International Journal of Recent Trends in Engineering & Research
ISSN (ONLINE) : 2455 – 1457
IMPACT FACTOR : 4.101

# A Novel Approach for Implementing Multi-cloud Security

**N.Pushpa Sudeepthi[1], N.Srinu[2], Dr.K.Venkateswara Rao[3]**

*[1]M.Tech,QISCET, Ongole*
*[2]Asst.Prof. Dept. of CSE,QISCET, Ongole*
*[3]Proffessor, Dept. of CSE,QISCET, Ongole*

**Abstract :** Now-a-days the usage of cloud computing has increased rapidly in many organizations. Cloud computing offers many aids like low cost and accessibility of data. Safeguarding the security of cloud computing is a major factor in the cloud computing environment, as users often store complex information with cloud storage providers but these providers may be untrusted. Allocating with "single cloud" providers is expected to become less popular with customers due to threats of service availability failure and the chance of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" has appeared recently. This paper reviews recent research related to single and multi-cloud security and addresses conceivable solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. The Main Stay of the project is to support the use of multi-clouds due to its ability to shrink security threats that affect the cloud computinguser.

**General Terms :** Security

**Keywords :** Cloud computing, single cloud, multi-clouds, cloud storage, data integrity, data intrusion, service availability.

## I. INTRODUCTION

The start of the word cloud computing is undefined. The term cloud is commonly used in science to describe a large collection of objects that visually look from a distance as a cloud and defines any set of things whose details are not additionally inspected in a given situation. The usage of cloud computing has improved quickly in various organizations.

Cloud service providers should statement secrecy and security concerns as a matter of high and urgent priority. Allocating with "single cloud" service providers is fetching less popular with customers due to probable problems such as service accessibilityfailure and the possibility that there are malicious insiders in the single cloud. In modern era, there hasbeen a move on the way to "multi-clouds",

"intercloud" or "cloud-of-clouds". This paper emphases on the concerns related to the data security aspect of cloud computing. As informations and statistics will be pooled with a third party, cloud computing handlers need to escape an untrusted cloud service provider. Guarding private and vital information, such as credit card details or a patient's medical histories from invaders or mischievous insiders is of critical importance. In addition, the possible for movement from a single cloud to a multi-cloud environment is observed and investigation related to security issues in single and multi-clouds in cloud computing aremeasured.

## II. BACKGROUND

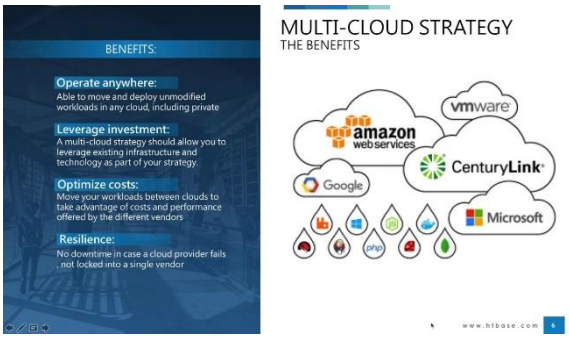



***Fig: Multi-Cloud strategy***

### 2.1 What is Multi-Cloud Approach

A multi-cloud methodology can consists of not only the hardware, software and organization idleness essential to improve fault tolerance, but it can also direct traffic from different customer seats or associates through the wildest promising portions of the system. Some clouds are well-matched than others for a specific task. For instance, a definite cloud might handle huge number of demands per unit time demanding small data transfers on the average, but a different cloud might performbetter for minor numbers of requests per unit time connecting large data transfers on the average. Some organizations use a public cloud to make resources existing to consumers over the Internet and a private cloud to offer hosted services to a partial number of people behind a firewall. A third kind of cloud, named hybrid cloud, possibly will also be used to accomplish various internal and external amenities.

