International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

ENERGY, DELAY AND PRIORITY AWARE DATA TRANSMISSION IN WIRELESS SENSOR NETWORK UNDER RELAIBLE NETWORK FORMATION CONSTRAINTS IN CLOUD COMPUTING

Mr. S. Prahadeeshwaran[1],Dr. G. Maria Priscilla[2]

[1]Research Scholar. [2]Prof & Head

Dept. of Computer Science

Sri Ramakrishna College Of Arts & Science Coimbatore.

ABSTRACT

Cloud computing is today's one of the most enticing technology areas due, at least in part, to its cost-efficiency and flexibility. It has brought new changes and opportunities to IT industry. It is the result of the evolution of a variety of techniques. Cloud computing security has become a hot topic in industry and academic research. This paper address an Explore the status of the development of cloud computing security, analyze that the cloud computing security faced with this paper proposed a cloud computing security framework, the purpose of this paper is attempted to being greater clarity landscape about cloud computing security.

I.INTRODUCTION

Since 2007, cloud computing has become hot issue, many companies began to attempt to use cloud computing services. The typical cloud computing service are Amazon'sEC2 and Google's Google App Engine, they use the Internet to connect to external users, and take the large number of software and IT infrastructure as a service provided to users. With the convenience, economy, high scalability and other advantages, cloud computing enables the enterprise liberation from the heavy pressure of the IT infrastructure management and maintenance. Cloud computing change the Internet into a new computing platform, is a business model that achieve purchase on-demand and pay-per-use in network, has a broad development prospects. It is the one of the areas that proposed to give priority to develop in national "Eleventh Five-Year Plan"; the development trend of high speed, heavy and dense in railway, makes all types of data including video and audio data in large-scale growing, so it brings enormous challenges to the information process of the cloud computing as the evolution of multiple technologies, has the key technical characteristics of dealing with the issues above]. But the development of cloud computing is facing many critical issues, the most prominent is the security issue, with the growing popularity of cloud computing, the importance of security show gradual upward trend, become an important factor in the development of cloud computing. 2009 Gartner survey showed that more than 70% of respondents said they do not intend to use the cloud computing at recent, the main reason is afraid of the data

security and privacy. And the burst of a number of security incidents continue to increase more people worried about the cloud. For example, in March2009, the event that a large number of user's files were leaked occurred in Google. Therefore, in order to organizations and businesses can make use of large-scale cloud services, cloud computing technology and platforms, rest assured that their data were migrated to the cloud, we must solve the issues that cloud computing security faced with. The purpose of this paper is attempted to bring greater clarity landscape about cloud computing security.

II.THE CONCEPT OF CLOUD COMPUTING AND CHALLENGES

A. The concept of Cloud Computing

Cloud computing is in under development, there are no widely accepted unified definition. In different stages of development or from a different perspective has a different Understanding on the cloud. U.S. National Institute of Standards and Technology (NIST) defines 5 key features, 3 service model and 4 deployment model of cloud[1], This definition is broad industry adoption.

B. Challenges

In 2008, the U.S. information technology research and consulting firm Gartner issued a "cloud computing security risk assessment" report, mainly from the vendor's point of view about security capabilities analyzed security risks faced by the cloud, listing seven major security risks that the cloud computing technology exist [2], as shown in Table I

TABLE I. SEVEN TOP SECURITY RISKS GARTNER

RISKS	DESCRIPTION
Privileged user access	Sensitive data processed outside the enterprise brings with it an inherent level of risk
Regulatory Compliance	Cloud computing providers who refuse to external audits and security certifications
Data location	When you use the cloud, you probably won't know exactly where your data is hosted
Data Aggregation	Even if you don't know where your data is, a cloud
Recovery	provider should tell you what will happen to your data and service in case of a disaster
Investigative Support	Investigating inappropriate or illegal activity may be impossible in cloud computing
Long-term Viability	You must be sure your data will remain available even after such an event

CS A published in 2009 "in key areas of the cloud Safety Guide" and updated to version 2.1 [3], mainly from the perspective of the attacker summarized the major threats that cloud computing environment may be faced, proposed 12key fields that security concerns, then issued a cloud concise reports security risks, the Security Guide was concentrated to the most common, the greatest threat to harmful levels, as shown in Table II.

