ISSN:0975-9646

A Resilient Two - Server Authentication Mechanism for Enhancing Security in Grid Environment

K.AnithaKumari[1], G.SudhaSadasivam[2]

[1] *Department of Information Technology,*
[2] *Department of Computer Science and Engineering,*
PSG College of Technology, Coimbatore, India.

***Abstract*— Most of the familiar protocols use single server for storing all the needed information to authenticate a user. Maintenance of security is of primary importance in any computing environment. Safe and effective authentication mechanism and evaluation methods of the entity are of utmost importance for the grid users to facilitate legitimate utilization of resources. It improves the legal user's credit rating and shields the system from illegal users. However the efficiency of the grid systems still requires improvement as exchanging certificates and verifying validity are compulsory. These systems are also infested by masquerade attacks. In this paper, we propose a resilient Authentication Architecture for Security, where authentication is based on strengthening parameters like variance and product. When a single server is compromised, a large number of user passwords, will be exposed. Our proposed approach uses an authentication protocol in order to improve the security in grid environment. The protocol utilizes fundamental concepts of triangle. Based on the parameters of the triangle the user authentication will be performed. In the proposed protocol, the password is interpreted and alienated into more than two units and these units are stored in two different servers. The privilege of accessing the requested resources is obtained by the user only when the combined authentication scheme from both the servers authenticates the user. The main advantage of utilizing the authentication protocol in computing is that an adversary user cannot attain the access privilege by compromising a single consolidated server because of the fact that split password is stored in two different servers. For flexibility and reusability this authentication mechanism is hosted as service in grid environment.**

Keywords-Two – Server Authentication, grid security, Attacks.

I. INTRODUCTION

Improved network bandwidth, powerful computers, and the acceptance of the Internet have motivated the constant necessity for latest and improved ways to compute [1]. The developing complexity of computations, superior processing power of the personal computers and the continually rising speed of the Internet have laid down the path for grid computing [2]. "Grid and cloud" computing has developed as a significant new field, distinguished from conventional distributed computing by its concentration on large-scale sharing of resources, high-performance orientation and in innovative applications [3]. Grid computing is concentrating on large-scale sharing of resources and collaboration over virtual organizations boundaries and enterprises [4]. As the goal of grid computing is to only provide secure grid service resources to legitimate users, the security issue becomes an important concern of grid computing [5].

The requirement for secure communication between entities on the Grid has determined the development of the Grid Security Infrastructure (GSI). GSI provides authentication, protection, integrity, confidentiality and for sensitive information transferred over the network in addition to the facilities to securely traverse the different organizations that are part of collaboration [6]. Secure invocation of Grid services brings out the necessity for a security model that reveals the security components that are required to be defined and accepted based on the Grid security requirements [8]. Security requirements within the Grid environment are stimulated by the requirement to support dynamic, scalable, distributed virtual organizations (VOs) [3]—collections of various and distributed individuals that are looking to share and use different resources in a synchronized fashion [7].

A general outline within Grid computing involves the formation of dynamic "virtual organizations" (VOs) [3] including groups of individuals as well as associated resources and services combined by a general purpose but not located inside a single administrative domain [9]. The concept of Virtual Organization (VO) [3] has been launched to define the relationships between a set of grid components comprising data, applications, computing resources and users [10]. For the successful operation of VO participants must have control over resource sharing policies via a secure infrastructure [11]. To avoid the illegal users from accessing the grid resources, it ought to be guaranteed that strong mutual authentication is necessary for users and server [5]. Users require to know if they are interacting with the "right" piece of software or human, and that their messages will not be altered or stolen as they traverse the virtual organization (if the users have such a requirement). Users will frequently need the ability to prevent others from reading data that they have stored in the virtual organization [12].

Grid systems and applications require standard security services comprising of integrity, privacy, authentication, access control [13]. Security plays a most major role in providing the integrity of data and resources, the confidentiality of the communication and the privacy of the user information for large scale deployment of Grid [14]. The sensitive information and resources in information systems are defended from illegitimate access by means of

the access control that is universally employed as a security mechanism [15].

At the base of any grid environment, there must be mechanisms to provide security including authentication, data encryption, authorization and so on [33]. Authentication is the foundation of security in grid [34]. Basically, authentication between two entities on remote grid nodes means that each party sets up a level of trust in the identity of the other party. In practical use, secure communication channel between the authenticated parties is set up by an authentication protocol, so that successive messages can be sent devoid of repeated authentication steps, even though it is possible to authenticate every message. The identity of an entity is typically some name or token that exclusively identifies the entity [16].Grid technologies use X.509 identity certificates to support user authentication. An X.509 Certificate with its corresponding private key forms a unique and exclusive credential, termed as grid credential, within the Grid and cloud. Grid credentials are utilized to authenticate both users and services [17]. In order to get the authentication from the server, users and services are required to provide credentials. A credential is a piece of information that is utilized to prove the identity of a subject. Security is frequently dependent on the strength of the protections guarding a user's credentials. The management of these credentials and secure storage is the user's responsibility. User mobility, usability and insufficient protection of workstations can cause major problems that often decline the security of user credentials [17]. Certificates passwords are some of the instances of credentials. Password-based authentication is still the most widely used authentication mechanism, mainly due to the ease with which it can be understood by end users and implemented [19].

