Impact of Misconfiguration in Cloud – Investigation into Security Challenges

K. Wood
Dep. of Computer Information Systems
University of Malta

E. Pereira
Computing and IS, Business School
Edge Hill University

Abstract

The purpose of this paper is to explore key concepts and ideas surrounding the security challenges of cloud computing, with particular reference to configuration having considerable impact on securing cloud services. It is critical that the concepts of exploitation and vulnerability, which evidence shows exist in Cloud use, are discussed and understood in order to enhance security protection and user awareness. There are considerable benefits of cloud computing systems, however this paper will primarily focus on the limitations that have emerged through inaccurate configuration setups of both the platforms and applications, and how these might be addressed. It also will highlight some research work in the area that offers possible solutions to the identified issues in Cloud security.

1. Introduction

Cloud Computing has become a widely discussed and challenging concept in recent years. This latest paradigm promises reliable services delivered through next-generation data centers that are built on virtualized compute and storage technologies [1]. Cloud may have the capability of vastly changing the approaches of implementation, usage and management of computing systems for both the public and private sector. Cloud Computing integrates and provides different types of services: Software-as-a-Service (Saas), the applications are delivered as services over the Internet; Platform-as-a-Service (PaaS) systems software made available over the Internet and Infrastructure-as-Service (IaaS), when the hardware made available for cloud users. The foundations of cloud infrastructure provide more flexibility and dynamism in the computing infrastructure then previous forms of distributed systems. The requirements and demands from users for cloud services vary, resulting in complex design and deployment of resources. It is essential that cloud providers operate within a flexible model to accommodate this. Last two years has seen a dramatic increase in Cloud providers, Figure 1 shows a classification of the cloud services and some of the major providers of these services. Major challenge for all cloud service providers is to offer secure environments that allow users to access underlying infrastructure and services without causing security breaches. Thus, security remains one of the major hurdles to cloud computing adoption [2]. Evidence suggests that security is often ignored until the threat has created chaos [3]. Some providers offer a service at a fairly low cost with very limited protection to users. Clearly, providers do not want to invest heavily in security measures that may not be needed and likewise customers do not want the extra cost added onto their cloud services. Another problem is that users are unaware of the limited protection they are actually receiving. The configuration errors are believed to be the biggest contributor to security issues in Cloud.

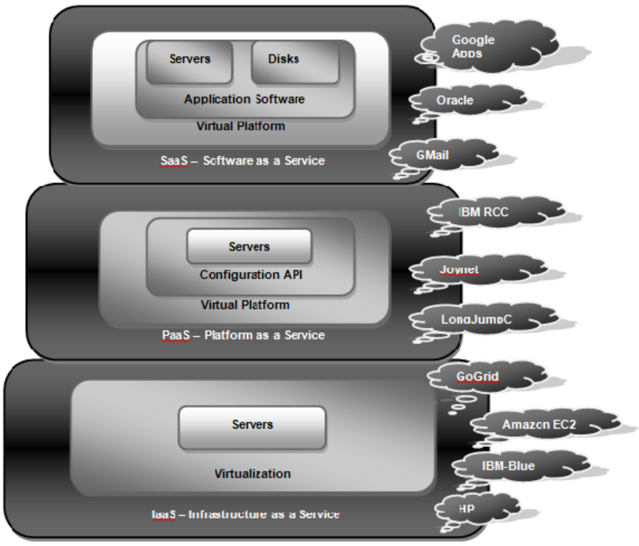

Figure 1. Cloud Services and their major providers

This paper explores the key concepts and ideas surrounding the security challenges within the cloud computing paradigm with particular reference to security in cloud configuration management. It will address the limitations of current configuration options and set ups rather than protection systems or performance by primarily focusing on the current limitations that have emerged through inaccurate configuration setups. It is hoped that by addressing these weaknesses, developers and researchers will explore configuration further to provide a more secure cloud system.

