A Multifactor Credential Translation and Verification Service for Computational Grid

Dr. T. Hemalatha¹, Dr. S. Pushpalatha²

¹Department of CSE, PSNA College of Engineering and Technology, Dindigul, India.
Correspondence Email-hemalathapsnr@gmail.com

²Department of CSE, PSNA College of Engineering and Technology, Dindigul, India.

Abstract

The authentication mechanism in Grid need to support local heterogeneity and need to support n-way security context. The objective of this work is focused on the interoperable issue in the existing Grid Security Infrastructure. An adaptable Multi factor Authentication framework for computational grid is proposed in this work and it is compared with existing Credential Federation Systems. The proposed system is designed using the concept of Service Oriented Architecture SOA a specific type of Distributed System in which the agents are software service which are designated to perform the complicated time and resource consuming task of Credential management and Credential Validation service. GSI does not support Kerberos based authentication. Hence in order to integrate Kerberos with GSI, a Credential Translation Service CTS is designed and implemented. This feature is incorporated in this design by developing a service that can handle Kerberos token and PKI Certificate. The performance of the proposed system is compared with existing credential federation systems.

Keywords: Grid Security, Credentials, Identity, authentication, Virtual Organization VO, Public Key Infrastructure, Certificate Revocation List.

1. Introduction

Grid is a distributed computing technology that provides consistent and pervasive access to higher end computational resources. Grid system is a mechanism to pool resources on-demand to improve the overall utilization of the system. There are different types of grid. They are data grid, computational grid, service grid, knowledge grid, information grid etc. The computational grid is a hardware and software infrastructure that provides dependable, consistent, pervasive and inexpensive access to high end computational capabilities [1]. It is used for sharing of expensive huge computational resources. The grid infrastructure consists of...
grid nodes and communication network. Several individuals and institutions are forming Virtual Organizations (VO) to pool resources [2]. There are several challenges in forming and managing virtual organizations, in which the existing grid security solutions forms the major barrier to the adoption of grid technology by the major community. There are several problems associated with the existing approaches for Grid security are excessive complexity, poor scalability, high deployment and maintenance overheads [3]. The existing solutions are heavy weight since the specific problems associated with the grid security context includes Complexity, extensive dependencies, scalability and usability. The existing solutions are complex and it’s very difficult to configure even for experienced professionals. The security of grid depends on the security of its middleware components which has several dependencies and many other factors. The existing grid security solutions suffer from scalability issues [4][5]. If it is not scalable, it will not be suitable for large organizations. Each and every node which joins the virtual organizations has to be properly configured by the manager and improper configured node will be left unnoticed. Some security solutions have the problem of usability.

The security requirements in grid need to support three factors viz. Scalable, Dynamic and Distributed VO. Grid encompasses several resources of different organization to form VO. Resources that are shared from different organization has its own requirement for authentication. Each domain is configured with different local security solutions, mechanisms and policies viz. simple user name and password, one time password, SSL and Kerberos [5]. Any solution must confront this heterogeneity. The authentication mechanism in Grid should support local heterogeneity and need to support n-way security context.

1.1. Key Functions in Grid Security Model:
Grid accesses resources in different organizations in a coordinated manner. Grid management is very important since it is heterogeneous in nature that consists of multiple entities, components, domains, policies and stake holders. The management related issues are Credential Management, and Trust management. The Credential Management is focused in this work since the potential of adopting this technology largely depends on the security. This forms the major barrier for adoption of Grid computing.

There are three main types of credentials. They are identity credentials, authentication credentials and authorization credentials. The first type of credential is used to identify a particular user. It is used to prove one’s identity. It’s a long term credential and generic in nature. The second type of credential is system specific with policies bonded to each. It is a short term credential. In computing system there are many multiple systems which require only authentication credential. The third type of credential is used to authorize users for accessing certain resources with certain restrictions. In this paper, the authentication credential is considered for further discussion.

The characteristics of credential management system includes Initiation (to
obtain initial credentials), secure and safe storage, access and renewal of credentials, translation, delegation and control of the credentials. Our goal is to improve the existing mechanisms in Initiation, translation and renewal of credentials by grouping users, resources and service providers into federations. Based on these characteristics the credential management system is divided into credential repository and credential federation systems. The credential repository system deals with securely storing new credentials, creating new credentials or proxy credentials on demand. Credential federation system is responsible for sharing of credentials across different realms or administrative domain. An Administrative Domain AD is a collection of resources controlled by a single physical authority belonging to a particular organization [11].

