International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Survey on Security Threats and Security Algorithms in Cloud Computing

Kapil A. Ughade[1], Prof. Nitin R. Chopde[2]

[1]Student of Master of Engineering (Computer Science & Engineering), Raisoni College of Engineering and Management, Amravati, India

[2] Head of Department of Computer Science & Engineering, Raisoni College of Engineering and Management, Amravati, India

Abstract: ***Cloud Computing is an emerging technology which provides services on demand from shared pool of computing resources. Cloud computing has at its core services like platform, infrastructure and software as a service. Benefits of cloud storage are easy access, performance, high availability, cost efficiency and many others. So each and every organization is moving its data to the cloud, that means it uses the storage service provided by the cloud provider. So there is a need to protect the data against unauthorized access, modification or denial of services, data loss, data breach etc. Cloud security is must which will break the hindrance the acceptance of the cloud by the organizations. There are a number of security algorithms which may be implemented to the cloud. This paper is a survey of different security issues to cloud and different cryptographic algorithms adoptable to better security for the cloud.***

Keywords: Cloud Computing**.** Security Threats, Security Algorithms, Blowfish, MD5.

1. Introduction

Internet has been the driving force that towards various technologies have been developed. In that one of the most discussed is cloud computing. Cloud is the future of computing. Cloud computing has been described by national institute of standards and technology (NIST) as Cloud is the network based environment which makes services available on demand. Cloud Computing [1, 2] is an emerging trend to deploy and maintain software and is being adopted by the industry such as Google, IBM, Microsoft, and Amazon. Cloud computing has at its core services like platform, infrastructure and software as a service. As the use of these services becomes widespread, then the security of outsourced user data becomes an important research topic. This paper describes the overview of cloud computing, algorithms used and its data security issues.

2. Literature Survey

Security in cloud is one of the major areas of research. The survey shows that, the researchers are focusing on efficient algorithms and encryption techniques to enhance the data security in cloud. Rahul Bhatnagar et al. (2013) in Security in Cloud Computing [14] have proposed an analysis of technical component and some research in threats for cloud computing Users and threats for cloud service provider then provide many security topics related for cloud security standardization.

Shivashankar ragi (2011) within a research thesis Security Approaches for Protecting Data in Cloud Computing [15] have described the security threats and identify the safety approaches for security in cloud computing and measured the protection challenges and security methods of cloud computing and lastly identi_ed from research methods quite a few challenges and techniques used now study plus in future research work in Cloud Computing. Sanjana sharma et al. (2012) in Security in Cloud Computing [16] have described the briey details of cloud computing and type of services and security issues and some challenges for data security in cloud environment and investigate the several approaches for security in cloud computing and nally provide a reliable security in cloud computing for future work. Cornwell [13] discussed the design of Bruce Schneier˝s Blowfish encryption algorithm along with a performance analysis and possible attacks. It was concluded about the effectiveness of Blowfish with the other well known algorithms DES, 3DES, and AES. It was concluded that Blowfish is able to provide long term data security without any known backdoor vulnerability or ability to reduce the key size. For the future scope Blowfish was considered safe and effective design although future reevaluations will be needed.

3. Top 5 Threats to Cloud Computing

3.1 Data Breach

"A data breach is a security incident in which protected, sensitive or confidential data is copied, viewed, transmitted, stolen or used by an individual unauthorized to do so." Data breaches include financial information such as credit card or bank details, personal health information (PHI), personally identifiable information (PII), trade secrets of corporations . Following are the Vulnerabilities that may outcome in data breach:

1) **Loss of Personally Identifiable Information (PII):** A cloud consumer has to provide sensitive information regarding themselves (like name, home address, phone number, credit card number etc.) for being able to use the cloud services. But if this precious information is mishandled by the Cloud Service Providers, it can lead to exposure of identity of the cloud consumer by people with malicious intent.
2) **Loss of Encryption Keys:** This refers to the loss of secret keys to other parties or password disclosure to unauthorized personal, or corruption or loss of those keys or their unauthorized use for non-repudiation. If a key is lost the user might not be able to read their own data as it

will be unreadable encrypted form that requires a key to decrypt it.