The rest of this paper is organized as follows: Section 2 discusses the major security challenges faced in cloud computing. Section 3 focuses on configuration management issues and the increasing concerns and problem of security threats through inaccurate configuration; Section 4 highlights how the problems need to be addressed and the necessity of standardized approaches to the configuration and deployment of cloud platforms and applications development and also considers the privacy concerns and changes faced in shared systems and configuration globally. Section 5 highlights current developments that could offer some assistance with the problem; Finally, Section 6 summarizes this paper and discusses future work

2. Background – Cloud security challenges

The concept of cloud computing presents a considerable range of issues regarding both the feasibility and security from the underlying infrastructure through to the use of applications. Any form of distributed system, such as grid or cloud, have to deal with a range of technical, social, and legal challenges whilst ensuring a high level of security. Careful consideration must be taken before entering into cloud systems. Users should investigate potential cloud providers before use and ask questions such as; what happens to their data? Where is the data going to be stored? What happens if the cloud provider goes bust or taken over? What security policies are present to ensure the user is protected? What happens if a security breach, through hacking or virus, occurs? These questions would seem to refer to a complex and more troublesome way to operate than through traditional single domain systems. Data that was previously protected within a private network is not exposed to public access threats, as through the internet. Such data is now shared with other data and resources in a massive shared internet based public network that is controlled by a third party cloud provider. Security risks are higher in distributed systems due to their open source environment. Users are heavily depended on the cloud providers trustworthiness and assurance that they will not be exposed to security risks. The fact that clouds can only function through the use of the internet presents further security challenges and raises other factors to consider, such as if 'down time' occurs, can the business still operate?

None of the cloud providers can yet fully answer above questions, however, the ICD market research [4] reports that "*Spending on IT cloud services is growing at over five times the rate of traditional, on-premise IT*", Figure 2, and by 2013 Cloud technology will be fastest growing and leading technology since Web phenomena. The same source rates security as the biggest challenge in Cloud. In the recent survey of chief information officers and IT executives, 75 percent of respondents highlighted security as the main concern in Cloud. This undoubtedly, puts more pressure on researchers, developers and providers.

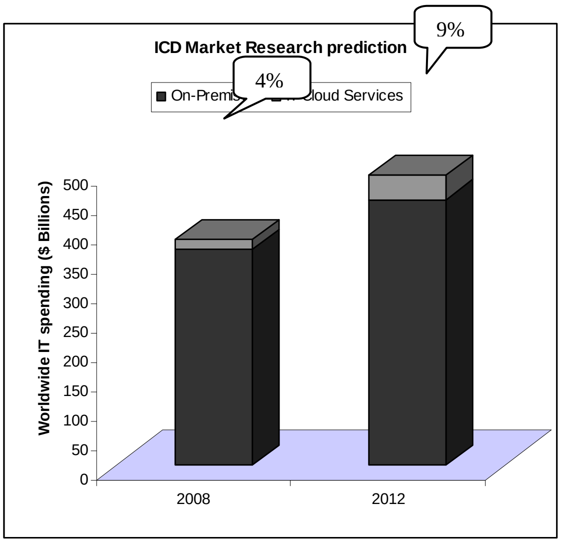

Figure 2. Potential growth on spending on Cloud services

For Cloud computing to operate the user must upload the code and data of their workload to a cloud provider, which in turn runs this workload without knowledge of its code internals or its configuration [5]. Every component on an Internet system must be configured. The challenge is that common configuration parameters must be shared, local customization must be supported, and policy domains must be respected that are not required in single domain systems. [6] The difficultly is in trying to establish how these components will interact with each other. With virtualization being a critical and central point of cloud networking, the boundaries of responsibility can be unclear, particularly over security and data storage. There are several well known and documented examples of loss of data, unavailable sites and security breaches through the lack of guidance and responsibility from both the customers and cloud provider. From the perspective of potential cloud users, it is critical that providers offer assurance that security is taken seriously and provide a secure platform as a high priority. One of major issues with cloud computing is the secure transfer and storage of applications and data between a user (private or business) and the cloud. Authentication becomes problematic as the user is no longer in control or using an internal system to store and retrieve data. There has been a recent claim that cloud providers revise their privacy policies and in some cases have used or are using customer's details, which is against privacy rights and agreements. Data loss is another main concern when using cloud systems. Providers have lost customer details as hackers have been able to gain access to customer data.