Each and every organization that participates in grid has established its own security mechanism and infrastructure. The policy for forming a Virtual Organization VO in grid must interoperate with those existing mechanisms instead of replacing such with a different one. The request to access the resources may span multiple security domains. The security challenges in grid comprises of Authentication, Confidentiality and Integrity. Due to the inherent nature of heterogeneity in grid several other unique security challenges need to be considered. They are different Authentication mechanism, credential management, authorization and policy integration. The functional requirement for authentication in Grid is Single Sign on. When an entity is delegating a task to another entity, authenticating the client to the entity is to be performed in a transparent manner and it need to support n-way security contexts. In computational grid, different types of job with varying complexity are submitted by the user. If a job may take a longer time than the life span of the delegated credential, then the status about the expiration of credential is notified to the end user or refreshes the credential until the job is completed.

In this paper we have used the Globus toolkit GT4 for further experimentation. The security for grid in Globus is achieved through Grid Security Infrastructure GSI [6]. In GSI three types of authentication is available. They are Username/password, Public Key Infrastructure PKI and Kerberos - a third party authentication mechanism (with slight modifications). The password based mechanism has got its own drawbacks which can be overcome by using shared secret challenge. In such mechanism shared secret should be changed periodically and man-in-the-middle attack is possible. The alternate to this is PKI. The PKI uses the digital certificates for authentication. Though PKI is very secure and tamperproof it suffers from scalability issues. Many of the individuals do not possess valid certificate on their own. The Certificate Authority CA is responsible for certifying the user who subscribes to CA. Users can obtain certificates from the delegated CA not from the single CA. This delegation model shown in figure 1 is used in Globus implementation. The digital certificates are issued by the Certificate Authority in Public Key Infrastructure. It allows the trusted
authority to sign information to be used for authentication purpose. Whenever a user submits the certificate it is validated by verifying the Certificate Revocation List (CRL). The CRL verification is a time and resource consuming task since they are cognitively difficult objects which requires additional overhead in certificate validation [7]. Online Certificate Status Protocol (RFC 2345) can check the status of the certificate in on-line [14]. The third party authentication service Kerberos is not directly supported by GSI. It is not possible to use Kerberos based Authentication mechanism in GT4. Integration of Kerberos with GSI can be done by implementation of Credential Conversion Service. But delegation is not possible with Kerberos and GSI domain.

![Delegated Certificate Authority Model](image)

**2. Related Work**
The credential management systems are divided into two main type’s viz. Generic and Specific. The generic credential management systems are deployed in the internet to serve different users and applications in order to cater the needs of security services. There are some specific types like Virtualized Credential Manager and KX.509 which are designed for grid. Virtualized Credential Manager is designed for Community Authorization Service CAS that has been developed as a part of the Globus toolkit [15][16]. The CAS is responsible for managing and governing the access policies for resources in VO [17]. It will take care of authorizing the user’s operation at resource level on behalf of the Grid Community. KX.509 is a protocol to acquire a temporary X.509 certificate on behalf of a user by submitting a Kerberos Ticket by the user [16]. Shibboleth is a federated Identity management system that exchanges information about their users The credentials are provided and stored at the place where it originates. It is integrated with globus toolkit named GridShib [20]. MyProxy toolkit is an online credential repository that is used to store and retrieve user credentials in X.509 certificates. The
functionalities of MyProxy credential manager are generation of short lived certificates, delegation, access control and Secure storage. A cryptographic co-processor is needed for this mechanism. Even though it is stronger it is vulnerable to dictionary attacks [19]. The above mechanisms are designed for X.509 certificates.

3. Proposed System - Multifactor Authentication Service Architecture

The architecture of the proposed system design is given in figure 2 and the notations used in the proposed system are given in table 1. The proposed system is designed for a specific challenge in a distributed system assumes a system model in which it can work effectively to provide its service for which it is designed for. Likewise in this proposed system an assumption of a Grid System Model is given in Figure 3.

