REMOTE ATTESTATION SCHEME USING CAMENISCH ET AL.'S DYNAMIC ACCUMULATOR WITH CERTIFICATE GENERATION

Moin Ali Syed, Amreen Sultana, Nishanth Kumar and Abdelshakour Abuzneid
Department Of Computer Science & Engineering
University of Bridgeport
Bridgeport, CT, USA

Abstract

Cloud computing is a dynamic computing platform that is used world-wide for computation by all the high level and low level companies like Amazon, Google etc. Cloud Computing provides the users to access their data and save it irrespective of their location. Many companies and clients rent virtual machines for running their applications and saving their highly confidential data. However this platform is not totally secure and it has many security issues related to it. [1] In this paper, we combine trusted cloud computing and anonymous remote attestation scheme using dynamic accumulators and put forward an enhancement for this scheme which uses certificate generation mechanism for allowing the cloud manager to keep a track on the users without actually knowing the credentials of users. We mainly focused on the problem of authentication, key generation and service revocation issues. We are utilizing both the dynamic Camelish et al.'s accumulator and one way accumulator functionalities combined with an X509 certificate by Certificate Authority (CA) to solve the issue of authenticating the user and identifying the user without revealing its credentials to the Cloud Service Provider (CSP).This makes the cloud manager revoke the access of a specified user for cloud computing service provider. In addition this infrastructure is able to trouble shoot the problem of storage in Trusted Coordinator (TC). [2]

Keywords

Trusted Coordinator; Camenisch et al.'s dynamic accumulator; Cloud computing, x509 Certificate, Certificate Authority, Cloud Manager.

Introduction

Cloud computing is the most emerging technology. Using cloud technology users can store large amount of data and can access to it whenever they needed. There are two main entities in the cloud. They are (1) customer and (2) cloud service providers (CSP). Customers rent for software, platform and infrastructure from the cloud service providers. In the cloud technology cloud service providers plays a crucial role. All the devices in the cloud are controlled and managed by cloud service providers (CSP). There are four types of clouds in the cloud technology. They are Public cloud, private cloud, community cloud and hybrid cloud. Cloud computing offers 3 types of services depends up on the usage. They are Software as a Service (SaaS), Platform as a service (PaaS) and Infrastructure as a Service (IaaS). [3]

1.1 Organization: In this paper we will introduce our problem clearly in section 2 then we will shed light on preliminaries required in 3.1, 3.2. Then we will propose our architecture in section 4. Then we will explain and conclude the paper.

2. Problem Statement

As we know the users of cloud rent their platform from the CSP, They have limited contracts with the CSP and they are allowed to access the cloud nodes by CM only if they are in the contract with them. But when the user wants to access the data of cloud, he has to submit his credentials for authentication to the CSP. By doing this he reveals his credentials to the CSP and the service provider can access his highly confidential data. To avoid this problem of data confidentiality we use an accumulator supported by Trusted Third Party (TTP) to generate anonymous credentials for the user, so that the CSP do not have any information of user credentials. By doing this the user's data will be safe. But the problem is the CSP needs to have a track on users as some of them go out of contract and some of the user's access has to be revoked. But as the system is anonymous CSP faces problem to track his users and revoke their access. We solve this by making a new architectural model which is discussed in Section 4.

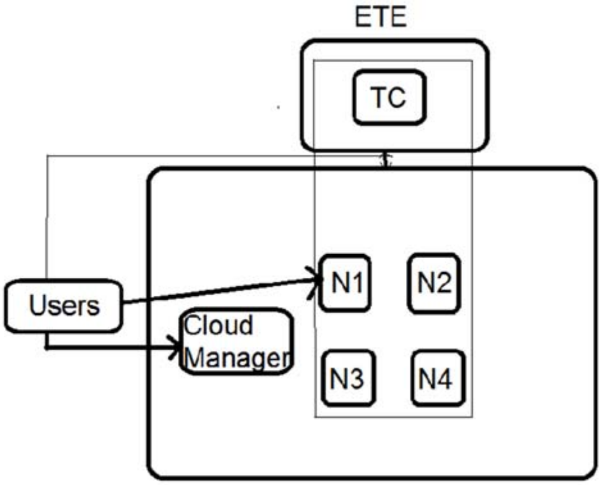

Fig 1: Existing Model of TCCP [4]

3. Preliminaries

3.1 Accumulators

Accumulators were introduced by Benelux and de Mare.They explained an algorithm which allows one to hash large group of values in to one value, which is called 'Accumulator'. And there was a witness when a value is accumulated. At the same time, it is not possible to find the witness for a value which is not accumulated. It was the problem in the accumulator. Then it developed and improved by Baric and Pfitzmann.These scientists provided a good solution to overcome the problem in the accumulator. The solution is 'Collision-Resistant Accumulator' based on the RSA algorithm.