Password authentication is considered as one of the most convenient and simplest authentication mechanisms [22]. On the other hand, password authentication protocols are prone to replay, password guessing and stolen-verifier attacks [20].Clearly untraceable on-line password guessing attacks and off-line password guessing attacks are the most convincing considerations in designing a password-based authentication scheme [22]. A great part of protocols for password-based authenticated key exchange system are designated for a single server environment where all the information about legitimate users is stored in one server. For that reason, a credential weakness is existed in this approach due to the fact that the user's password is revealed if this server is ever compromised. A solution includes splitting the password between two or more servers which provides strong reason; a credential weakness is existed in this approach due to the fact that the user's password is revealed if this server is ever compromised. A solution includes splitting the password between two or more servers which provides strong reason; a credential weakness is existed in this approach due to the fact that the user's password is revealed if this server is ever compromised. A solution includes splitting the password between two or more servers which provides strong security proofs for authentication protocol [23]. The dual-server model that includes two servers at the server side, one of which is a public server exposing itself to users and the other of which is a back-end server staying behind the scene; users contact only the public server, but the two servers work jointly to authenticate users [24].

This paper proposes a novel dual authentication protocol which utilizes dual servers for authentication to improve the grid security. The novelty of the protocol is the usage of the fundamental concepts and basic elements of the triangle to authenticate. With these triangle parameters, the user credential is interpreted and then stored in two servers which provide substantial security evidences for authentication protocol. The dual authentication protocol gives authentication to the grid user if and only if both the servers are jointly involved in the authentication mechanism. It is not possible to obtain the password by hacking a single server. Moreover, our protocol offers effective security against the attacks like replay attack, guessing attack and stolen-verifier attack as the user authentication is a combined mechanism of two servers. Also, it provides the security to the valid users as well as securing the user credentials, as an additional feature. Succinctly, the protocol provides secured environment while the grid user entered into the VO and the services access from the grid.

The rest of this paper is organized as follows. In section II, we discuss the related works in detail**.** In section III & IV, we introduce our proposed authentication scheme and algorithm. It also highlights the advantages of our approach over the results of performance and security analysis. In section V & VI design and security analysis were discussed and in section VII results were discussed. Finally, the conclusion and future directions are presented.

II. RELATED WORK

Wei Jiea et al. [25] have proposed a scalable GIS architecture for information management in a large scale Grid Virtual Organization (VO). The architecture was comprised of the VO layer, site layer and resource layer: at the resource layer, information agents and pluggable information sensors were deployed on every resource monitored. The information agent and sensor approach provided a flexible framework that facilitated particular information to be captured; at the site layer, a site information service component with caching capability aggregates and maintained up-to-date information of all the resources monitored inside an administrative domain; at the VO layer, a peer-to-peer approach was utilized to construct a virtual network of site information services for information discovery and query in a large scale Grid VO. In addition to that, they proposed a security framework for the GIS, which provided security policies for authentication and authorization control of the GIS at both the site and the VO layers. Their GIS has been implemented based on the Globus Toolkit 4 as Web services compliant to Web Services Resource Framework (WSRF) specifications. The experimental results showed that the GIS presented satisfactory scalability in maintaining information for large scale Grid and cloud. Haibo Chena et al. [26] have presented

the work of Daonity which was their effort to strengthening grid security. They identified that a security service which they named behavior conformity be desirable for grid computing. Behavior conformity for grid computing was an assurance that ad hoc related principals (users, platforms or instruments) forming a grid VO should each act in conformity with the rules for the VO constitution. They applied trusted computing technologies in order to attain two levels of virtualization: resource virtualization and platform virtualization. The former was about behavior conformity in a grid VO and the latter, that in an operating system. With those two levels of virtualization working together it was possible to construct a grid of truly unbounded scale by VO together with servers from commercial organizations.

Yuri Demchenko [27] has provided insight into one of the key concepts of Open Grid Services Architecture (OGSA) and Virtual Organizations (VO). They have analyzed problems related to Identity management in VOs and their possible solution on the basis of utilizing WS-Federation and related WS-Security standards. The paper provided basic information about OGSA, OGSA Security Architecture and analyses VO security services. A detailed description was provided for WS-Federation Federated Identity Model and operation of basic services for instance Security Token Service or Identity Provider, Attribute and Pseudonym services for typical usage scenarios. G. Laccetti and G. Schmid [28] have introduced a sort of unified approach, an overall architectural framework for access control to grid resources, and one that adhered as much as possible to security principles. Grid security implementations were viewed in the light of the model, their main drawbacks were described, and they showed how their proposal was able to prevent them. They believed that a main strategy could be to adopt both PKI (Public Key Infrastructure) and PMI (Privilege Management Infrastructure) infrastructures at the grid layer, ensured that a sufficient transfer of authentication and authorization made between the Virtual Organization and Resource Provider layers. That can be attained by expanding those features at the OS layer as system applications and services.

Xukai Zoua et al. [29] have proposed an elegant Dual-Level Key Management (DLKM) mechanism by means of an innovative concept/construction of Access Control Polynomial (ACP) and one-way functions. The first level provided a flexible and secure group communication technology whereas the second level offered hierarchical access control. Complexity analysis and Simulation demonstrated the efficiency and effectiveness of the proposed DLKM in the computational grid as well as the data grid and cloud. An example was demonstrated.

Li Hongweia et al. [30] have proposed an identity-based authentication protocol for grid on the basis of the identity-based architecture for grid (IBAG) and corresponding encryption and signature schemes. Commonly, grid authentication frameworks were attained by means of applying the standard SSL authentication protocol (SAP). The authentication process was very complex, and therefore, the grid user was in a heavily loaded point both in computation and in communication. Being certificate-free, the authentication protocol aligned well with the demands of grid computing. By means of simulation testing, it was seen that the authentication protocol was more lightweight and effective than SAP, in particular the more lightweight user side. That contributed to the better grid scalability.