TABLE II. SEVEN TOP SECURITY RISKS CSA RISKS

	DESCRIPTION
Abuse and Nefarious Use of Cloud Computing	By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity
Insecure Interfaces And APIs	It increases risk as organizations may be required to relinquish their credentials to third parties in order to enable their agency.
Malicious Insiders	A provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.
Shared Technology Issues	The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment. Your account or service
Data Loss or Leakage Account	The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.
Account or Service Hijacking.	Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.
Unknown Risk Profile	Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture.

Other challenges to be aware of: [3]

• Security auditing and data monitoring: the dynamic nature of the virtual machine, how can organizations ensure the audit ability of records and monitor their data?

• Data privacy: As a user, we lose control over physical security, how can we ensure that data will not leakage and privacy can be protected.

• Key management: If the information is encrypted, then who controls the encryption/decryption key? Customer or

Service provider ?

• Data Integrity: It is not exist that a common standard to ensure data integrity.

III.TRUSTED CLOUD COMPUTING

In 2011 RSA Conference [9], EMC Executive Vice President Arthur described a strategy for ending the lack of trust about cloud computing, pointed out the reason of many companies still not deployed the critical applications in cloud computing environment is the lack of trust, and use the virtualization technology can achieve the cloud environment controllable and visible which two are the key elements of credibility. Santos et al [14] presents a trusted cloud computing platform TCCP, based on this platform, IaaS service providers can offer their subscribers a sealed box execution environment to ensure customer confidentiality of the virtual machine is running. In addition, it allows the user test IaaS service provider if it is safe before start the virtual machine.

IV.IDENTITY MANAGEMENT AND ACCESS CONTROL

Organization for the Advancement of Structured Information Standards (OASIS) [10] collect and coordinate the relevant terms and vocabulary definition about cloud computing, developed the open standards of identity deployment, supply and management, through the collection of use cases to identify the existing gaps in identity management standards in order to explore the interoperability scenarios in the existing standards. Under the cloud computing model, the researchers concerned about how access control through non-traditional means of implementation of the data object class access control. Which received the most attention is the access control methods based on cryptography, including: key generation and distribution based on hierarchical access control policy enforcement methods [16,17]; attribute-based encryption algorithm (such as key encryption based on the attribute rules program (KP-ABE) [13], and based proxy re-encryption[14] methods

V.THE KEY TECHNOLOGIES OF CLOUD COMPUTING SECURITY

A. Virtualization

Virtualization technology is a core technology of cloud computing, the virtual machine is the basic unit of the cloud computing platforms, cloud providers provided services to clients by virtual machines must ensure the security and isolation. Sometimes, however, because of the business needs, the virtual machine need communication with others, which destroyed the isolation? The traffic between virtual machines is difficult to monitor, it will lead to malicious attacks between virtual machines there exists malicious virtual machine. The

company, Altar [6], has developed Virtual firewall for the issues of traffic between the virtual machines, and monitor the traffic between the virtual machines. Wei et al [7] focus on the security of virtual machine image file, the proposed image file management system to achieve the image file access control, source tracking, filtering and scanning, can detect and fix security breach issues. In the un-trusted operating system environment,[8] proposed a secure virtual architecture to provide a safe operating environment and network interface to store the virtual machine.

B. Trusted Cloud Computing

In 2011 RSA Conference [9], EMC Executive Vice President Arthur described a strategy for ending the lack of trust about cloud computing, pointed out the reason of many companies still not deployed the critical applications in cloud computing environment is the lack of trust, and use the virtualization technology can achieve the cloud environment controllable and visible which two are the key elements of credibility. Santos et al [14] presents a trusted cloud computing platform TCCP, based on this platform, IaaS service providers can offer their subscribers a sealed box execution environment to ensure customer confidentiality of the virtual machine is running. In addition, it allows the user test IaaS service provider if it is safe before start the virtual machine.

