in terms of the fundamental issues, i.e., confidentiality, integrity, availability, audit and compliance.

KEYWORDS: Availability, Cloud Computing, Cloud Security, Confidentiality, Elasticity, Integrity, Multi-Tenancy, Security

INTRODUCTION

Cloud computing is being eye-catching by various organizations, as it reduces the just round the corner plan of resource provisioning. There are various definitions of cloud computing given by organizations in their own manner. National Institute for Standards and Technology (NIST) [1] defined cloud computing as **"**a model, which can enable conveniently the network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, Applications and services) on demand, that can be rapidly provisioned and released with minimal management effort or service provider interaction**"**. Berkeley [2] defined cloud computing as "to include application software delivered as services over the Internet, systems software and the hardware in the data centers that facilitate these services**"**. There are a variety of types of issues in a cloud computing environment which need to be addressed. According to a survey conducted by International Data Corporation (IDC), the most critical issue to be found was security. The major concern is to make sure, the security of data in a cloud computing environment. One party encrypts a message and sends the corresponding cipher text to a second party, who then decrypts the cipher text to recover the message. In order to prevent it from the interested third party, there should be no recovery of information about the message from the cipher text. In addition, the cipher text should itself reveal no information about the message. Increasingly, data storage and computation is outsourced to these interested parties, which gives rise to the need for an

encryption scheme that allows computation on the cipher texts. So, to overcome this Craig Gentry researcher at IBM proposed the Homomorphism encryption on June 25, 2009 [21].

AN OVERVIEW OF CLOUD COMPUTING

Over the past decade, cloud computing has become the most outstanding information technology developments. The aim of this new approach is to provide IT services in a manner similar to common utilities such as water, electricity and telephone. In this regard, computational resources and services are provided to clients via the Internet. Furthermore, the service provider is responsible for the availability and security of these offered services. To fulfill clients' demand, numerous deployment models are proposed [3] [4] [5] [6].

CLOUD DEPLOYMENT MODELS

According to NIST, cloud providers offer four main deployment models to meet enterprises' needs. So, it is crucial to understand the advantages and disadvantages of each model.

Private Cloud: In this category, computer resources and software are reserved to several departments belonging to the same enterprise. Furthermore, the cloud data center can be on-premises, which is mainly implemented and administered within IT departments. Also, it can be outsourced to an external provider. In general, this model seeks to ameliorate the security level. Indeed, it allows enterprises to control and manage their sensitive data, especially in the on-premise deployment. In the off-premise model, VPN technology is used to secure communication between clients and cloud providers. In addition to security reasons, a private cloud is an adequate solution to comply with various regulatory standards that are applicable to both private and public sectors. Despite its numerous advantages, deploying on-premise private cloud necessitates technical staff to maintain and manage the platform and software. Thus, it would dramatically increase operating costs.

Public Cloud: In this concept, cloud providers use the same data center to offer computational resources to different enterprises. To achieve this goal, virtualization technology is used to enable resource pooling. Also, administrative tasks, such as maintenance, upgrade and license are ensured by service providers. The aim is to reduce IT service costs and to guarantee reliability and scalability. Furthermore, these delivered services are available anywhere and anytime. In spite of its great benefits, security and privacy are still obstacles that hinder the wide adaptation of this concept.

Hybrid Cloud: It is an environment that uses a mix of private and public cloud. In this model, enterprises take advantage of the private cloud to secure critical data. In parallel, less sensitive data and applications are deployed in the public cloud. As a result, this approach seeks to improve security and reduce costs. Additionally, it is an appropriate method to address load spikes issues. Despite its enormous advantages, controlling workloads and ensuring interoperability between the private and public clouds are still a challenge to this concept.

Community Cloud: In general, this deployment model permits companies and organizations that have a common interest and policy to share applications and infrastructures. The aim of this approach is to promote coordination and collaboration among all community members. However, there are several problems that arise with this model, particularly when members of a community belong to different countries.