Dynamic accumulators allow one to add or delete inputs to the accumulator. It reduces cost of adding and removing and makes sure it is independent on the Accumulated values. This is implemented by strong support of RSA algorithm. In an efficient way we can prove that the committed value in the accumulator by 'Zero Knowledge Test'. Behind this certification process is a prime number 'e'. This value will be added to the accumulator when the user is added. Similarly, this value will be deleted from the accumulator when the user is removed. [4]

There may be affected or unwanted users in the group. Then group manager has the authorization to remove the unwanted member's key from the list. There is a drawback in checking and proving membership of the authorised.

3.2 X.509 Certificate

X.509 certificate is the part of X.500 series that defines a directory service. This directory maintains information about the database of users. Example: user name, network address, password and all the other information of users. X.509 is an important standard and is used in variety of context. It was started in 1988. X.509 works on the principle of public key cryptography and digital signatures.

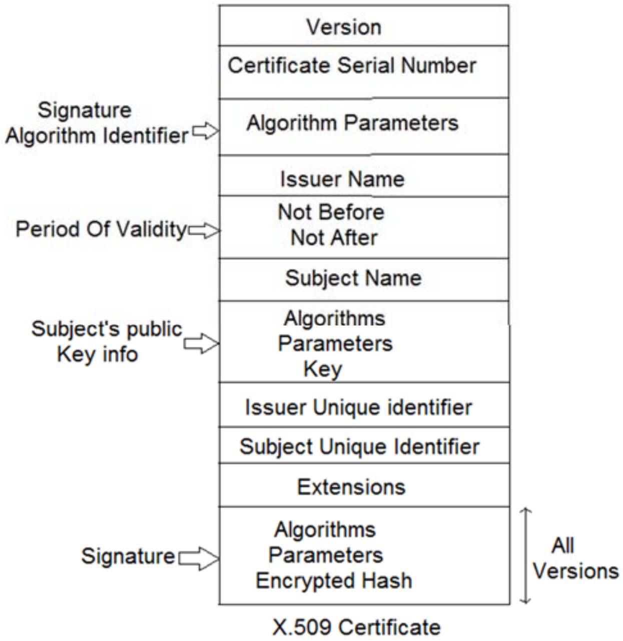

Fig 2: Signature format [5]

The standard certificate can be defined as CA << A >> = CA {V, SN, AI, CA, UCA, A, UA, Ap, T^A }

4. Proposed Architecture

The above block is the proposed architecture for our solution. This block mainly contains trusted third party (TTP), cloud manager (CM), trusted nodes and users. The problem is occurs in the cloud system when the cloud manager failed to find out the unwanted users who are not eligible to access the data. So here we are providing a solution through certificate authority in the trusted third party (TTP).There are many users ready to access the nodes. But cloud manager does not have any idea about how many users are accessing the nodes and the location of accessing users. [4]

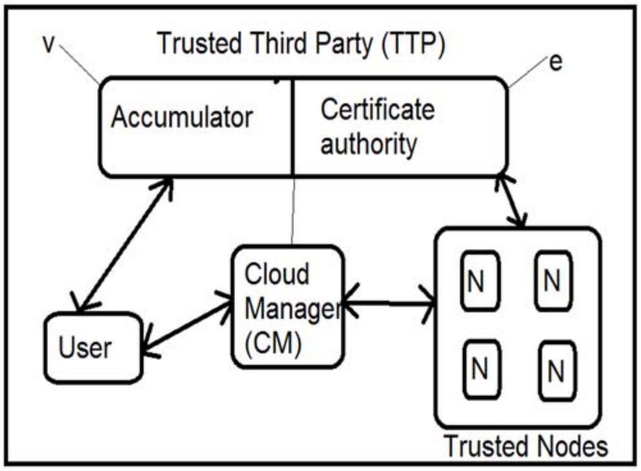

Fig 3: Architecture of Cloud network [4]

Certificate authority helps the system to overcome the problem in cloud network. Certificate authority should be in touch with each block in the network for the effective communication. Certificate authority will generate a certificate (e) for each user on each day. That certificate will be shared to each user and the cloud manager (CM).Each user should have certificate generated by the TTP when they go to cloud manager. So cloud manager will compare the both certificates given by user and TTP. If the certificate matches then it allows users to access the nodes. If it does not match it denies the user request. In this way we can eliminate the unwanted users who are not eligible to access the data. [6]

4.1 Features in the construction of Dynamic Accumulator:

The accumulated values consist of prime numbers only.

1. Dynamic accumulator is constructed to add or delete the values from accumulator.
2. An efficient algorithm to delete a user with a witness.
3. Efficient zero-knowledge protocol to prove stored values in the accumulator.