### 2.2 Reasons why Multi-Cloud Infrastructure is the Future

- Optimized ROI
- Superior Security
- Low Latency
- Autonomy
- Less Disaster Prone

### Optimized ROI

All cloudsaremade in a different way. These dissimilarities not only protect physical infrastructure components but also cover a wide range of features, functionality, pricing models and policies, among other aspects. Lack of transparency around the underlying functionality and rapid changes in the dynamic enterprise IT landscape make it near impossible to predict which cloud is the right fit for your apps and business needs. Different vendors offer integration and support for different platforms and constantly change the capabilities they have to offer. The right fit is therefore determined in reference to individual metrics, for individual apps, and for individual business needs – all of which means unnecessary trade off and compromised choices.

But it doesn't have to be that way. With the multi-cloud environment, you can spin up whatever cloud resources are on offer without having to compromise your choices. Multi-cloud structuredeals a rich set of cloud selections to solve demanding needs across a wide range of computing and business functions, thereby improving returns on cloud investments.

**Superior Security**

Giving up control over mission-critical apps and data is often cited as the primary concern that deters cloud adoption among industry laggards. Though the perceived risks are often overblown considering the lack of security capabilities on premise, vendors cannot expect to change this mind set without offering adequate visibility, transparency and regulate their public cloud structure – which they don't. A promising but costly solution to these concerns is the private cloud environment established on-site, empowering organizations with granular control, transparency and visibility into IT resources.

Multi-cloud structurepermits organizations to continue hybrid cloud environment that permits a combination of security and cost savings at the same time. The most security-focused workloads are kept in the private cloud while running regular business data and apps in cost-effective public cloud networks.

**Low Latency**

Access to data and apps stored at distant locations across the cloud network is not instantaneous. Minor delays are caused when data traffic has to travel across several nodes before reaching end-users. This delay, called latency is inherent in cloud services delivered from servers at distant locations. With the multi-cloud infrastructure, the datacenter closest to end-users can serve the requested data with minimum server hops. This capability is especially useful for global organizations that needs to serve corporate data across geographically disparate locations while maintaining a unified end-user experience.

**Autonomy**

Vendor lock-in is the IT paradox of cloud adoption. Vendors modernize the process of migrating assignments to their cloud, and then link customer data and applications to their infrastructure such that it is complex and expensive for customers to leave. With this practice, vendors refute a key driver of cloud migration: the capacity to run apps without having to worry about the underlying infrastructure. As a result, vendors monopolize pricing and force organizations to stick with them over the long haul.

Multi-cloud infrastructure authorizes organizations to mix and match platforms and vendors such that their jobs are not locked-in to individual cloud providers. Moving vendors gets easier, simplified and fairly programmed at times since task performance is never tied to individual vendors. With the lower vendor lock-in, customers get the autonomy to address changing business needs for performance, security and returns on investments.

**Less Disaster Prone**

Multi-cloud organizationrepresents the philosophy behind the earliest proverb that says don't put all of your eggs in the same basket. Vendors typically offer at least 99.5 percent accessibility as part of their SLA guarantee. Distribute your workload across multiple cloud networks with each offering the same low SLA guarantee and the possibility of concurrent and simultaneous downtime across all clouds still goes down exponentially. Even if this possibility is not negligible, organizations can enjoy greater options in reacting proactively to mitigate risks when needed.

Modern cloud services are delivered from multiple, redundant data centres as part of a single cloud network. Multi-cloud infrastructure takes the very concept behind modern cloud services to the next level, and in some cases, creates a cloud of cloud or inter-cloud services. The difficulty, price and threats of running a multi-cloud environment may appear grown, but the only real difference is the need to monitor a network of networks with tools that deliver end-to-end visibility across all network resources.

