Secure Cloud Computing Framework with Automatic Intrusion Detection and Prevention System

[1]C.Pabitha, [2]M.Chandra, [3]D. Daisy Veroni, [4]J. Jane Nivaditha

[1]Assistant professor, [2,,3,4]UG Scholar
Department of Computer Science and Engineering

***Abstract*—In cloud computing providing security to petabytes of data is very important. A recent survey on cloud security States that the security of user's data has the highest priority as well as concern. Therefore, to provide secure cloud framework we have proposed a system named secure cloud computing framework with automatic intrusion detection and prevention system. With multi-layered security we can protect data in real-time and it has three layers of security as follows identity management, intrusion detection and prevention, encryption, cloud storage. To enhance security we proposed to add automatic intrusion detection and prevention technique for Brute force, SQL injection, wrapping attacks. Finally the data owner files are encrypted using RC6 and stored in public cloud storage named drop box.**

***Keywords*— Cloud Computing, Brute force attack, wrapping attack, Sql injection, SSL attacks.**

I. INTRODUCTION

Cloud computing and its approval has been a topic of talk in the past few years. It has been an schedule for organizational adoption due to benefits in cost-savings, improvement in work efficiencies, business agility and quality of services. With the rapid rise in cloud computing, software as a service (SaaS) is particularly in demand, since it offers services that suit users' need. For example, fordiagnose challenging diseases and cancers, information about medical research are helpful. Financial analytics can ensure accurate and fast simulations to be available for investors. Education as a service improves the quality of education and delivery. Mobile applications allow users to play online games and easy-to-use applications to interact with their peers. While more people and organizations use the cloud services, security and privacy become important to ensure that all the data they use and share are well protected. Some researchers assert that security should be implemented before the use of any cloud services in place. This makes a challenging adoption scenario for organizations since security should be enforced and implemented in parallel with any services. Although organizations that adopt cloud computing acknowledge benefits offered by cloud services, challenges such as security and privacy remain a scrutiny.

The data centers have encountered challenges of rapid increase in the data. For example, in a data center that the lead author used to work with, daily increase of 100 terabytes of data was usual. If the organization has experienced a rapid rise of data growth and is unable to respond quickly and efficiently, problems such as data traffic, data security and service level agreement issues can happen. In this paper, we focus on the data security while experiencing a large increase of data, whether they are from the external sources such as attack of viruses or Trojans; or they from the internal sources if users or clients acquire hundreds of terabytes of data per day. The paper proposes a novel detection & a prevention mechanism of Attacks such as sql injection, bruteforce, wrapping attacks. This is a research challenge for data security which is essential for the better management of the data center to handle a rapid increase in the data.

Aside from the data center security management for active growth in data, the software engineering process should be robust enough to withstand attacks and unauthorized access. The entire process can be further consolidated with the development of a framework to tighten up the technical design and implementations, governance and policies associated with good practices.

This motivates us to develop a framework, Cloud Computing Adoption Framework (CCAF), to help organizations successfully adopt and deliver any cloud services and projects.

II. LITERATURE SURVEY

Cloud computing – a relatively recent term, builds on decades of research in virtualization, distributed computing, utility computing, and more recently networking, web and software services. It provide reduced information overhead for the end-user, great flexibility, reduced total cost of ownership, on-demand services and many other things.[1]

Security, and privacy to a lesser amount, have been active research areas in measure for a long time. Methods and techniques have been developed to protect data, programs, and to protect data from attacks through various techniques. The open Internet environmenthas increased complexity of security and privacy.[2]

The sharing of data on cloud serversbringsnew challenges for data security and access control, which are not within the same trusted domain as data owners. Many cryptographic methods are used to keep sensitive user data confidential against untrusted servers. These methods lead to computational overhead for data owners. Theunresolved problem are simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control.[3]Even though potential gains achieved from the cloud computing, the model security is still questionable. The problem in security becomes more complicated on cloud model as new

dimensions have entered into the problem scope allied to the model architecture, multi-tenancy, elasticity, and layers addiction stack.[4]

