International Journal of Scientific & Engineering Research, Volume 3, Issue 12, December-2012
ISSN 2229-5518

Enhancing Data Security in Cloud Computing

Yuvraj Gupta

Abstract— Cloud Computing is a new mechanism to deliver products from producer to consumer in a very different and efficient style of computing. It has revolutionized not only the IT industry but has also revolutionized the hardware and software industry. It is growing leaps and bounds and has only bright sky ahead. But will you love to see a bright sky with embraces of black holes? Obviously you won't, similarly security is the main issue which acts as a blackhole to the whole system of it specialists in this domain. The main mission of security is to limit access to the authorized person, who can see, modify only that data which they are associated with. When we talk about the security of data in Cloud Computing the vendor has to ensure assurance to convince the customer on the security issues. Organizations are using cloud computing for confidential issues for their business applications though guaranteeing the security is difficult. This paper is divided into different sections such as:

- Introduction to Cloud.
- Benefits of Cloud.
- Cloud Data Security.
- Enhancement in Security.
- Conclusion.

This paper will enlighten the various improved methods for dealing with data security in the domain of biometrics, cryptography, public key infrastructure and Cloud Standards in the venture of Cloud Computing. We will focus on the security enhancement of cryptography and biometrics by their combinations. This paper is aimed at being a reference point to understand the basic security ideas for the newcomers and intended to promote more activities and research in these critical and very important security issues which has to be addressed.

Index Terms— Cloud Computing. Benefits of Cloud, Data Security, Enhancing Data Security, Cryptography, PKI, Biometrics, Cloud Data Security, Cloud Standards

1 INTRODUCTION

Cloud Computing can be seen as the latest revolution in Information and Communication Technology. In Cloud IT services are abstracted from provided on demand as well as underlying infrastructure in a multi-tenant environment. Cloud enables on demand network access to a shared pool of computing resources (such as servers, applications, network, storage) that can be provisioned with minimal management effort. Cloud has the option of pay per use annuity payments wherein large upfront capital investment in IT infrastructure can be converted into smaller units based on requirement. The best starting point to think of the cloud is internet. User just logs in to his computing device. Cloud is a new computing paradigm that opens the door to bold new possibilities. Cloud will change the way the world works, plays, lives and learns. Enterprises have started moving their whole servers, applications on the cloud to ensure 24/7 access, improved customer experience, pay as per use which helps in cost cutting, interoperability and scalability. Cloud computing has taken it to new heights with flexible scalable computing to match industry demand while reducing capital expenditure.

IT has dealt with 3 basic metrics:

- Demand
- Capacity
- Performance

Fundamental tradeoff of it makes capacity comes from many resources. We can express it as: Processing Time=Workload/Resources. But cloud just changes this equation forever, as capacity is virtually unlimited provided you're willing to pay as per use.
Processing Time=Workload/ ∞.
In other words this is a massive oversimplification as we can have as much performance we want until you're paying for it.

2 BENEFITS OF CLOUD

2.1 Accelerates your business by providing limitless scalability and transforming ideas with a greater speed into marketable services and products.

2.2 Brings powerful IT resources to the world. Organizations across the globe can access information technologies which were earlier out of reach, computing infrastructure and world class applications are available without considerable investment up front.

2.3 Unlocks revenue potential and makes new business models available for any business.

• *Yuvraj Gupta is currently pursuing undergraduate degree program in computer science engineering with specialization in Cloud Computing and Virtualization Technology in University of Petroleum And Energy Studies,Dehradun, India.*
Mob No- +91-9997572251
E-mail: gupta.yuvraj@gmail.com

2.4 Companies can now collaborate more efficiently to drive business value and innovations

2.5 Cloud reduces operating risks as well as improves information management. Protects sensitive information and simplifies disaster recovery.

2.6 Cloud transforms the economics of the industry from capital driven to pay-as you go. Costs are metered according to the requirements and usage. SLA guarantees the capabilities when you need them. There is greater utilization of the underlying infrastructure.

2.7 The core advantage of cloud computing is its ability to access high performance computing systems on the basis of sharing and time model.

2.8 Use of standard technology is encouraged and facilitated while delivering the latest technology and with full optimization of resources.

