Data Security in Cloud using Blowfish Algorithm

Govinda.K[1] Mythili D[2] Geetha Priya S[3]
[1,2,3]Department of Computer Science Engineering
[1,2,3]SCSE, VIT University, Vellore, India

Abstract— Cloud computing is computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. The strives of environment is dynamic, customizable and reliable with the quality of services. Security issues in the cloud as it is anywhere else. Lots of people share different point of views in cloud computing. Some of the people believe that it is unsafe to use Cloud Computing .Clouds can be classified as public, private or hybrid. This paper handle security issue in cloud using blowfish algorithm.

Key words: Security, Data, Cloud, OPEX, CAPEX

I. INTRODUCTION

Cloud computing relies on restricting sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, Rackspace, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

The term "moving to cloud" also refers to an organization moving away from a traditional CAPEX model (buy the dedicated hardware and depreciate it over a period of time) to the OPEX model (use a shared cloud infrastructure and pay as one uses it).

Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing have led to a growth in cloud computing. Cloud vendors are experiencing growth rates of 50% per annum.

II. LITERATURE REVIEW

Security and privacy are the two major concerns about cloud computing. In the cloud computing world, the virtual environment lets user access computing power that exceeds that contained within their physical world. To enter this virtual environment a user is required to transfer data throughout the cloud. Consequently several security concerns arises [4] [7] [8] [16]

A. Information Security

1) Losing Control over Data:

Outsourcing means losing significant control over data. Large banks don't want to run a program delivered in the cloud that risk compromising their data through interaction with some other program. Amazon Simple Storage Service (S3) APIs provide both bucket- and object level access controls, with defaults that only permit authenticated access by the bucket and/or object creator. Unless a customer grants anonymous access to their data, the first step before a user can access data is to be authenticated using HMAC-SHA1 signature of the request using the user's private key. Therefore, the customer maintains full control over who has access to their data.

2) Data Integrity:

Data integrity is assurance that data changes only in response to authorized transactions. For example, if the client is responsible for constructing and validating database queries and the server executes them blindly, the intruder will always be able to modify the client-side code to do whatever he has permission to do with the backend database. Usually, that means the intruder can read, change, or delete data. The common standard to ensure data integrity does not yet exists [8]. In this new world of computing users are universally required to accept the underlying premise of trust. In fact, some have conjectured that trust is the biggest concern facing cloud computing.

3) Risk of Seizure:

In a public cloud, you are sharing computing resources with other companies.. Exposing your data in an environment shared with other companies could give the government "reasonable cause" to seize your assets because another company has violated the law. Simply because you share the environment in the cloud, may put data at risk of seizure. The only protection against the risk of seizure for user is to encrypt their data. The subpoena will compel the cloud provider to turn over user's data and any access it might have to that data, but cloud provider won't have user's access or decryption keys. To get at the data, the court will have to come to user and subpoena user. As a result, user will end up with the same level of control user have in his private data center.

4) Incompatibility Issue:

Storage services provided by one cloud vendor may be incompatible with another vendor's services should you

decide to move from one to the other. Vendors are known for creating what the hosting world calls "sticky services" – services that an end user may have difficulty transporting from one cloud vendor to another.

5) Failure in Provider's Security:

Failure of cloud provider to properly secure portions of its infrastructure – especially in the maintenance of physical access control – results in the compromise of subscriber systems. Cloud can comprise multiple entities, and in such a configuration, no cloud can be more secure than its weakest link. It is expected that customer must trust provider's security. For small and medium size businesses provider security may exceed customer security. It is generally difficult for the details that help ensure that the right things are being done.

6) Cloud Provider Goes Down:

This scenario has a number of variants: bankruptcy, deciding to take the business in another direction, or a widespread and extended outage. Whatever is going on, subscriber risk losing access to their production system due to the actions of another company Subscriber also risk that the organization controlling subscriber data might not protect it in accordance with the service levels to which they may have been previously committed. The only option user have is to choose a second provider and use automated, regular backups, for which many open source and commercial solutions exist, to make sure any current and historical data can be recovered even if user cloud provider were to disappear from the face of the earth.

III. PROPOSED METHOD

Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric (that is, a secret or private key) block cipher that uses a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use. (The U. S. government forbids the exportation of encryption software using keys larger than 40 bits except in special cases. Blowfish was designed in 1993 by Bruce Schneider as an alternative to existing encryption algorithms. Designed with 32-bit instruction processors in mind, it is significantly faster than DES. Since its origin, it has been analyzed considerably. Blowfish is unpatented, license-free, and available free for all uses.