3) **Brute Force Attacks:** A brute force attack is a technique which is used to crack password. This technique uses combinations of dictionaries and software programs to test hundreds of thousands of password combination per second and cracking passwords in a few minutes taking advantage of computing ability of cloud

3.2 Data Loss

Data loss is referred to as the permanent unavailability of data. Data loss was the second headmost threat in 2013 as the hackers would gain access to sensitive data and erase it. While implementing securities those data sets should be considered that are heavily accessed. Following are the Vulnerabilities:

1) **Loss of Encryption Keys:** If the key used to encrypt the data or the passwords are disclosed somehow, then there may be chance that a malicious person might use this information to gain access to the data and delete it. If there is no backup available the user might loose the data permanently.
2) **Cloud Service Termination:** It refers to risk of user loosing their data in case the CSPs run out of business. On September 2013, a CSP Nirvanix announced that they will be shutting down their services due to lack of sufficient funds and the users have two weeks to migrate their data from the cloud or the data will be lost permanently.
3) **Hardware or Software Failure:** Hardware or software failure may result in data loss. Data specially the data in transit have a great chance of being lost in event of a system crashing because of a software or hardware fault.
4) **Natural Disaster:** Natural disasters such as hurricane, earthquakes, floods etc. are problems pertaining to a specific region. So if the cloud storage is located physically in one such region then there are chances that the data might get lost in event of such disasters, if the data is not backup routinely.

3.3 Insecure Interfaces and API's

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Orchestration, provisioning, monitoring and management are all performed using these interfaces. The availability and security of general cloud services is dependent upon the security of these basic APIs. Following are the Vulnerabilities: Malicious or unidentified access, limited monitoring/logging capabilities, inflexible access controls, API dependencies, anonymous access, reusable tokens/passwords and improper authorizations.

3.4 Daniel-of-Service

Denial-of-service attacks are attacks meant to prevent users of a cloud service from being able to access their applications or their data. By forcing the victim cloud service to consume inordinate amounts of finite system resources such as processor power, disk space, network bandwidth or memory , the attacker causes an intolerable system slowdown and leaves all of the legitimate service users confused and angry as to why the service isn't responding. Following are the Vulnerabilities

1) **Zombie Attack:** [3] Through Internet, an attacker attempts to flood the victim by sending requests from innocent hosts in the network. These types of hosts are known as zombies. In the Cloud, the requests for Virtual Machines (VMs) are accessible by each user through the Internet. An attacker can flood the huge number of requests through zombies. Such an attack interrupts the expected behavior of Cloud affecting availability of Cloud services.
2) **HX-DOS Attack:** It is combination of XML and HTTP messages that are intentionally sent to flood and destroy the communication channel of the cloud service provider [4].

3.5 Account or Service Traffic Hijacking

Account or service traffic hijacking includes attack methods such as exploitation, fraud and phishing of software vulnerabilities. Most often, this is a outcome of stolen credentials, which can allow illegitimate users access to critical areas of cloud computing services. With the threat of compromised availability, integrity and confidentiality of their cloud computing services, companies must be secured with protection strategies to prevent and contain stolen credentials and maintain top cloud computing security. Following are the Vulnerabilities

1) **Session Hijacking:** Session hijacking attack [5] is only possible if https is not used at all or only during the login process. The main problem with this attack is that especially if a cloud email service is affected, the attacker might get to know certain other passwords and personal information.
2) **SQL Injections:** *[6]* Hackers exploit the vulnerabilities of web servers and inject a malicious code in order to bypass login and gain unauthorized access to backend databases. Hackers can manipulate the contents of the databases, remotely execute system commands, retrieve confidential data or even take control of the web server for further illegal activities, if successful.
3) **Cross-site Scripting:** It occurs when a cloud application sends a page containing user supplied data to the browser without validation, filtering, or escaping. Hackers inject malicious scripts, such as VBScript, ActiveX, HTML, JavaScript and Flash into a vulnerable dynamic web page to execute the scripts on victim's web browser. Thereupon the attack could conduct illegal activities.
4) **Wrapping Attack Problem:** This attack occurs between the web browser and the server by altering the Simple Object Access Protocol (SOAP) messages for two persons, the user and the attacker. When using XML signatures for authentication or integrity, the most well known attack is XML Signature Element Wrapping.
5) **Man in the middle Attack:** If secure socket layer (SSL) is not properly configured, then any attacker is able to gain access the data exchange between two parties. In Cloud, an attacker is able to gain access the data communication among data centers.

6) **Social Engineering Attack:** By heavily relying on human interactions, victim is tricked into disclosing valuable information such as password.
7) **Malware Injection Attack:** In this attack, an adversary attempts to inject malicious service or code, which appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping [7].
8) **Phishing Attack:** Phishing attacks are well known for manipulating a web link and redirecting a user to a false link to get sensitive data. It may be possible that an attacker use the cloud service to host a phishing attack site to hijack accounts and services of other users in the Cloud.