Alongside the security aspects, user need to understand the different types of cloud available and understand that even though cloud promises more enhanced performance and usability, not all applications are suitable for use on cloud platforms as not all applications can be transformed into cloud applications. Therefore in some cases businesses will be restricted in how they are able to use clouds and will have to still maintain their current systems to use applications that are unavailable on clouds. The cost of supporting two different systems will not be possible for many businesses.

3. Configuration Management in Cloud

Configuration is the most critical process of any heterogeneous network. This is because it impacts the network in terms of security, performance, resilience, predictability. Distributed computing paradigms have changed system configuration management more than could have been predicted as the dynamism of such systems require more complex set up and maintenance. Most network outage is created by operator errors during the configuration. [6]

There have being several examples of miss configuration highlighted in the media over recent years. Examples include the configuration mistake in 2008 by Pakistan Telecom who wanted to cut YouTube access within the country; however the mistake actually leads to them blocking YouTube globally for two hours. Another mis configuration occurred in Sweden SE Zone in 2009. This resulted in shutdown of all websites and email systems under the country's code top- level domain for several hours. Both of these events had international interest and show the impact of a configuration errors can occur and the impacts they can have in a cloud system. Configuration management is responsible for the structuring of any form of software or hardware and in addition is influential in the evolution of the system. Configuration occurs from the initial installation of the operating system and application software, right through to the setting of system parameters, configuration of files and accounts and the configuration of software. Overall, configuration management is essential to establish and maintain consistency of a system. It has been defined as the management of security features and assurances through control of changes. [7] Due to the increased demands on distributed systems, configuration management is a growth area within research and industry in order to provide a more secure and efficient platform to user to operate within [8]. Our research, based on in depth literature survey, shows that configuration errors can have significant impact on different aspects of cloud technology. Some of them are discussed below.

3.1. Virtualization

Virtualization has played a critical role in the development of distributed systems. The aim is to simplify aspects of IT management. It has lead to logical abstraction of physical systems which allows either multiple physical systems to appear as a single logical system, or a single system to be partitioned. The latter, shows multiple independent logical systems. These both have provided advantages in sharing resources between users, regardless of distance. Virtualization can offers real benefits in the flexibility, structure and scalability of IT. However these advantages have being undermined by change and configuration management issues like drift, integrity, availability and performance. These concerns are present in cloud computing and has lead to several report cases of lack of confidence from users in this technology. Managing the configuration stages within a virtual environment has resulted in problems as the approaches to application and systems deployment has to be changed. IT staff and users have had to learn and understand this new infrastructure and changes in the role and use of configuration management. Users have yet to adopt full-scale virtualization in to their businesses, primarily due to limited understanding and training in this area. Virtualization is the key in cloud computing and deployment. Therefore further attention must be placed on the role and importance of virtualization in order for challenges such as configuration to be dealt with correctly and for cloud computing to be used in a secure manner.

3.2. Failure and Fault tolerance

Fault tolerance is largely unexplored in cloud models and tools. [9] Therefore it is important to access a range of configuration techniques and tools to evaluate and distinguish the impact these have on a typical cloud system. Disaster Recovery (DR) services are limited with many providers, It is the responsibility of the provider not the user to ensure that regular back up occurs and a disaster recovery strategy is in place. Due to a lack of standardised policies and procedures, this often does not occur. As Cloud providers are basically doing the minimum required of them, there are more opportunities for risk to occur. According to the findings of Computer Security Institute Report, about half of all incidents arose from inside activity [10]. This can be through not understanding the system and the configuration processes or users who are motivated to create damage. Administration and development needs to deal with this situation in a more consistent manner across different cloud platforms. Therefore it is essential to access the dynamics of a range of configuration techniques and tools to evaluate and distinguish the impact these have on a cloud system.

