International Journal of Security (IJS)

ISSN : 1985-2312

VOLUME 4, ISSUE 1

PUBLICATION FREQUENCY: 6 ISSUES PER YEAR

International Journal of Security (IJS)

Volume 4, Issue 1, 2010

Edited By
Computer Science Journals
www.cscjournals.org

Editor in Chief Dr. Wei Wang

International Journal of Security (IJS)

Book: 2010 Volume 4, Issue 1
Publishing Date: 31-03-2010
Proceedings
ISSN (Online): 1985-2320

IJS Journal is a part of CSC Publishers
http://www.cscjournals.org

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers

Editorial Preface

This is the first issue of volume fourth of The International Journal of Security (IJS). The Journal is published bi-monthly, with papers being peer reviewed to high international standards. The International Journal of Security is not limited to a specific aspect of Security Science but it is devoted to the publication of high quality papers on all division of computer security in general. IJS intends to disseminate knowledge in the various disciplines of the computer security field from theoretical, practical and analytical research to physical implications and theoretical or quantitative discussion intended for academic and industrial progress. In order to position IJS as one of the good journal on Security Science, a group of highly valuable scholars are serving on the editorial board. The International Editorial Board ensures that significant developments in computer security from around the world are reflected in the Journal. Some important topics covers by journal are Access control and audit, Anonymity and pseudonym, Computer forensics, Denial of service, Network forensics etc.

The coverage of the journal includes all new theoretical and experimental findings in the fields of computer security which enhance the knowledge of scientist, industrials, researchers and all those persons who are coupled with computer security field. IJS objective is to publish articles that are not only technically proficient but also contains information and ideas of fresh interest for International readership. IJS aims to handle submissions courteously and promptly. IJS objectives are to promote and extend the use of all methods in the principal disciplines of computer security.

IJS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Security (IJS)

Editorial Board

Table of Contents

Volume 4, Issue 1, March 2010.

Pages

TUX-TMS: Thapar University Extensible-Trust Management System

Shashi shashi@thapar.edu
Centre of Excellence in Grid Computing
Computer Science and Engineering Department
Thapar University
Patiala-147004, INDIA

Seema Bawa seema@thapar.edu
Centre of Excellence in Grid Computing
Computer Science and Engineering Department
Thapar University
Patiala-147004, INDIA

Abstract

In a Grid Computing scenario, where the market players are dynamic; traditional assumptions for establishing and evaluating trust, do not hold good anymore. There are two different methods for handling access controls to the resources in grids: first by using policy based approach; where logical rules and verifiable properties are encoded in signed credentials and second by using reputation based approach; where trust values are collected, aggregated and evaluated to disseminate reputation among the market players. There is a need for dynamic and flexible general-purpose trust management system. In this paper TUX-TMS: an extensible reputation based Trust Management System is presented for establishing and evaluating trust in grid systems.

Keywords: Trust, Trust Management System, Grid Computing, Reputation, Feedback

1. INTRODUCTION

Distributed Environments are touching new heights, becoming more useful, popular and more complex with the emergence of service oriented architecture and computing technologies like peer-to-peer, autonomic, pervasive and grid etc [21]. Grid Computing has evolved into a major computing paradigm, having increased focus on secured resource sharing, manageability and high performance. Grids are distributed computing platforms which are heterogeneous and dynamic in nature. The original vision of Grid computing aimed at having a single global infrastructure and providing users with computing power on demand [19]. Efforts to address this issue include providing interoperability among different Grids and Grid middleware [20], and creating trust federations between Grids to grant users in one Grid easy access to another. Grid systems involve the risk of executing transactions without prior experience and knowledge about each other’s reputation. Recognizing the importance of trust in such environments, there is a necessity of designing strategies and mechanisms to establish trust. Reputation systems [1] provide a way for building trust through social control by utilizing community based feedback about past experiences of domain to help in making recommendation and judgment on quality and reliability of the transactions. In this paper, we propose TUX-TMS (Thapar University Extensible- Trust Management System) for establishing trust in Grid Environments. The proposed

Trust system evaluates trustworthiness of the transacting domain on the basis of number of past transactions, feedback ratings and recommendations.