III. SYSTEM ARCHITECTURE

Secure Cloud Computing Framework composed of following parties: User,Admin,cloud server.
User can encrypt files from his block and his own key. Encrypt them with the key, followed by signing the resulting encrypted blocks and creating the storage request. For each file, this key will be used to decrypt and rebuild the original file during the retrieval phase. Here we use the encryption algorithm RC6.The encrypted file is transferred to the admin.The roles offered by admin are it can authenticate users during the storage/retrieval phase.To make it more secure, the data is again encrypted using RC6 encryption algorithm.

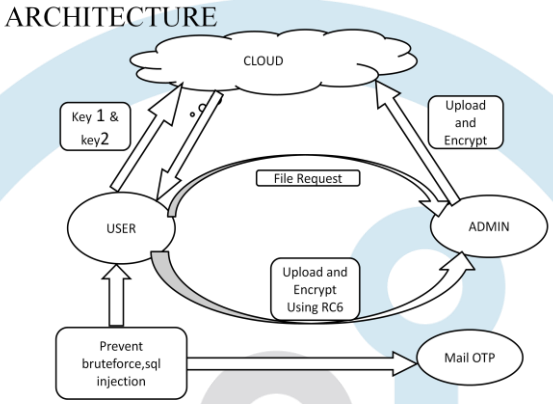

Figure 2.1

SECURITY ENABLERS OF SCCF

Identity Management

- The identity management is divided into two roles: users and the security manager as follows.
- Users: Users can encrypt each key from his block and his own key. They can split files into blocks, encrypt them with the key, followed by signing the resulting encrypted blocks and creating the storage request. For each file, this key will be used to decrypt and rebuild the original file during the retrieval phase. The user also uses single sign-on to access each block with a compact signature scheme.
- Admin: Three roles are offered by the security manager. First, it can authenticate users during the storage/retrieval phase. Second, it can access control. Third, it can encrypt/decrypt data between users and their cloud.

Automatic Intrusion Detection and Prevention

In this module automatic Intrusion detection system (IDS), encryption, deep packet inspection (DPI) and report the results to the controller. The main goal of Open Sec is to allow network operators to describe security policies for specific flows. The policies include a description of the flow, a list of security services that apply to the flow and how to react in case malicious content is found. The reaction can be to alert only, or to quarantine traffic or even block all packets from a specific source. Hence we have considered automatic intrusion detection and alerting network operator automatically when intruder tries brute force, SQL injection and wrapping attack.

CLOUD SECURITY ATTACK

Brute Force

A brute force attack is a technique used to break passwords. Keep on trying multiple times until it finds the correct one to access. Cloud platform is perfect for hackers for this type of attack. In approximately 20 minutes, Roth fired 400,000 passwords per second into the system and the cost of using EC2 service was only 28 cents per minute.A password and cryptography attack that does not attempt to decrypt any information, but continue to try a list of different passwords, words, or letters. For example, a **brute-force attack** may have a commonly used passwords and cycle through those words until it gains access to the account. Every key combination of key is needed to try until correct password is found in complex brute-force attack. Due to the number of possible combinations of letters, numbers, and symbols, a brute force attack can take a long time to complete (several hours,

days, month, years to run). The time to complete password depend on strength of encryption. The higher the type of encryption used (64-bit, 128-bit or 256-bit encryption), the longer it can take.