3.3. Security Policies

Security policies are often specified [11] by configuring access control lists associated with individual resources. Configuration tools need to combine the different polices to generate a configuration environment that does not conflict between the different aspects of the system. Oppenheimer [12] states that most troublesome configuration issues arise in specifying how components are to interact with one another. This includes the components of applications, transfer of data, provider and user workloads. Each has very different requirements. Establishing an approach to ensure the configuration between different workstations, applications and provide storages that does not lead to security breaches needs to be explored in more depth by researchers and developers. As the demand for cloud computing changes, the configurations need to remain intact.

For the purpose of our investigation into security challenges created through the configuration processes, it is best to consider configuration as good or bad configuration management. According to a study produced in [13] 2006 by *North American Network Operators Group* (NANOG) 700 hundred misconfigurations occur per month. This is surprisingly high, even though it appears the errors are not well documented or published, leading to further misconfiguration occurring that is unknown. Through mismatched software and hardware on an network infrastructure due to incorrect or misconfiguration results in opening the network to a wide range of attacks as the system is more vulnerable than if the system had been correctly configuration.

3.4. Misconfiguration issues in Cloud

Configuration management is the most important part of network management. Changes, additions and deletions from the network need to be coordinated with the network management systems. Incorrect configuration can have dramatic effects on the security and safety of users, applications and the overall system. [14] Due to the nature of clouds, users are relaying on shared resources over the internet. It only takes one error or mistake such as those mentioned earlier to place the whole system in jeopardy. A more recent Study by IBM [15] showed that 69 percent of users had concerns regarding the data security and privacy that were the primary barrier to public cloud adoption.

Bad configuration or incorrect configuration as it is often referred to, can occur due to several possibilities. Within distributed systems, the most common occurrences are down to incorrect configuration approaches taken. Tools are used as they are familiar to the administrator, but they do not work efficiently on complex and large scalable systems, which is the purpose and role of distributed systems. The challenges of understanding incorrect approaches are further complicated as some systems can still operate but - at increased risk. Often performance is notably affected by users or down time and security breaches, such as viruses, are more common. The problem for the administrator is establishing which components of the system were firstly incorrectly configured as the problem can move into other components, which means they have to be examined and repaired , creating additional problems and lengthening the process of diagnosis and correction of problems. The longer the problem is left unattended, the more likelihood that it will travel through the system leading to greater risk of damage and cost. Unlike single networks, distributed systems can have millions of users across one platform across the globe so the system cannot be shut now for a few hours for maintenance to occur without serious knock-on effects for the users. Developing a system, especially a shared system which has underlying problems due to bad configuration will only lead to future security problems or performance. No user wants to find out they have placed trust in the cloud provider with their date and resources and in return are in a more valuable position and with an increase risk of attack through poor planning and inaccurate configuration management.

It is complex to develop and maintain applications on a cloud computer system and users need to be aware of what applications will work and will not work on a cloud platform. As briefly discussed in section 1, one of the biggest challenges of cloud systems is the task of transferring large amount of data and applications across a range of users securely. Therefore the configuration processors need to be secure to prevent security breaches within the four areas: authentication, authorization, integrity and confidentiality.

In theory, it is clear that good configuration could be achieved through good planning, efficient resources and awareness of security threats. However in practice it is not always that straight forward. For example, as cloud systems are able to be scalable, applications currently on the system might work without any problems. When it comes to upgrading, deleting or adding users or applications the outcome cannot be always predicted in advance. It could be that adding or deleting will present gaps during the configuration stages that in turn will lead to further problems. Also in the case of some applications being deployed, it might be necessary to change the configuration parameters; again this could have affects on the rest of the system. It is important to understand these different circumstances to gain a better insight into the fault tolerance of the cloud and the behaviour of the system.