Yan Zhenga et al [31] have aimed at designing a secure and effective method for grid authentication by means of employing identity-based cryptography (IBC). Nevertheless, the most extensively accepted and applied grid authentication was on the basis of the public key infrastructure (PKI) and X.509 certificates, which made the system, have lesser processing efficiency and poor anti-attack capability. An identity-based signature (IBS) scheme was first proposed for the generation of private key during grid authentication. On the basis of the proposed IBS and the IBE schemes, the structure of a grid authentication model was given, followed by a grid authentication protocol explained in detail. According to the theoretical analysis of the model and the protocol, it could be discussed that the system has enhanced both the security and efficiency of the grid authentication when compared with the traditional PKI-based and some IBC-based models.

Hai-yan Wanga. C and Ru-chuan Wanga [32] have proposed a grid authentication mechanism, which was on the basis of combined public key (CPK) employing elliptic curve cryptography (ECC). Property analysis of the mechanism in comparison to the globus security infrastructure (GSI) authentications showed that CPK-based grid authentication might be applied as an optimized approach towards efficient and effective grid authentication.

Trigon authentication performs one iteration of authentication whereas in polygon performs three iterations which is more secure than trigon. The strengthening parameter generated in trigon is 1 and in polygon its 3, and hence polygon authentication is more efficient and secure.Our proposed work on a novel dual authentication protocol utilizes dual servers for authentication to enhance the grid security. The novelty of the protocol is the usage of the fundamental concepts and basic elements of the triangle to authenticate.

III. PROPOSED USER REGISTRATION PROCESS FOR TRIANGLE BASED DUAL AUTHENTICATION

Grid systems are large-scale, dynamic, distributed and heterogeneous systems. These characteristics lead to more security challenges. In grid environment, job execution needs to invoke resources in different domains where the authentication plays a crucial role of authenticating a user. From the security perspective, the grid environment is actually composed up of a number of security domains which deploy different security mechanisms. In order to conduct secure cross-domain collaboration in grid, as well as to fight against attacks in cloud we should fully consider the problems of authentication. In this paper, we propose a novel Triangle based Authentication Architecture for Security in grid environments. To achieve the dual authentication, it

necessitates the user to register with the Authentication server. The procedures followed in the Authentication server and the Backend server during registration of the user is as follows.

The users have to register with the Authentication server, so that it can hold a part of the interpreted password with itself and another part in the Backend server. The users who require services from the VO have to register initially with the Authentication server using their username and password. The Authentication server calculates the P_i, P_i' as given in (1). Along with this, the Authentication server also generates two large prime numbers, namely, a and a', which are considered as the two sides of a first triangle and b and b', which are considered as the two sides of a second triangle. It is difficult to hack the values of a, a,' b and b' as they are large prime numbers (as per RSA Factoring Challenge). Here, P_i is taken as the angle between a and a' and P_i' is taken as the angle between b and b'. Now, the Authentication server can easily determine the opposite side of the angle P_i, termed as a' ' and P_i', termed as b' '. With these triangle parameters, the user determines α, Vaa', and $P_{aa'}$ as follows

$$Vaa' = a - a' \quad (1)$$

$$Vaa'' = a - b' \quad (2)$$

$$Vaa''' = b - c' \quad (3)$$

$$Paa' = a * a' \quad (4)$$

$$Paa'' = a * b' \quad (5)$$

$$Paa''' = b * c' \quad (6)$$

$$\alpha = 2\,Paa' - a'' \quad (7)$$

$$\alpha' = 2\,Paa'' - b'' \quad (8)$$

$$\alpha'' = 2\,Paa''' - c'' \quad (9)$$

α is the strengthening parameter used as the index to represent user credentials.

Vaa' and Paa' are the variance and the product of the sides a and a' respectively. Vaa" and Paa" are the variance and the product of the sides b and b' respectively. Vaa"' and Paa"' are the variance and the product of the sides c and c' respectively. With the parameters a, a', a'', b, b', c and c' as the sides of triangle Pi be the angle between the sides a and a' are generated and triangle will be assumed as in the figure1

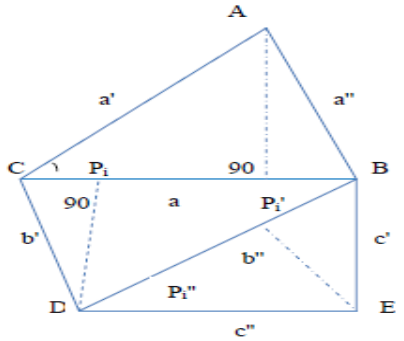

Fig. 1. A sample triangle generated using the parameters a, a', a'', b, b', c and c' and P_i

After the calculation of α, $V_{aa'}$, $V_{aa''}$, $V_{aa'''}$, $P_{aa'}$, $P_{aa''}$ and $P_{aa'''}$. The authentication server stores the α, α' and α" value and its corresponding username in a database and forwards $V_{aa'}$, $V_{aa''}$, $V_{aa'''}$, $P_{aa'}$, $P_{aa''}$ and $P_{aa'''}$ to the Backend server along with the username. The Backend server maintains the $V_{aa'}$, $V_{aa''}$, $V_{aa'''}$, $P_{aa'}$, $P_{aa''}$ and $P_{aa'''}$ for the corresponding username in a database. Hence, the password is interpreted and alienated into two units and stored in two separate servers, thereby achieving the concept of dual authentication. The process is repeated for all the users who wish to register in the server, so that both the servers can maintain all the users' account. When any of the users try to access the VO, they will be validated by these servers using the account information and then allowed to access the VO by providing T_{VO}. If the user is an adversary and if it tries to use wrong password or username, the server can validate effectively, asserts the user as invalid and sends a warning to the adversary. The dual authentication code proposed here is designed based on the fundamentals of triangle and the design steps are discussed in the section below.