**2.2 What is Cloud Architecture**

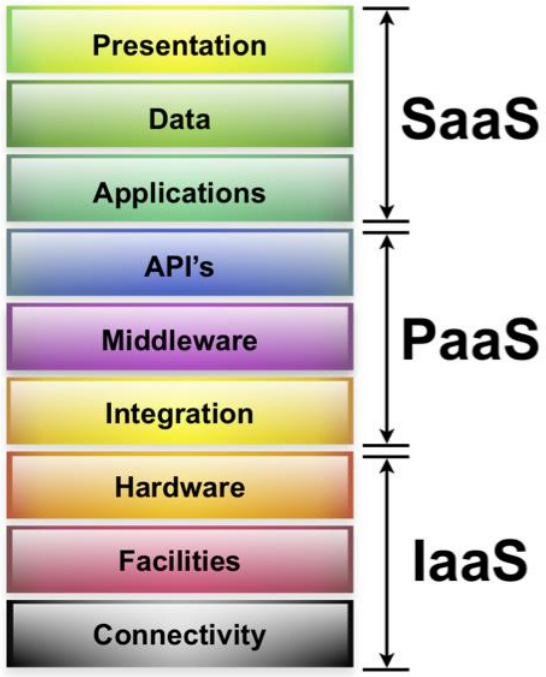
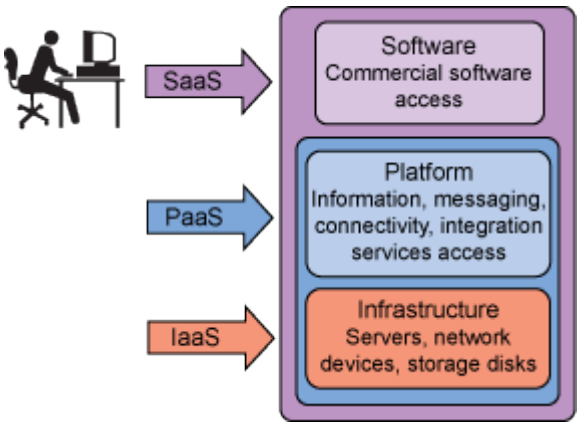
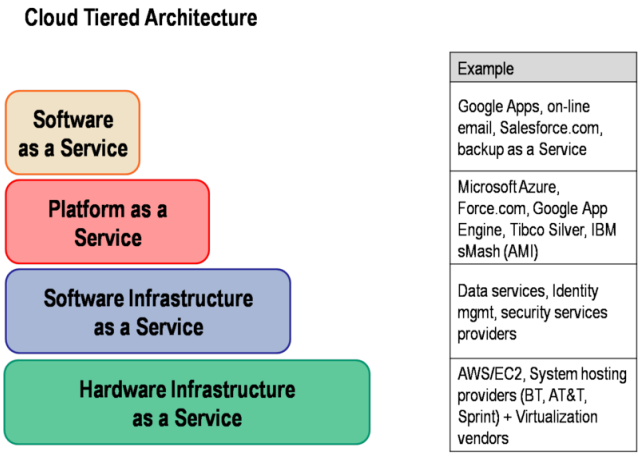



*Fig: Basic Architecture.*

SaaS: Software as a Service
PaaS: Platform as a Service
IaaS: Infrastructure as a Service




## 2.3 Cloud Tired Architecture



## III. CLOUD SERVICE PROVIDERS EXAMPLES

Cloud service providers (CSP) are enterprises that deals with network services, infrastructure, or business applications in the cloud. The cloud services are presented in a data centre than can be accessed by companies or individuals using network connectivity.

There are severalkinds of services that can be used "in the cloud" by CSPs, including software, often denoted as Software as a Service (SaaS), a computing platform for developing or hosting applications, known as Platform as a Service (PaaS); or an entire networking or computing infrastructure, known as Infrastructure as a Service (IaaS). The partitions, still, are not always clear, as many providers may offer severalflavors of cloud services, include traditional web or application hosting providers. For example, you might go to a cloud provider, such as Rackspace, who started as a web hosting company and buy either PAAS or IAAS services. Several cloud providers are concentrating on exact verticals, such as hosting healthcare applications in a secure IAAS environment.

