SECURE LOGGING AS A SERVICE –PROACTIVE ATTRIBUTE BASED ENCRYPTION-A SURVEY

S.M.Suganya[1], M.MohanKumar[2]

[1]PG Scholar, Dept of Computer Science & Engineering,
Sri Vidya College Of Engineering and Technology, (India)
[2]Asst. Professor, Dept of Computer Science & Engineering,
Sri Vidya College Of Engineering and Technology, (India)

ABSTRACT

Confidentiality assures that the information is not disclosed to unauthorized individuals. It also assures privacy to the information. Integrity provides information being changed only by authorized user. Availability assures that systems work promptly and services are not denied to unauthorized users. Maintaining log records for an organization is very important for finding any malicious activity like modifying the data, deleting the data, etc., that has occurred within the organization and to trouble shoot the problems. In order to attain confidentiality, integrity, privacy of log records, proper encryption is being done and encrypted data is placed in the cloud to reduce storage cost. This paper is an analysis of various algorithms used for the purpose of maintaining confidentiality of log records and the parameters associated with the log records like correctness, verifiability, confidentiality, tamper resistance.

Keywords—Cloud, Confidentiality, Encryption, Integrity, Log, Privacy

I. INTRODUCTION

Cloud computing[1] is Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on-demand. The cloud computing is a culmination of numerous attempts at large scale computing with seamless access to virtually limitless resources. There are three major services in cloud[2] [3]Saas, Pass and Iass. Saas provides application, Paas provides the platform to run those applications like OS, DB and Iaas provides infrastructure like network and processor. A numerous Service schemes are blooming in the field of cloud and one of the services is SLAS[4] [Secure Log As Service], which is used to securely maintain the log records. Log keeps record of events that has occurred based on date, day, time and who has accessed those records. So it is easy to verify the log when there is a need of trouble shooting. Log information can be helpful to an attacker in gaining unauthorized access to system. An attacker on accessing the data tries to modify log record in order to delete the trace of his entry. So log records should be secured but on timely manner, the size of log record increases. Hence large storage is needed, therefore it should move to cloud to reduce storage cost. Maintaining log for long time is difficult and expensive. Trusted Cloud provides this service that reduces cost, storage space and provides high security. Cloud provider may be curious about the data so encryption is done before it is placed in the cloud. Only authorised user of the organisation can access those data.

II. EXISTING APPROACHES-SYSLOG, SYSLOG-NG, SYSLOG-SIGN, REALIABLE SYSLOG.

Syslog [6]can be used for computer system management and security auditing as well as generalized informational, analysis, and debugging messages.syslog generates a system log message.**s**yslog() generates a log message that will be distributed by the system logger. syslog-ng[5] is the trusted log management infrastructure for hundreds of thousands of users worldwide. Organizations use syslog-ng to reliably and securely collect, process and store log messages from across their IT environments.It implements the basic syslog protocol, extends it with content-based filtering, rich filtering capabilities, flexible configuration options and adds features such as using TCP for transport.

Table 1: Comparison of Secure Logging as a Service with Existing Approach

Protocol	**Security Requirements**			
	Confidentiality	**Authentication**	**Integrity**	**Reliable Delivery**
Syslog	No	No	No	No
Syslog-ng	Yes	No	Yes	Yes
Syslog-sign	No	Yes	Yes	No
Reliable syslog	Yes	Yes	Yes	Yes
SLAS	Yes	Yes	Yes	Yes

III. ARCHITECTURE

Log generating admin generates log records, monitor the entire organization network,.It sends the log records to log encryptor as batches. Log encryptor get the log from log generating admin and encrypt the log records and place it in cloud, a separate entity called log decryptor is used to retrieve log records from cloud. Cloud provide storage space to hold encrypted log record of various organization (security is maintained). The proposed system includes generation of log records and securing the log records, where authentication to logging cloud with log encryptor and log decryptor is done through Diffie-Hellman algorithm through key exchange between the log encryptor and the log decryptor. In order to avoid active attack during key exchange, a shared key is used, that has been updated using proactive secret sharing scheme[7]. Only the log decryptor having the valid share can do key exchange with the log encryptor. Encryption of log records is done by the log encryptor using Reverse Encryption Algorithm (REA)[15] .Instead of generating the key randomly for encryption, if it is based on the attribute of log records like log time, date,etc.,it would be better and stores the encrypted data to the cloud. Retrieval of log record is done through the log decryptor.REA for encryption allows the key to be appended with the data to form ciphertext through certain operations,so it is not necessary to have a separate key management for encryption.