4. Problems to be addressed

Several sources claim configuration errors are the biggest contributor to service failures. Between 40- 60% of downtime and other problems are due to configuration errors. There is little evidence of diagnosis testing conducted in configuration which is one reason for the high number of problems that are created. Efficient configuration management is critical to ensure security, performance, fault tolerance, intrusion tolerant and commutation flow between the different components. Each component needs to be configured and tailored to the needs of the individual machine.

The components have been designed to have a finite set of configuration parameter which will help ensure some level of consistency. However these parameters are static where as the components have dynamic state, these do not change during the component's normal operation [17] therefore by setting these to behave in a particular way end to end functionality should be achieved through a connectable system.

Certain parameters act as guides to aid administrators to define the setting of the configuration however these parameters can vary within:

- Installation of Operating Systems
- Installing of software
- Network configuration, servers and other network devices
- Internet providers – such as Cloud providers run through the internet
- Access control/User/Admin Rights
- Hardware configuration
- Driver's configuration
- Updating configuration
- Applications

A single configuration error can result in a lengthy and costly task of assessing the system to establish where the error occurred and also dealing with the knock on effects the error would have had on the rest of the system. This highlights the danger of inaccurate configuration deployment and poor configuration management. A single point of failure can result in unauthorized access, data loss, performance failure and other security breaches. It is important to note, that no system is 100% secure as new technologies bring additional complications to existing systems. New approaches and monitoring techniques are required to ensure the system is a safe as possible and security threats are dealt with as quickly. Problems can emerge through incompatibility of different resources, human error or through illegal attacks which are known as cybercrimes such as hackers and Denial of service (DoS).

As there is increasing pressure to create larger scale systems which offer more flexibility. Systems are being developed using components. This allows systems to be upgraded and added during run-time which places further pressure and the configuration consistency of the system. In order to reduce the complexity of this, automation techniques have been developed. However there are underlying issues that must be considered:

- Constraint-based specifications of configuration
- Planning of configuration – initial and change processes
- Autonomic controls – are there limitations?
- Level of automatic involvement in the decision-making processes
- Level of human involvement in the decision-making processes
- Balance of human and automatic interaction
- Manual via automatic – which suits your system?

Configuration challenges and problems are nothing new in computing. The majorly of systems administrators are use to building large, complex distributed systems via configuration. [16] There is evidence to show that an operator's ability to manage a network decreases as the network becomes more complex. Cloud computing present more challenges due to its highly distributed and federated environment, as well as being scalable the loading and types of resources differ therefore placing additional pressures on configuration. This highlights the significant problem that is facing the future of cloud and the need for could configuration management to be effective. As there is several new layers to this form of network then typical networks (e.g. virtualization) each layer needs to be examined and problems detected and resolved as these will impact the cloud layer. The challenge is even more complex as the administrators have either no control or limited control as the cloud provider takes over from businesses and users. The challenge for users, especially IT businesses that are using a cloud provider is that they have no access to the underlying infrastructure in a private cloud. Therefore if a visibly problem is highlighted they cannot directly resolve the problem. It is the responsibility of the provider to monitor and management configuration problems and resolves them. The rapid success of cloud in recent years has meant that those employed by cloud providers to develop these systems have basically learnt on the job. There are currently no guidelines and standards that ensure cloud vendors provide a suitable and secure as possible platform. Having different elements of a system that is controlled by different parties means it is difficult and unrealistic to think that the different layers will be configured efficiently without resulting in any security breaches or increase risk of attack.