CLOUD COMPUTING SERVICE MODELS

The effect of the information system on the public and private sectors is considerable. Indeed, institutions rely on IT technologies to improve service quality [22]. For that reason, cloud providers offer various services to meet enterprises' needs. In this context, cloud computing seeks to facilitate IT technology adoption in enterprises. To meet clients' demand, three service models are available, which are explored below.

Software as a Service*:* In this approach, software and tools are delivered to public and private companies via the Internet. As a result, consumers have access to remote cloud applications used mainly within an enterprise, such as human resources, payroll and logistics management, etc. In this regard, users send the requests to the service provider. The latter relies on advanced software to execute client's requests. Next, the result of these requests is returned to the client. Moreover, the cloud provider is in charge of the maintainer of delivering services. Fig 1 presents this model in the healthcare sector.

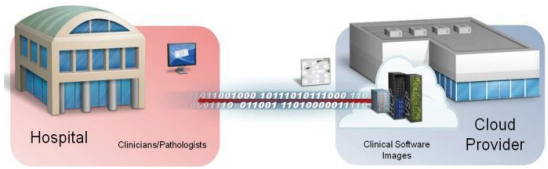

Figure 1: Software as a Service Delivery Model

Platform as a Service: This concept aims at providing cost-efficient computational resources and tools to clients via the Internet. In this regard, program development tools, programming languages and databases are offered as a service, as illustrated in Fig 2. In addition, cloud providers guarantee the availability and maintenance of the delivered platform. Consequently, enterprises use this platform to develop and implement specific software and services.

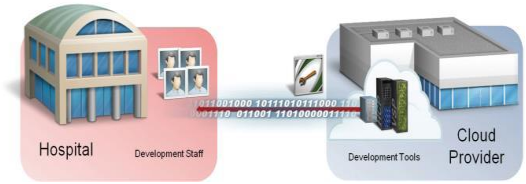

Figure 2: Platform as a Service Delivery Model

Infrastructure as a Service: In this model, cloud providers offer needed computational resources, such as virtual machines, network devices, and storage system for enterprises, as illustrated in Fig 3. For that purpose, cloud providers use the virtualization technique to guarantee scalability and availability. In general, this delivered infrastructure is used to store data and perform on-line backup.

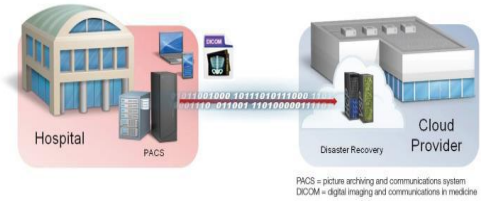

Figure 3: Infrastructure as a Service Delivery Model

CHARACTERISTICS FOR CLOUD SECURITY

Multi-Tenancy

Multi-tenancy, as the term implies, refers to having more than one tenant of the cloud living and sharing other tenants the provider's infrastructures, including computational resources, storage, services, and applications [23]. By multitenancy, clouds provide simultaneous, secure hosting of services for various customers utilizing the same cloud infrastructure resources.

Multi-tenancy is a feature, unique to resource sharing in clouds, especially in public clouds. Essentially, it allows cloud providers to manage resource utilization more efficiently by partitioning a virtualized, shared infrastructure among various customers.

Higher degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. To reach the high scales of consumption desired, service providers have to ensure dynamic, flexible delivery of service and isolation of user resources. Multitenancy in cloud computing is realized typically by multiplexing the execution of VMs for potentially different users on the same physical server [7].

Virtualization and multi-tenancy are bigger issues on using cloud computing. As the cloud is a shared resource environment, organizations want to ensure that all tenant domains are properly isolated from each other that, no possibility exists for data or transactions to leak from one tenant domain into the next. Clients need the ability to configure trusted virtual domains or policy-based security zones [8].

From a customer's perspective, the notion of using a shared infrastructure could be a huge concern. This definitely raises an eyebrow, because of inadequate segregation among cloud customers. What happens when a security vulnerability causes one customer to view (and in the worst case to change) another customer's data? The other customer might not have evil intents, but you never know. However, the level of resource sharing and available protection mechanisms can make a big difference.