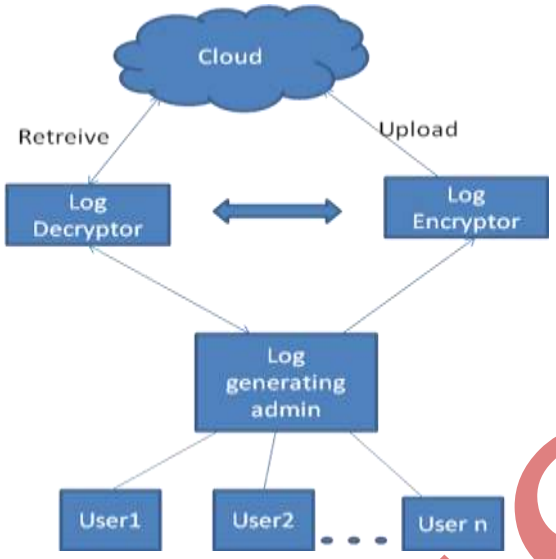

Fig. 1: Architecture for logging as a service in cloud

Table 2: Roles and Responsibilities of Entities

Entity	**Roles and responsibilities**
Cloud	Service for storing the log record in order to reduce the storage cost
Log decryptor	Decrypts the log from cloud and send it to log generating admin
Log encyptor	Encrypts the log from log generating admin and store it in cloud
Log generating admin	Monitor the entire organization network,Generates the log,Send the needed information(log) to log encryptor,Ask required information from cloud through log decryptor.
Users	Several users are connected to the log generating admin in client server environment so that users activity are recorded in the log file

IV. COMPARING SECRET SHARING SCHEME AND PROACTIVE SECRET SHARING SCHEME

In secret sharing scheme[7], the secret is split into ' n' parts giving each participant its own unique part, where any subset of 't' parts is sufficient to reconstruct the secret. The major drawback here is an attacker can successively compromise each host until he compromises 't' hosts because the time to compromise the share is more. Proactive secret sharing scheme[10][11] periodically renew the shares (without reconstructing the secret) so that it prevents an adversary from gaining the knowledge of the secret before it expires. So an attacker has less time to compromise t shares

V. ENCRYPTION MECHANISM

5.1 Homomorphic Encryption

Homomorphic encryption[8] is the conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form. Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption.In order to reduce communication overhead, without compromising privacy and security of log data homomorphic encryption is performed instead of general encryption. Homomorphic encryption permits computation on encrypted data.

5.2 Comparing Advanced Encyprtion Standard and Blow Fish

AES [9]was designed to be efficient in both hardware and software.Encryption consists of 6 rounds of processing for 88-bit keys,8 rounds for 152-bit keys, and 7 rounds for 223-bit keys. Except for the last round in each case, all other rounds are identical. Blowfish is a symmetric (that is, a secret or private key) block cipher that uses a variable-length key, from 32 bits to 78 bits, making it useful for both domestic and exportable use. It was designed in 1553 by Bruce Schneier as an alternative to existing encryption algorithms. It is 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.It has a 31-bit block size whereas AES has a 88-bit block size,As for strict brute force complexity, if 223-bit keys are sufficiently resistant to brute- forcing then using a longer key makes no sense. But theoretically speaking, Blowfish uses all 78 bits of the key, so a brute-force attack would take on average 2^74 guesses at the key, whereas AES would take 2^222 guesses on average

5.3 Message Authentication Code (MAC)

MAC[9] is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. Integrity assurances detect accidental and intentional message changes, while authenticity assurances affirm the message's origin.A MAC algorithm, sometimes called a **keyed** (**cryptographic**) **hash function** (however, cryptographic hash function is only one of the possible ways to generate MACs), accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a *tag*). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