4. Security Algorithms

4.1 Blowfish

Blowfish is block cipher 64-bit block- can be used as a replacement for the DES algorithm. Its structure is similar to IDEA algorithm[8][9]. It takes a variable length key, ranging from 32 bits to 448-bits [10]. Blowfish is successor of Two fish. The blowfish algorithm was first introduce in 1993 by Bruce Schneider, and has not cracked until now. It is also noteworthy to point out that this algorithm can be optimized in hard ware applications, is often used in software applications, although it is like most other ciphers. The encryption is simply like feistal network of 16 rounds.

Blowfish is a symmetric block encryption algorithm designed in consideration with,
Fast : It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.
Compact: It can run in less than 5K of memory.
Simple: It uses XOR, addition, lookup table with 32-bit operands.
Secure: The length of key is variable, it can be in the range of 32~448 bits: default 128 bits key length.
It is useful for applications where the key does not change often, like an automatic file encryptor or communication link.
Royality-free and unpatented

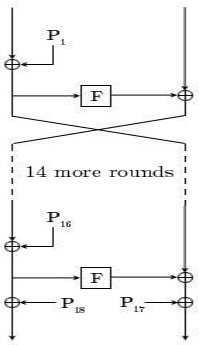

Figure 1: The Feistel structure of Blowfish
[Source: http://en.wikipedia.org/wiki/File:BlowfishDiagram.png]

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. It will follows the feistel network and this algorithm is divided into two parts : Key-expansion and Data Encryption.

1) **Key Expansion**
It will converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Blowfish uses big number of subkeys and these keys are generate earlier to any data encryption or decryption.
The p-array consists of 18 subkeys of 32 bit :
P1,P2,……..,P18
Four 32-bit S-Boxes consists of 256 entries for each:
S1,0, S1,1,……. S1,255
S2,0, S2,1,…….. S2,255
S3,0, S3,1,…….. S3,255
S4,0, S4,1,.....S4,255

2) **Data Encryption**
It is having a function to iterate 16 times of network. Every round consists of key-dependent permutation and data-dependent substitution and a key. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

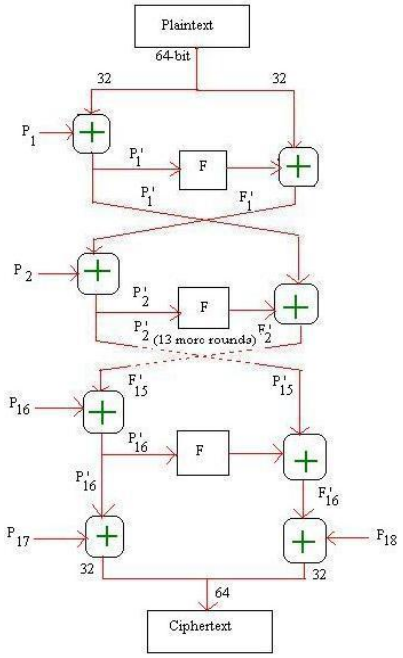

Figure 2: Blowfish Encryption

Divide x into two 32-bit halves: xL, xR
For i = 1to 16:
xL = XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR

4.2 MD5

A message-digest algorithm is also called a cryptographic hash function or a hash function. It accepts a message as

input and generates output of a fixed-length, which is commonly less than the length of the input message. The output is called a message digest, a fingerprint or a hash value.

There are three kinds of operations in MD5: Cyclic Shift Operation, Modular Addition and Bitwise Boolean Operation. All these three operations are very fast on a 32-bit machine. Hence MD5 is quite fast.

MD5 algorithm developed by Ron Rivest and introduced in the year 1991. It is used to verify the integrity of the message. The main goal of this algorithm is security, speed, simplicity, compactness, and little-endian architecture. It processes block of 512-bit and generates 128-bit message digest. The processing consisting of the following steps:

1. Append padded bits
2. Append length
3. Initialize MD buffer
4. Process blocks.
5. Hashed Output

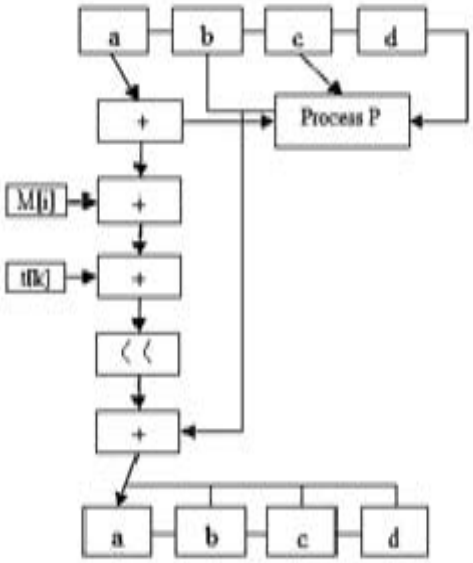

Figure 3: One MD5 Iteration

Step 1:- Append padded bits
The message is padded so that its length is congruent to 448, modulo 512 means extended to just 64 bits shy of being of 512 bits long. A single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits equals 448 modulo 512.
Step 2:-Append length
A 64 bit representation of b is appended to the result of the step 1. The resulting message has a length that is an exact multiple of 512 bits.
Step 3:- Initialize MD buffer
A four-word buffer (A,B,C,D) is used to compute the message digest. Here each of A,B,C and D is a register of 32 bit. These registers are initialized to the following values in hexadecimal:
word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10
Step 4:- Process blocks
Four auxiliary functions that accept as input three 32-bit words and produce as output one 32-bit word.
F(X,Y,Z) = XY v not(X) Z
G(X,Y,Z) = XZ v Y not(Z)
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X v not(Z))
The bits of X, Y, and Z are totalitarian and balance the each bit of F (X, Y, Z) will be totalitarian and balance. The functions (X, Y and Z) = P, in that they do job in "bitwise parallel" to produce the reliable output from the bits of X, Y and Z. If the bits of X, Y, and Z are independent and unbiased, the each bit of G(X,Y,Z), H(X,Y,Z), I(X,Y,Z) and F(X,Y,Z) will be independent and unbiased.
Step 5:- Hashed Output
The message digest produced as output is A, B, C and D. That is, output begins with the low-order byte of A, and end with the high-order byte of D.There are 4 rounds performed in MD5 which is of 128 bits. Fig 3 shows One MD5 iteration **[11] [12].**

5. Conclusion

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, including platforms, infrastructure and applications that are available from cloud service providers as online services. People may be confused by the range of offerings and the terminology used to describe them and will be unsure of the benefits and risk. Security is a major requirement in cloud computing while we talk about data storage. There are number of existing techniques used to implement security in cloud. In this paper, we discussed MD5 and Blowfish algorithms. Our future will be considering some problems related to existing security algorithms and implement a better version of MD5 and Blowfish.

References

[1] Anthony Bisong, Syed, M. Rahman "An overview of the security concerns in Enterprise cloud computing," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.
[2] I. Foster, Y. Zhao, I. Raicu, and S. Lu, 2008, "Cloud Computing and Grid Computing 360-Degree Compared, In: Grid Computing Environments Workshop", 2008. GCE '08, p. 10, 1.
[3] Dhiren Patel, Bhavesh Borisaniya, Avi Patel, Chirag Modi,Muttukrishnan Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," Springer Science+Business Media New York 2012.
[4] E.Anitha, Dr.S.Malliga, "A Packet Marking Approach To Protect Cloud Environment Against DDoS Attacks," Information Communication and Embedded Systems (ICICES), 2013 International Conference
[5] Christof Kauba, Stefan Mayer, "When the Clouds Disperse Data Confidentiality and Privacy in Cloud Computing," University of Salzburg

[6] Te-Shun Chou , "SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES" International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013
[7] Kazi Zunnurhain and Susan V. Vrbsky, "Security Attacks and Solutions in Clouds ," The University of Alabama
[8] S. Basu, "International Data Encryption Algorithm (IDEA) – A Typical Illustration", Journal of Global Research in Computer Science, vol. 2, no. 7, pp: 116-118, July 2011.
[9] M. Leong, O. Cheung, K. Tsoi and P. Leong, "A Bit Serial Implementation of the International data Encryption Algorithm IDEA", Proc. IEEE Symposium on Field-Programmable Custom Computing Machines, pp:122-131, 2000.
[10] Vinaya.V, Sumathi.P," Implementation of Effective Third Party Auditing for Data Security in Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, May 2013.
[11] Rivest R., 1992, "The MD5 Message-Digest Algorithm,"RFC 1321,MIT LCS and RSA Data Securit y, Inc.
[12] Kahate, Atul, 2003, "Cryptography and Network Securit y", Tata McGraw-Hill ,India.
[13] Cornwell Jason W, "Blowfish Survey", Department of Computer science, Columbus State university, Columbus, GA, 2010
[14] Rahul Bhatnagar, Suyash Raizada, Pramod Saxena, SECURITY IN CLOUD COMPUTING,International Journal For Technological Research In Engineering, ISSN (Online) : 2347 4718, December - 2013.
[15] Venkata Sravan Kumar, Maddineni Shivashanker Ragi, Security Techniques for Protecting Data in Cloud Computing, Master Thesis Electrical Engineering School of Computing Blekinge Institute of Technology SE – 371 79 Karlskrona Sweden, November 2011.
[16] Sanjana Sharma, Sonika Soni, Swati Sengar, Security in Cloud Computing, National Conference on Security Issues in Network Technologies, 2012.