IV. THE PROPOSED TRIANGLE-BASED DUAL AUTHENTICATION PROTOCOL

Taking the security as the main constraint in grid computing environment. We are proposing a dual authentication protocol, which will authenticate the user by a combined mechanism of two servers, namely, authentication server and backend server and then allows the user to access the VO for services. Here, the public server is mentioned as the authentication server as it performs the major authentication mechanism. The authentication procedure we have developed is on the basis of the fundamental concepts of a triangle.

Initially, the user who wants the services of VO has to login to the Authentication server using the username and password. Here, u_i and pw_i refers to username and password of i^{th} user. The Authentication server calculates the Password index (Pi, $P^{'i)}$ from the password as

$$P_i = \begin{cases} \frac{P_{AI}}{10^{n-2}}; if\ P_{AI}(j) \geq 180 \\ \frac{P_{AI}}{10^{n-2}};\ else \end{cases} \quad (10)$$

$$P'_i = \begin{cases} \frac{P'_{AI}}{10^{n-2}}; if\ P'_{AI}(j) \geq 180 \\ \frac{P'_{AI}}{10^{n-2}};\ else \end{cases} \quad (11)$$

$$P''_i = \begin{cases} \frac{P''_{AI}}{10^{n-2}}; if\ P''_{AI}(j) \geq 180 \\ \frac{P''_{AI}}{10^{n-2}};\ else \end{cases} \quad (12)$$

In (10), (11) and (12) P_{AI}, P'_{AI} and P''_{AI} is the ASCII-interpreted value of the given password pw_i, n is the total number of digits in P_{AI}, P'_{AI} and P''_{AI}.

$P_{AI}(j)$, $P'_{AI}(j)$ and $P''_{AI}(j)$ represents the first j digits of P_{AI}, P'_{AI} and P''_{AI}. P_{AI}, P'_{AI} and P''_{AI} can be calculated by the following steps.

- Change the pw_i into its corresponding ASCII value.
- Calculate the three-fourth of total digits of the ASCII value modulo 180, which results the first three digits of P_{AI},P'_{AI} and P''_{AI}.
- Append the remaining one-fourth of the ASCII digits to P_{AI},P'_{AI} and P''_{AI}.

Then, from $P_{i,}$ P'_i and P''_i the authentication server determines the authentication index (A_I) for u_i is

$$A_I^{(i)} = \frac{P_i}{2} \quad (13)$$

$$A'^{(i)}_I = \frac{P'_i}{2} \quad (14)$$

$$A''^{(i)}_I = \frac{P''_i}{2} \quad (15)$$

Then the Authentication Server searches for the username index $\alpha_{i,}$ $\alpha'_{i,}$ α''_i for the corresponding u_i which has already been stored in the server database during the process of the registration. Subsequently, α_i is sent to the backend server along with $u_{i.}$ When the backend server receives the index $\alpha_{i,}$ $\alpha'_{i,}$ α''_i and the username from the Authentication server, it searches for $V_{aa'}$, $V_{aa''}$, $V_{aa'''}$, $P_{aa'}$, $P_{aa''}$ and $P_{aa'''}$ the variance and the product of the sides a' ,a'', b, b', c and c' respectively, which have been saved in the backend server database during the process of registration. From these values, the Backend server calculates an Authentication Token A_{Ti} , A'_{Ti} , A''_{Ti} and sends it to Authentication server to authenticate the $u_{i.}$ The A_{Ti} , A'_{Ti} , A''_{Ti} and sends it to the Authentication server to authenticate the $u_{i.}$ The A_{Ti} , A'_{Ti} , A''_{Ti} can be calculated as

$$A_{Ti} = \frac{\alpha_i + V'^2_{aai}}{2P'_{aai}} \quad (16)$$

$$A'_{Ti} = \frac{\alpha'_i + V'^2_{aai}}{2P''_{aai}} \quad (17)$$

$$A''_{Ti} = \frac{\alpha''_i + V''^2_{aai}}{2P'''_{aai}} \quad (18)$$

In (16), (17) and (18), $V_{aa'}$, $V_{aa''}$, $V_{aa'''}$, $P_{aa'}$, $P_{aa''}$ and $P_{aa'''}$ during individual user registration from the Backend server, the Authentication server authenticates the user based on the token from the Backend server and the index calculated at the Authentication server. The authentication code (or) condition which authenticates the u_i is given by (proved in section III.B)

$$SinA_I^{(i)} = \left(\frac{1-A_{Ti}}{2}\right)^{1/2} \quad (19)$$

$$SinA'^{(i)}_I = \left(\frac{1-A'_{Ti}}{2}\right)^{1/2} \quad (20)$$

$$SinA''^{(i)}_I = \left(\frac{1-A''_{Ti}}{2}\right)^{1/2} \quad (21)$$

The authentication process is performed by the authentication condition given in (19), (20) and (21).When the condition is satisfied, the user is decided to be valid and the server sends a token for VO access T_{VO} to the user. Using the Token T_{VO} the user can contact the VO and accomplish its tasks and access the resources in the VO. If the condition is not satisfied, then word of warning is given to the user. As a consequence, the user has no T_{vo} to contact the VO and hence no resource sharing. Thus, the proposed dual authentication protocol based on two servers effectively validates the user and allows the user for resource sharing in the grid environment.

V. DESIGN OF ALGORITHM

To mitigate the limitation of authentication techniques as explained in section I, we present a triangle based authentication scheme.