5.4 Proactive Secret Sharing Scheme

Proactive secret sharing scheme[10][11] is a method to update distributed keys (shares) in a secret sharing scheme periodically such that an attacker has less time to compromise shares. This contrasts to a non-proactive scheme where if the threshold number of shares are compromised during the lifetime of the secret, the secret is compromised. If the players (holders of the shared secret) store their shares on insecure computer servers, an attacker could crack in and steal the shares. Since it is not often practical to change the secret, the uncompromised shares should be updated in a way that they generate the same secret, yet the old shares are invalidated. In order to update the shares, the dealer (i.e., the person who gives out the shares) generates a new random polynomial with constant term zero and calculates for each remaining player a new ordered pair, where the x-coordinates of the old and new pairs are the same. Each player then adds the old and new y-coordinates to each other and keeps the result as the new y-coordinate of the secret.All of the non-updated shares the attacker accumulated become useless. An attacker can only recover the secret if he can find enough other non-updated shares to reach the threshold. This situation should not happen because the players deleted their old shares. Additionally, an attacker cannot recover any information about the original secret from the update process because it only contains random information.The dealer can change the threshold number while distributing updates, but must always remain vigilant of players keeping expired shares.

5.5 Attribute-Based Encryption

Attribute-based encryption (ABE)[13][14] is a vision of public key encryption that allows users to Encrypt and decrypt messages based on user attributes. This functionality comes at a cost. In a typical implementation, the size of the cipher text is proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes used during decryption. Specifically, many practical ABE implementations require one pairing operation per attribute used during decryption.Attributes for log records like time, date is taken ,it is converted into binary format through ascii code and xor calculation is done between the binary values. The resultant binary value is converted to hexa- decimal value and is considered as a key.

5.6 Reverse Encryption Algorithm (REA)

Reverse Encryption Algorithm[15] is a symmetric stream cipher that can be effectively used for encryption and safeguarding of data. It takes a variable length key, making it ideal for securing data. The REA algorithm encipherment and decipherment consists of the same operations, only the two
operations are different:

1) Added the keys to the text in the encipherment and removed the keys from the text in the decipherment.
2) Executed divide operation on the text by 1 in the encipherment and executed multiple operation on the text by 1 in the decipherment. We execute divide operation by 1 on the text to narrow the range domain of the ASCII code table at converting the text.

5.6.1 Encryption Algorithm of the REA

The following steps are

Step1: Input the text and the key.
Step2: Add the key to the text.

Step3: Convert the previous text to ascii code.

Step4: Convert the previous ascii code to binary data.

Step5: Reverse the previous binary data.

Step6:Gather each 8 bits from the previous binarydata and obtain the ascii code from it.

Step7: Divide the previous ascii code by 1.

Step8: Obtain the ascii code of the previous result divide and put it as one character.

Step9:Obtain the remainder of the previous divide and put it as a second character.

Step10: Return encrypted text.

5.6.2 Decryption Algorithm of the REA

The following steps are

Step1: Input the encrypted text and the key.

Step2: Loop on the encrypted text to obtain ascii code of characters and add the next character.

Step3: Multiply ascii code of the first character by 1.

Step4: Add the next digit (remainder) to the result multiplying operation.

Step5: Convert the previous ascii code to binary data.

Step6: Reverse the previous binary data.

Step7: Gather each 8 bits from the previous binarydata and obtain the ascii code from it.

Step8: Convert the previous ascii code to text.

Step9: Remove the key from the text.

Step10: Return decrypted data.

5.7 Diffie-Hellman Algorithm

Diffie-Hellman algorithm[9][16] is to enable two users to securely exchange a key that can be used for subsequent encryption of messages.All users agree on global parameters:large prime integer or polynomial q,α a primitive root mod q.Each user (eg. A) generates their keychooses a secret key (number): $x_A < q$ compute their public key: $y_A = \alpha^{xA}$ mod q.Each user makes public that key y_A. shared session key for users A & B is K_{AB}: $K_{AB} = \alpha^{xA.xB}$ mod q= y_A^{xB} mod q (which B can compute) = y_B^{xA} mod q (which A can compute) K_{AB} is used as session key in private-key encryption scheme between Alice and Bob if Alice and Bob subsequently communicate, they will have the same key as before, unless they choose new public-keys attacker needs an x, must solve discrete log .

5.8 TOR (Onion Router)

Cryptography hides the content of data (integrity)but it does not hide who is sending, receiving the data. Anonymity is hiding who is sending the data.TOR network[17][18] encrypts original data, like IP address multiple times and sends it through virtual circuit comprising successive randomly selected Tor relay. Each relay decrypts a layer of encryption to reveal only the next relay in the circuit in order to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing, or even knowing, the source IP addres. Anyone watching the connection, will see random traffic coming from some random spot on the internet

VI. METRICS ASSOCIATED WITH SECURE LOGGING

6.1. Correctness

Log record is important because it shows the history of the system so that collected log records should be correct. It should be same when it was generated.