![Architecture of the Proposed System Design – MAS](image)

![Grid System Model of the Proposed System](image)

The different variants of grid require a security infrastructure to secure its resources and to provide the grid services in a secured manner. Initially the different Grid Service Providers registers with the Regulating Authority RA of MAS by sharing its authentication policies and

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTS</td>
<td>Credential Translation Service</td>
</tr>
<tr>
<td>CVS</td>
<td>Credential Validation Service</td>
</tr>
<tr>
<td>TCA</td>
<td>Trusted Certificate Authority</td>
</tr>
<tr>
<td>Kerberos AS</td>
<td>Kerberos Authentication Service</td>
</tr>
<tr>
<td>MAS</td>
<td>Multifactor Authentication Service</td>
</tr>
<tr>
<td>VO</td>
<td>Virtual Organization</td>
</tr>
<tr>
<td>PBA</td>
<td>Password Based Authentication</td>
</tr>
<tr>
<td>KER</td>
<td>Kerberos</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>RA</td>
<td>Regulating Authority</td>
</tr>
<tr>
<td>AD</td>
<td>Administrative Domain</td>
</tr>
<tr>
<td>MAC_Address</td>
<td>Address of the Medium Access</td>
</tr>
</tbody>
</table>
Job submission Interface. On successful registration the Grid relies on the Multifactor Authentication Service (MAS) for its credential management. Every Administrative Domain relies on MAS for authentication mechanisms like obtaining the Initial credentials, Credential Validation, Translation and renewal. The registration process comprises of sequence of steps involved between the VO and the regulating authority is indicated in the figure no.2 labeled as a–e is given below.

a. A Virtual Organization VO / Administrative Domain AD registers with RA (Initially). During Job submission the RA handshakes with VO.

b. Interfaces with the VO Regulating Authority

c. On success of step a, the RA updates the VO’s authentication policies as a separate instance in XML Schema

d. The credential submitted by any VO is validated by Credential Validation Service

e. On success the keys are stored in key store

The keys are stored in encrypted form in a hash table using hash function. In order to prevent any kind of attack the salt is generated from the end user’s MAC address. concatenated with the secret key.

\[ \text{Salt} = f(MAC \ || \ CR) \]

\[ f \rightarrow \text{function} \]

\[ \text{Hash_value} = \text{hash}(	ext{Salt} \ || \ \text{IDvo}) \]

\[ \text{hash} \rightarrow \text{one way hash function} \]

\[ \text{Key} = \text{DKR}_{\text{MAS}}[\text{HT}(	ext{Hash_value})] \]

\[ \text{HT} \rightarrow \text{Hash Table} \]

In this proposed work the computational grid is setup using globus toolkit. When a user submits a job using user friendly portal, the following sequences of steps are involved between the user and the MAS. The User interaction with the grid portal for the process of job submission is shown in figure no. 2 labeled as 1–8 is given below.

1. The User interacts with the Grid portal and perform registration for getting the service

2. Client submits his/her details \{FName, LName, Affiliation, Address, Mail_ID\}. Registration is done by storing all the details in a XML data store. On success the user will receive a mail containing the user name and password and a confirmation link to proceed further. When the registration is confirmed, the portal enters in to the next phase of job submission in which the user has to submit the source code and the supporting files which includes Input files, any other package / header / libraries in the form of archive.

3. The Registration Module invokes the Credential Translation Service CTS.

4. The CTS submit the request to acquire a PKI Certificate and/or Kerberos Ticket based on the VO Policy on behalf of the client.

5. On success of step 4, the credential is stored in the RA – Key store

6. Request is forwarded to the Job Handler \{Job,Cred_List\}
a. Job → {Source Code, Input Data}
b. Cred_List → {Cred1/Cred_List}; Cred1 – Single Credential; Cred_List – More than one Credential

7. Job Handler collects the Job from the End_user Registration Module repository and hand over through the Job submission interface to the compute grid.

8. On successful execution the proposed model returns the result back to the client in synchronous or asynchronous fashion based on the Service Level Agreement SLA.

3.1 Credential Translation Service
Every registered user is assigned with a unique user-id and this user id is used for storing and fetching the details in XML data store. The role of CTS is to perform a part of credential management system that includes Initiation (to obtain initial credentials), renewal of credentials, and translation. When a registered user submits a job without submitting any credential except the user name and password allotted at the time of initial registration with RA, the CTS obtains the credentials from the configured certificate authority and Kerberos AS on behalf of the client. In turn the CA and KAS perform validation, and return the credential based on the job type. If the job type is complex it issues a long time credential else short time credential is issued with period of validity. The credentials are stored in the key store as given below

Salt = f(MAC||UN||Enc[PWD])
f → function

Hash value= hash(salt||unique ID)

hash → hash function

Key = DK_{R,MAS}[HT(Hash_value)]