C. Identity Management and Access Control

Organization for the Advancement of Structured Information Standards (OASIS) [10] collect and coordinate the relevant terms and vocabulary definition about cloud computing, developed the open standards of identity deployment, supply and management, through the collection of use cases to identify the existing gaps in identity management standards in order to explore the interoperability scenarios in the existing standards. Under the cloud computing model, the researchers concerned about how access control through on-traditional means of implementation of the data object class access control. Which received the most attention is the access control methods based on cryptography, including: key generation and distribution based on hierarchical access control policy enforcement methods [16,17]; attribute-based encryption algorithm (such as key encryption based on the attribute rules program (KP-ABE) [13], and based proxy encryption[14] methods

VI.NEW PROBLEMS

In this section we outline new problem areas in security that arise from cloud computing. These problems may only become apparent after the maturation and more widespread adoption of cloud computing as a technology. Cheap data and data analysis. The rise of cloud computing has created enormous data sets that can be monetized by applications such as advertising. Google, for instance, leverages its cloud infrastructure to collect and analyze consumer data for its advertising network. Collection and analysis of data is now possible cheaply, even for companies lacking Google's resources. What is the impact on privacy of abundant data and cheap data-mining? Because of the cloud, attackers potentially have massive, centralized databases available for analysis and also the raw computing power to mine these databases. For example, Google is essentially doing cheap data mining

when it returns search results. How much more privacy did one have before one could be Go-ogled? Because of privacy concerns, enterprises running clouds collecting data have felt increasing pressure to anonymize their data. EPIC has called for Gmail, Google Docs, Google Calendar, and the company's other Web applications to be shut down until appropriate privacy guards are in place [23]. Google and Yahoo!, because of pressure from privacy advocates, now have an 18 month retention policy for their search data, after which it will be anonymized. This means that some identifying data will be removed such as IP addresses and cookie information. The anonymized data is retained though, to support the continual testing of their algorithms. Another reason to anonymize data is to share data with other parties. These may be to support research (e.g., the AOL incident [4]) or to subcontract out data mining on the data (e.g., the Netflix data set [16]). This note that anonymizing data is a difficult problem. For example, in [33] the Netflix data set was partially de-anonymized, and in [45] the then-Governor of Massachusetts was identified as a patient of Massachusetts General Hospital from an anonymized list of discharged patients. Tools are needed for effective anonymization, which will increase in importance as clouds proliferate and more data is collected that needs to be analyzed safely or shared.

An example of indirect data-mining that might be performed by a cloud provider is to note transactional and relationship information (see World Privacy Forum Report [36]). For example, the sharing of information by two companies may signal a merger is under consideration.

Cost-effective defense of availability.

Availability also needs to be considered in the context of an adversary whose goals are simply to sabotage activities. Increasingly, such adversaries are becoming realistic as political conflict is taken onto the web, and as the recent cyber attacks on Lithuania confirm [15]. The damages are not only related to the losses of productivity, but extend to losses due to the degraded trust in the infrastructure, and potentially costly backup measures. The cloud computing model encourages single points of failure. It is therefore important to develop methods for sustained availability (in the context of attack), and for recovery from attack. The latter could operate on the basis of minimization of losses, required service levels, or similar measures.

Increased authentication demands

The development of cloud computing may, in the extreme, allow the use of thin clients on the client side. Rather than a license purchased and software installation on the client side, users will authenticate in order to be able to use a cloud application. There are some advantages in such a model, such as making software piracy more difficult and giving the ability to centralize monitoring. It also may help prevent the spread of sensitive data on untrustworthy clients. Thin clients result in a number of opportunities related to security, including the paradigm in which typical users do not have to worry about the risks of any actions – their security is managed by the cloud, which maintains the software they run. This architecture stimulates mobility of users, but increases the need to address authentication in a secure manner. In addition, the movement towards increased hosting of data and applications in the cloud and lesser reliance on specific user machines is likely to increase the threat of

phishing and other abusive technologies aimed at stealing access credentials, or otherwise derive them, e.g., by brute force methods.

