Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security on Cloud Using Cryptography

Akansha Deshmukh, Harneet Kaur Janda, Sayalee Bhusari
Department of Information Technology Yeshwantrao Chavan College of Engineering,
Nagpur, Maharashtra, India

Abstract— As the data produced by the enterprises that need to be stored and utilized (e.g. emails, personal health records, photo albums, tax documents, financial transactions, etc.) is rapidly increasing, data owners are motivated to outsource their local complex data management systems into the cloud for its great flexibility and economic savings. Cloud storage allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. In cloud storage, the data will be stored in storage provided by cloud service provider (CSP's). Cloud service providers must have a viable way to protect their client's data, especially the data from disclosure to unauthorized users. But in data privacy protection and data retrieval control is most challenging research work in cloud computing. Also service provider must provide authentication for valid user otherwise security reduce and cloud system may collapse. This paper mainly focus on core secured cloud storage services i.e. Cryptography to provide cryptographic techniques for securing data and computation in a cloud environment. Cryptography in cloud computing is a new secure service regarding security and privacy in cloud.

Keywords - Cloud Computing, Cryptography, Caas, Encryption and Decryption services.

I. INTRODUCTION

Cloud computing is the most envisioned paradigm shift in computing world. It's services are these days generally being applied in several IT scenarios. Cloud computing is a recently developed technology for complex systems with large-scale services sharing among multiple users. Therefore, authentication and integration of both users and services is a significant issue for the trust and security of the cloud computing unique platform has brought new security issues to contemplate. Cloud computing is essentially the management and provision of applications, information and data as a service. These services are provided over the internet, often on a pay-as-you-go based model. Cloud computing provides a convenient way of accessing computing services, independent of the hardware you use or your physical location. It relieves the need to store information on your PC, mobile device or gadget with the assumption that the information can be quickly and easily accessed via the net. Cloud computing provides clients with a virtual computing infrastructure which enables them to store data and run applications. Cloud computing introduces new security challenges as client can't fully trust cloud providers. Cryptography in cloud computing depends on a secure cloud computing architecture. Cloud computing is a computing model that is driven by economies of scale and is distributed on large scale. Cloud architectures are developed according to latest and urgent demands. That is, the resources are dynamically provided to a user as per his request ,and taken back after the job is done. Cloud computing is a service pool which includes the hardware and operating system infrastructure, the formation of systems management software, system and platform, and virtualization components.

II. CLOUD SERVICE MODELS

There are three main types of cloud service:
A. Software as a Service (SaaS)
B. Platform as a Service (PaaS)
C. Infrastructure as a Service (IaaS)

A. Software as a Service (SaaS)

In the business model using software as a service (SaaS), users are provided access to application software and databases. Cloud service providers give users the access to infrastructure and platforms that run the applications. SaaS is also known as "on-demand software" and is usually cost is estimated on a pay-per-use basis and also a separate subscription fee. A model of software deployment whereby a provider licenses an application to customers for use as a service on demand. The applications can be accessed from various client devices through a thin client and cloud interface such as a web browser (eg web-based email). SaaS breaks the link between machines and solutions,which results in enabling customers to license only what they need. Business functions which require a high degree of integration with other institutional systems may present more interoperability issues. SaaS allows a potential business to cut down the IT operational costs by facilitating outsourcing hardware and software maintenance and support to the cloud provider. This enables the business to shift the big IT operations costs away from hardware or software and personnel expenses, towards meeting other important goals. Moreover, as the applications are hosted centrally, updates can be released without the

necessity for users to install new software. One con of SaaS is that the users' data are stored on the cloud provider's server. Therefore, there could be unauthorized access to the data. For this reason, users are increasingly adopting intelligent and reliable third-party key management systems to help secure their data.

B. Platform as a Service (PaaS)

In the PaaS models, cloud providers deliver a "computing platform", which includes operating system, programming language execution environment, webserver and database. In this model the consumer develops or deploys applications onto the cloud infrastructure using provided programming languages and tools supported by the cloud provider.

Application developers can develop and run their software on a cloud platform without the expenditure and complexity of buying and managing the hardware and software layers behind the software. With some PaaS offers like Windows Azure, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually. The latter has also been proposed by an architecture aiming to facilitate real-time operations in cloud environments. The consumer does not involve in managing or controlling the underlying cloud infrastructure including network, servers, operating systems, or storage. Users will have full control over the deployed applications and possibly application which hosts environment configurations.

C. Infrastructure as a Service (IaaS)

In this service model the institution which wants to use cloud services outsources all of its infrastructure including servers, storage, associated networking, etc to an external provider. This category of model is sometimes referred to as Hardware as a Service. In the most basic cloud-service model, providers of IaaS offers user a computers physical or virtual machines and other resources. (A hypervisor, such as Hyper-V or Xen or KVM or VMware ESX/ESXi, runs the virtual machines as guests. Pools of hypervisors within the cloud operational support- system can support large numbers of virtual machines and the ability to scale services up and down according to cus

tomers' varying requirements.)The service provider owns the equipment and is responsible for housing, running and maintaining it. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components, for example, hosting of firewalls. IaaS clouds often offer additional resources example, virtual-machine disk image library, raw (block) and file-based storage, load balancers,firewalls, IP addresses, virtual local area networks (VLANs), and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds that is dedicated virtual private networks.