HT → Hash table

3.2 Credential Validation Service
Grid is a Federated environment composed of resources and users from a particular geographical location. Based on geographical area and administrative control we have different types of grid with different usage policies. Each AD is configured with its own PKI Infrastructure for securing the grid. To overcome the inherent drawbacks in the existing system, the web services are developed to provide the Certificate Validation Service CVS to cater the needs of authentication mechanism in PKI. Web Service is based on simple request response based client server model that relies on web service protocol stack. A client can be any application, service or any device that needs to validate X.509 certificate. Each CVS is associated with a Certificate Authority within its Administrative Boundary. In this proposed model the client i.e. any grid node in the grid can identify the location of CVS by two ways

1. Any grid node participating in the grid is configured with a table consists of Issuer’s distinguished name/ID and corresponding URL of the CVS.

2. The UDDI registry in WSA holds the URL and WSDL contract of the web service.

CVS uses the CRL mechanism of validation. Agents are configured with PKI and CVS in every AD. The agent model is deployed in every grid to form a secure VO. If the MAS
is willing to validate the certificate issued by different authority corresponding to a different grid in case cross VO is formed, the corresponding URL is returned back to the client. The service is invoked by passing the certificate serial number and the corresponding Issuing Authority. The CVS updates the latest CRL from the corresponding CA in administrative domain and current revocation status of certificate is returned by the corresponding CVS. Any grid node (client) sends a request message to the designated CVS in its Administrative boundary which is carried over HTTPS. In order to avoid replay attack a Nonce is generated and sent along the request message. The request message consists of hashed Certificate Serial number and Issuer ID. Since this method of certificate validation can overcome the performance issue of scalability in the existing mechanism the requirements of the proposed system which are identified are given below.

Requirements of Credential Validation Service CVS
1. The proposed system is expected to provide real time certificate status by checking the X.509 Certificate CRL of the corresponding CA via HTTP or LDAP.
2. The CVS should satisfy the three features viz. discoverable, fault tolerant and low latency.
3. Since there are multiple CA’s in grid environment the Chaining of CVSs is needed.

Sequence of interactions are involved between the CVS and MAS are given below

**Interaction 1a:** Once the user registers successfully, the PKI certificate is submitted if it is possessed by the user in order to authenticate the access to the resources in the grid else the CTS is invoked to acquire a new certificate. In addition the registration module in MAS generates NONCE Nc (Number used ONCE) to avoid replay attack. The certificate holds the following information CertificateSerialNumber CSN and Issuer Name IN. The MAS and CVS uses RSA algorithm for providing secrecy to the messages

\[ \text{Cert}_C = \text{EK}_{OTP}(\text{Certificate}_C \parallel \text{N}_C) \]

**Interaction 1b:** In the previous interaction if the user submits a Kerberos Service Granting Ticket, the SGT is forwarded to the Kerberos AS to verify if it is valid or not. If it is valid the CVS invokes CTS to contact the Official CA to acquire a new PKI certificate. A short lived certificate is issued to CTS. From this point onwards it will proceed as mentioned below.

**Interaction 2:** It involves between the grid resource and CVS. The grid master node decrypts the message \( \text{Cert}_C \) using \( \text{OTP}_C \) and validates the certificate by passing the signed encrypted message containing CertificateSerialNumber, Issuer Name and NONCE (Number used ONCE) to the CVS. The secret key algorithm AES is used to provide secrecy to the communication.

\[ \text{Certificate}_C = \text{DK}_{OTP}(\text{Cert}_C) \]

\[ \text{GMN} \rightarrow \text{CVS} \]

\[ M_1 = \text{EK}(\text{EK}_{R \_GMN}(\text{CertificateSerialNumber} \parallel \text{IssuerName} \parallel \text{N}_G \_M \parallel h(\text{CSN}, \text{IN}, \text{N}_G \_M))) \]

**Interaction 3:** The message \( M_1 \) is processed by CVS and extracts the Certificate Serial Number CSN and Issuer Name IN. It checks if the issuer name IN is the official authority for the current CVS. If yes it checks the
table that holds the CSN and the status. If there is no entry in the table, it checks the validity of CRL. If it is valid it accesses the TBSCertList array to verify the status of the certificate by checking the certificate serial number. On completion it returns the status as any one of the valid response as \{“GOOD”, “REVOKED”, “UNKNOWN”\}. In concurrence, it creates an entry in the table and stores the CSN and Status.

