Middle-East Journal of Scientific Research
24 (Special Issue on Innovations in Information, Embedded and Communication Systems): 132-137, 2016
ISSN 1990-9233; © IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.IIECS.23151

Certificate Revocation List Validation Mechanisms in Public Key Infrastructure Using Map-Reduce Technique

T. Sujitha and T. Hemalatha

Department of Computer Science and Engineering,
PSNA college of Engineering and Technology, Dindigul - 624619, India

Abstract: Public Key Infrastructure (PKI) is a system required to provide public-key encryption and digital signature in all internet enabled applications. It helps to manage keys and certificates. Cloud computing is a distributed environment which is gaining a great attention in provisioning of computer resources and managing the security issues related to the data usage in cloud. For maintaining security between the cloud provider and the cloud consumer, the verification of certificate in PKI is essential. It can be done by two ways: (1) Online Certificate Status Protocol (OCSP) updates the status of revocation list frequently in online. But the main disadvantage is that it requires always online to safety check with the server thereby the server may get overloaded during peak hours and it is not an effective technique to mitigate against HTTPS server private key. (2) Certificate Revocation List (CRL) is generated and published periodically by the Certificate Authority (CA). It prevents spoofing or denial-of-services attack. Hence most of the internet applications prefer CRL to check the status of the certificate in offline. Since CRL is huge in size it consumes more processing power and time when an enormous user accesses the CRL issuer in PKI. Hence, an alternate mechanism is proposed in this work to overcome the drawbacks in existing CRL validation mechanism, by obtaining the status of PKI Certificate by using Map-Reduce technique in CRL Mechanism, It is suitable for cloud since cloud is a derivative of Distributed computing. Map-Reduce Algorithm improves the throughput and speed-up processing over traditional method. The objective of this proposed system is to efficiently minimize the time and resource utilization during certificate validation in distributed computing environment.

Key words: Public Key Infrastructure · Certificate Revocation List · Revoked Certificate · Online Certificate Status Protocol · Certificate Authority

INTRODUCTION

Public Key Infrastructure (PKI) is an authentication approach that facilitates security services in an internet application with the intent to securely exchange data over networks. Any client side application that runs in internet or cloud requires three main security services viz. authentication, digital signature and encryption. Some of the popular PKI applications are web application, network applications, S/MIME secure email, electronic document processing and etc. It helps in management of keys and certificates and also to maintain a trustworthy environment. The purpose of a PKI is to provide secure, convenient and efficient acquisition of public key.

The certificate validation mechanism is to check the revoked certificates and to deny the unauthorized access. The scalability of PKI could be significantly limited by the certificate revocation mechanism. The validation mechanism works well and it is more suitable for latest high performance computing infrastructure such as distributed, parallel, grid and cloud computing. From the analysis of existing mechanism, it has been reported that the cost and time taken for certificate validation in PKI has been increased tremendously. The time and resource utilization during the process can be reduced to great extent by applying Map – Reduce technique in certificate validation mechanism. The objective of this system is to deploy a service-specific middleware to perform the data-intensive and computation intensive task in PKI.

Corresponding Author: T. Sujitha, Department of Computer Science and Engineering,
PSNA college of Engineering and Technology, Dindigul - 624619, India.

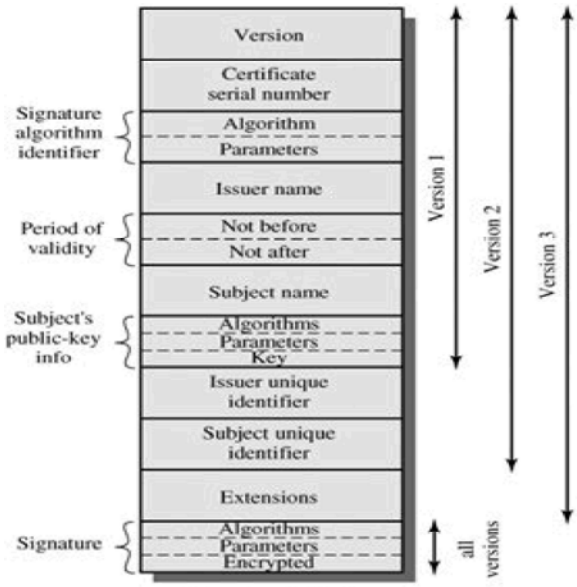

Fig. 1: Structure of Certificate in PKI [1]

The Fig. 1 is the structure of certificate for three different versions of certificate standards. The version 1 is considered as the default, the version 2 is used in most case and the version 3 has the extensions. It contains the certificate serial number, Public – Key info, signature algorithm and period of validity.