A. Goals and Strategy

1. To provide a secure authentication mechanism for grid environments.
2. To reduce computation time taken by authentication algorithm
3. To protect systems against attacks

The authentication code provided in (19), (20) and (21) takes the eventual decision of whether the user who logins is valid or adversary. The steps by which the authentication code is developed are described elaborately as follows.

The semi-perimeter S_P of the triangle depicted above is determined as

$$S_P = \frac{a+a'+a''}{2} \quad (22)$$

$$S'_P = \frac{a+a''+a'''}{2} \quad (23)$$

$$S''_P = \frac{a+a'+a'''}{2} \quad (24)$$

But it is known that,

$$Sin^2(A_I) = \left(\frac{(S_P-a)-(S_P-a')}{a.a'}\right)^2 \quad (25)$$

$$Sin^2(A'_I) = \left(\frac{(S'_P-a')-(S'_P-a'')}{a'.a''}\right)^2 \quad (26)$$

$$Sin^2(A''_I) = \left(\frac{(S''_P-a'')-(S''_P-a''')}{a''.a'''}\right)^2 \quad (27)$$

Square of the RHS value of (25), (26) and (27) takes the form

$$\frac{(S_P-a)-(S_P-a')}{a.a'} = \frac{\left[\left(\frac{a+a'+a''}{2}\right)-a\right]\left[\left(\frac{a+a'+a''}{2}\right)-a'\right]}{a.a'} \quad (28)$$

$$\frac{(S'_P-a')-(S'_P-a'')}{a'.a''} = \frac{\left[\left(\frac{a+a''+a'''}{2}\right)-a'\right]\left[\left(\frac{a+a''+a'''}{2}\right)-a''\right]}{a.a''} \quad (29)$$

$$\frac{(S''_P-a'')-(S''_P-a''')}{a''.a'''} = \frac{\left[\left(\frac{a+a'+a'''}{2}\right)-a'\right]\left[\left(\frac{a+a'+a'''}{2}\right)-a'''\right]}{a.a'''} \quad (30)$$

Applying (25), (26) and (27) in (28), (29) and (30) can be reorganized as follows

$$Sin^2(A_I) = \frac{2aa'}{4aa'} - \left(\frac{a^2+a'^2-a''^2}{4aa''}\right) \quad (31)$$

$$Sin^2(A'_I) = \frac{2a'a''}{4a'a''} - \left(\frac{a'^2+a''^2-a'''^2}{4a'a'''}\right) \quad (32)$$

$$Sin^2(A''_I) = \frac{2a''a'''}{4a''a'''} - \left(\frac{a''^2+a'''^2-a''''^2}{4a'a'''}\right) \quad (33)$$

As given in (7), (8) and (9),

$$2aa' = a''^2 + \alpha \quad (34)$$

$$2aa'' = a'''^2 + \alpha' \quad (35)$$

$$2aa''' = a''''^2 + \alpha'' \quad (36)$$

Using (28), (29) and (30) in (25), (26) and (27) can be written as

$$Sin^2(A_I) = \frac{1}{2} - \left(\frac{a^2+a'^2-2aa'+\alpha'}{4aa'}\right) \quad (37)$$

$$Sin^2(A'_I) = \frac{1}{2} - \left(\frac{a'^2+a''^2-2aa+\alpha''}{4aa''}\right) \quad (38)$$

$$Sin^2(A''_I) = \frac{1}{2} - \left(\frac{a''^2+a'''^2-2aa+\alpha'''}{4aa'''}\right) \quad (39)$$

$$Sin^2(A_I) = \frac{1}{2} - \left(\frac{(a-a')^2+\alpha'}{4aa'}\right) \quad (40)$$

$$Sin^2(A'_I) = \frac{1}{2} - \left(\frac{(a'-a'')^2+\alpha''}{4aa''}\right) \quad (41)$$

$$Sin^2(A''_I) = \frac{1}{2} - \left(\frac{(a''-a''')^2+\alpha'''}{4aa'''}\right) \quad (42)$$

Substituting (1), (2), (3),(4),(5) and (6) in (40),(41) and (42) gives

$$Sin^2(A_I) = \frac{1}{2} - \left(\frac{V'^2_{aa}+\alpha}{4P'_{aa}}\right) \quad (43)$$

$$Sin^2(A'_I) = \frac{1}{2} - \left(\frac{V''^2_{aa}+\alpha'}{4P''_{aa}}\right) \quad (44)$$

$$Sin^2(A''_I) = \frac{1}{2} - \left(\frac{V'''^2_{aa}+\alpha''}{4P'''_{aa}}\right) \quad (45)$$

The re-arranged format of the above equation is given

$$Sin^2(A_I) = \frac{1}{2}\left(1 - \left(\frac{V'^2_{aa}+\alpha}{2P'_{aa}}\right)\right) \quad (46)$$

$$Sin^2(A'_I) = \frac{1}{2}\left(1 - \left(\frac{V''^2_{aa}+\alpha'}{2P''_{aa}}\right)\right) \quad (47)$$

$$Sin^2(A''_I) = \frac{1}{2}\left(1 - \left(\frac{V'''^2_{aa}+\alpha''}{2P'''_{aa}}\right)\right) \quad (48)$$

Substituting A_T which is given in (16), (17) and (18) into (46), (47) and (48) we get

$$Sin^2(A_I) = \left(\frac{1-A_T}{2}\right)^{1/2} \quad (49)$$

$$Sin^2(A'_I) = \left(\frac{1-A'_T}{2}\right)^{1/2} \quad (50)$$

$$Sin^2(A''_I) = \left(\frac{1-A''_T}{2}\right)^{1/2} \quad (51)$$

From the above steps, the authentication code utilized for the proposed dual authentication protocol is designed and can also serve as a proof for the effectiveness of the protocol. The protocol devised is based on the triangle parameters and effectively provides an enhanced security, because both the authentication server and the backend server have been involved in the authentication mechanism. So, compromising a single server and enjoying the VO services is impossible by any means.