**Interaction 4**: The CVS returns the response message $M_2$ to the caller. $M_2$ consists of the status of the Certificate,Nonce generated by the Grid Master Node - $N_{GMN}$, and Nonce generated by the CVS - $N_{CVS}$. $M_2$ is stored until the client/grid user completes the Job. Once the job is completed it deletes the entry from its own location.

$$\text{CVS} \rightarrow \text{GMN}$$

$$M_2 = \text{EK}_{R\_CVS}(\text{Status} \; || \; N_{GMN} \; || \; N_{CVS},$$

$$h(\text{Status} \; || \; N_{CVS} \; || \; N_{GMN}))$$

**Job Handler**

The job handler interfaces with the grid middleware GT4 to integrate the proposed system with the Grid to enhance the Credential Management in Grid security layer. The proposed credential validation service can act like business logic to detach the overhead involved in managing the credential in existing grid middleware. The grid has been integrated with the Portable Batch System (PBS). The job is submitted to the globus gatekeeper using the command globus-job-submit. The globus-job-submit forward the job request to the gatekeeper which in turn returns the job-ID. The job-ID is used by the user to fetch the status of the job.

4. **Implementation**

The proposed system is implemented in Java and the modules CTS and CVS are implemented as web services. The design considerations of the web services are Synchronous messaging, reliability and security. The functionality is analyzed and tested with different setup. A loosely coupled DCE (Distributed Computing Environment) is setup using our own implementation in which Kerberos AS is configured to provide Authentication. Then a grid is setup with globus toolkit and the proposed scheme is executed and compared with the existing SSL based authentication used in Globus toolkit. Since the amount of time and resources needed for CRL validation mechanism is high, it is detached from the Client Machine or the CA authority server. The CVS is implemented as a Web service; it can be deployed in a separate machine. This machine is referred as CRL Responder. The CRL Responder validates the recent CRL and returns the status of the certificate in a secured manner.

4.1 **Performance analysis of the Proposed Mechanism**

A simple grid setup was created with 10 workstations with two different configurations. The grid hosting environment is created with globus. The web services are implemented using Java API and CRL Validation Service using Bouncy Castle Security API. The Web service implementation is deployed and tested on the following system configuration of Processor type with speed 2.13 GHz, 4 GB RAM size and a 32 bit OS with network connectivity. The time taken for execution of CVS and CTS is estimated for the following test cases a) With Single CVS,
CTS and Single CA and Kerberos AS b) With Single CTS, Multiple CVS and Multiple CA and single Kerberos AS. Initially the user registers and authenticates to the MAS portal in an AD with a single CA by requesting/submitting his PKI Credential. The credential is verified by the CVS. The user’s details are stored as an XML instance in XML Repository. The CVS is invoked by passing the CertificateSerialNumber CSN and Issuer Name IN. The server and client uses RSA algorithm for providing secrecy to the messages. CVS validates the request by verifying the latest CRL and returns the status. If a client doesn’t possess a PKI certificate, the certificate request is generated by the RA to the respective CA which is associated to a Grid. On getting access to the grid the job is submitted to the grid through Job Handler. The time required for Credential acquisition and translation is estimated and compared with the SSL authentication is shown in Fig. 4.

4.2 Security Analysis of the MAS
The performance analysis of the proposed mechanism is presented in the previous section. In this section, the CVS is analyzed with respect to different attacks which it can withstand are given below

**Man-in-the-middle attack**
An attacker H who tries to perform a man-in-the-middle attack in the interactions 3, & 4 needs to apply brute force attack. The attacker has to break the cipher by trying all possible keys from the key size of $2^{1024}$. It is infeasible and practically proven that breaking the cipher with key size of 1024 bits is impractical and not of much use.

Replay Attack

In all the interactions the Nonce is used in order to prevent the replay attacks. Initially the One Time Password OTP is generated based on the Physical Address (MAC) of the client machine and the time at which the request is received. Since the nonce is concatenated and hash is computed for the message containing nonce value, the replay attack is detectable and further the service will not be offered.

![User Vs Total time taken for Authentication using PKI](image)

**Fig.4. User Vs Total time taken for Authentication using PKI**

**Modification Attack**
In all the interactions from 2 to 4 one way hash function is applied and the computed hash value is encrypted along with the entire message. Even if the attacker tries to break the cipher by trying chosen plain text attack or known plain text - cipher text attack, since the nonce value is generated randomly and appended with the message it is infeasible to succeed in the above mentioned attack.

**Brute force attack**
This type of attack is a cipher text only attack. Trying out all possible key is
infeasible for larger key sizes. The symmetric encryption AES can be used as an alternate algorithm to provide secrecy between the interactions which are made between CVSs in different Administrative Domains.