6.2. Verifiability

It must be able to check that all the entries in the log record are available or not and it must be ensured that data in log record have not been altered.

6.3. Confidentiality

Log records should not be easy to search, to collect the personal information of others. Access should be provided to only legitimate users

6.4. Privacy

While in transition, log records should not be tracked by unauthorized persons.

6.5. Tamper Resistance

A log should be provided security in such a way that only log generating admins are allowed to introduce valid entries.

Table 3: Comparison Of Algorithms

Algorithm	Advantage
Homomorphic Encryption	It is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services.
Advanced Encyption Standard	It is faster in both hardware and software and it's 88-bit block size makes it less open to attacks via the birthday problem than 3DES with its 31-bit block size.
Blowfish	It is one of the strongest algorithms available and the speed of the algorithms and key strength is also very good. It is suitable and efficient for hardware implementation. Besides, it is unpatented and no license is

	required.
Attribute Based Encryption	Instead of generating a key randomly for encryption,it would be better if the key is generated based on the attributes in the log file.
Reverse Encryption Algorithm	As the key for encryption is appended with the data as encrypted data,so a separate key maintenance and management is not necessary
Diffie-Hellman	It is considered secure against eavesdroppers ie, it provides prevention against passive attack

VII. CONCLUSION

Logging plays an important role in proper operation of an organization. Maintaining logs securely over a long period of time is difficult and expensive. Usage of cloud for data storage, so that cost is reduced. An anonymous upload, retrieve and delete protocols on log records in the cloud is provided. So that security is achieved, and others may not able to modify the log information.

REFERENCES

[1] Michael Miller,Cloud Computing : Web-Based Applications That Change the Way You Work and Collaborate Online (English) 1st Edition,*Atlantic Publishers*,August 2011

[2] Smart cloud-Rethink IT Reinvent business, *http://ibm.com/smartcloud* @2012 IBM Corporation

[3] Foundations of IBM Cloud Computing Architecture, Ron Bower, Jeff McNeelyLee Zhang *http://ibm.com/smartcloud* @2010 IBM Corporation

[4] Indrajit Ray, Kirill Belyaev, Mikhail Strizhov, Dieudonne Mulamba, and Mariappan Rajaram "Secure Logging As a Service Delegating Log Management to the Cloud" *IEEE Systems Journal, Vol. 7, No 2*, June 2013

[5] BalaBit IT Security (2011, Sep.). Syslog-ng—Multiplatform Syslog Server and Logging Daemon [Online]. Available*: http://www.balabit.Com/network-security/syslog-ng*

[6] C. Lonvick, "The BSD Syslog Protocol", Request for Comment RFC 3164, *Internet Engineering Task Force, Network Working Group*, Aug. 2001

[7] A. Shamir, "How to share a secret," Commun. *ACM, vol. 22, no. 11,pp. 612–613*, Nov. 1979.

[8] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI "Homomorphic Encryption Applied to the Cloud Computing Security "*Proceedings of the World Congress on Engineering 2012 Vol I WCE* 2012,July 4 - 6, 2012, London, U.K

[9] William Stallings,Cryptography and network security*Pearson publications* ,fifth edition,January 2010

[10] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive secret sharing or: How to cope with perpetual leakage," in Proc. *15th Ann. Int.Cryptology Conf.*, Aug. 1995, pp. 339–352.

[11] http://en.wikipedia.org/wiki/Proactive_secret_sharing

[12] http://en.wikipedia.org/wiki/Message_authentication_code

[13] Vipul Goyal,Omkant Pandey,Amit Sahai ,Brent Waters

[14] "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data "*ACM CCS 2006*

[15] http://en.wikipedia.org/wiki/Attribute-based_encryption

[16] Ayman Mousa,Elsayed Nigam,Sayed El-Rabaie,Osama Faragallah "Query Processing Performance on Encrypted Databases by Using the REA Algorithm" *International Journal of Network Security Vol. 14*, No. 5, 2012, pp. 280-288

[17] http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[18] Linus Nordberg Jacob Appelbaum "Anonymity and Censorship:The Tor Network" *IETF 87 - Berlin 1st* August 2013

[19] https://www.torproject.org/