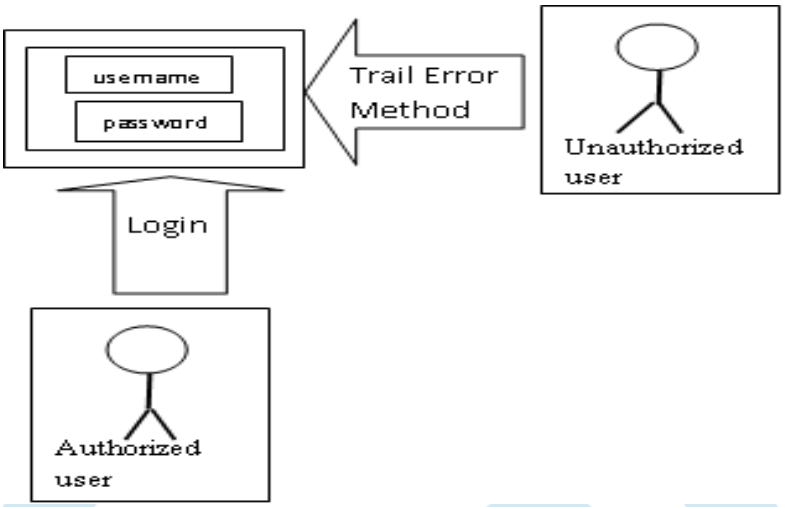

Figure 1.

Popular tools in brute force attack as follows:

1. Aircrack-ng
2. John the Ripper
3. Rainbow Crack

1.Aircrack-ng:Aircrack-ng is popular wireless password cracking tool. This tool is support the platform windows, Linux.
2.John the Ripper: This tool is developed by Unix. It is available of fifteen different platform (Unix,windows, DOS,BeOSand OpenVMS).
3.Rainbow crack: This tool is available for windows,Linux and all latest version of platform.

SQL INJECTION

SQL Injection is one of the most widely exploited web application vulnerability of the web area. Malware injection attack is one category of web-based attacks, in which hackers accomblishment suspectability of a web application and embed malicious codes into it that changes the course of its normal execution. Among all of the malware injection attacks, SQL attack and cross-site conseiving attack are the two most common forms [5]. SQL injection attack increased 69% in Q2 2012 compared to Q1, according to a report by secure cloud host provider FireHost [6]. For web applications which do not validate the user's input, the unauthorized user inject SQL statements to SQL command. By this hackerssteal data from online businesses' and organizations'
For the vulnerable web application, any malicious SQL query or command is executed by hackerthrough the web application. By using this the important details stored in the database can be retrieved easily. By exploiting an SQL injection it is also possible to drop (delete) tables from the database. SQL injection can also be used to add, modify, and delete record in a database affecting data integrity. Therefore with an SQL Injection the malicious user has full access to the database. SophosLabs's blog reported that an SQL injection attack has been successfully used to plant unauthorized code on 209 pages promoting the PlayStation games, "SingStar Pop" and "God of War" [7]. SQL injection attacks can be launched by a botnet. The Asprox botnet used a thousand bots that were equated with an SQL injection kit to fire an SQL injection attack [8]. The bots first sent encoded SQL queries containing the exploit payload to Google for searching web servers that run ASP.net. The web sites which are returned from those queries,bots started an SQL injection attack. Approximately 6 million URLs attachment to 153,000 different web sites were casuality of SQL injection attack by the Asprox botnet[9].

