Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Cloud Storage Using Access Control Models

M.Sharadwi[1] , Dr.S.Murali Krishna [2]
Dept of CSE & JNTUA
India

Abstract-- The data backups are outsourced to third party cloud storage services so as to reduce data management costs. The security must be provided for the data that is kept on the cloud. We propose an access control model that extends FADE system to take time, email and encryption account, and use term rewriting systems to specify access control policies in this model. The declarative nature of the model facilitates the analysis of policies and the evaluation of access requests. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. In public key cryptography each user or the device taking part in the communication generally have a pair of public and private keys and also the set of keys that are used for the cryptographic operations. The private key is given only to the authorized users where as public key is distributed to all the users who takes part in the communication. public key algorithm requires a set of predefined constants to be known by all the devices taking part in the communication

Key Words: cloud computing, access control, email, time, Cryptography.

I. INTRODUCTION

"Cloud computing" is a more simple technology than many other new set of business models and technologies. It is rapidly increasing as the platform that will be used in the next coming generation of digital products and services. Cloud computing tells us about how the consumers, companies and government agencies store the required information, how that information is exchanged between them and how the computing power is utilized. Therefore a new set of policy discussions are emerged, and at the same time considering the importance of old applications. In the era of "cloud computing", discussions about the policy will continue the debate about standard questions: the terms related to market access for services and the rules for IP, privacy, security and more. However, the Cloud must be understood at once as a dynamic enhanced utility, competitive service, an ICT platform/infrastructure, a marketplace, and a production environment. The persistent, disrupting multi-role character of "cloud computing" demands the new set of questions to be arises. First, though, what exactly is Cloud Computing? A wide variety of services are marketed by the firms as "Cloud Solutions," leading – often deliberately - to some confusion. If it includes all the online services, the term loses meaning and risks are considered primarily. Cloud Computing delivers computing resources – data storage, computation and networking – to the users at a time, to the location and in the quantity they wants to consume, with costs based only on the used resources. In simple words "Cloud" transforms computing resources from a capital expense to an operational expense. Users simply acquire from providers the "amount of computing" they require without investing in their own computing infrastructure.

Figure 1: Cloud storage

Cloud Computing helps in hiding the software platforms and applications from the underlying computing resources and physical hardware on which they depend. for example in Amazon's Elastic Cloud Service , the company never wants to reveal about the data related to customers, the physical servers used and the data stored in the servers. This "Virtualization" enables greater flexibility in how datacenters are constructed, workloads are managed since providers

without reconfiguring the services that depend on them can vigorously add, remove or modify hardware resources. The "Virtualization" emerged in the 1960s and is not new in the technology- but when combined with very highly developed systems management software today's "Cloud Fabric" environments enable truly global scale computing environments. Cloud Computing changes the location of data processing or – more correctly – makes the location of data processing irrelevant – technically if not in policy terms. In usual models of computing, applications and data are used as local that runs on a personal computer (PC) for consumers and in private data centers for firms. The location of application execution and data storage is pre-defined by the design of the system. The cloud model applications stores the data and can be run in any global environment which can merge many data centers in multiple physical locations. The storage and execution locations are no-longer pre-defined by design but are now programmed real-time decisions based on the availability of computing resources at any particular time.

II. Related Work

A secure overlay cloud storage system called FADE is implemented that achieves well defined access control and file assured deletion which is policy based. The files that are stored on the cloud are associated with file access policies, and the files must be deleted assuredly to make them unrecoverable to anyone upon requests of file access policies. To attain the security to the cloud, FADE is built upon the set of cryptographic key operations that are maintained by a committee of key managers that are independent of third-party clouds.

Figure 2 illustrates an overview of the FADE system,

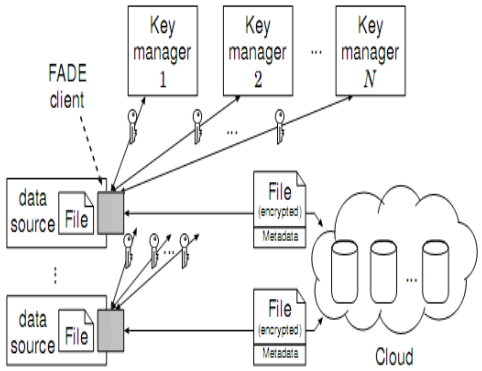

Fig 2: The Fade System

III. TIME-BASED ACCESS

The recent growth of digital communication has increased the demand of security for protecting resources and preserving the integrity and confidentiality of data. Thus, in recent years considerable interest has been centered on the area of access control models. Access control is concerned with the actions that can be executed from the given subject. For the centralized systems, one of the most popular choices is the Role-Based Access Control (RBAC) model. In RBAC, users are assigned to roles by a security administrator; roles usually map to job titles in an organization, and as such, this model is well-suited for relatively static environments.