VI. SECURITY ANALYSIS

Replay attack: Replay attack is called as 'man in the middle' attack. Adversary stays in between the user and the server and hacks the user credentials when the user communicates server. Normally, to overcome this, the user has to frequently change the credential randomly. But it is less probable to do that. Our protocol is strong and robust when the replay attack happens in between the two servers as the credentials are interpreted and alienated into two parts.

Guessing attack: Guessing attack is nothing but the adversaries just communicates the servers by randomly guessed credentials. The effective possibility to overcome this attack is to choose the password by maximum possible characters, so that the probability of guessing the correct password can be reduced. As the proposed uses random generation of prime numbers for the calculation of the sides of the triangle, it is more difficult to guess the password.

Stolen-verifier attack: Instead of storing the original password, the server is normally storing the verifier of the password. If the password steals the verifier from the server, then it will impersonate or masquerade as the legitimate user. But this not happen in any two server protocol, as the password is alienated into two modules. Hence, we can justify that our protocol is also more strong and robust against the attack, as the password is interpreted and then alienated into two modules and stored in the two servers.

VII. RESULTS AND DISCUSSIONS

Experimental show that the structure is more simple and flexible than traditional authentication frameworks and it can improve performance and efficiency of the system. In order to deploy our approach without breaking original security mechanism, we extend this authentication to be hosted as service in grid environments.

The proposed dual authentication protocol has been implemented in the platform of JAVA (version 1.6). The protocol is tested with five valid and five invalid users. Each of the five valid users has their own username and password. Initially, they have created their user account by registering with their username and password, making them valid in the VO. The triangle parameters have been determined during the registration process as stated earlier and they have been stored in the database maintained at the servers.

TABLE 1. USERNAMES, PASSWORDS AND THE TRIANGLE PARAMETERS BASED ON THE USER PASSWORDS PROVIDED AT THE TIME REGISTRATION

S.I.No	Username	Password	α	$V_{aa'}$	$P_{aa'}$	α''	$V_{aa''}$	$P_{aa''}$	α'''	$V_{aa'''}$	$P_{aa'''}$
1	user1	admin	-5.36677781014488 5E10	-428352.0	2.49004791649E11	5.46160208678 1714E10	9732.0	1.04941306333E11	5.77457090688 262E10	-35586.0	1.13191757251E11
2	user2	ascii	3.29395077022154 24E11	153256.0	2.02702126217E11	4.86239954459 7925E11	9526.0	2.79357215927E11	1.63195187911 67047E11	266784.0	1.34625761617E11
3	user3	test5	-4.39329592125250 5E11	-808910.0	1.08793675379E11	2.03520359426 31636E9	80650.0	4.32108 0299E9	-6.04330386799 8784E11	-816310.0	3.13882 18679E10
4	user4	Test10	1.17026960947075 24E12	201240.0	6.26891901289E11	-6.97945257614 0273E11	867396.0	2.81821 97821E10	-1.35871640785 75943E10	-158356.0	5.94883 0541E9
5	user5	Test8	4.25527050123278 93E11	492756.0	3.38179809157E11	-7.37369874258 5206E11	868348.0	8.42918 8349E9	-6.63152576632 7795E11	-823996.0	8.00336 4797E9

The α, α', α'' values for the five valid users mentioned in the Table I have been stored in the authentication server database and $V_{aa'}$, $V_{aa''}$, $V_{aa'''}$, $P_{aa'}$, $P_{aa''}$ and $P_{aa'''}$ have been stored in the database of Backend server for the corresponding usernames. Instead of keeping the actual passwords, the servers maintain the interpreted passwords derived from the triangle parameters. When the servers authenticate any user, the servers determine some authentication elements based on the values which have been stored in the database and the login credential provided by the user. Using such authentication elements, the servers generate an authentication code and validate the user.

The A_I for each user has been calculated by the authentication server and the A_{Ti}, A'_{Ti}, A''_{Ti} for each user has been calculated by the Backend server. Based on these values, the authentication server generated the authentication code and checked whether it has been satisfied or not. When

the authentication code has been satisfied by any of the user, the servers asserted that the user is valid and permits users to utilize the services offered by the VO. The effective performance of the protocol in enhancing the security of the grid environment by identifying valid and adversary users. Each user was provided a separate T_{VO} if and only if the user credential supplied by the concerned user satisfied the authentication code. The user credential that did not satisfy the authentication code was declared as invalid credential and the concerned user was asserted as an adversary. This is because that the authentication code will be satisfied if and only if the user credentials submitted for authentication are properly registered. Hence, the protocol effectively pinpointed the adversary and denied the services for that adversary user.

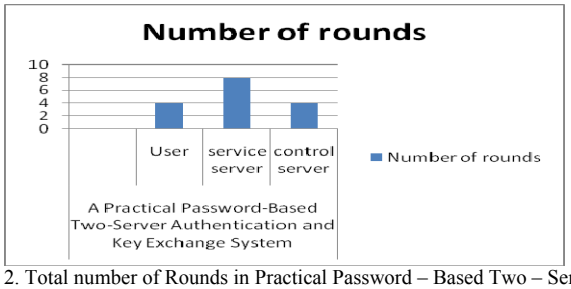

Fig. 2. Total number of Rounds in Practical Password – Based Two – Server Authentication

Figure 2 shows the proposed schemes based on computation rounds between user, Service or Authentication Server and Control or Backend Server.