Related Works:

A.Components of Public Key Infrastructure

- Certificate Authority (CA) acts as root of trust and issuer of the corresponding certificate and CRL. It supports wide variety of administrative functions. Normally, a CA checks with a Registration Authority (RA) to verify the details provided by the requestor of a digital certificate. If the Registration Authority verifies the requestor information, then the CA can issue a certificate [2].
- Registration Authority (RA) often called as a Subordinate. It is a trusted system that runs services to verify the validity of certificates that has been issued by a root CA. It issues certificates to particularly identified and authenticated individuals permitted by the CA. The services provided by RA can be either physically separate or combined with a CA.
- CRL Issuer is an interface between the CA and Certificate Repository. It collects the CRL from the corresponding CA which is a trusted party in PKI, after a formal registration.
- Certificate Repository is a database of PKI, saves certificate requests of issued and revoked certificates from the RA or CA. The commonly used repository service for certificate storage is a Lightweight Directory Access Protocol (LDAP) server. The CA will store certificates to the repository and the clients retrieve the certificates from the repository using an LDAP based user application access.
- Certificate Store saves issued certificates. It also accounts the pending or revoked certificate requests from the local computer.
- Key Archival Server saves encrypted private keys in a certificate database in case of any failure for recovery purposes i.e., Certificate Database is lost [2].

Certificate Validation Mechanism: The Certificate Validation in PKI is processed in two ways such as CRL and Online Certificate Status Protocol (OCSP). In certificate validation, when any certificate is issued, it has a validity period that is defined by the CA. Usually the validity period is one or two years. If the certificate has past that period or expired, then the authentication should fail. The brief description about the two validation approaches are discussed in detail.

Certificate Revocation List: The Certificate Revocation List (CRL) is a list which holds the serial numbers for certificates that had been revoked for various reasons. It is that the entities of the certificates present in the CRL should not be trusted. The CRL is issued by the trusted CA and it is stored in certificate repository via CRL issuer. The CRL issuer generates and publishes the certificate in defined intervals.

For example, if the private key associated with a certificate is lost, then any authentication using that certificate should be denied. This is done by adding the serial number of a particular certificate to the CRL. Similarly, the certificate of a user or organization is included in the CRL for various reasons. When their certificates are replaced, the expired certificates have to be marked as “untrustworthy” [2].

The Fig. 2 is the structure of CRL which has the signature algorithm, issuer name of the particular certificate and the revoked certificates. The ‘This update’ is a date on which the list is created. The ‘next update’ is a date on which the new CRL will be issued and this CRL is treated as “INVALID”.

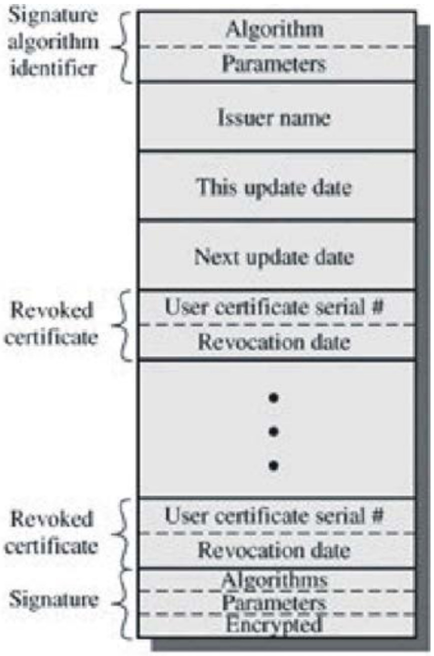

Fig. 2: Structure of CRL [1]

a)Advantages:

- In CRL, certificates are validated in offline.
- It prevents spoofing or denial-of-services attack.

b)Disadvantages:

- CRL's are not updated frequently i.e., at defined interval of time.
- The CRL list grows to unmanageable sizes

c)Use of CRL File:

- During the validation process, the browser will choose a way to check for revocation; if a CRL is preferred, it will download the CRL file from an URL specified by the certificate and does further verification.
- If a CA indicates that a server's particular certificate was revoked, the user will be stopped from accessing the unauthorised sites.