5. Possible Solutions

As resources can be easier shared among users and also be moved between vendors in cloud. Moving anything for one system to another can lead to problems if the transfer of information is not transferred in sequence. Any break could result in a security breach that could affect the whole system and users. One solution to the problem has been the use of automation deployment and configuration within clouds. There are advantages of this approach butt the automatic function is restricted and guided by polices and resources. Within a rapidly changing system there is still a need for human involved especially in decision making. A combination is required to achieve this. As configuration and deployment within cloud is so uncertain and unreliable. It appears that's the only possible solution would be to development a unified configuration framework. This form of framework would provide some consistency and a unified standard for all cloud developers and vendors to work at to ensure configuration mistakes are reduced. For this solution to work, it will take years of planning and commitment from the cloud community to work together to create a better configuration approach. Through a configuration baseline you can establish a level of consistent control, therefore controlling the state of the system to prevent unauthorized changes. If aspects of a cloud are not synchronized through configuration then security risk will increase.

In order to address the problem it is critical to have an understand the whole infrastructure and layers and what is deemed as good and bad practice in both configuration and protection of a system. Again, without any clear guidelines this can be difficult to fully achieve. In order to secure the cloud, the state of configuration management needed to be examined.

As systems evolve and there is a need for researchers to recognize that configuration management tools and approaches need to evolve. There is limited consistency between tools leading to difficulties in interoperable and comparing tools available therefore these suggests the ‘level’ of acceptable configuration will differ. Because an application or user is deployed on a system due to a form of configuration does not mean it has been completely successful or the more suitable approach.

Such diversity has lead to a gap in consistency, usability and capability. The majority of configuration tools and techniques development are not for regular use or well documented which means they are tended to be ignored of unheard of meaning they provide little or no transfer knowledge to the field. Therefore this suggests that no suitable tool has been fully developed, however there are some exist tools that are useful and promising. Researchers need to focus on improving these existing tools rather trying to reinvent new approaches and with further work the existing tools could provide reliability solutions. It maybe the case that some researches work in isolation and wish to establish a new approach towards configuration however there appears to be evidence of recent collaboration work between LCFG and PoDIM [17] it is hoped this collaboration will provide a workable solution to the configuration problem in the future.

Meanwhile, some researchers have already attempted to address some of the misconfiguration issues by developing new mechanisms and tools. S. Bleikertz et al [18] developed an evaluative mechanism for validating configuration of complex cloud infrastructure to reduce security risks. This approach allows validating correct set-ups of security policies such as Amazon's security groups. It also helps in assessing the end-user configuration of multi-tier architectures deployed on IaaS cloud such as Amazon CE2. This security assessment tool allows users to correct potential misconfiguration and to refine certain set-ups to minimize the security risks.

To improve the configuration process several configuration management tools such as puppet [19] and cfengine [20, 21] have been developed. These developments have been designed to aid administrators in the configuration of cloud systems.

The possible solutions to improve configuration are automatic approaches rather than the manual system administration approaches that are used. According to [22] manual tools do not have the ability to work successfully within large and varied computer infrastructures. There are services such as Vebtura Networks FMt, which provides fault tolerant middleware. Through automatic network configuration, tracking and auto-discovery [23], these services will allow the system to determine the most appropriate approach to examining the different aspects and variables of a grid, particularly the application layer, to gain a better understanding of the impact of configuration. It is possible to predict certain outcomes of testing; however there will be cases that will provide unexpected results.