To deliver secure multi-tenancy, there should be isolated among tenants' data (at rest, processing and transition) and location transparency, where tenants have no knowledge or control over the specific location of their resources (may have high level control on data location, such as country or regional level), to avoid planned attacks that attempt to co-locate with the victim assets [9]. In Infrastructure-as-a-Service (IaaS), isolation should consider VMs' storage, processing, memory, cache memories, and networks. Ion Platform-as-a-Service (PaaS), isolation should cover isolation among running services and API's (Application Programming Interface's) calls. In Software-as-a-Service (SaaS), isolation should isolate among transactions carried out at the same instance by different tenants and tenants' data.

Elasticity

Elasticity implies, being able to scale up or down resources assigned to services based on the current demand. Scaling up and down of a tenant's resource gives the opportunity for other tenants to use the tenant's previously assigned resources. This may lead to confidentiality issues. For example, when Tenant A scaled down so it releases resources, these resources are now assigned to Tenant B who in turn uses it to deduce the previous contents of Tenant A. Moreover, elasticity contains a service placement engine that maintains a list of the available resources from the

provider's offered resources pool. This list is used to allocate resources to services. Such placement engines should incorporate cloud customers' security and legal requirements, such as competitors' services should be avoided being placed on the same server, data location should be within the tenants' country boundaries. Placement engines may include a migration strategy, where services are migrated from one physical host to another or from cloud to another in order to meet demands and efficient utilization of the resources. This migration strategy should take into account the same security constraints. Furthermore, security requirements defined by customers should be migrated to the service and initiate a process to enforce security requirements on the new environment, as defined by cloud customers, and updates the current cloud security model.

Multiple Stakeholders

In a cloud computing model, there are different stakeholders involved: cloud provider, service provider, and customer. Each stakeholder has their own security management systems/processes and their own expectations (requirements) and capabilities (delivered) from/to other stakeholders. This leads to the following issues.

- Each stakeholder has their own security management processes used to define their assets, expected risks and their impacts, and how to mitigate such risks.
- Providers and customers need to negotiate and agree upon the applied security properties. However, no standard security specification notations are available that can be used by the cloud stakeholders to represent and reason about their offered/required security properties.
- With regard to the multi-tenant environment, the protection requirements for each tenant might differ, which can make a multi-tenant cloud a single point of compromise. A set of security requirements defined on a service by different tenants that may conflict with each other. So security configurations of each service should be maintained and enforced on the service instance level and at runtime, taking into account the possibility of changing requirements based on current customers' needs to mitigate new risks.
- In addition, each tenant could have different trust relations with the provider and some tenants could actually be malicious attackers themselves thus generating complex trust issues.

Third-Party Control

The major security challenge is the third-party issue, that is, the owner of the data has no control on their data processing. The biggest change in Information Technology (IT) department of the organization using cloud computing will be reduced control even as they are being tasked to bear increased responsibility for the confidentiality and compliance of computing practices in the organization.

A related concern is proper governance of cloud related activity. Just as in traditional IT outsourcing, using cloud services requires the customer to give up control over his IT infrastructure. To make customers take this step easier, cloud providers should make the management and maintenance of cloud services more transparent and auditable by the customers. This should include recording logs and complete administrative sessions affecting the part of the cloud infrastructure used by the customer - and if requested by the customer making these accessible.

Third-Party Control is probably the prime cause of concern in the cloud. With the growing value of corporate information, third party access can lead to a potential loss of intellectual property and trade secrets. There is also the issue of a malicious insider, who abuses access rights to tenant information. The fear of corporate espionage and data warfare also stems from third party control. Provider compliance with regulations such as those on auditing also raises questions about how that can be effected on site in a globally distributed multitenant environment [11]. A situation can also arise, in which the user becomes locked-in to a particular vendor. This can be due to a difficulty in migrating data to a new vendor.