Online Certificate Status Protocol: Online Certificate Status Protocol (OCSP) allows a PKI-enabled application to contact an OCSP server (also called an *OCSP responder*) to check for revocation status in real time. The response is signed back to prevent tampering. OCSP has the primary benefit of requiring minimum network bandwidth, enabling near real-time status checks for high - volume operations [3].

a)Advantages:

- In OCSP, the certificates are validated in online.
- It solves the size problem in the CRL approach
- The certificates are verified without consuming more memory and computation resource.
- OCSP is networks friendly compared to CRL.

b)Disadvantages:

- It requires always online to connect with the server thereby the server may get overloaded during peak hours.
- The OCSP Responder creates bottleneck when the requests are processed in queue.
- There is possibility of single point failure in OSCP responder.

Analysis of Existing System

Size of CRL File: Each CRL file has its own size depending upon number of revoked certificates in it. From the report given by the WebSeeker [3], it is shown that the maximum file size in megabytes and the minimum file size are in few bytes.

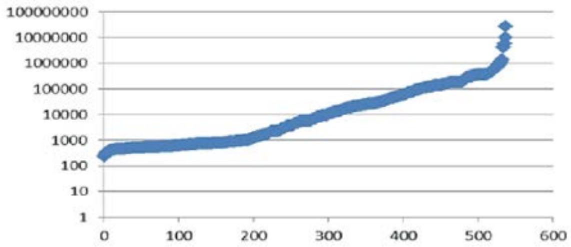

Fig. 3: Growth in CRL File size [3]

The above Fig. 3 shows that among the considered 600 CRL files, only 200 files are below 1000 bytes, which clearly indicates that most CRL file is large in size [3].

Reason for Certificate Revocation:

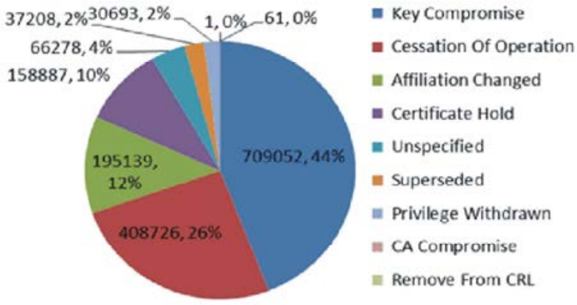

Fig. 4: Reasons for Certificate Revocations [3]

From Fig. 4, it clearly shows that the reason for the majority of certificates (44%) is revoked due to the fact of “key compromise” which is considered as quite serious problem in this method.

Key Compromise: When a user’s private key is lost or stolen for any other illegal purpose has to be compromised

Cessation of Operation: When the certificate subject no longer need the certificate further.

Affiliation Changed: When the certificate subject does not belong the specified organization or changes to other organization.

Certificate Hold: When the certificate subject temporarily wants to revoke the current certificate.

Unspecified: When the certificate subject has no reason for the certificate to be revoked then it is unspecified.

Superseded: When a new certificate is replacing the existing certificate.

CA Compromise: When a CA’s private key is stolen for some illegal access then the certificate of CA itself has to be compromised