**Below is a list of some of the major CSPs and their approaches:**

| Cloud Service Provider | IAAS | PAAS | SAAS |
|---|---|---|---|
| Amazon | **X** | **X** | |
| Century Link | **X** | **X** | |
| Google | **X** | **X** | **X** |
| IBM | **X** | **X** | **X** |
| Microsoft | **X** | **X** | **X** |
| Rackspace | **X** | **X** | |
| Sales force.com | | **X** | **X** |
| SAP | **X** | **X** | **X** |
| Verizon Terre Mark | **X** | **X** | |

## IV. SECURITY RISKS IN CLOUDCOMPUTING

**The Following are the common Security Issues Faced by all companies:**

### 1. Loss or theft of intellectual property

Companies increasingly store sensitive data in the cloud. An investigation by Sky-high found that 21% of files uploaded to cloud-based file sharing services contain complex data including intellectual property. When a cloud service is broken, cyber criminals can gain contact to this complex data. Absent aopening, certain services can even pose a risk if their terms and conditions claim ownership of the data uploaded to them.

### 2. Compliance violations and regulatory actions

These days, most companies operate under some sort of regulatory control of their information, whether it's HIPAA for private health information, FERPA for confidential student records, or one of many other government and industry regulations. Under these mandates, companies must know where their data is, who is able to access it, and how it is being protected. BYOC often violates every one of these tenets, putting the organization in a state of non-compliance, which can have serious repercussions.

### 3. Loss of control over end user actions

When companies are in the dark about workers using cloud services, those employees can be doing just about anything and no one would know—until it's too late. For instance, a salesperson who is about to resign from the company could download a report of all customer contacts, upload the data

to a personal cloud storage service, and then access that information once she is employed by a competitor. The preceding example is actually one of the more common insider threats today.

**4. Malware infections that unleash a targeted attack**
Cloud services can be used as a vector of data exfiltration. Sky high uncovered a novel data exfiltration technique whereby attackers encoded sensitive data into video files and uploaded them to YouTube. We've also detected malware that exfiltrates sensitive data via a private Twitter account 140 characters at a time. In the incident of the Dyre malware variant, cyber criminals used file sharing services to deliver the malware to targets using phishing attacks.

**5. Contractual breaches with customers or business partners**
Contracts among business parties often restrict how data is used and who is authorized to access it. When employees transfer restricted data into the cloud without authorization, the business contracts may be disturbed and legal action could follow. Consider the instance of a cloud service that maintains the right to share all data uploaded to the service with third parties in its terms and conditions, thereby breaching a secrecydeal the company made with a business partner.

**6. Diminished customer trust**
Data breaches inevitably result in diminished trust by customers. In one of the larges breaches of payment card data ever, cyber criminals stole over 40 million customer credit and debit card numbers from Target. The breach managedthe customers to stay away from Target stores, and led to a loss of business for the company, which finallyobstructed the company's revenue.

**7. Data breach requiring disclosure and notification to victims**
If complex or structured data is placed in the cloud and a breach arises, the company may be required to reveal the breach and send notifications to possible victims. Certain regulations such as HIPAA and HITECH in the healthcare industry and the EU Data Protection Directive require these disclosures. Resulting legally-mandated breach exposes, regulators can impose fines against a company and it's not uncommon for consumers whose data was compromised to file lawsuits.

**8. Increased customer churn**
If customers even suspect that their data is not fully protected by enterprise-grade security controls, they may take their business elsewhere to a company they can trust. A growing response of criticizers are instructing consumers to avoid cloud companies who do not safeguard customer privacy.

**9. Revenue losses**
News of the Target data breach made headlines and many consumers stayed away from Target stores over the busy holiday season, leading to a 46% drop in the company's quarterly profit. The company valued the breach ultimate cost $148 million. As a result, the CIO and CEO resigned and many are now calling for increased oversight by the board of directors over cyber security programs.

## V. MULTI-CLOUDS COMPUTING SECURITY

Cloud computing and storage offersthe customers with skills to store and process their data in third-party data centres. Organizations use the cloud in a wide-variety of different service models (with acronyms such as SaaS, PaaS, and IaaS) and deployment models (private, public, hybrid, and community). Security issueslinked with cloud computing fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud). The responsibility is shared, however. The provider

must confirm that their infrastructure is protected and that their clients' data and applications are safe, while the user must take actions to support their application and use strong passwords and authentication measures.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the sixth biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data centre. Moreover, data centres must be regularlychecked for doubtful activity.