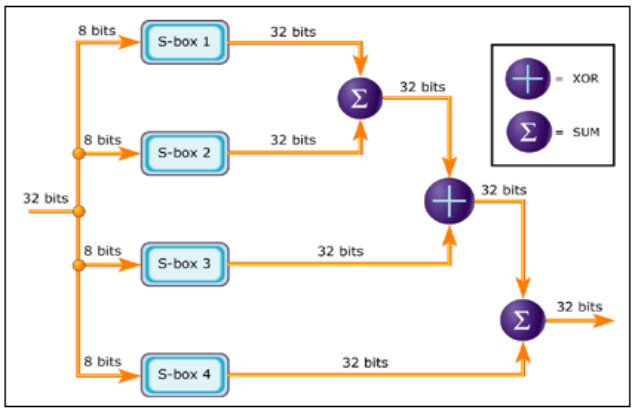

Fig. 1: Block diagram of Blowfish

Encrypt the all zero string using the Blowfish algorithm, using the modified P-array above, to get a 64 bit block. Replace P1 with the first 32 bits of output, and P2 with the second 32 bits of output (from the 64 bit block). Use the 64 bit output as input back into the Blowfish cipher, to get a new 64 bit block. Replace the next values in the P-array with the block. Repeat for all the values in the P-array and all the S boxes in order.

(The second 64 bit block is dropped into the P-array)

The Blowfish algorithm is now ready for encryption. The encryption is a simply Feistal network of 16 rounds. For the input of 64 bits, do:

Divide x into two 32-bit halves: xL, xR

For i = 1 to 16:

xL = xL XOR Pi

xR = F(xL) XOR xR

Swap xL and xR

Next i

Swap xL and xR (Undo the last swap.)

xR = xR XOR P17

xL = xL XOR P18

Recombine xL and xR

The F function is: F(xL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 232 where a,b,c,d are four 8 bit quartered derived from xL.

Decryption is the same as encryption, except the P-arrays are used in reverse.

Output

Some example input and output of the Blowfish algorithm.

$ ./Blowfish 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Key: 0 0 0 0 0 0 0 0

Plaintext: 0 0 0 0 0 0 0 0

IV. CONCLUSION

The phenomenon in cloud computing shows a interest through worldwide because of its lower ownership, scalability, competitive differentiation, reduced complexity for customers, and faster and easier services.cloud offers several advantages, people can see cloud computing from different points of view. Some people think that cloud is unsafe. But few people find it safer for provisioning, especially small businesses. Several large organizations and some government agencies are still holding back. They indicate that they will not consider soon because they have no good way to quantify their risks. To gain total acceptance from all potential users cloud computing require some standardization in the security. In this paper we implemented security in cloud using blowfish as a future work some other technique can be used.

REFERENCE

[1] http://csrc.nist.gov/groups/SNS/cloud-computing/index.html,
[2] Cisco White Paper,
[3] http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/white_paper_c11-532553.html, published 2009, pp.1-6.
[4] John Viega, McAffee, Cloud Computing and the Common Man," published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009.
[5] George Reese, "Cloud Application Architectures", First edition, O'Reilly Media, April 2009, ISBN 9780596156367, pp. 2-4, 99-118.

[6] http://en.wikipedia.org/wiki/Cloud_computing.
[7] http://communication.howstuffworks.com/cloud computing1.htm.
[8] John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the World of Cloud Computing," published on the IEEE Journal on Cloud Computing Security, July/August 2009, Vol. 7, No.4, pp. 61-64.
[9] John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation, Management, and Security", CRC Press, August 17, 2009, ISBN 9781439806807, pp. 147-158, 183-212.
[10] Amazon White Paper, http://aws.amazon.com/about-aws/whats-new/2009/06/08/new-aws-security-center-and-security-whitepaper/, published June 2009.
[11] Marco Descher, Philip Masser, Thomas Feilhauer, A Min Tjoa, David Huemer, " Retaining Data Control to the Client Infrastructure Clouds", published on the IEEE, 2009 International Conference on Availability, Reliability and Security, pp. 9-15.
[12] David Bernstein, Erik Ludvigson, Krishna Sankar, Steve Diamond, Monique Morrow, "Blueprint for the Intercloud – Protocols and Formats for Cloud Computing Interoperability, submitted to IEEE, 2009 Fourth International Conference on Internet and Web Applications and Services, pp. 328-335.
[13] Liang-Jie Zhang, Qun Zhou, "CCOA: Cloud Computing Open Architecture", published on IEEE, 2009 IEEE International Conference on Web Services, pp. 607-615.
[14] Amazon White Paper, "Introduction to Amazon Virtual Private Cloud", Available: http://aws.amazon.com/about-aws/whats-new/2009/08/26/introducing-amazon-virtual-private-cloud/, published Aug 26, 2009, pp. 6-8.
[15] Rajkumar Buyya, Chee Shin Yeo, SrikumarVenugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities", grid Computing and Distributed Systems and Software Engineering, The University of Melbourne, Australia.
[16] Jinesh Varia, Amazon Web Services, "Building GrepTheWeb in the Cloud, Part 1: Cloud Architectures", Available: http://developer.amazonwebservices.com/connect, July 2008, pp. 1-7 Jon Brodkin, "Gartner: Seven Cloud Computing Security Risks", Available: http://www.infoworld.com, published July 2008, pp. 1-3.