4.3 Comparison between existing federated credential federation system

In the Multifactor Authentication Service, the support for Kerberos Authentication mechanism in the grid is introduced by proposing a Framework for federation of VO.s. This framework acts like a regulating authority so that the service providers can register and publish their security policies. The Grid users can consume the services provided by the grid infrastructure without having any complexity in authenticating itself to various VO and its resources in a transparent manner through this proposed system.

| Table 2. Comparison between existing federated credential federation system and proposed system |
|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|
| Feature                                         | MyProxy                                         | VCMAN                                          | KX.509                                          | MAS                                             |
| Type of Service                                 | Repository                                      | Federation Mechanism                           | Federation Protocol                             | Federation Service                              |
| Identity                                        | X.509                                           | X.509                                         | X.509 and Kerberos                             | Multiple                                        |
| Credential Type                                | Keys                                             | Keys and Tokens                               | Tickets and Tokens                             | Token, Keys and UN & Password                   |
| Security                                        | Secure                                           | Secure                                       | Secure                                          | Secure                                          |
| Vulnerability                                  | Vulnerable to Dictionary Attacks                 | Requires the support of CAS. CAS is vulnerable to Denial of Service and Masquerading. | Replay attack may be possible while using long lived X.509 credential. | Completely Secured and Obfuscated by using OTP/Random number and Web Service Security. |
| Others                                          | Pull based Model                                 | Push based Model                              | Pull based Model                               | Pull based Model                                |

5. Conclusion and Future work

Every grid is managed by a regulating authority with its own official certificate authority. The proposed mechanism has provided an enhanced Credential Management service named Multi factor Authentication Service to support the grid infrastructure for credential initiation, translation and verification. It is tested with two different grid setup and overall time taken and resource consumed for the operation is estimated. It provides the Credential Management Service with an optimal Quality of Service QoS. The proposed mechanism provides a hierarchical Certificate Validation System synonymous to DNS. The result of this mechanism is found to be promising for such distributed computing environment and there by the problem of scalability with respect to credential handling and validation.
mechanisms can be overcome. Thereby an autonomic dynamic secure configuration service can be setup to configure a secure environment in a flexible manner.

**Declarations section**

**Availability of supporting data**
I Don’t have any Supporting data

**Competing interests**
I Don’t have any Competing Interest

**Funding**
No

**Authors' contributions**

**Dr. T. Hemalatha - Research Guide**. She is a Contributions of the Full Work. Her interests are in Network Security, Grid & Cloud Computing, Machine Learning, Distributed System and Adhoc & Computer Networks. She is a life member of ISTE and CSI.

**Dr. S. Pushpalatha – Co author**. Her research interests include Mobile Adhoc Networks, Wireless Sensor Networking, Security and Big Data Analytics. She has been a part of committee member of various national and international conferences. She is a life member of ISTE and a member of IEEE.

**Acknowledgements**

**First Author:**

**Dr. T. Hemalatha** received Bachelors degree in Computer Science & Engineering from Thiagarajar College of Engineering in 1994 and Masters Degree in Computer Science & Engineering from College of Engineering - Guindy, Anna University in 2004. She completed her Doctoral degree under Anna University in the domain of Security in Grid and Cloud computing technologies. Currently, she is a Professor at PSNA College of Engineering and Technology, Dindigul, Tamilnadu, India. Her interests are in Network Security, Grid & Cloud Computing, Machine Learning, Distributed System and Adhoc & Computer Networks. She is a life member of ISTE and CSI.

**Second Author**

**Dr. S. Pushpalatha** received her Ph.D. degree from Anna University, Chennai in the year 2016. She is currently a Professor in Computer Science and Engineering Department, PSNA College of Engineering and Technology, Dindigul, Tamilnadu, India. She is having 23 years of teaching experience and 3 years of Industrial Experience. Her research interests include Mobile Adhoc Networks, Wireless Sensor Networking, Security and Big Data Analytics. She has been a part of committee member of various national and international conferences. She is a life member of ISTE and a member of IEEE.

**References**


22. http://grid.ncsa.illinois.edu/myproxy/about/

23. www.w3.org/TR/ws-arch

24. www.w3.org/TR/2000/NOTE-SOAP-20000508
25. [www.w3.org/TR/2001/NOTE-wsdl-20010315](http://www.w3.org/TR/2001/NOTE-wsdl-20010315)