3 CLOUD DATA SECURITY

Security has emerged as the most important barrier to faster and widespread adoption of virtualization as well as cloud computing. It depends from person to person as well as industry to industry how they analyze the concept of security in Cloud Computing. The main questions while shifting to cloud are:

1. How secure is the data?
2. Where is the data?
3. Who has access?
4. Can you trust the company or third party?
5. How much confidential will your data be?
6. How does cloud provider keep different clients data separated and inaccessible from other clients?

Few answers regarding security discussed above:

- As the data is in the cloud different companies and countries have different requirements as well as controls placed on access because we may not realize that the data must reside in some physical location.
- Every cloud provider should have all the agreements in writing to provide maximum transparency to provide the different level of security required by different customers.
- Every cloud provider must have fixed service level agreements regarding various things such as data privacy, limit of third party access to the confidential data etc.
- Access control is a key concern as insider attacks also possess a huge risk. Anyone who has been entrusted with proper authentication to the cloud could be a potential hacker. If anyone doubts this, consider in 2009 an insider was accused of planting a logic bomb on Fannie Mae servers, if launched it would have caused massive damage.
- The standards have been defined to ensure that third parties have sufficient control in handling data. ISO 27001 and SAS 70 have been adapted to ensure maximum cloud security.

3.1 Common Mistake and Challenges in Cloud Security

3.1.1 Failing to use cryptography when cryptographic security is a viable option. Everything should be encrypted by default.

3.1.2 Failing to use cryptographically secured protocols when you have a choice. Using ftp, telnet or http rather than a secured version of these plaintext protocols is simply negligent.

3.1.3 Network packet sniffing is a pastime on many machines that take part in sending packets back and forth between your laptop and a cloud-based service. Although these protocols should have been retired long ago, they are still common and being available they are used. No cloud implementation should allow these.

3.1.4 Sending sensitive data in unencrypted e-mail. Sending passwords, pins, or other account data in unencrypted e-mail exposes that data in multiple places.

3.1.5 Hackers are a real concern for data management as per Cloud service providers; they can compromise the data which ranges from selling sensitive information to competitor or damage the businesses.

3.1.6 Attackers use bot attackers or botnets to perform distributed denial of service attacks through which we face blackout.

3.2 Benefits of Enhanced Security in Cloud

3.2.1 Reduced data loss: By maintaining the data on the cloud, employing strong access control and limiting a person download to only what they need, cloud computing would limit the amount of information that could potentially be lost.

3.2.2 Monitoring: By having data on the cloud it is easier to monitor the security from anywhere rather than worrying about the security of number of clients and servers.

3.2.3 Instant Swapover: we now don't require spending hours trying to replicate the data or fix the breach incase of moving the data to another machine. Abstracting the hardware would allow it instantly.

3.2.4 Secure builds: With a cloud solution model we do not require to buy third party security software to secure our network, but these tools can be made into a complete package which would be available on pay per use and could enhance our system with the type of security which we will require. We can perform the patches and upgrades offline. It will enhance the ability to test the impact of our security changes in offline mode as well.

3.2.5 Improved software security: As the vendors would face a stiff competition and wouldn't like to lose their business they would develop more efficient security software as the vendor knows the most efficient secured product will win the game.

3.2.6 Security testing: Security testing would become quite cheap as it will be shared and pooled among the cloud users for the SAAS providers. With cloud code scanning tools the code developed by developers would check the code for vulnerabilities.

4 Security Enhancement by Combining Biometrics to Cryptography

A combination of cryptography and biometrics has immense scope of providing a higher security platform in various fields. The most important issue in cryptographic systems is the key management. Therefore in order to combine biometrics with cryptography we have to relate to the issue of how to combine biometrics along with cryptographic keys.

The 3 important steps involved while combining biometrics with cryptography are biometrics key release, biometrics key generation and biometrics key binding. In key release mode, if the biometric matching is successful then only the user will be able to view the key. In key generation mode, we require the key of a cryptographic system which is being derived from the biometric template hence providing a platform for the security systems as the unique biometrics results in an unique key which is based on some feature or transform extraction.in the key binding mode, the system secures the user biometrics with the cryptographic key at the time of using it for the first time i.e. Enrollment. The key would only be displayed if all the user details match perfectly with the cryptographic keys. The key generation/ binding mode is very much secured as compared to key release mode because key release mode involves the key release and user authentication as two separate and different parts rather than involving a dual mode exchange by the user as well as the cryptography. The conventional cryptography systems depend on the accuracy of the matching of the key and do not require any complex pattern recognition. The key matching process should be very accurate and could not tolerate even smallest of error. As the biometrics are known to be not absolutely accurate and is known to be quite variable, therefore researchers face the challenge of bridging the gap between fuzziness of biometric matching and exactness of the cryptographic system with much higher accuracy rate.