Therefore, transparency of what security is enforced, what risks exist, and what breaches occur on the cloud platform and the hosted services must exist between cloud providers and customers. This is what is called "trust-but-verify" [10], where cloud customers should trust in their providers, while cloud providers should deliver tools to help customers to verify and monitor security enforcements.

SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing is the major evolution in information technology. It seeks to outsource computation tasks to an external entity. To accomplish this goal, it is based on multiple advanced techniques: virtualization, Parallel and Distributed System (PDS) and Web 2.0 to fulfill clients' needs. As a consequence, it inherits security problems related to these technologies.

Virtualization

The aim is to create several virtual versions of the same physical resource, such as server and device. Therefore, various operating systems and applications can be run on a single physical server. With this technique, cloud providers can reduce operating costs while enhancing performance and reliability. Additionally, this new technique has outstanding features: scalability, fault tolerance, and storage migration. However, virtualization technique brings security problems [12]: VM isolation, VM image sharing, VM escape, Hypervisor issues and VM migration.

Data and Storage

In principle, cloud computing is a distributed platform aimed at providing cost-efficient computational resources. Consequently, clients' data reside on servers that can belong to different data centers. Hence, this technique is the major source of multiple challenges: resource provisioning, load balancing, job scheduling and scalability. Moreover, the migration to cloud computing comes with additional security risks [13]: multi-tenant environment, data backup, improper media sanitization and data recovery vulnerability.

Web Technology

Cloud providers rely on web-based technologies for offering remote services to the client. In fact, delivered computational resources are accessible via the Internet. To achieve this goal, clients use application programming interfaces (APIs) to manage and gain access to cloud resources. Moreover, APIs enable clients to connect application-layer with clouds. Despite its promising features, APIs brings risks and security challenges [14]: Injection SQL, Cross-Site Scripting (XSS), broken authentication and session management, Cross-Site Request Forgery (CSRF), etc.

SECURITY REQUIREMENTS IN CLOUD DATABASE

Cloud database is a novel approach that seeks to ensure scalability, availability and cost saving. For that reason, both private and public companies are interested in adopting this technology. However, the shift to the cloud database arises security and privacy problems. So, it is necessary to highlight privacy requirements to consider before outsourcing data to cloud database [15] [16] [17].

Integrity

In general, it seeks to guarantee the consistency and accuracy of user data stored in cloud database. Consequently, it aims at preventing unauthorized users from changing sensitive information. To accomplish this objective, various techniques are used, such as encryption, checksums, etc. Furthermore, it is vital to deploy permissions and access control tools. To enhance security, backup is also used to store the affected data.

Data Integrity refers to protecting data from unauthorized deletion, modification or fabrication. Managing an entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused or misappropriated. Moreover, integrity preserving mechanisms offer a greater visibility in determining who or what may have altered data or system information, potentially affecting their integrity.

In cloud computing, solution integrity refers to the ability of the cloud provider to ensure the reliable and correct operation of the cloud system in support of meeting its legal obligations, e.g., Service Level Agreements (SLAs), and any technical standards to which it has to conform. This encompasses protecting data while it is on the cloud premises, both cryptographically and physically; preventing intrusion and attack and responding swiftly to attacks such that damage is limited; preventing faults and failures of the system and recovering from them quickly to prevent extended periods of service outage; and protection of cloud tenants from the activities of other cloud tenants, both direct and indirect.

Confidentiality

Confidentiality refers to only authorized users or systems having the permission and ability to access protected data. Confidentiality is to ensure that user data which resides in the cloud cannot be accessed by unauthorized party. This mechanism is used to protect client information against unauthorized users. Consequently, only rightful clients can have access to sensitive data. In cloud database, client data should be kept secret against the cloud provider himself. For that, user's data need to be encrypted before transmitting them to the cloud database. In this context, several cryptographic techniques are used to achieve this purpose.