In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result, there is a chance that one user's private data can be seen by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

The wide use of virtualization in executing cloud infrastructure carries unique security worries for customers or occupants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This hosts an additional layer - virtualization - that itself must be correctlystructured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For instance, a break in the administrator workplace with the management software of the virtualization software can cause the whole datacentre to go down or be reconfigured to an attacker's liking.

### 5.1 Cloud Security Controls

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are set in place to protect any weaknesses in the system and shrink the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:

**Deterrent controls**

These controls are projected to shrink attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed.

**Preventive controls**

Preventive controls make the system stronger against occurrences, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

**Detective controls**

Detective controls are planned to identify and respond appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue. System and network security monitoring, including intrusion detection and prevention measures, are usually employed to detect attacks on cloud systems and the supporting

communications infrastructure.

**Corrective controls**
Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

## VI. FUTURE WORK

Like various IT solutions, cloud computing services have been supported from a position of administrative efficiency. As the time goes, if you get your cloud services from a single provider, you'll enjoy the reduced trouble of consolidating third party business relationships, receive IT services at bargain prices, and have an easier time coordinating those services.

It's true that using fewer service providers can offer some nice perks, but cloud computing is moving in the opposite direction at many companies. Instead of securing the benefits of placing cloud services under one umbrella, businesses are mining the advantages of the antithetical approach: receiving cloud services from multiple provider's — a discipline known as "multi-cloud computing." According to a mid-2016 report from Business Cloud News (BCN), "57% of organizations have no multi-cloud strategy at all, whereas 35% do not have a private cloud strategy, and 28% lack one for apublic cloud." According to IT commentators ranging from Google to *Forbes*, these three groups have one thing in common: All of them will increasingly adopt multi-cloud strategies as the technology improves and proliferates.

**The Sun Behind the Clouds**
Multi-cloud computing brings the need to maintain multiple cloud provider relationships instead of maintaining just one. In the aftermath of the Great Recession, when company decision makers are still accustomed to viewing every kind of business functionality through the lens of cost cutting, it begs the question: What do companies get in return for taking extra time to oversee those relationships?
The answer is simultaneously vague and clear: It depends on the needs of the company in question. However, the characteristics of some companies set them up to benefit from multi-cloud computing more than other companies.

**Company Size**
For example, company size can be a big determinant of multi-cloud benefits. According to a 2017 report from Network World, "It's inevitable big companies with many divisions and their own agendas and vendor alliances will end up with multiple clouds … Settling on a single cloud model would create compromises for such [companies] that would ultimately dilute [the cloud's] benefits and the business use case."

**Cloud Performance**
Additional value proposition of multi-clouding involves the performance of cloud properties. From the same Network World report: "Organizations tend to prefer a multi-cloud strategy to get out of the 'keeping all your eggs in one basket' problem that can leave them susceptible to a range of issues, such as cloud data centre outages, bandwidth problems, and vendor lock-in."

**Data Compliance**
Concern over data compliance also leads to using multiple clouds. This alleviates the worry about the level of data exposure in places where cloud services are largely ungoverned. Companies that do this

can store offsite backup data close to home, while opportunistically receiving other cloud services from providers in other locations.

**Hybridization: A Sensible Approach**

For comparison's sake, cloud computing is commonly discussed using two basic cloud models: public clouds, which are outsourced; and private clouds, which are deployed and maintained in-house. However there's additionalstandard cloud model — the hybrid cloud — that has taken on new meaning in the age of multi-clouding.

Forward-looking companies utilize this model of hybridization when it comes to efficient, yet security-focused storage and network processes. While public or third-party clouds offer a wealth of resources when it comes to data storage, they're still vulnerable to hacks, data breaches, or other security failures. For organizations that need a heightened level of security, hybrid models of private servers plus outsourced public solutions provide the best of both worlds: convenience *and* peace of mind.

**Data Migration**

Hybrid clouds are precisely what they sound like: a hybridization of public clouds and private ones. Hybrid clouds are often used for efficiency's sake. Cloud functions that apply to the user's core business practices may be kept in-house, while functions that are tertiary to core practices — and should ideally be handled by an expert third party — are outsourced.