4.1 Enhancement in Security with Biometrics

Types of Biometrics:

4.1.1 Fingerprint recognition: As fingerprints have been recognized as a primary and accurate method of identification. Authentication (1-to-1): matches a person's identity to their respective biometrics with one or more security technologies (PKI token, password etc). It uses the ridge endings on a person finger to form minutiae. The number and location vary from finger to finger as well as from person to person.

4.1.2 Face recognition: The principle solely is the analysis of the shape, positioning and pattern of facial features.it is highly complex technology and largely software based. Its primary advantage is that it is hands free and a user identity is matched and confirmed by simply staring at the screen.

4.1.3 Iris recognition: It is based on the analysis of the iris of the eye, visible features (corona rings etc). It is regarded as the most safe, accurate biometrics technology and capable of performing 1-to-many matches without sacrificing the accuracy. It is a highly mature technology with a proven track record in number of applications.

4.1.4 Retina recognition: It is the pattern of blood vessels that emanate from the optic curve and disperse throughout the retina which depends on individuals. A retina scan cannot be faked as it is quite impossible to forge a human retina. It is highly accurate and has an error rate of 1 in 10,000,000.

The application of biometrics cannot be uniform for each and every level of people. For different level of people we need entirely different type of technology which would be the best for them. We can conclude that:

For Defence sector as it contains very sensitive information which they cannot afford to leak we must deploy retina recognition as well as iris recognition at different levels of their hierarchy organization.

For Financial sector we must use the technology of face recognition as well as fingerprint recognition which could be more enhanced with the use

of one time passwords for funds transfer, access to internet banking etc.

For privacy of the emails we can have powerful email encryption as well as decryption tool which would insure data security and proper handling of sensitive information. At the login page passwords should be replaced with one time password for enhanced security.

4.2 Public Key Infrastructure (PKI)

It is used to secure data transmission and authentication system, secures privately exchanged data with the help of public keys and private keys which is obtained via a trusted authority. It uses encryption, digital signatures, digital certificates, decryption, certificate authorities, certificate revocation and storage.

4.2.1 Components of public key infrastructure are:

4.2.1.1 Certification authority (CA): The CA issues the certificate and is responsible for identifying correctness of the identity of the person and verifies the certificate and digitally signs it. It also generates key pairs.

4.2.1.2 Revocation: When a system publishes certificates there should be a system to let the people know when these certificates are invalid. The challenge to this is that a distributed denial of service attack on the directory or database of stored certificates might create appearance of a fake certificate.

4.2.1.3 Registration Authority: They are used by the CA to perform necessary identity checks regarding the person or company to prevent from forgery.

4.2.1.4 Certificate publishing method: It is the fundamental of PKI systems where certificates are published such as directories, databases, e-mails etc so that the user finds it.

4.2.1.5 Certificate management system: The management system through which certificates are published, renewed, temporary or permanently suspended or revoked.

PKI is the most evolved form but few things could be implemented:

PKI should be embedded in every system which would automatically encrypt the data for the sender and decrypt the data for the receiver with the help of public or private keys.

The keys could be enhanced with introduction of biometrics between the encryption and decryption process which would make it a complex structure to break upon.

The encryption algorithm could be more rigid and strong.

5 Cloud Standards

As the cloud computing is involving at a very high rate of speed though it is at an early stage of development. There is an urgent need of a global cloud computing standards but there is a risk of fragmentation and diffusion which could even make people wary of adopting it. For any business to move into cloud there is a need of high level of trust which is based on knowing exactly what profit will the business have, how it will get and when. Therefore a trusted set of standards are required which every service provider would adhere which would help bringing more and more companies in adopting cloud computing in a widespread manner. Standardization would allow greater flexibility for a company to move from one service provider to another. We need to consolidate more on various aspects of cloud such as cloud management, governance and security. We need different standards for different applications such as standards for cloud architecture, cloud applications, service oriented architecture, web services standards, web application frameworks etc.