In cloud computing, confidentiality plays a major part especially in maintaining control over organizations' data situated across multiple distributed databases. Asserting confidentiality of users' profiles and protecting their data, which is virtually accessed, allows for information security protocols to be enforced at various different layers of cloud applications.

Confidentiality can be achieved through proper encryption techniques taking the type of encryption into consideration: symmetric or asymmetric encryption algorithms, also key length and key management in case of the symmetric cipher. Actually, it is all based on the cloud provider. It also depends on the customers' awareness that they can encrypt their information prior to uploading it. Also, the cloud provider should ensure proper deployment of encryption standards using NIST standards in [18].

Data confidentiality in the cloud is correlated to user authentication. Protecting a user's account from theft is an instance of a larger problem of controlling access to objects, including memory, devices, software, etc. Authentication is the process of establishing confidence in user identities, while they are presented to an information system. Lack of strong authentication can lead to unauthorized access to users account on a cloud, leading to a breach in privacy.

Availability

Availability is one of the most critical information security requirements in cloud computing. SLAs are the most important documents, which highlight the trepidation of availability in cloud services and resources between the cloud provider and customer. It means that clients have access to cloud database anywhere and anytime. However, many factors affect the availability of this delivered service: denial of service (DoS), network deficiency, etc. To overcome these challenges, cloud providers use multiple techniques: load balancing, fault tolerance techniques and replication. Also, cloud database is based on Distributed Architecture to Improve Reliability.

The goal of availability for cloud systems (including applications and infrastructures) is to ensure the users can use them at any time, at any place. This is one of the prime concerns of mission and safety critical organizations. Availability concerns also extend to the need to migrate to another provider, uptime periods of current provider or long term viability of the cloud provider [19] [20].

System availability includes a system's ability to carry on operations, even when some authorities misbehave. The system must have the ability to continue operations, even in the possibility of a security breach. Availability not only refers to data and software, but also to hardware being available to authorized users upon demand. The cloud provider needs to guarantee that information and information processing are available to customers upon demand, which may subsume the heavy reliance on the ubiquitous network's availability.

Availability of Sass application ensures that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application.

Authentication

In principle, this technique seeks to determine and validate client identity. For that reason, the authentication server entails clients to provide their identification information. The latter should match the stored credential. In general, authentication is the fundamental mechanism of any access control tools. In fact, it guarantees that only Authorized clients have access to cloud database.

Authorization

The purpose of this process is to secure access to the cloud database. For that end, it defines and specifies access rights to services, resources and activities. As a consequence, it denies and guarantees access to clients' data. In this regard, cloud providers deploy a security policy to guarantee that all users within an enterprise comply with security rule requirements.

Auditing

This technique seeks to provide full visibility into database activities. So, it is essential to record all the events that happen within a database system. To achieve this goal, monitoring Tools are used to create a report. The latter contains mainly vital information used, mainly to determine when and by whom, the database' objects are accessed or modified.

CONCLUSIONS

Cloud database is an approach that aims at reducing operating costs and improving availability and reliability. As a result, this technology has permeated the public and private organizations due to its various benefits. Indeed, it provides a scalable structured repository to store and manage data. As cloud computing offers so many luxuries, but still organizations are very reluctant to store their data on cloud. One of the obstacles in the implementation of cloud computing is security of data. Cloud data security encompasses a broad range of security constraints from an end-user and cloud provider's perspective, where the end-user will primarily will be concerned with provider's data security policy, how and where their data is stored, and who has access to the data. For a cloud provider, on the other hand, cloud computing data security issues can range from the physical security of the infrastructure and the access control mechanism of cloud assets, to the execution and maintenance of security policy. Cloud security is important because, it is probably the biggest reason why organizations fear the cloud.