5.1. Privacy Regulation and Impact

One of the underlining issues of distributed systems is that they have to be deployed, configured, and monitored to ensure security breaches are kept to the minimal and protect different users. Consistency is critical especially to ensure user safety and privacy, yet this is currently lacking in cloud configuration techniques and also the flow of data through a cloud system. Cloud privacy regulations have yet to be taken as priority in order to protect cloud systems and users. Lack of standardized regulations on privacy and protection has lead to confusion of user's rights and the responsibility of the Cloud Service Provider (CSP) to act ethically and meet privacy requirements. There are no consistent international regulations and legislations on this matter. Therefore, in terms of cloud deployment and use, a user's data might be protected in one country but is not the case in another. Each country or group of countries such as those within the EU zone has their own form of privacy regulation. The difference between the legislations across the world is clearly noticeable through a comparison. The European Union (EU) privacy laws follow a strict and comprehensive approach which have been developed and influenced by the government and businesses within both the public and private sector. From this joint contribution, a framework has been developed which ensures the privacy codes of practice can be integrated within all sectors across the EU. EU favors very strict protection of privacy, while in US there tend to be a more relaxed approach to privacy legislation. US legislation tends to have no or limited government involvement. It is deemed the responsibility of businesses and industry bodies to develop specific industry sector legislations on privacy. This results in different laws being enforced on privacy across the US. The lack of consistency within the US has led to the EU deeming the US as unsafe and lacks the necessary privacy protection standard they expect. In an attempt to meet the concerns of the European, the US has recently developed the UK Safe Harbor Privacy Principles which attempts to ensure US based businesses comply with the EU Directive 95/46/EC on the protection of personal data. By offering US businesses the option of registering to this in order to meet the European Union requirements has meant the EU still has concerns of the US privacy approaches and that this do not go far enough to protect EU users and their data. For instance, EU has privacy regulation that does not allow transmission of some type of personal data outside the EU. This has a great impact on cloud services, some of the non EU cloud providers have already considered to offer storage facilities in the EU.

Furthermore, there is no continuity currently between those countries which are within the Middle East region. Several Middle Eastern countries have established legislation on data protection and privacy which has been enforced due to the increased recognition of the importance of privacy and data protection legislation in order to be unitize technologies and develop their own systems to further advance and data interaction. The major issue within the Middle East is that these laws have been slow to be developed and have yet to be fully supported by all governments and businesses. Therefore privacy and security concerns remain over the safety of data transfer within this area. Further commitments on their privacy laws are essential if they wish to utilize cloud computing technologies and for both the CSPs and foreign users to be willing and comfortable in transferring and storing their data to that part of the world.

Investigating into the privacy laws of Asia, Pacific and African is more problematic due to differences within economies and cultures compared to the EU and US. There is limited legislation and practice within these regions. Factors such as political surveillance, the public attitudes, views on civil society and individual rights remain sensitive areas. Therefore, the development of international practices and international privacy legislation need to acknowledge such difference. In terms of deploying cloud systems international users must be aware of the difference government and legislation regarding privacy.

5.2. Addressing the privacy concerns

In order for cloud computing to work it is dependent on internet connectivity, besides having to have a constant and reliable connection. Those countries which are restricting user access and privacy to web sites and web applications will prevent cloud technologies from being available. In order to support cloud deployment and configuration further research and development of configuration techniques must be developed. Enforcing with support the process of configuration through the life cycle of a cloud system or cloud application and allow detection of problems which emerge at an early stage before a potential security attack has developed into a serious security breech. In turn, this would increase performance and user confidence in clouds.

Regulatory compliances over the location of data and geo-redundancy are critical aspects to consider if cloud computing is to reach it fully potential. Encryption of data is one possible solution but this needs further investigation and is used throughout.

6. Conclusions and Future work

Through analyzing the available literature on both general configuration management and configuration management with particular reference to cloud configuration, there is a clear lack of clarity and evident of any standards to support the configuration process emerging. Evidence backs up this argument that misconfiguration is a common problem within all systems not just in clouds. In the case of cloud future development, configuration is a threat to the overall security of the system. It is critical that the configuration processes and management is well documented to ensure any problems can be found quickly before any damage occurs. Fault tolerance needs to be explored in cloud module and configuration tools. As the cloud services vary, there is a definite need to access the range of configuration techniques and distinguish between the approaches that are best suited for each type of cloud.