III. SECURITY IN CLOUD COMPUTING

Security has always been the main issue for IT Executives when it comes to cloud computing and its adoptation. In two survey carried out by IDC in 2008 and 2009 consecutive years security topped the list. However, cloud computing is aggregation of technologies, operating systems, storage, networking, virtualization, each fraught with inherent security issues. For example, browser based attacks, denial of service attacks and network intrusion became carry over risks into cloud computing world. The benefits of using cloud computing are very well known and several of the benefits are outlined above. However, cloud computing is not without its pitfalls. The majority of which center around security of data that is stored in the cloud. There are potentials for a new wave of large- scale attacks via the virtualization platform. Cattedu et al. described the “Fear of the Cloud” by categorizing security concerns into three traditional concerns, availability and third party data control Research firm Brunett posited seven security risk ranging from data location and segregation to recovery and long-term viability. A customer’s data security relies on security service from cloud computing providers, however, current structure of cloud computing services are provided by independent operators. Organizations such ISACA and Cloud Security Alliance publish guidelines and best practices to mitigate the security issues in the cloud [1920]. First, the user’s information security provides commerce and management. Second, the information leakage can be caused by technology flows of providers. What’s more, cloud computing is an open environment. Hence, any weakness will cause information security risks of the whole system.

IV. CRYPTO CLOUD COMPUTING

Cloud computing is a combination of IaaS, PaaS, SaaS. To construct a secure cloud computing system, security at infrastructure, service platforms and application software levels have to be studied for a secure cloud computing system. Information encryption is one of effective means to achieve cloud computing information security. Traditionally, information encryption focuses on specified stages and operations, such as data encryption. For cloud computing, a system level design has to be implemented. Crypto cloud computing is a new secure cloud computing architecture. It can provide protection of information security at the system level, and allows users access to shared services conveniently and accurately. Crypto cloud computing protects individual’s connections with the outside world. It can protect the personal privacy without any delay of information exchange. Crypto cloud computing is based on the Quantum Direct Key system. Quantum Direct Key (QDK) is a set of advanced asymmetric offline key mechanism. In this mechanism, all entities get public and private key pair according to their ID. Each entity only holds its own private key, but has a public key generator to generate any public key. In this system, an entity can produce the public key of any other entities offline, no any third-party agency (such as CA) is necessary. Crypto cloud computing based on QDK can avoid network traffic congestion, and other drawbacks using current encryption system. In the crypto cloud computing system, each entity

encrypts data using his/her own private key. All elements in the system such as cloud computing infrastructure units, platform, virtualization tools and all involved entities have their own keys. While fulfilling their own functions of information exchange and processing, all these elements will use the public key and private key to perform authentication first. What's more, events occur in the cloud computing are also assigned a unique key. Thus, crypto cloud system assures the security and credibility of information exchange.

Current cloud computing structure is developed for data and computing sharing. Security is not priority of system. On the contrary, encryption and security are inherently integrated in the crypto cloud computing based on the QDK. QDK authorized function units are bricks of crypto cloud computing. Besides primary function of data encryption /decryption, crypto cloud computing also provides many security related functions. For example, all channels sign transmit data using with their own keys, and the receiving terminals can avoid hijacking by verifying signature. What's more, the exact position of security leakage can be identified determined by analyzing digital signatures of forged data. Based on such capabilities, crypto-related functions can be provided as services in cloud, which is named as 'Crypto as a service (CAAS). Crypto cloud computing is not only the advances in information technology, but also innovation of logical relationship. In crypto cloud computing system, non-system data is not allowed to store and transmit. Private Key and offline public key, play a role of identification and certification in the process of information exchange. In this way, the cloud establishes a relationship of trust with a customer. Data identification depends on the logical relationship of mutual trust or need, and the logical relationship depends on the cloud customer.

V. IMPORTANCE OF CRYPTO CLOUD COMPUTING

Crypto cloud computing is a new framework for cyber resource sharing. It protects data security and privacy. Well, in cloud environment, crypto cloud computing guarantees the information security and integrity during whole procedure. Security management of cloud computing can also be performed by authorizing the signatures of every element involved. What's more, a user can retrieve all related resources using his QDK key. There is no personal privacy under the current cloud framework, as pointed out by Mark Zuckerberg, 'the Age of Privacy Is Over '. [7]However, with the development of crypto cloud computing, we can resolve the conflict between services data sharing and privacy security. It opens up new prospects for the development of information sharing technology.