4.2 Construction of Dynamic accumulator [4]

- $\boldsymbol{F_k}$Is the function and its length of integers is 'k'.
  A random value n=p*q (: length=k)
  Where a=2a'+1 and b=2b'+1
  Where a, a', b, b' are prime numbers.

- f=f_n
  Input is (u, x) =V_f*$Z_{X,Y}$
  Output is v= V_f
  V_f=u and $Z_{X,Y}$ ={e (prime num's)}

- f=f_n
  V is the output and u is the input.
  Then, v=f (u, x) =u^xmod n

- 'w' is the witness for a value x,
  Then v=f (w, x)
  We can add and delete values from the accumulator.

- A value z is added to v,
  Then,
  v'=f (v, z') =$v^{z'}$mod n
  And witness of z can be,
  w'=f (w, z')

- A value z is deleted from v,
  Then,
  v'=$v^{z' mod\ (a-1)(b-1)}$

5. Remote Attestation Scheme

Trusted platform module (TPM) protects the secret keys by providing safe shield around it. In this process, TTP accumulates the trusted nodes to 'v'. Depends up on the usage users will get from TTP. Node 'N' gives attestation to a user in different way before the launch of virtual machine

(VM) on node 'N'.TTP is responsible for authentication of nodes and maintenance of accumulators.

This process has '4' stages,

1. Initialization of System
2. Maintaining trusted nodes
3. Remote attestation Mechanism
4. Certificate Generation

FLOW CHART

Drawing a flow chart for the process for explaining the flow of required steps.

1. Initialization of System

Here, TTP mainly uses system parameters. It then uses a probabilistic algorithm on input (k) to product a random element 'f' depends on n, domain $X_{A,B}$ andv_f.

2. Maintaining trusted nodes

A node 'N' should be registered in TTP before providing service.

1. Node 'N' sends its data to TTP.
2. After authentication, TTP choose
   a_N€$Z_{A,B}$ And finds w_N=v, where
   v=f (v,a_N) =v^{aN}mod n
   Then TTP sends (w_N, a_N) to node 'N' in a secure way. a_N is AIK of
   Node 'N'.
3. Similarly, TTP finds out other nodes witness $\{w_{NI}\}$ and sends it to node 'N' securely. If a node doesn't work properly TTP deletes N's AIK. [4]

3. Remote attestation Mechanism

To secure VM establishment,

1. Virtual machine is launched on nodes.
2. Agree with the session key in the attest protocol. [7]

For instance, suppose that the user is authenticated with the cloud manager (CM). It implies the Node 'N' has (w_N, a_N) and the user has 'V'. Node 'N' should then prove that its AIK a_N is accumulated in to v. Zero knowledge protocol is not easy to use in our scheme. So, Diffie-Hellman key agreement added to our scheme for the process of attestation.[4]

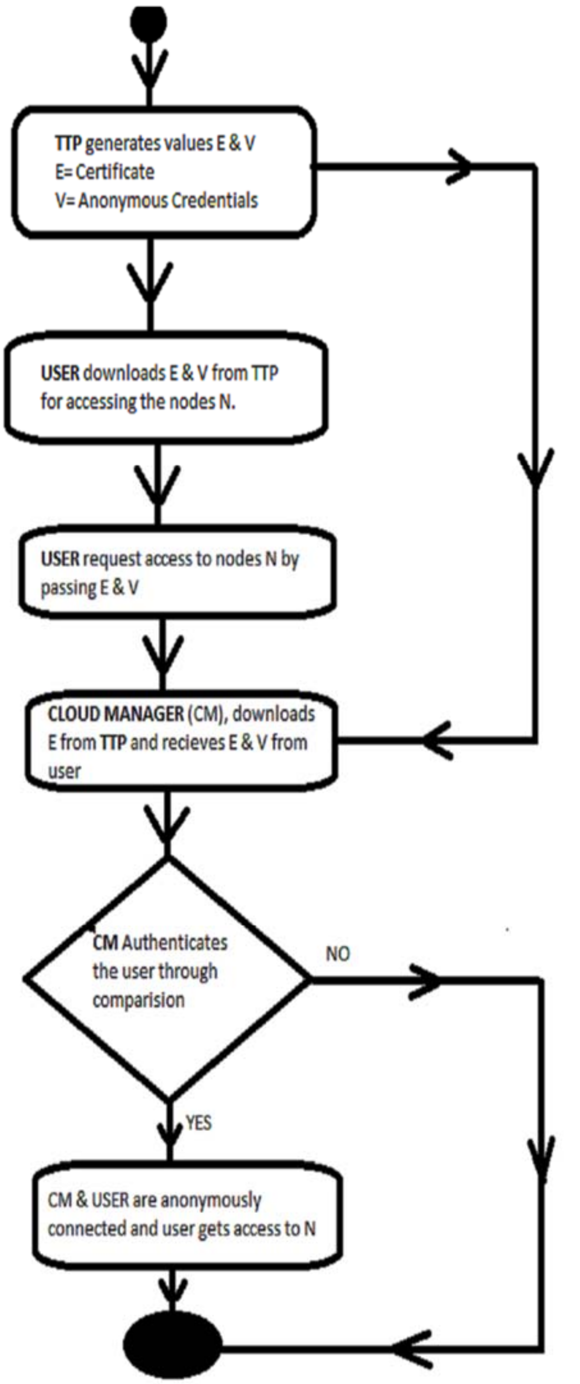
TTP generates values E & V
E= Certificate
V= Anonymous Credentials
USER downloads E & V from TTP for accessing the nodes N.
USER request access to nodes N by passing E & V
CLOUD MANAGER (CM), downloads E from TTP and recieves E & V from user
CM Authenticates the user through comparision
NO
YES
CM & USER are anonymously connected and user gets access to N