High mobility of users and services in the emerging mobile applications entails the need for access control the time of the request into account in order to decide whether to grant or deny an access request. Several extensions to RBAC have been proposed to incorporate spatial-temporal information in the model. One of the first time-based RBAC models was proposed.

User Identity: User who are given the access permission can be either in Internal (User database) or External Identity

Time &Date: User would be granted access only on Weekends i.e. Saturday / Sunday

Authorization Profile: User would be able to access certain services i.e., read only, read/write, full control

Example: Policy Elements that constitute a Policy i.e. a Time based Access policy to allow VPN users access only on Weekend would have Weekend (Sat/Sun) as a Condition to match & apply an Authorization Profile to a user to grant them network/resource access, We focus on "Session Conditions" i.e. the conditions on time and date that specifies time/date on which you wish to grant access. These Conditions are based on current date & time so it's essential to have NTP/time-zone.

IV. EMAIL-BASED ACCESS

The employees and contractors of the Firm who are authorized can access the individual's electronic "mail box" on the Firm's email system. All the access that is done must be within the Firm's caution. Your approval to the firm which has an access to the electronic mail box must be given, as given by your signature below, before that an email account must be assigned. In addition, it is expected that each employee will be assigned the relevant password to their personal email account and not reveal their password to unauthorized individuals. Each email user should "sign out" their PC after there work gets finished and leave for the day or when they will be on leave from their desk for a particular period. If your pc is signed in and if you are not on the desk for a particular period of time, unauthorized users can completely access your email account and also they can even access your account if email password is known. We should also remember that the message that is present in the inbox can be forwarded to others without our knowledge. In the Firm's network servers, an email message does not consist of Automatic Backup and Retention of Messages, No backup or duplicate copy.

Therefore, email messages that are deleted by both the sending and receiving part (ies) will not exist in any electronic medium

V. CRYPTOGRAPHY WITH ELLIPTIC CURVES

The main attraction of ECC when compared to RSA is that, an equal security level is assigned to the key which is of least size, thereby reducing processing overhead. In this cryptography, the addition operation is the complement of modular multiplication in RSA, and multiple additions is the complement of modular exponentiation. To form this type of cryptographic system using elliptic curves, we need to find a "hard problem". All systems rely on the difficulty of a mathematical problem for their security [6]. To explain the concept of difficult mathematical problem, the notion of an algorithm is required. In order to analyze how long an algorithm takes, the computer scientists introduced the idea of polynomial time algorithms and exponential time algorithms. This algorithm runs quickly if it is polynomial time algorithm, otherwise runs slowly if it is exponential time algorithm. Therefore, easy problems associate with polynomial time algorithms, and difficult problems associate with exponential time algorithms. When looking for a mathematical problem on which to base a public key cryptographic system, cryptographers search for a problem for which the fastest algorithm takes exponential time. The longest time taken to compute the best algorithm for a problem, the public key cryptosystem based on that problem will be made more secured. Three types of systems [2] are considered secure and efficient: the Integer Factorization Systems (RSA), the Discrete Logarithm systems (DSA) [5], and the Elliptic Curve System (Elliptic Curve Discrete Logarithm System)[3,4]. In RSA, given an integer n which is the product of two large primes p and q such that

$$n = p \times q.$$

It is easy to calculate n given p and q but it is difficult to determine p and q given n for large values of n. The U.S. government's Digital Signature Algorithm (DSA) is based on discrete logarithm problem modulo a prime p. Given an integer g between 0 and p-1, and y which is the result of exponentiation of 'g ', we have