The remaining paper is organized as follows: The taxonomy, parameters and trust metrics are discussed in section 2, 3 and 4, respectively. In section 5, we have discussed our proposed Trust model. Section 6 highlights the implementation strategies adopted to illustrate how our model evolves and manages trust. Results are briefly discussed in Section 7. Related work in covered in Section 8. Section 9 concludes our work.

2. TAXONOMY FOR TUX-TMS

We have considered following taxonomy for our TUX-TMS:

- **Service Requestor**: A service requestor is an entity or domain, which requests some services such as computing, storage etc. from the service providers.
- **Service Provider**: A domain which provides some services to the user or an entity requesting some service.
- **Services**: Services such as computational, data storage, printing, using software licenses or scientific instruments which may be provided to the service requestor.
- **Transaction**: When a service requestor uses the services of the service providers and pays the amount for the services used and submits feedback for the same.
- **Trust Context Factor**: At any time t, the purpose of using services of a service provider by a service requestor can be termed as the trust context factor Ω, which may vary from application purpose. The trust weights may be assigned and evaluated likewise.
- **Service consumed**: A service is said to be consumed when a transaction has completed.
- **Service Initiated**: Services are initiated when jobs are mapped onto resources.

3. TRUST PARAMETERS

We have considered following trust parameters for our TUX-TMS:

3.1.1. Trust

Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is not a fixed value associated with the entity's behavior and applies only within a specific context at a given time [11].

3.1.2 Reputation

Reputation can be taken as a means of building trust, as one can trust another based on a good reputation. Therefore, reputation can be a measure of trustworthiness, in the sense of reliability. We will allow reputation to be assessed from the recommendation score and the trustworthiness of the domain. The recommendation can be submitted as highly recommended or not recommended on the context of service used.

3.1.3 Trust asymmetry

If an entity X trusts another entity Y, then Y should also trust X is not necessarily, yes. This situation can be termed as trust asymmetry, the solution to which is trust symmetry [12]. Here, the user needs to position itself as the resource provider host(s) to estimate their trusts on the user from user's point of view, i.e. to evaluate the trust reflection.

3.1.4 Aggregation of past behavior

A domain stores the values of past transactions so as to determine and estimate the trustworthiness of the domain for future transaction purposes.

3.1.5 Trust Level

Trust can be categorized into various levels ranging from very low trust level to extremely high trust level. Whereas, trust level *et* i.e extremely high trustworthy is not provided by any existing trust relationship. The trust level of a domain varies from not trustworthy to extremely high trustworthy.

3.1.6 Trust Inheritance

In a dynamic grid environment, market players are allowed to join or leave as per the policies agreed upon. When an entity joins a domain, it inherits the recommendation trust table [9] of the domain. There is a member weight associated with every entity to indicate if the entity is a new or an old member with its domain and it is up to the individual domain to decide what constitutes an entity to fall in one of these member weights.

3.1.7 Identity Trust

Identity trust is concerned with verifying the authenticity of an entity and determining the authorizations that the entity is entitled to access and is based on techniques including encryption, data biding, digital signatures, authentication protocols and access control methods [9].

3.1.8 Behavior Trust

Behavior trust is concerned with monitoring and managing of the entity's behavior which is accumulated and evaluated with a period of time, an entity or domain is involved with transactions.

3.1.9 Evolving trust as a newcomer

As a newcomer, the trust values are empty and have to evolve over a period of time after a number of transactions.

3.1.10 Trust Threshold

It is taken as a minimum value required depending on the sensitivity of the application, service requested or provided to establish trust relationship with any entity.

3.1.11 False recommendation

An entity or domain can submit malicious or fraudulent recommendation about an entity after a number of transactions due to business competition, enmity or to degrade the reputation of an entity. Therefore, the recommendation values are aggregated for an entity to ensure reliable and trustworthy services.