Mash-up authorization

As adoption of cloud computing grows, we are likely to see more and more services performing mash-ups of data. This development has potential security implications, both in terms of data leaks, and in terms of the number of sources of data a user may have to pull data from – this, in turn, places requirements on how access is authorized for reasons of usability. While centralized access control may solve many of these problems, that may not be possible – or even desirable.

One example in this area is provided by Facebook. Facebook users upload both sensitive and non-sensitive data. This data is both utilized by Facebook to present the data to other users, and also utilized by third party applications that are run by the platform. These applications are typically not verified by Facebook. Hence, there is a drive to create malicious applications that run in Facebook's cloud to steal sensitive data, e.g., see [21].

VII.CONCLUSION

Cloud computing is the most popular notion in IT today; even an academic report [5] from UC Berkeley says "Cloud Computing is likely to have the same impact on software that foundries have had on the hardware industry." While many of the predictions may be cloud hype, we believe the new IT procurement model offered by cloud computing is here to stay. Cloud fears largely stem from the perceived loss of control of sensitive data. Current control measures do not adequately address cloud computing third-party data storage and processing needs. In our vision, we propose to extend control measures from the enterprise into the cloud through the use of Trusted Computing and applied cryptographic techniques. Our vision also relates to likely problems and abuses arising from a greater reliance on cloud computing, and how to maintain security in the face of such attacks. Namely, the new threats require new constructions to maintain and improve security. Cloud computing deployment model led the physical boundary of the network disappears, the cloud facing the challenges of access control. Virtualization technology is the core technology of Cloud computing, users are most concerned about data security, so virtualization security and data security are the main problem of the cloud computing security. Cloud computing security needs consider both technology and strategy, including: audit, compliance and risk assessment. At the aspect of strategy management of security mechanism, we should concern on the strategy of network security and management field.

REFERENCE

[1] Amazon S3 Availability Event: July 20, 2008. http://status.aws.amazon.com/s3-20080720.html.

[2] Amazon's terms of use. http://aws.amazon.com/agreement.

[3] An Information-Centric Approach to Information Security. http://virtualization.sys-con.com/node/171199.

[4] AOL apologizes for release of user search data. http://news.cnet.com/2100-1030_3-6102793.html.

[5] Armbrust, M., Fox, A., Griffith, R. et al. Above the Clouds: A Berkeley View of Cloud Computing. UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 2009.

[6] Boneh, D and Waters, B.Conjunctive, Subset, and Range Queries on Encrypted Data. In The Fourth Theory of Cryptography Conference (TCC 2007), 2007.

[7]Chor, B., Kushilevitz, E., Goldreich, O., and Sudan, M. Private Information Retrieval. J. ACM, 45, 6 (1998), 965-981.

[8]CLOIDIFIN. http://community.zdnet.co.uk/blog/0,1000000567,2000625196b,00.htm?new_comment.

[9]Cloud Bursts as Coghead Calls It Quits. http://blogs.zdnet.com/collaboration/?p=349

[10] Disaster-Proofing The Cloud. http://www.forbes.com/2008/11/24/cio-cloud-disaster-tech-cio-cx_dw_1125cloud.html.

[11] Don't cloud your vision. http://www.ft.com/cms/s/0/303680a6-bf51-11dd-ae63-0000779fd18c.html?nclick_check=1.

[12] EMC, Information-Centric Security. http://www.idc.pt/resources/PPTs/2007/IT&Internet_Security/12.EMC.pdf.

[13] End-User Privacy in Human–Computer Interaction. http://www.cs.cmu.edu/~jasonh/publications/fnt-end-user-privacy-in-human-computer-interaction-final.pdf.

[14] ESG White Paper, The Information-Centric Security Architecture. http://japan.emc.com/collateral/analyst-reports/emc-white-paper-v4-4-21-2006.pdf.

[15] Chang YC, Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data. Report 2004/051. Cryptology ePrint Archive, 2004. http://eprint.iacr.org/2004/051/ Resource Management Policy for Cloud Testbed of China Railway.

[16] Agarwal S, Sprick B. Access control for semantic Web services. In: Proc. of the IEEE IntT Conf. on Web Services. 2004. 770-773.