REFERENCES

1. Peter Mell, and Tim Grance, Draft NIST Working Definition of Cloud Computing(2009)
2. Michael Armbrust et al. Above the Clouds: A Berkeley View of Cloud Computing http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/ EECS-2009-28.html, Technical report EECS-2009- 28, UC Berkeley, (Feb 2009)
3. B.P. Rimal, A. Jukan, D. Katsaros and Y. Goeleven, "Architectural requirements for cloud computing systems: an enterprise cloud approach," Journal of Grid Computing, Vol. 9, No. 1, 2011, pp. 3-26.
4. W. Voorsluys, J. Brobergand and R. Buyya, "Introduction to cloud computing, in cloud computing: principles and paradigms," Ed. by R. Buyya, J. Broberg, A. Goscinski (New York: Wiley), 2011, pp. 1-41.
5. R.P Patel, "Cloud computing and virtualization technology in radiology," Technical Report, Clinical Radiology Elsevier, 2012, pp. 1095-1100.
6. L. Qian, Z. Luo, Y. Du and L. Guo, "Cloud computing: an overview," In Proceedings of 1st International Conference on Cloud Computing Beijing, China, 2009, pp. 626–631.
7. T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, Proceedings of ACM Conf. on Computer and Communications Security (CCS 2009), November 2009, pp. 199-212.
8. [IBM, IBM point of view: security and cloud computing, ftp://public.dhe.ibm.com/common/ssi/sa/wh/n/tiw14045usen/TIW14045 USEN -HR.PDF.
9. T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, you, get off of my cloud: exploring information leakage in

third-party compute clouds, Proceedings of ACM Conf. on Computer and Communications Security (CCS 2009), November 2009, pp. 199-212.

10. D. K. Holstein, Stouffer, K., Trust but verify critical infrastructure cyber security solutions, in HICSS 2010, pp. 1-8.
11. [11] R. Chow, et al., Controlling data in the cloud: Outsourcing computation without outsourcing control. In ACM Workshop on Cloud Computing. Security, 2009
12. Mazhar Ali, Samee U. Khan, Athanasios and V. Vasilakos, "Security in cloud computing: opportunities and challenges," Information Sciences, Elsevier, 2015, pp. 357–383.
13. Diogo A, Liliana F, B. Soares and Joao V. Gomes, Mario M, Freire, Pedro R and M. Inacio, "Security issues in cloud environments: a survey," International Journal of Information Security, Springer, April 2014, pp. 113-170.
14. Open Web Application Security Project, 2013 Top 10 List, available:http:// owasp.org/index.php/Top_10_2013-Top_10 [Accessed 02 April 2016].
15. Krishna Kamal Kapa and Roger Lopez, "Database as a service (DBaaS) using enterprise manager 12c," Oracle Open World, 2012.
16. IMAL SAKHI, "Database security in the cloud," Stockholm, 2012, availible: http:// div-portal.org/smash/get/diva2:557762/FULLTEXT01.pdf [Accessed 08 April 2016].
17. Luca Ferretti, Michele Colajanni and Mirco Marchetti "Supporting security and consistency for cloud database," Cyberspace Safety and Security, Lecture Notes in Computer Science, Volume 7672, 2012, pp. 179-193.
18. L. M. Kaufman, Data security in the world of cloud computing, IEEE Security & Privacy, vol. 7, no. 4, 2009, pp. 61-64.
19. R. Chow, et al., Controlling data in the cloud: Outsourcing computation without outsourcing control. In ACM Workshop on Cloud Computing Security, 2009.
20. J. Brodkin, Gartner: Seven cloud-computing security risks. In: Infoworld 2008 http://www.infoworld.com/d/security-central/gartnersevencloudcomputing- security-risks-53?page=0, 1
21. Rachna Jain," Homomorphic Encryption Over Integers," International Conference on Computing for Sustainable Global Development, IEEE, 2016,978-9-3805-4421-2.
22. Mbarek Marwan, "Applying Homomorphic Encryption for Securing loud Database," IEEE, 2016, 978-1-5090-0751-6.
23. Huaglory Tianfield, "Security Issues In Cloud Computing," International Conference on Systems, Man and Cybernetics,IEEE Oct 14-17, 2012, COEX, Seoul, Korea.