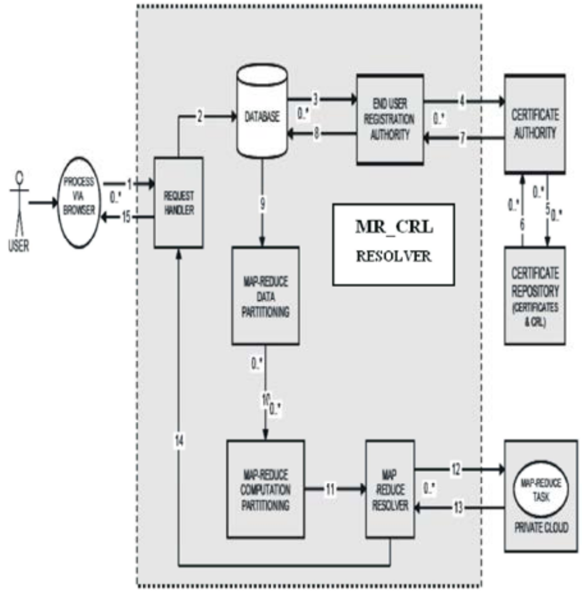

Fig. 5: Architecture for MR_CRL Validation Mechanism in PKI

Design Overview - CRL Validation Mechanism: The objective of the proposed model is to design a service–specific middleware to perform the complicated task of certificate validation mechanism. As shown Fig. 5, the server invokes this system model upon receiving the request from the client.

Description of MR_CRL Resolver: The MR_CRL Resolver is a service specific middleware that is specifically designed to perform the computation – intensive and data – intensive task of CRL Validation in PKI.

Methodology Description: The proposed logic is divided into two stages as follows:

- Authenticated request is made for certificate validation check (Serial Number and Issuer Name).
- Check the validity of the CRL using the fields “This update” and “Next update” in the database.

Stage 1: The principals involved in this stage are a trusted Third Party Certificate Authority and End User Registration Authority (EURA) in the MR_CRL Resolver. In this stage, every CA must undergo an authorized registration with EURA and then update the recent CRL in the Database.

- The End User Registration Authority verifies whether the Certificate Authority has been registered or not.
- If the Certificate Authority has registered with MR_CRL then check for the recent CRL.
- The Certificate Authority fetches the recent CRL from the Certificate Repository present in its CA (issuer) administrative boundary.
- The Certificate Authority pushes the recent CRL from the Certificate Repository.
- The Certificate Authority has to register. Hence the registration process is carried out in End User Registration Authority.
- The End User Registration Authority updates the CRL list in the database.

Stage 2: The End User interaction with MR_CRL Resolver. In this stage, when the user request for CRL validation, the process will be initiated by fetching the recent CRL from the Database and process the CRL using the Map – Reduce technique to obtain the status of the requested certificate in PKI.

- The Map – Reduce Library get the CRL from the database updated by the Certificate Authority.
- The obtained data set is passed through Map-Reduce Library for Data Partitioning then the partitioned data is sent for Computation Partitioning.
- Copies of the data set are then passed into Map-Reduce Resolver i.e., select a master node and worker nodes.
- After the identification of master and worker node; the tasks are assigned to the each node.
- Map-Reduce task is performed and the result is sent back to the Map-Reduce Resolver.
- The certificate validation result is passed to the user/browser via Request Handler.
- Thus the user retrieves the result for its CRL validation check in PKI so that it may be served further or denied to provide its service in case it its PKI Certificate is revoked.

Experimental Results

Experimental Setup: The experimental setup is carried out using the Apache Hadoop to run a CRL validation program using the Map – Reduce programming model in two different installation modes. Hadoop supports two different types of modes. They are Pseudo distributed mode and fully distributed mode. In the Pseudo distributed mode the entire cluster is configured in a single system. This mode setup mimics the distributed environment, such that all the processes run on system's JVM. In the Fully distributed mode, the installation of all the required packages is done in several systems, where each system is designated for a specific purpose. For this experimentation, Hadoop Cluster is setup with five nodes where one Name node and five Data nodes are configured in which the Name node acts as a Data Node. As shown in Fig. 6, the Name node acts as a Master to control and monitor the worker nodes, in which master is configured to act both as master and worker.

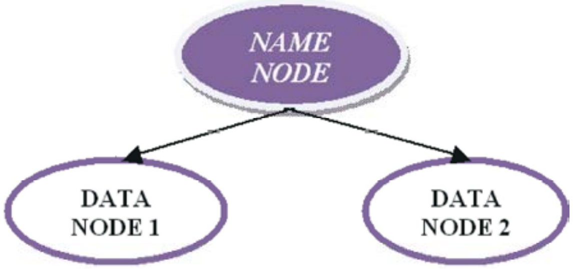

Fig. 6: Experimental Setup in Fully distributed mode

Name Node: A name node acts as a master node which keep track of each blocks in a cluster and its locations. It is also known as "Task Tracker".