This condition also offers a highly flexible way for companies to fully outsource multi-clouding. Instead of implementing a public multi-cloud in one fell swoop and incurring a steep learning curve for using the new system(s), companies can migrate services from private clouds to public servers one by one, in a manner less jarring to cloud-based processes.

**Proprietary Data**

Another advantage of gradually migrating from private to public clouds is that companies have more time to evaluate service providers. The suppliers store a company's business data — albeit, in encrypted form — on their servers. Considering that proprietary data is the most valuable asset most companies possess, the more time they have to vet offsite data storage providers, the better.

This takes us to a question that many companies face when they evaluate the benefits of multi-cloud computing: What if company policy prevents third party service providers from storing proprietary information in a public cloud?

You could develop an initiative to change company policy, but it would be timelier — and probably involve a lot fewer clashes of opinion — to simply keep using a hybrid model, in a reduced capacity. Merely save the cloud for apps that take in sensitive data you can't share. This doesn't reduce the effectiveness of a multi-cloud setup but rather plays into its general philosophy: Use the best cloud for a particular, cloud-supported IT function.

**Cloud Computing Tomorrow**

Because of these worries, multi-cloud computing is composed to transform from a general trend into a venerable practice in numerous industries that have business-critical cloud computing needs. But the growth of using multiple clouds doesn't necessarily mean the number of the clouds in multi-cloud setups will increase.

Moderately, the aim will be to custom as many clouds as necessary to address the drawbacks of using one cloud from a single provider — even if that provider is a company providing its own cloud on a private model. Moving from cloud to cloud to perform tasks can be complicated, especially right out of the gate. But cloud service providers are working to make changing between clouds graduallybecoming efficient. The more efficient it becomes, the more multi-cloud computing will thrive.

## REFERENCES

1. M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp.1-9.
2. Amazon, Amazon Web Services. Web services licensing agreement,October3,2006.
3. M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, 1998, pp.173-186
4. S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), 2003, pp.20-26.
5. E. Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud computing roundtable", IEEE Security & Privacy, 8(6), 2010, pp.17-23.
6. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp1-11.
7. Sun, http://blogs.sun.com /gbrunett/entry/ amazon_ s3_silent_data_corruption.
8. H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), 2010, pp.24-31.
9. M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing", HotSec'10: Proc. 5thUSENIX Conf. on Hot topics in security, 2010,pp.1-8.
10 J. Viega, "Cloud computing and the common man", Computer, 42, 2009, pp.106-108.
11. M. Vukolic,"The Byzantine empire in the /intercloud", ACM SIGACT News, 41,2010, pp. 105-111.
11. C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in cloud computing", ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010, pp.1-9.
12. P.Mahajan,S.Setty,S.Lee,A.Clement,L.Alvisi, M. Dahlin and M. Walfish, "Depot: Cloud storage with minimal trust", OSDI'10: Proc. of the 9th USENIX Conf. on Operating systems design and implementation, 2010, pp. 1-16.
13. U. Maheshwari, R. Vingralek and W. Shapiro, "How to build a trusted database system on untrusted storage", OSDI'00: Proc. 4thConf. on Symposium on Operating System Design & Implementation, 2000, p.10.
14. D. Malkhi and M. Reiter, "Byzantine quorum systems", Distributed Computing, 11(4),1998, pp. 203-213.
15. J. Hendricks, G.R. Ganger and M.K. Reiter, "Low- overhead byzantine fault-tolerant storage", SOSP'07: Proc. 21st ACM SIGOPS symposium on Operating systems principles, 2007, pp.73-86.
16. A. Juels and B.S. Kaliski Jr, "PORs: Proofs of retrievability for large files", CCS '07: Proc. 14th ACM Conf. on Computer and communications security, 2007, pp.584-597.
17. Clavister, "Security in the cloud", Clavister White Paper,2008.
18. A.J. Feldman, W.P. Zeller, M.J. Freedmanand E.W. Felten, "SPORC: Group collaboration using untrusted cloud resources", OSDI, October2010, pp.1-14.
19. S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), 2003, pp.20-26.