3.1.12 Trust and Reputation Decay

The value of trust decays with time as grid environments are dynamic in nature and market players are allowed to volunteer or withdraw as per the policies agreed upon. Therefore, the trust value decays, which enforces the domain to re-establish the value when it participates in the grid.

3.1.13 Feedback

Feedback is a taken as a value p such that $0 \leq p \leq 1$, which can be issued by the service requestor about the quality of a service provided by a service provider in a single transaction and vice versa.

3.1.14 Trustworthiness

An entity's trustworthiness is an indicator of the quality of the entity's services over a period of time. It is often used to predict the future behavior of the entity. Intuitively, if an entity is trustworthy, it is likely that the entity will provide good services in future transactions.

3.1.15 Trust relationships

Determining trust relationship is essential while accessing resources/services. We have assumed the three Trust Relationships for our system: Direct Trust, Indirect Trust and Recommended Trust.

3.1.16 Intrusion Detection and Audit Trails

Intrusion Detection is a process of monitoring the events occurring in the system or network and analyzing them for signs of possible violations. Of the security policies agreed upon such that a garbage collector will clear the unused data upon completion of task or job etc. Audit trails are responsible for establishing accountability of users for their actions and provide evidence, if any.

3.1.17 Trust and Reputation Update

After the transaction, intrusion detection and audit trail has taken place the feedback is updated in the databases for trustworthiness and recommendation.

3.1.18 Risk Assessment

The service quality provided over the service quality expected leads to calculation and assessing the risk involved in the transaction**.**

3.1.19 Interoperability

The trust model should be able to interoperate at various levels such as protocol, policy and identity level.

4. TRUST METRICS IN TUX-TMS

A trust metric is a measure of how an entity of a domain is trusted by the other entities. TUX-TMS is a transaction based feedback system, where the feedback is mandatory with each transaction. In TUX-TMS, the trust metrics derived are:

- The trustworthiness is an indicator of the quality of the entity's or domain services. The higher the value, the higher the trustworthiness of the domain.
- The feedback scores that a domain or entity receives from other domains in terms of service provided. This value is average of the feedback score over a number of transactions. As the number of transaction increases, the composite feedback score decreases. We have assumed various trust relationships between domains: indirect, recommendation and direct trust relationship.
- The trust and reputation decays as the time progresses and the trust needs to be established again between the domains after a period of time has lapsed.
- Risk assessment establishes the risk level involved in transacting with a domain.

5. THE PROPOSED TRUST MANAGEMENT SYSTEM

The main focus of this paper is on design and development of TUX-TMS-an extensible Reputation based Trust Management System for establishing trust and assessing trustworthiness of domains in grids environments. Reputation based systems rely on feedback score to evaluate trustworthiness of a domain [15].

5.1 Components of TUX-TMS

Various components have been used in our TUX-TMS.

I. **Identity Management System:** An identity management system maintains repository of the user credentials and interacts with various Trusted Third Parties (TTP) to check for validation of the credentials provided by the user. The Identity Management System incorporates authentication, authorization, confidentiality, log related and trust related functions

II. **Trustworthiness:** The trustworthiness is evaluated and calculated from past transaction scores and the feedback provided for the service provided by both service requestor and service provider.

III. **Reputation Engine:** The reputation engine provides the recommended score of an entity or domain.

IV. **Trust Inheritance**: The entity which is a part of a domain inherits some value ∆€ from the domains depending upon the credibility of the domain. For a malicious domain, the value is very low.

V. **Risk Assessment**: The value depends on the rank of the domain in the DET. Higher the rank, minimal is the risk involved in transacting with the domain.
VI. **Trust and Reputation Decay**: The trust and reputation decays on the basis of the time an entity or domain is not transacting. The trust decay factor() decays and the trust and reputation values are to be regained again by the domain for future use purposes.
VII. **Trust Inference Engine**: A trust inference engine takes the value of Trustworthiness, Reputation, Risk Assessment and trust inheritance for calculating the threshold value to allow a domain to transact.
VIII. **IDS and Audit trail**: If a TA (trusted agreement) is violated, the transaction performed is rejected and the feedback scores are not updated in the databases.

