Secure Logging as a Service –Proactive Attribute Based Encryption-A Survey

Dr. Vijay Bhardwaj

[1,2]Guru Kashi University, Talwandi Sabo

ABSTRACT

Confidentiality ensures that the information is not shared with anybody who isn't supposed to know. It also ensures that the information is kept private. Integrity ensures that only authorised users have access to information. Availability ensures that systems respond quickly and that unauthorised users are not denied access to services. Maintaining log records for an organisation is critical for detecting and troubleshooting any harmful behaviour, such as data modification, deletion, and so on, that has happened within the business. Proper encryption is used to ensure the security, integrity, and privacy of log records, and encrypted data is stored in the cloud to save money on storage. This study examines alternative techniques for preserving log record secrecy, as well as the factors connected with log records such as accuracy, verifiability, confidentiality, and tamper resistance.

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

I. INTRODUCTION

Cloud computing[1] is Internet-based computing in which shared resources, software, and information are made available on demand to computers and other devices. Cloud computing is the result of countless attempts to provide seamless access to nearly infinite resources at a huge scale. Saas, Pass, and Iass are the three key cloud services[2] [3]. Saas offers applications, Paas provides the platform on which those applications are executed, such as the operating system and database, and Iaas provides infrastructure, such as the network and processor. In the world of cloud computing, there are several service schemes, one of which is SLAS[4] [Secure Log As Service], which is used to securely preserve log information. The log maintains track of occurrences by date, day, and time, as well as who has viewed the information. As a result, when troubleshooting is required, it is simple to validate the log. An attacker can use log information to gain unauthorised access to a system. When an attacker has access to the data, he attempts to edit the log record in order to erase his entry's trail. As a result, log records should be protected, although doing so on a timely basis increases the size of the log record. As a result, huge storage is required, thus it should be moved to the cloud to save money on storage. Keeping a log for a long period is tough and costly.

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

Syslog [6]can be used for generic informative, analytical, and debugging messages, as well as computer system administration and security audits. A system log message is generated by syslog. The system logger will transmit a log message generated by syslog(). For hundreds of thousands of users throughout the world, syslog-ng[5] is the trusted log management infrastructure. Organizations use syslog-ng to collect, analyse, and store log messages from across their IT systems in a reliable and secure manner. It implements the fundamental syslog protocol and adds features such as content-based filtering, sophisticated filtering capabilities, configurable setup choices, and TCP transmission.

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

The log producing administrator creates log records and keeps track of the whole organization's network. It transmits log entries in batches to the log encryptor. The log encryptor receives the log from the log producing admin and encrypts the log records before storing them in the cloud. The log decryptor is used to recover the log data from the cloud. The cloud provides storage space for many organisations' encrypted log records (security is maintained). The proposed system involves the production of log records and the securing of log records, with authentication to the logging cloud using the Diffie-Hellman algorithm and key exchange between the log encryptor and the log decryptor. A shared key, which has been updated via a proactive secret sharing scheme[7], is utilised to avoid active attack during key exchange. Only log decryptors with a valid share can exchange keys with log encryptors. The log encryptor uses the Reverse Encryption Algorithm (REA)[15] to encrypt log records. Instead of creating the encryption key at random, it would be better to base it on the attributes of log records such as log time, date, and so on, and then store the encrypted data in the cloud. The log decryptor is used to retrieve log records.

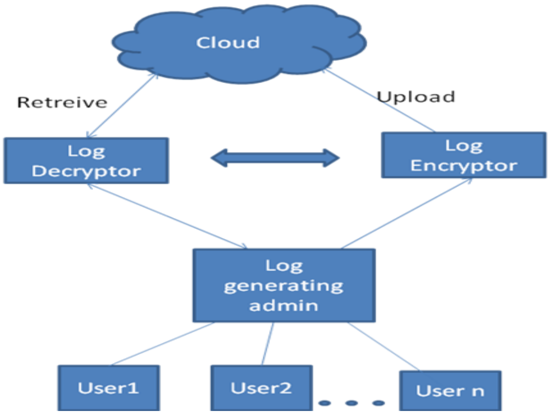

Fig. 1: Architecture for logging as a service in cloud

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

The secret is split into'n' pieces, providing each participant their own unique part, and any subset of 't' parts is sufficient to reconstruct the secret in a secret sharing scheme[7]. Because the time to compromise the share is longer, an attacker can gradually compromise each host until he compromises all 't' hosts. Proactive secret sharing schemes[10][11] renew shares on a regular basis (without reassembling the secret) to prevent an opponent from learning the secret before it expires. As a result, an attacker will have a shorter time to compromise t shares.

V. ENCRYPTION MECHANISM

5.1 Homomorphic Encryption

The conversion of data into ciphertext that can be studied and worked with as if it were still in its original form is known as homomorphic encryption[8]. Complex mathematical processes can be performed on encrypted data without compromising the encryption using homomorphic encryptions. Instead of using conventional encryption, homomorphic encryption is used to decrease communication cost while maintaining the privacy and security of log data. Computation on encrypted data is possible with homomorphic encryption.

5.2 Comparing Advanced Encyprtion Standard and Blow Fish

AES [9]was created with efficiency in mind, both in terms of hardware and software. Encryption takes six rounds for 88-bit keys, eight rounds for 152-bit keys, and seven rounds for 223-bit keys. Except for the last round in each scenario, the rest of the rounds are the same. Blowfish is a symmetric (secret or private key) block cypher with a variable-length key ranging from 32 to 78 bits, making it suitable for both domestic and international application. Bruce Schneier created it in 1553 as an alternative to current encryption techniques. It is substantially quicker than DES since it is built for 32-bit instruction processors. It has been extensively studied since its inception. Blowfish is unpatented, without a licence, and free to use for any purpose. It uses a 31-bit block size instead than the 88-bit block size used by AES. In terms of pure brute-force difficulty, choosing a larger key makes little sense if 223-bit keys are adequately resistant to brute-force attacks. However, because Blowfish uses all 78 bits of the key, a brute-force attack would need an average of 274 attempts at the key, whereas AES would require an average of 2 ^22 guesses.

5.3 Message Authentication Code (MAC)

MAC[9] is a brief piece of information that is used to verify a communication and ensure its integrity and validity. Authenticity guarantees confirm the communication's origin, whereas integrity assurances identify inadvertent and purposeful message alterations. A MAC algorithm, sometimes known as a keyed (cryptographic) hash function (although cryptographic hash functions are only one of the many ways to produce MACs), takes a secret key and an arbitrary-length message to authenticate as input and returns a MAC (sometimes known as a tag). By allowing verifiers (who also have the secret key) to identify any modifications to the message content, the MAC value protects both the data integrity and the validity of the message.

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.

5.7 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 .

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

The proper running of an organisation relies heavily on logging. It's difficult and expensive to keep logs safe for an extended length of time. The use of the cloud for data storage reduces costs. On log records in the cloud, anonymous upload, retrieve, and delete methods are given. As a result, security is established, and others may not be able to alter the log data.

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/