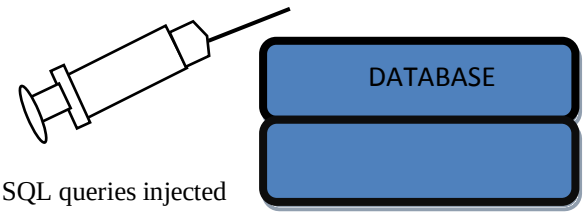

Figure 2

WRAPPING ATTACK

The attack uses a method known as XML signature wrapping and shows vulnerabilities while executing the web service request. In wrapping attack, the message structure of the SOAP is modified by inserting the malicious element in Transport Layer Service (TLS) and after inserting the malicious code, the attacker interrupted working of cloud server.
When a client requests services to a web server through a web browser, the service is communicated using Simple Object Access Protocol (SOAP).The confidentialityand data integrity of SOAP messages in transit between clients and serversthrough HTTP protocol with an Extensible Mark-up Language (XML) format, WS-Security (Web Services Security), for web service is applied. Encryption technique to encrypt the content of the message andit uses digital signature to get the message signed. This makes the client authenticated and the server can validate that the message is not tampered with during transmission.
When signed requests are validated by web servers XML signature wrapping is used to exploit a weakness in wrapping attack[10]. The attack is done during the translation of SOAP messages between a legitimate user and the web server. The user's credentials are duplicated during the login period, the hacker embeds a bogus element (the wrapper) into the message structure, place the original message body under the wrapper, content of the message is replaced with malicious code, and then message is send to the server. Since the original body is still valid, it tricking the server to authorize the message which has been altered. As a result, the hacker is able to gain unauthorized access to protected resources and process the intended operations.Since cloud users regularly request services from cloud measuring service providers through a web browser, wrapping attacks can cause damage to cloud systems as well. Amazon's EC2 was discovered to be vulnerable to wrapping attacks in 2008 [11]. The research showed EC2 had a weakness in the SOAP message security validation mechanism.It intercept signed SOAP request of a legitimate user. As a result, hackers could take unprivileged actions on victim's accounts in clouds. Using XML signature wrapping technique, the Amazon AWSvulnerability is exploited in the demonstration of account hijacking attack [12]. By altering authorized digitally signed SOAP messages, the researchers were able toobtain unauthorized access to a customer's account, delete and create new images on the customer's EC2 instance, and perform other administrative tasks.
A proposed solution is to use the SOAP message duringmessage passing from the web server to the web browser. A redundant bit (STAMP bit) will be added onto the signature value when it is appended in the SOAP header. When the message reaches its destination the STAMP bit is checked. If the STAMP BIT has been altered, then a new signature value produced by the browser and the new value is sent back to the server as recorded to modify the authenticity checking [13].

SSL ATTACK

SSL is a method of encryption used by various network Communication protocol.Conceptually,SSL runs above TCP/IP, arranging security to users interacting over other protocols by encrypting communications and authenticating communicating parties.SSL attack aim to intercept data that is send over a encrypted connection.A successful attack enables access to unencrypted information.

IV. SECURITY TECHNIQUES IMPLEMENTATION

ACCOUNT LOCKOUT POLICY

There are a number of techniques for preventing brute force attack. The first is to implement an account lockout policy. For example, the account is locked out for more thanthree failed login attempts until an administrator unlocks it. A better, albeit more complicated technique is progressive delays. The lock-out time increases with each subsequent failed attempt. This prevents automated tools from performing such an attack.

CHALLENGE RESPONSE TEST

Another technique is to use a challenge-response test to prevent automated submissions of the login page. The reCAPTCHA tools can be used to solve a simple math problem to assure the user is, in fact, a person. This technique is efficient, but has accessibility concerns and usability of the site is affected.

USING PREPARED STATEMENT

Adapted statements are resilient against SQL injection as a result parameter values, which are transmitted later using a different protocol, need not be correctly escaped.If the original statement template is not derived from external input,SQL injection cannot occur.

SANITIZATION AND VALIDATION

The most important precautions are data sanitization and validation, which should before be in place. Sanitization regularly involves running any acknowledged data through a function (such as MySQL's mysql_real_escape_string() function) to ensure that any dangerous characters (like " ' ") are not passed to a SQL query in data.

Validation is slightly different, in that it attempts to ensure that the data acknowledged is in the form that is expected. At the most basic level this includes assuring that e-mail addresses contain an "@" sign, that only digits are equiped when integer data is expected, and that the length of a piece of data submitted is no longer than the maximum expected length.acceptance is often carried out in two ways: by blacklisting dangerous or unwanted characters (although hackers can often get around blacklists) and by vitalizing only those characters that are allowed in a given occurance, which can involve more work on the part of the programmer. Although validation may take place on the client side, hackers can modify or get around this, so it's essential that you also validate all data on the server side as well.