Data Node: A data node holds the metadata of the data files. It is also known as "Job Trackers". In data nodes, each block are replicated across each multiple machine.

Implementation Details: For implementing the above mentioned experimental setup, we have considered 5 systems with Ethernet LAN and switch based OFC connectivity. The experiment was performed on the systems with I3 processor of speed 2.53GHZ and RAM of 4GB. The software used for this experimental setup to create a loosely coupled cluster configuration is setup with Hadoop 2.7.0 along with JVM 1.8 and Hbase which is the adaptable version that has taken for Hadoop and JVM installation.

Experimental Results: The bouncy castle and IAIK JCE security API is used to implement CRL validation mechanisms. The local CA is established using OpenSSL and CRLs are generated using this package in X.509. IAIK JCE packages are used for this experimentation. The clients are simulated from the campus area network covering maximum 3 to 4 LANs that lies in the same network and then the CRL is exported for further experimentation. The experimental results are shown in Fig. 7 which depicts that by using Map-reduce technique for CRL Validation Mechanism, the time and resource utilization had minimized for verification of certificates in PKI.

- Parameters that are considered for analysis of the proposed design
  - Size of the CRL
  - Number of Users
  - Response Time
- Analysis and demonstration of execution time with Map – Reduce technique and without Map – Reduce technique for considered samples.
- Number of Worker nodes can be increased and decreased and Estimation is done accordingly for the above mentioned attributes.

The experimentation is done by using various CRLs of varying sizes and users are increased at periodical interval of time. Then the response time is calculated whenever the result of a certificate validation is done. The results are plotted in the graph which is shown in Fig. 7. From the results, it is evident that in any kind of DCE, the Map-Reduce programming can efficiently parallelize the task by cooperatively utilizing the loosely coupled distributed resources and thereby reduces the computational overhead and improve the performance by reducing the response time. The Response time can still be reduced to multifold if it is done in a very vast DCE having several hundred nodes.

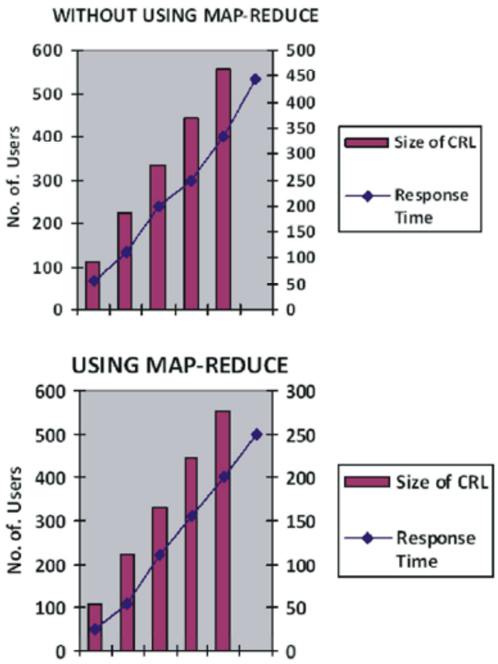

Fig. 7: Performance Analysis for CRL Validation Mechanism using Map-Reduce and without Map-Reduce

CONCLUSION

Across world, the public and private sectors, governments and industries are deploying large-scale, Public Key Infrastructure with the intent of improving security and increasing efficiency. The overall PKI performance has significant impact on certificate validation mechanisms. Since the CRL validation mechanism is a resource consuming and time consuming, Map-Reduce technique is used in validation process. Thereby, Map-Reduce algorithm improves the throughput and speed-up processing, to efficiently minimize the time and resource utilization during certificate verification in PKI.

REFERENCES

1. Horise, 2013. Certificate Revocation List [online]. Available from: <http://community.websense.com/blogs/securitylabs/archive/2013/07/11/digging-into-certificate-revocation-lists.aspx>.
2. Saphana, 2014. Hadoop Overview [online]. Available from: <http://saphanatutorial.com/how-yarn-overcomes-mapreduce-limitations-in-hadoop-2-0/>.
3. Gibson Research Corporation. Security Certificate Revocation Awareness. Available from: <https://www.grc.com/revocation/ocsp-must-staple.htm>.