$$y=g \text{ ^ } x \pmod p \text{ for some } x.$$

The discrete logarithm problem modulo p is to determine the integer x for a given pair g and y. The Elliptic Curve Cryptosystem (ECC), whose security rests on the discrete logarithm problem over the points on the elliptic curve? The main appeal of ECC over RSA and DSA is that it is the best known algorithm for solving the underlying hard mathematical problem in ECC (the elliptic curve discrete logarithm problem (ECDLP) takes full exponential time. Both RSA and DSA take the sub-exponential time. This means that considerably smaller parameters can be used in ECC than in other systems such as RSA and DSA, but with the same levels of security .A typical example is that the size in bits of the keys used in different public key systems, with a comparable level of security (against known attacks), that is a 160-bit ECC key is equivalent to RSA and DSA with a modulus of 1024 bits. The lack of a sub-exponential attack on ECC offers potential reductions in processing power and memory size. These advantages are especially important in applications on constrained devices. In practical terms, the performance of ECC depends mainly on the efficiency of finite field computations and fast algorithms for elliptic scalar multiplications. In addition to the several known algorithms for these computations, the performance of the ECC can be rapidly increased by selecting the particular underlying finite fields and/or elliptic curves. For ECC, we are concerned with a constrained form of elliptic curve that is defined over a finite field. The cryptography is referred to as the elliptic group mod p, where p is referred as a prime number. This is defined as follows. Select two nonnegative integers, a and b , that satisfies less than p:

$$4a3 + 27\ b2 \pmod p \neq 0.$$

Then Ep(a, b) denotes the elliptic group mod p, whose elements (x, y) are pairs of nonnegative integers that satisfies the less than p rule:

$$y2 \equiv x3 + ax + b \pmod p$$

Along with the point at infinity Q. The elliptic curve discrete logarithm problem can be defined as follows. The prime p and an elliptic curve stated as follows.

$$Q= xP$$

Here the xP represents the point P on the elliptic curve which can be added to it x times. Then the elliptic curve discrete logarithm problem issued to determine the x by considering P and Q. It is easy to calculate Q with the given x and P, but it is very hard to determine the x by using given Q and P.

ECC Encryption/Decryption:

Several approaches to encryption/ decryption using elliptic curves have been analyzed. One of them is described here. The first task to be done in this system is, the plain text message m is to be encoded and should be sent as x-y point Pm. The point Pm must be encrypted as a cipher text and later should be decrypted. We should also notice that we cannot simply encode the message as the point coordinates x or y, since all such coordinates are not present in Ep(a, b). There are approaches to encoding. We developed a scheme that will be reported elsewhere. Consider the key exchange system, where an encryption/decryption system takes the parameters point G and an elliptic group Ep (a, b). If a user is considered as A then he selects a private key nA and generates a public key

$$PA = nA \times G$$

If a message is to be sent from Pm to B, the message has to be sent in the encrypted form, the user A chooses a positive integer x randomly and generates the cipher text Cm which consists the pair pf points

$$Cm = \{xG, Pm + xPB\}$$

Note that A has used B's public key PB. To decrypt the cipher text, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:

$$Pm + xPB – nB(xG) = Pm + x(nBG) – nB(xG) = Pm$$

A has covered the message Pm by adding xPB to it. The value of x is known only to A, so even though PB is a public key, none can remove the covered xPB. But, A also includes a "clue," which is enough to remove the mask if one knows the private key nB. If the attacker wants to recover the message, he has to compute x given G and xG, which is hard. There is the question about what network layers should security be implemented in. Should it be implemented at the IP layer, or at the transport layer or at the application layer? For this reason it is desirable to create an API that implements encryption and later this API can be used at any layer deemed to be most appropriate for a given circumstance. After analyzing the broad picture, we have developed an Application

Programmer's Interface (API) that implements ECC, allowing it to be used in a variety of applications. Shows how the API fits into the overall network model. As the model suggests, the ECC API is intended to be used in the security layer to automatically encrypt/decrypt all data that flows to or from the application layer. This model allows the application to be oblivious to encryption issues by designating that responsibility to the security layer. The security layer in turn will depend on the API in order to carry out its task. A major advantage of this model is that existing applications do not have to be rewritten to utilize the ECC API; instead they can be executed as they are and still benefit from the new encryption scheme. ECC API is implemented in Java language instead of C language for the following reasons:

1) Java is portable so the API can be used on virtually any device with computing power and with any operating system.
2) The new Java (JIT) compiler is quotedto compile Java programs with optimizations that allow the programs to run about as fast as programs written in C.

The advantage of portability was the deciding factor in choosing Java.