5.2 Architecture of TUX- TMS

The architecture of the TUX-TMS is depicted in Figure1. An end user i.e. service requestor/service provider is requested to login into the TUX-TMS using his credentials. If the user is already registered with the TUX-TMS, the Identity Management System checks the authentication and verifies the information provided such as security certificates or else if a user is new, he is requested to register. First, the Trust Inheritance, Risk Assessment and the values of Trustworthiness (TD) and Recommendation (RD) are checked and then a user is allowed a set M [D, Sp, S] where D stands for Domain, Sp for service Provider and S stands for the service a user is allowed to perform. The user can further calculate and check the values of trust of the Service Provider by first checking the trust values, recommended value and further calculate the risk involved in transacting. If the user is satisfied with the values, he can perform the transaction. After the transaction, a user is requested to fill in the Feedback of the trustworthiness and recommendation based on questionnaire. After a service requestor, the service provider is requested to fill up the feedback form. Thereby, making the transaction complete. An Intrusion Detection System and audit trails checks the information provided to be from the intended players and the trust values and recommendation values are updated in their respective databases. If the values are reported from the malicious origin, the values are discarded and the malicious domains are blacklisted. TUX-TMS DB is responsible for maintaining the database.

6. IMPLEMENTATION STRATEGIES

We have performed initial experiments to evaluate feasibility and benefit of our TUX-TMS.
We have taken 8 departments, 7 Schools and five hostels for experimental purpose which has approx. 100 systems each and provides services such as computation, printing and data storage. The database details have been stored in TUX-TMS DB. The tables ETT (Entity Evaluation table) has been designed using following attributes: Service Requestor (SR), Service Provider (SP), Number of transactions (N_T), Feedback Score (F_s), Recommendation Score (R_c), Trust Relationship (TR), Total Entity Value (TEL), Trust Context Factor (Ω). There are other repositories Domain Evaluation Table (Domain Evaluation Table), Service Provider Data (SPD) and Temporary Storage Table (TST).
In TUX-TMS, a domain's trustworthiness is defined as the degree of trust other domains can have on one domain to initiate communication or participate in any kind of transaction. The trustworthiness can be computed using trust decay factor Td*ecay* with the feedback score.

$$Tdecay = \sum Tw / \sum Nt \tag{1}$$

$$Rdecay = \sum Rc / \sum Dn \tag{2}$$

$$Tfin(D) = \alpha * Tr + \beta * Rc + \gamma \tag{3}$$

$$Ra = Rank / Tdn \tag{4}$$

$$TI = Tfin - Ra * 100 \tag{5}$$

Here, Tw: Trustworthiness
T_{decay}: Trust Decay Factor
N_T: Number of transactions

D: Domain
R_{decay}=Reputation Decay
Dn: Total number of domains with whom transaction has taken place
T_{fin}=Total trust value
T_{dn}: Total number of domains in the system
Ra=Risk Assessment
R_{ank}=Rank of a domain
TI=Trust Inheritance
α, β, γ=Constants used for belief, disbelief and plausibility

Algorithm 1. *TUX_TMS(ETT, DET, TST,SR_ID, SPD, domain)*

```
Input: ETT, DET, TST,SR_ID, domain    Output: ETT, DET, TST
If authenticated then
   If authorized then
       Resource_request
      TW <= Trust_Inference_Engine(DET, domain, r, sr, rp, R, P)
       Resource_requested <= select k from TST_ID
       If trust_requirement of ID=Resource_requested from SPD<TW  then
          Notify_ID about request
          If  ID approves then
              T_id <= Transaction ID
              Transaction occurs
             Transaction ends
         End if
       End if
    If enter_feedback then
       Valid_tid <= Verify_Transaction(t_id)
       If Valid_tid = true then
           Valid_user <=Perform_IDS( SR_ID)
           If Valid_user=true then
              Add_feedback(TEL_sr, TEL_sp, R, P)
          End if
      End if
    End if
  End if
 Else register
End if
```

Here, the Feedback Score can be calculated by giving a value p, such that 0≤ p≤1 score may be provided for both the Service Requestor and the Service Provider. The service is rated on the basis of trust and reliability only.