Fig 4 : Flow Chart

4. Certificate Generation

X.509 certificate is generated by CA (Certificate Authority) in order to provide a certified relation between the client and the user. The user downloads the certificate along with the accumulated values from TTP (Trusted third party). [8]The user needs this certificate to get verified by cloud manager. The cloud manager can keep track on all the users by using this certificate. Because there might be many users of cloud who are accessing the data when they are not supposed to access it. Due to anonymity in nature of the users it becomes very important for the cloud managers to have something like X.509 certificate for keeping a track. This certificate needs to be revoked on daily basis by the CA. So that the cloud manager can identify the changes in the certificate. By doing this the cloud manager can catch the users who are using the same old certificate. [5]

Algorithm: [9]

Step 1: openssl req -x509 -days 365 –newkey rsa:2048 -keyout my-key.pem -out my-cert.pem

Step 2: Enter PEM pass phrase: " "

Step3: Enter details:
Country Name (2 letter code) [AU]: ' '
State or Province Name (full name) [Some-State]: ' '
Locality Name (eg, city) []: ' '
Organization Name (eg, company) [Internet Widgits Pty Ltd]: ' '
Organizational Unit Name (eg, section) []: ' '
Common Name (e.g. server FQDN or YOUR name) []: ' '

Step 4: Private key openssl pkcs 12 –export –in my-cert.pem-inkey.pem –out moin-test-cert.pfx

Step 5: Openssl pkcs12 –in moin-test-cert.pfx -clcerts -nokeys-out moin-test-cert-public.pem

6. Conclusion

In this paper, we define the use of certificate generation in the remote attestation scheme. This certificate is generated by the Trusted Third Party (TTP). The certificate will be shared to users and cloud manager (CM).CM compares both the certificates and allows authorised users to access the trusted nodes (N).The attestation protocol also uses Deffie-hellman key agreement mechanism. The zero knowledge proof and the completeness proof make this protocol complete. This scheme also reduces the storage cost and reduces the burden of management for TTP and users.

References in the text of the paper should be indicated with ascending numbers in superscript form. For example: J. A. Author, et al.[1] demonstrated that…it was shown in multiple studies[2-6] that…based on earlier studies[2,4], the most effective instructional techniques for first-year students were… See example of authors listed in the 'References' section shown below.

References

[1] Xiao-Yong, L., et al. *A trusted computing environment model in cloud architecture*. in *Machine Learning and Cybernetics (ICMLC), 2010 International Conference on*. 2010.

[2] Fan, Y., et al. *Establishment of Security Levels in Trusted Cloud Computing Platforms*. in *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*. 2013.

[3] Sen, P., P. Saha, and S. Khatua. *A distributed approach towards trusted cloud computing platform*. in *Applications and Innovations in Mobile Computing (AIMoC), 2015*. 2015.

[4] Yong, Z., L. Xiangxue, and Q. Haifeng. *An anonymous remote attestation for trusted cloud computing*. in *Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on*. 2012.

[5] Stallings, W., *NETWORK SECURITY ESSENTIALS:APPLICATIONS AND STANDARDS*. 2011. p. 432.

[6] Kai, H. and L. Deyi, *Trusted Cloud Computing with Secure Resources and Data Coloring.* Internet Computing, IEEE, 2010. **14**(5): p. 14-22.

[7] Zhidong, S. and T. Qiang. *The security of cloud computing system enabled by trusted computing technology*. in *Signal Processing Systems (ICSPS), 2010 2nd International Conference on*. 2010.

[8] Jan Camenisch, A.L., *Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials.* 2002.

[9] Mousliki, s. *How to generate key and cert using openSSL*. 2012