Recommended Future Research

Although cloud computing is being widely used today, there still exists several security concerns involved with storing ones data in the cloud. Providing defenses for these security concerns is an active area of research and rightly so.[16] Some of the issues can be addressed with existing technology and techniques, while others, such as threat exposure due to multi-tenancy, may need to be addressed with new techniques and research. Much more research needs to be done in the field of searchable cryptography before the virtual storage with searchable encryption approach discussed in this paper becomes a really viable solution for real-life deployment. One of the main problems with cloud computing is that the competitiveness of the provider's service offering could depend on having a certain degree of multi-tenancy.[15] By having many customers' data stored on the same physical hard drives, it is very possible for someone to gain control over a process that may have access to another customer's data. More research needs to be done on ways to segregate user data when stored on common media.

While the protection of data in transit can easily be accomplished through existing encryption processes, securing data in storage requires the additional tasks of key management (using existing techniques). The environment of cloud computing is unique in that the data is owned by the customer while the physical resources (hardware & software) are owned by the provider. In this type of environment, key management practices have yet to evolve.[6] This is another area where more research and possibly standards need to be applied in order to meet the encryption requirements of data in storage. While there are solutions to most of the security concerns, there is not a good technology or encryption technique made specifically for this type of computing. Cloud computing can providers can offer secure services, but using technology that was never meant for this type of computing presents several security concerns as mentioned in this paper.[13] We don't recommend people stay away from clouds, on the contrary, we recommend that companies need to carefully weigh the current security deficiencies and the benefits before making a decision to implement cloud computing. The future of the cloud looks good as more and more people and researchers are being attracted by the topic and pursuing research to improve on its drawbacks.

VII. CONCLUSIONS

The Cloud computing as a technology would be adopted if the areas of concerns like security of the data will be covered with full proof mechanism. The strength of cloud computing is the ability to manage risks in particular to security issues. Our suggested model will present an outline sketch of architecture to be adopted by architects involved in implementing the cloud computing. Security algorithms mentioned for encryption and decryption and ways proposed to access the multimedia content can be implemented in future to enhance security framework over the network. In the future, we will try to explore our research by providing algorithm implementations and producing results to justify our concepts of security for cloud computing. In order for this approach to work as intended, the cloud service provider must co-operate with the user in implementing solution. Some cloud service providers base their business models on the sale of user data to advertisers. These providers probably would not be willing to allow the user to use their applications in a way that preserves user privacy.

ACKNOWLEDGEMENT

We would like to express our gratitude and appreciation to all those who helped use to complete this paper. A special thanks to our guide, Ms. Pallavi Matkar whose help, stimulating suggestions and encouragement, helped us in writing this paper. At last, we are thankful to our families & friends whose encouragement and constant inspiration helped us to complete this paper work verbally and theoretically.

REFERENCES

[1] National Institute of Standards and Technology Computer Security Division http://csrc.nist.gov/groups/SNS/cloud-computing

[2] Web Search For A Planet: The Google Cluster Architecture. Retrieved April 6, 2011, available at: http://labs.google.com/papers/googlecluster-ieee.pdf

[3] What is Cloud. Retrieved April 6, 2011, available at: http://www.rackspace.co.uk/cloud-hosting/learn-more/whatis-cloud/

[4] What is Cloud Computing. Retrieved April 6, 2011, Available:http://www.microsoft.com/business/engb/solutions/Pages/Cl oud.aspx

[5] R. Rivest, L. Adleman, and M. Dertouzos. On datbanks and privacy homomorphisms. In Foundations oSecure Computation, pp. 169–180, 1978.

[6] R. Rivest, A. Shamir, and L. Adleman. A method foobtaining digital signatures and public-key cryptosystems In Comm. of the ACM, 21:2, pages 120–126, 1978

[7] James Mark Kelly,Columbus state University CPSC 6128 Spring 2010- Cloud computing and cryptography

[8] Seny Kamara and Kristin Lauter, "Cryptographic Cloud Storage, in Proceedings of Financial Cryptography": Workshop on Real-Life Cryptographic Protocols and Standardization 2010, January 2010.

[9] Hugo A.W.Ideler "Cryptography as a service in a cloud computing environment" Master Thesis(Eindhoven University Of Technology Department Of Mathematics And Computing Science)

[10] John K. Waters. 2010. Cryptographers Warn About Security Danagers in the Cloud at RSA. In Application Development Trends. March 09, 2010. http://adtmag.com/articles/2010/03/09/cryptographers-security-danagers-cloud-rsa.aspx.

[11] Security Issues in Cloud Computing: The Potentials of Homomorphic Encrypt Aderemi A. Atayero,Oluwaseyi Feyisetan- Journal of Emerging Trends in Computing and Information Sciences IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. Retrieved April 8, 2011 from http://blogs.idc.com/ie/?p=210

[12] New IDC IT Cloud Services Survey: Top Benefits and Challenges. Retrieved April 8, 2011 from http://blogs.idc.com/ie/?p=730

[13] Catteddu, D. and Hogben, G." Cloud Computing: benefits, risks and recommendations for information security." Technical Report. European Network and Information Security Agency, 2009.

[14] "Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. White Paper.Information"