Considering the malicious intent of some entities who would try to increase the rating of an entity by giving more score for the services provided, the overall score will reduce as the number of transactions will increase, by calculating the score on the basis of equation 3 for the domains transacting.

$$Fs(D) = \sum Fs / \sum Nt \tag{6}$$

The rating R of a Domain D can be calculated as

$$Tw = Fs(D) + TR + \Omega \tag{7}$$

Here,
Fs=Feedback Score
Nt=Total number of transaction
TR=Trust Relationship
Ω=Trust Context Factor

Algorithm 2. *Trust_Inference_Engine(DET, domain, r, sr, rp, R, P)*

```
Input:  DET, domain, r, sr, rp, R, P                                   Output: DET, TST
call Decay_Trust(DET)
call Risk_Assesment( DET, domain )
call Trust_Inheritance( DET, domain )
threshold_SR <= w1 * Tdecay of DET(r) + w2 * Rdecay of DET(r) + w3 * Trust Inheritance of
DET(r) - w4 * Risk_Assesment of DET(r)
for i=1 to length(DET) do
        if   threshold of SPD(i) < threshold_SR then
                TST_ID   <= i
                TST_SR<= threshold_SR
        end if
end for
```

The trustworthiness of the domain with high feedback scores increases. The threshold value is used to determine a demarcation between domains with higher reputation. Algorithm 2 is of the trust inference engine which takes the value of risk assessment, trust inheritance and trust and reputation decay values before determine the threshold. The threshold is further required for providing services to the service requestors as per their values.

Algorithm 3*. Decay_ Trust(DET)*

```
Input: DET                                                             Output: DET
for i=1 to length(DET) do
        ∑Tu of DET(i) <= ∑Tu of DET(i) – Tdecay of DET(i)
        ∑Rc of DET(i) <= ∑Rc of DET(i) – Rdecay of DET(i)
        Tdecay of DET(i) <=∑Fs of DET(i) / ∑Nt of DET(i)*100
        Rdecay of DET(i)<= ∑Rc of DET(i) / ∑Dn of DET(i)*100
End for
```

Here, Decay_Trust( ) decays the values of trustworthiness by total trustworthiness value by total number of transactions incurred and reputation values by number of domains transacted with. These decayed values are added to estimate rank of a domain in Domain Evaluation Chart (DEC).

Algorithm 4. *Risk_Assessment (DET, domain)*

```
Input: DET                                                             Output: DET
for i=1 to length(DET) do
        if DET[i].Domains= domain then
                DET[i].risk <= rank/max_rank * 100
        end if
end for
```

Risk_Assessment () calculates the risk involved in interacting with one particular domain and is calculated dividing the by rank of a domain in The risk is assessed by percentage of rank of a domain by total number of domains in DEC (Domain Evaluation Chart).

Algorithm 5. *Trust_Inheritance (DET, domain)*

```
Input: DET                                                             Output: DET
for i=1 to length(DET) do
        if DET[i].Domains= domain then
                DET[i].safety_factor <= 100-DET[i].risk
                DET[i].Trust Inheritance <= DET[i].TEL * DET[i].safety_factor
        end if
end for
```

The trust inherited is the percentage of risk assessed subtracted by 100 and is stored for the domains which are interacting for the first time.

A malicious user may try to increase values of untrustworthy domain by giving good feedback scores. The rating R is calculated by reducing the score as the number of transaction increases. A window *W (N, T)* is applied which calculates N number of transactions in a time interval T and further decreases the value of the domains by using equation 4.

The trust value is decayed using equation 2 after a fixed interval of time. As the value becomes 0, the domain is updated as non functional in Trust Finder and a log file is maintained at a remote server which can be invoked as per need basis. The domain whose trust score becomes 0 is enforced to establish trust again by re-establishing trust relationships and transacting with other domains.