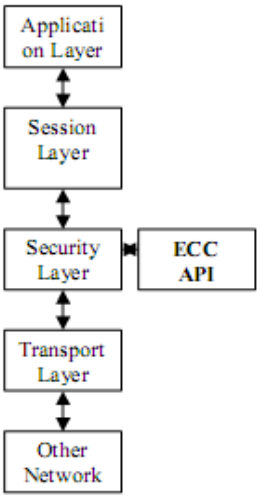

Fig 3: Where API fits in the overall network

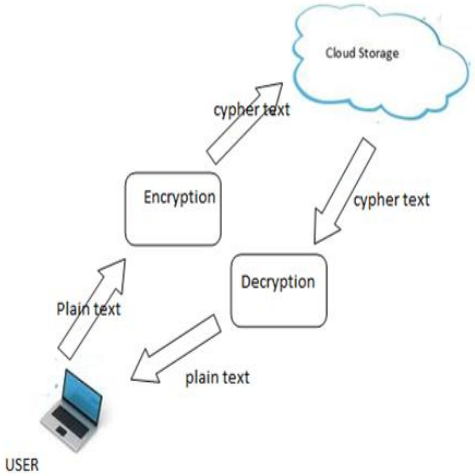

Figure 4: Cryptography with Elliptic Curves

The API will allow calling programs to encrypt or decrypt data using keys provided by the caller. The API will also be capable of generating new keys from scratch that can be subsequently used. The API is designed keeping in mind the low computing resources available to it. We developed a front-end program to demonstrate the functionality of this front-end program utilizes the ECC API to encrypt a plain text data file. The program can be used on computing devices in order to

store the ECC API. Confidential data securely onto the device. In addition to encryption and decryption, ECC API can be applied to other applications such as Digital Signatures, Mutual Authentication.

VI. CONCLUSION

The security guarantees must be provided for the outsourced data,which is maintained by the third party cloud providers .By using time, email and cryptography we can provide the more security for user data.

References

[1] R.L. Rivest, A. Shamir, and L.M. Adleman, " A Method for Obtaining Digital Signatures and Public- key Cryptosystems ", communications of the ACM, Volume 21, pages 120-126, February 1978.
[2] Certicom Corp., "An Introduction to Information Security", umber 1, March 1997.
[3] N.Koblitz, "Elliptic Curve Cryptosystems ",mathematics of Computation., Number 48,pages 203- 209,1987.
[4] V.S. Miller," Use of Elliptic Curves in Cryptography ",Advances in Cryptology- Proceedings of CRYPTO '85, Springer Verlag Lecture Notes in Computer Science 218, pages 417-426, 1986.
[5] Elliptic curve cryptography, https://en.wikipedia.org/wiki/ Elliptic_curve_cryptography
[6] RSA (algorithm),http:// en.wikipedia.org/wiki/RSA_(algorithm)
[7] JavaTM Cryptography Extension (JCE), Reference Guide.http: //docs.oracle.com/javase/1.5.0/docs/guide/security/je/JCERefuide e. Html.
[8] Berta,I.Z.,and Z. A. Mann. "Implementing Elliptic Curve Cryptography on PC and Smart Card", Periodica Polytechnica Ser. El. Eng. Vol 46. NO 1-2, PP 47. 2002.
[9] Brown, M., D. L. Hankerson, J. L_opez and A.Menezes. "Software implementation of the NIST Elliptic curves over prime fields". In Progress in Cryptology - CT-RSA, D. Naccache, Ed, vol. 2020 of Lecture Notes in Computer Science, pp. 250-265. 2001.
[10] Neal Koblitz, Alfred J. Menezes, "A Survey of Public- Key Cryptosystems". Advanced Computing & Communication Technologies (ACCT), Second International Conference, 2012.
[11] F. Baader and T. Nipkow.Term rewriting and all that. Cambridge University Press, Great Britain, 1998.
[12] S. Barker and M. Fern´ andez. Term rewriting for access control.
[13] G. Barthe, G. Dufay, M. Huisman, and S. Melo de Sousa. Jakarta: toolset to reason about the JavaCard platform. In Proc. of e-SMART'01, volume 2140 of LNCS. Springer-Verlag, 2002.
[14] M. Y. Becker C. Fournet and A. D. Gordon. Design and semantics f a decentralized authorization language. In Proc. of CSF'07, pages 3–15, IEEE Comp. Society, 2007.
[15] C. Bertolissi and M. Fern´ andez. A Rewriting Framework for the Composition of Access Control Policies. In Proc. of PPDP 2008, ACM Press.
[16] C. Bertolissi, M. Fern´ andez, and S. Barker. Dynamic event-based access control as term rewriting. In Proc. of DBSEC'07), volume 4602 o f LNCS. Springer-Verlag, 2007.