One of the major standard which is required is the adoption of a global it law which could be explained easily via an example:

An ABC company in India has adopted cloud computing service with XYZ company as service provider located in Usa. If there is any dispute regarding any security breach with respect to data or privacy then who would be responsible? Where will the legal case be fought? What outcome will it have on company's reputation? What effect will it have on world economy? Who would pay or bear the compensation of the customer? If the data is attacked where will ransoms come to for threats?

These thoughts would ponder but one of the trickiest question to answer is where the case would be fought? Whether it would be in India or USA, whether it will be fought according to USA laws or Indian laws. Nothing has been definite and part of Global Standards, for this it requires a strong global law which would reduce dispute between 2 countries and service of cloud computing would flow more easily.

6 CONCLUSION

Currently cloud computing is at the starting stage. As an enterprise realizes its benefits over a period, usage of cloud is expected to increase and increase. Cloud would facilitate delivery of more and more cost effective it services. Cloud computing is a rapidly evolving model with new capabilities, innovations and updates being regularly announced and has to be utilized to gain maximum yield. We need to address to the challenges of security to turn it from weakness to strength with the help of advancements in cryptography, biometrics, PKI and Cloud Standards. Cloud Service Providers must safeguard the security and privacy of personal data which they host of their customers. The adoption of cloud system users must be reassured that privacy and security is not compromised. Responsible Management of data is the most central part of creating the trust as without trust enterprises would be reluctant in adopting cloud based services. The advantages of cloud computing - its ability to bring powerful IT resources and world class applications with low investment cost, store data in remote places, interoperability and resource pooling. In this paper security mistakes, challenges and benefits which are currently faced in Cloud Computing industry has been addressed and highlighted. Managing security is one of those aspects where a great deal of investment and research must take place for evolving this technology. The other aspect is the standardizing of Cloud Computing security standards for data security, data management, protocols etc. Cloud Computing has the potential of being the frontrunner in building up of a secured and economically viable IT solution. The cloud needs to target small and medium size companies for migrating their businesses to the cloud which would reduce costs and would give them the opportunity to access technologies and applications which were earlier beyond the reach of organizations.

REFERENCES

1. Biometrics: A Further Echeleon of Security- Siddhesh Angle, Reema Bhagtani, Hemali Chedda.
2. "The NIST Definition of Cloud Computing (Draft)". National Institute of Science and Technology. Retrieved 24 July 2011.
3. Enterprise Cloud Computing By Gautam Shroff
4. International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (2), 2011 Security Perspective of Cloud Computing with Survey of Security Issues- S.Thirukumaran, M.Sanjay Ram, A.Vijayaraj
5. Comparing Passwords, Tokens, and Biometrics for User Authentication- Lawrence O'Gorman
6. Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations- Jing Dong and Tieniu Tan
7. Data Security Model for Cloud Computing- Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing
8. Cloud Security And Privacy- An Enterprise Perspective on Risks And Compliances.
9. Towards Analyzing Data Security Risks in Cloud Computing Environments- Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma
10. Cloud Security- A Comprehensive Guide to Secure Cloud Computing
11. Data Security in the World of Cloud Computing- John Harauz, Lori M. Kaufman, Bruce Potter
12. Cloud Security Issues -Balachandra Reddy Kandukuri , Ramakrishna Paturi V, Atanu Rakshit
13. Effectively And Securely Using The Cloud Computing Paradigm- Peter Mell, Tim Grance- NIST Information Technology Lab
14. The Management of Security in Cloud Computing- Ramgovind S, Eloff MM, Smith E
15. Cloud Computing a world Changing Power- Dr.Fang Binxing
16. Cloud Computing is not (Just) Virtualization Security- Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra,Diego Zamboni
17. Strategies for assessing cloud security- IBM Global Technology Services Thought Leadership White Paper.
18. Security And Cloud Computing- Dr. Michael Waldner
19. Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography- M.Sudha, M. Monica.
20. http://labs.safelayer.com/en/research-and-development/focus-areas/security-trust-and-privacy/460-cloud-computing-security-and-trust-workshop
21. Security Perspective of Cloud Computing with Survey of Security Issues- S.Thirukumaran, M.Sanjay Ram, A.Vijayaraj.
22. Enhancing Security and Privacy in Biometrics- Based authentication systems- N.K. Ratha, J.H. Connell, R.M. Bolle.
23. Gartner report "Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014." The report is available on Gartner's website at http://www.gartner.com/resId=1378513.
24. Business Week June 2010: businessweek.com.
25. Assessing the Security Risks of Cloud Computing c 2008 Gartner, Inc.