ENCRYPTION

RC6 (**Rivest cipher 6**) is a symmetric key block cipher derived from RC5. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits. RC6 is symmetric to RC5, using data-dependent rotations, RC6 could be viewed as interweaving two parallel RC5 encryption processes. However,extra multiplication not in RC5, but in RC6 it is used to make the rotation dependent on every bit in a word, and not just the least significant few bits.

a + b integer addition modulo 2w
a- b integer subtraction modulo 2w
a⊕b bitwise exclusive-or of w-bit words
a∗b integer multiplication modulo 2w
a <<< b rotate the w-bit word a to the left by the amount given by the least significant lg w bits of b
a >>> b rotate the w-bit word a to the right by the amount given by the least significant lg w bits of b

RC6has taken advantage of the extensive knowledge base, both from RC5 and the AES evaluations.The simplistic structure has contributed to its evaluation and security. Despite certain AES-specific architectural limitations, RC6 has proved to be a multi-sided and active encryption mechanisms. Requirements of AES was quite strict for all candidates involved, but RC6 handled many of the criteria in an efficient manner. The fact that RC6 is not vulnerable to any known attacks reinforces its strength. Evaluation of the structure of the algorithm highlights the ever-resounding goal: simplicity.

32 bit multiplication is efficiently implemented on many processor and it is one of the advantages of RC6. For most applications, an implementation of RC6 in software is probably the best choice. For key set up RC6 could be written with 256 bytes of code, block encryption, and block decryption. Unlike many others, RC6 does not use look-up tables during encryption. RC6 code is readily fit in today's on chip cache memory. RC6 is a secure, compact and simple block cipher. It provide better performance, flexibility.

V. CONCLUSION

The cloud computing became an important topic in industry, academia and government services with the development of technology. We explained the rationale, overview, components in the SCCF, where the design was based on the requirements and the implementation was illustrated by its multi-layered security.By focusing more on security, privacy and policies cloud computing can be best applicable information technology solution.

REFERENCE

[1]Mladen A.Vouk “Cloud Computing – Issues, Research and Implementations”,Proceedings of the ITI 2008 30th Int. Conf. on Information Technology Interfaces, June 23-26, 2008

[2] Lin Liu,Eric Yu,John Mylopoulos “Security and Privacy Requirements Analysis within a Social Setting” Department of Computer Science, University of Toronto, Toronto, Canada, M5S 1A4

[3]U.Jyothi K., Nagi Reddy, B. Ravi Prasad, Review of "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing"International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 2 Issue 8 August, 2013

[4] Mohamed Al Morsy, John Grundy and Ingo Müller,"An Analysis of The Cloud Computing Security Problem" In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[5] A. S. Choudhary and M. L. Dhore, "CIDT: Detection of Malicious Code Injection Attacks on Web Application," International Journal of Computer Applications, Vol. 52, No. 2, pp. 19-26, August 2012.

[6]Web Application Attack Report for the Second Quarter of 2012http://www24.firehost.com/company/newsroom/web-application-attack-report-second-quarter-2012

[7] Visitors to Sony PlayStation Website at Risk of Malware Infection, July 2008.http://www.sophos.com/en-us/press-office/press-releases/2008/07/playstation.aspx

[8]N. Provos, M. A. Rajab, and P. Mavrommatis, "Cybercrime 2.0: When the Cloud Turns Dark," ACMCommunications, Vol. 52, No. 4, pp. 42–47, 2009.

[9]S. S. Rajan, Cloud Security Series | SQL Injection and SaaS, Cloud Computing Journal, November 2010.

[10]M. McIntosh and P. Austel, "XML Signature Element Wrapping Attacks and Countermeasures,"2005 workshop on Secure web services, ACM Press, New York, NY, pp. 20–27, 2005.

[11] N. Gruschka and L. L. Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited,"IEEE International Conference on Web Services, Los Angeles, 2009.

[12]Researchers Demo Cloud Security Issue with Amazon AWS Attack, October 2011.http://www.pcworld.idg.com.au/article/405419/researchers_demo_cloud_security_issue_amazon_aws_attack/

[13] K. Zunnurhain and S. Vrbsky, "Security Attacks and Solutions in Clouds," 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, December 2010.