This paper presents a discussion of concepts and ideas surrounding configuration concerns within cloud. It is clear from that secure configuration requires controls for provisioning, administration, monitoring, validation, and also management. There is evidence through examples highlighted in this paper that secure configuration does not always occur. A small human error in configuration can lead to a security breach. This paper demonstrated the important of understanding both system configuration management as well as security. It is only through having such understanding that development of more efficient configuration approaches for cloud computing will occur. Due to rapid developments in cloud computing, additional research is necessary to develop a robust, well performing and most importantly a secure heterogeneous cloud environment. Unless this occurs this technology cannot reach its full potential It is hoped that this paper has provided readers with a better conceptual understanding of security concerns and the critical role that configuration plays within distributed systems. It is also important to note that lack of security design now will only increase cost in the future as the cost of a security breach can be high and also reduce user confidence. By examining security challenges and highlighting areas for research now, a more secure uniform framework can be developed and improve the reliability of cloud systems.

7. References

[1] R. Buyya, C. S. Yeo, and S. Venugopal. Market oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities. *Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications*, 2008.

[2] Messmer. E(2009) ‘Are Security Issues Delaying the CloudComputing’ http://www.networkworld.com/news/2009/042709-burning-security-cloud-computing.html.

[3] G. Reese, (November 2008)‘Key Security Issues for the Amazon Cloud’ http://broadcast.oreilly.com/2008/11/key-security-issues-for-the-am.html.

[4] , Frank Gens,” IT Cloud Services Forecast – 2008, 2012: A Key Driver of New Growth”, 8 October 2008 http://blogs.idc.com/ie/?p=224. (Access date: 04/02/11).

[5] Mihai C., Sailer R., Scholes D., Sgandurra D., Zamboni D., (2009) ‘Cloud Security Is Not (Just) Virtualization Security’

[6] Child.D et al., (2008) Devolved Management of Distributed Infrastructures with Quattor 22nd Large Installation System Administration Conference (LISA ’08).

[7] ‘Configuration management delivers business resiliency,’ The Yankee Group, Nov 2002.

[8] Mathiaz's Weblog ‘Are configuration management tools still needed in the cloud?’ http://ubuntumathiaz.wordpress.com/2009/04/30/are-configuration-management-tools-still-needed-in-the-cloud/.

[9] Holt. A (2003) Three languages for fabric configuration Proc UK e-Science All Hands Meeting.

[10] Talia, P. Trunfio, (2003), Toward a synergy between P2P and Grids, IEEE Internet Computing 7 (4) pp 94–96

[11] Fred B. Schneider, Enforceable security policies, ACM Transactions on Information and System Security (TISSEC), v.3 n.1, p.30-50, Feb. 2000.

[12] Angelis G., Gritzalis.S and Lambrinoudakis. C (2003) Security policy configuration issues in Grid computing environments.

[13] Oppenheimer D., 'The importance of understanding distributed system configuration'

[14] Mather T., Kumaraswamy S., and Latif S., (2009) 'Cloud Security and Privacy' O'Reily.

[15] Stevenson. D (1995) Network Management: What it is and what it isn't.

[16] IMB, (2010) 'Dispelling the vapor around cloud computing'.

[17] Narain S., (2004), Towards a foundation for building distributed systems via configuration. http://www.argreenhouse.com/papers/narain/Service-Grammar-Web-Version.pdf.

[18] S. Bleikertz, M. Schunter, C. W. Probst, D. Pendarakis, K. Eriksson, "Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds", CCSW'10, ACM, 8 October, 2010, Chicago, Illinois, USA
[19] Puppet, http://reductivelabs.com/trac/puppet.

[20] Luke Kanies, Puppet: Next-generation configuration management; login: the USENIX Association newsletter, 31(1), February 2006. ISSN 1044- 6397.

[21] Burgess, M., (1995), "A Site Configuration Engine," *Computing Systems*, Vol. 8, p. 309,

[20] Burgess M., (2004) Principles of Network Administration [2nd Edition], Wiley Publisher.

[22] Delaet T., Wouter J., (2008) 'High-level system configuration'.

[23] Hayden M., (2003), Failure Scenarios and Mistakes Commonly Found in Distributed Systems.