A. Implementation - Authentication as Service

A service is an entity that provides some capability to its clients by exchanging messages. A service is defined by identifying sequences of specific message exchanges that cause the service to perform some operation. By thus defining these operations only in terms of message exchange, we achieve great flexibility in how services are implemented and where they may be located. A service-oriented architecture is one in which all entities are services, and thus any operation visible to the architecture is the result of message exchange.

Prerequisites are:

build.xml

globus-build-service.sh

1. Creation of auth.wsdl File
2. Create namespace2package. mappings for mapping instances, bindings and services.
3. Write Implementation program.
4. Create deploy-server.wsdd [globus@g20 service]$ vi deploy-server.wsdd
5. Create deploy-jndi-config.xml [globus@g20 service]$ vi deploy-jndi-config.xml
6. Build the service [globus@g20 ~example]$ sh globus-build-service.sh -d org/add/service/ -s schema/add/hello.wsdl
7. After the successful building Grid Archive(GAR) file has been created. Now we have to deploy the GAR file using globus-deploy-gar command. [globus@g20~example]$ globus-deploy-gar org_add_service.gar
8. After successful deployment of the GAR file start the globus container.[globus@g20 ~]$ globus-start-container
9. Write Client Program for authentication.\\
10. Before running the compiler, make sure to run the following:

    source$GLOBUS_LOCATION/etc/globus-devel-env.sh

    The globus-devel-env.sh script takes care of putting all the Globus libraries into your CLASSPATH.

    [globus@gcluster example]$ source /usr/local/globus-4.0.7/etc/globus-devel-env.sh
11. [globus@gcluster example]$ javac org/add/client/Client.java
12. [globus@gcluster example]$ java org/add/client/Client

Fig. 3. Server Side Authentication

Figure 3 shows the authentication papramaters generated in Control Server during the authentication Process.

VIII. CONCLUSION

The irony is that today, secrecy is not the key to the goodness of a cryptographic algorithm.In this paper we present a high secure triangle based authentication algorithm in 2D that can be used in grid environments. Our proposal appears to be significantly more efficient and effective. In future this algorithm can be implemented in 3D to enhance security. The proposed authentication protocol enhanced the grid security as the authentication mechanism utilized two servers for authentication mechanism. The implementation of our dual authentication protocol showed its effective performance in pinpointing the adversaries and paving the way to valid users for access with the VO for the sharing of resources. This paper also proposes a mathematical proof for the protocol. This protocol can be included as a service in grid environments. In globus it is hosted as an authentication service in addition to X.500 protocol and existing policies. The utilization of this protocol will make the grid environments more secure.

REFERENCES

[1] Alexander Kemalov, "A Security Policy in GRID Architecture", International Conference on Computer Systems and Technologies, 2005.

[2] J.Crampton, H.W.Lim, K.G.Paterson and G.Price, "A Certificate-Free Grid Security Infrastructure Supporting Password-Based User Authentication" In Proceedings of the 6th Annual PKI R&D Workshop 2007, pp. 103-118, Gaithersburg, Maryland, USA, 2007.

[3] David W. O Callaghan, Brian A. Coghlan, "Bridging Secure WebCom and European Data Grid Security for Multiple VOs over Multiple Grid and clouds", in proceedings of the Third International Symposium on Parallel and Distributed Computing/Third International Workshop on Algorithms, Models and Tools for Parallel Computing on Heterogeneous Networks (ISPDC/HeteroPar'04),ispdc, pp.225-231, 2004.

[4] Dr. Dennis Kafura and Dr. Markus Lorch , "A security architecture to enable user collaboration in computational grid and clouds", CISC Research Report 04-05.

[5] Eun-Jun Yoon, Eun-Kyung Ryu and Kee-Young Yoo, " Attacks and Solutions of Yang et al.'s Protected Password Changing Scheme", Informatica, vol.16 , no. 2, pp. 285-294, April 2005.

[6] Foster, I., Kesselman, C., Tsudik, G. and Tuecke, S, "A Security Architecture for Computational Grid and clouds" in proceedings of the ACM Conference on Computers and Security, pp. 83-91, 1998.

[7] Foster. I., Kesselman. C. and Tuecke. S, "The Anatomy of the Grid and cloud: Enabling Scalable Virtual Organizations", International Journal of High Performance Computing Applications", vol. 15, no.3, pp. 200-222, 2001.

[8] Haibo Chena, Jieyun Chenb, Wenbo Maoc and Fei Yand, "Daonity – Grid security from two levels of virtualization", Information Security Technical Report, Vol.12, no.3, pp. 123-138, 2007.

[9] Hai-yan Wanga. C and Ru-chuan Wanga,"CPK-based grid authentication: a step forward", The Journal of China Universities of Posts and Telecommunications, Vol.14, no. 1, pp.26-31, March 2007.

[10] Her-Tyan Yeh, Hung-Min Sun and Tzonelih Hwang, "Efficient Three-Party Authentication and Key Agreement Protocols Resistant to Password Guessing Attacks", Journal of Information Science and Engineering, vol.19, no.6, pp. 1059-1070, 2003.

[11] Ionut Constandache, Daniel Olmedilla, Frank Siebenlist and Wolfgang Nejdl, "Policy-driven Negotiation for Authorization in the Semantic Grid and cloud", Technical report, L3S Research Center, October 2005.

[12] G. Laccetti and G. Schmid, "A framework model for grid security", Future Generation Computer Systems, vol. 23, no. 5, pp.702-713,June 2007.

[13] Li Hongweia, Sun Shixina and Yang Haomiaoa, "Identity-based authentication protocol for grid and cloud", Journal of Systems Engineering and Electronics, Vol. 19, no. 4, pp.860-865, August 2008.

[14] Lin, C.L., and T. Hwang, "A password authentication scheme with secure password updating", Computer & Security, vol.22, no.1, pp.68–72, 2003.

[15] Li Wang, Wenli Wu, YingJie Li and XueLi Yu, "Content-aware Trust Statement for semantic Grid and cloud", in proceedings of the Second International Conference on Semantics, Knowledge and Grid and cloud, pp.95 - 95, November 2006.

[16] Marty Humphrey, Mary R. Thompson and Keith R. Jackson, "Security for Grid and clouds", in Proceedings of the IEEE ,vol. 93, no. 3, pp.644 - 652, March 2005.

[17] Mary R. Thompson, Doug Olson, Robert Cowles, Shawn Mullen and Mike Helm," CA-based Trust Model for Grid Authentication and Identity Delegation", Global Grid Forum CA Operations WG Community Practices Document, Oct 2002.

[18] Michael Szydlo and Burton Kaliski , "Proofs for Two-Server Password Authentication" , In proceedings of the Cryptographer's Track at the RSA(CT-RSA 2005) Conference, pp. 227-244, San Francisco, CA, USA, 2005.

[19] N. Nagaratnam, P. Janson, J. Dayka, A. Nadalin, F. Siebenlist, V. Welch, I. Foster, S. Tuecke, The security architecture for open grid services, document,http://www.cs.virginia.edu/~humphrey/ogsa-sec-wg/OGSA-SecArch-v1-07192002.pdf, July 17 2008.

[20] M.Nithya and R.S.D.Wahida Banu, "Towards Novel And Efficient Security Architecture For Role Based Access Control In Grid Computing", IJCSNS International Journal of Computer Science and Network Security, vol. 9, no.3, March 2009.

[21] Rongxing Lu, Zhenfu Cao, Zhenchuan Chai, and Xiaohui Liang, "A Simple User Authentication Scheme for Grid Computing, International Journal of Network Security, vol.7, no.2, Pp.202–206, September 2008.

[22] Shashi Bhanwar, and Seema Bawa, "Securing a Grid and cloud", in Proceedings of World Academy of Science, Engineering and Technology, vol.32, August 2008.

[23] Shushan Zhao Aggarwal. A and Kent. R.D, "PKI-Based Authentication Mechanisms in Grid Systems", in proceedings of the International Conference on Networking, Architecture and Storage, pp.83-90, Guilin, July 2007.

[24] Stephen Langella, Scott Oster, Shannon Hastings, Frank Siebenlist, Joshua Phillips, David Ervin, Justin Permar, Tahsin Kurc and Joel Saltz, "The Cancer Biomedical Informatics Grid (caBIG) Security Infrastructure", in Proceedings of 2007 AMIA Annual Symposium, Chicago, Illinois, 2007.

[25] Thawan Kooburat and Veera Muangsin, "Centralized Grid Hosting System for Multiple Virtual Organizations", 10th Annual National Symposium on Computational Science and Engineering (ANSCSE10), Chiangmai, March 2006.

[26] V.Vijayakumar and R.S.D.Wahida Banu, "Security for Resource Selection in Grid Computing Based on Trust and Reputation Responsiveness", IJCSNS International Journal of Computer Science and Network Security, Vol.8, no.11, November 2008.

[27] Von Welch, Frank Siebenlist, Ian Foster, John Bresnahan, Karl Czajkowski, Jarek Gawor, Carl Kesselman, Sam Meder, Laura Pearlman and Steven Tuecke, "Security for Grid Services", in proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing, pp.48- 57, June 2003.

[28] Wei Jiea,Wentong Caib, Lizhe Wangc and Rob Proctera, "A secure information service for monitoring large scale grid and clouds", Parallel Computing, Vol.33, no. 7-8, pp. 572-591, August 2007.

[29] Wenliang Du, Jing Jia, Manish Mangal, and Mummoorthy Murugesan, "Untreatable Grid Computing", in Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS'04), pp. 4 - 11, 2004.

[30] Xukai Zoua, Yuan-Shun Dai and Xiang Rana, "Dual-Level Key Management for secure grid communication in dynamic and hierarchical groups", Future Generation Computer Systems,Vol. 23, no. 6,pp. 776-786,July 2007

[31] Yanjiang Yang, Robert H. Deng and Feng Bao, "A Practical Password-Based Two-Server Authentication and Key Exchange System", IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 2, April-June 2006.

[32] Yan Zhenga, Hai-yan Wanga and Ru-chuan Wang, "Grid authentication from identity-based cryptography without random oracles", The Journal of China Universities of Posts and Telecommunications, Vol.15, no. 4, pp.55-59, December 2008.

[33] Yuanbo Guo, Jianfeng Ma and Yadi Wang, "An Intrusion-Resilient Authorization and Authentication Framework for Grid Computing Infrastructure", in proceedings of the Workshop on Grid Computing Security and Resource Management, Springer Berlin / Heidelberg, Vol.3516, pp.229-236, 2005.

[34] Yuri Demchenko, "Virtual organizations in computer grid and clouds and identity management", Information Security Technical Report, vol.9, no. 1, pp.59-76, January-March 2004.

[35]:http://192.168.100.3:8443/wsrf/services/DefaultTriggerService

[36]:http://192.168.100.3:8443/wsrf/services/TrigonBasedAuthenticationService

[37]:http://192.168.100.3:8443/wsrf/services/TriggerService

[38]:http://192.168.100.3:8443/wsrf/services/gsi/AuthenticationService