Algorithm 6. *Add_Feedback(ETT)*

```
Input: ETT                                              Output: DET,  ETT
for i=1 to length(DET) do
        receiver <= SR of DET ( i )
        if receiver = R then
           TEL_SR<= SR of TEL of ETT(i)
        end if
        provider<= SP of DET( i )
        if provider = P then
           TEL_SP <= SP of TEL of ETT(i)
        end if
end for
ETT_SR <= TEL_SR + sr
ETT_SP <= TEL_SP + sp
for j=1 to length(DET) do
        if R = Domain Name of Domain Evaluation Table then
           ∑Fs of Domain Evaluation Table <= ∑Fs of Domain Evaluation Table + sr
           ∑Rc of Domain Evaluation Table <= ∑Rc of Domain Evaluation Table + sr
           ∑Nt of Domain Evaluation Table <= ∑Nt of Domain Evaluation Table + 1
        end if
        if P = Domain Name of Domain Evaluation Table then
           ∑Fs of Domain Evaluation Table <= ∑Fs of Domain Evaluation Table + sp
           ∑Rc of Domain Evaluation Table <= ∑Rc of Domain Evaluation Table + sp
           ∑Nt of Domain Evaluation Table <= ∑Nt of Domain Evaluation Table + 1
        end if
end for
```

Add_Feedback() aggregates the feedback for service requestor as well as provider for trustworthiness and recommendation.

In case the domain is not able transact or report status due to connection failure or hardware failure. The Trust Finder database is updated and domain is communicated to report status. The domain is erased form the Trust Finder database after waiting for a reply for a time interval t.

7. RESULTS AND DISCUSSIONS

In addition to developing a theoretical model for TUX, we also conduct a comprehensive performance analysis using various trust metrics as discussed in Section 4, The figures shown are self explanatory however a brief analysis is given here:

Firstly, to evaluate and establish trustworthiness and reputation of a domain in a dynamic environment as Grid, we have taken feedback of the players i.e. service requestor and service provider’s into account. On the basis of which, we have further calculated their ranks based on their trustworthiness and recommendation score.

In Figure 2, as the rank of the domain decreases, the values of trustworthiness and reputation as well decrease. Due to dynamic nature and uncertainty in grid environment, the values of trustworthiness and reputation are used only after decaying them with the T_{decay} and R_{decay} functions as shown in Figure 3.

In Figure 4, it is observed that he risk involved in transacting with a domain increases with the decreases in rank of a particular domain. Figure 5, 6 and 7 shows that the behavior of α, β and γ when we observe the service as printing, computational and data storage varies.

In Figure 8, the trust inherited is decreased with the increase in the rank of the domains.

8. RELATED WORK

In grid environments, there are two different types of trust management systems: Reputation based and policy based [17]. A number of trust models have been proposed by different researchers for evaluation of trust in a grid.

Li Xiong and Ling Liu have proposed a PeerTrust[2] model. PeerTrust-is a reputation based trust supporting framework, which includes a coherent adaptive trust model for quantifying and comparing trustworthiness of peers based on a transaction-feedback system and a decentralized implementation of such model over a structured P2P overlay network.

B. Dragovic and E. Kotsovinos's XenoTrust [3] is built on the XenoServer Open Platform [4]. Unlike simple peer-to-peer recommendation services, XenoTrust is concerned with pseudonymous users, associated with real-world identities, running real tasks on real servers for real money within a global-scale federated system whose constituent parts may have different notions of "correct" behavior. NICE trust management system [5] was developed at the University of Maryland. The NICE framework, is a platform for implementing cooperative applications over the Internet, which can be defined as a set of applications that allocate a subset of resources, typically processing, bandwidth, and storage, for use by other nodes or peers in the application. Therefore, grid computing is naturally an application for the NICE trust management framework.

Secure Grid Outsourcing (SeGO) system [6], [7] was developed at the University of Southern California. SeGO is developed for secure scheduling of a large number of autonomous and indivisible jobs to grid. A unique feature of the work is that the authors use a fuzzy inference approach to binding security in trusted grid computing environment. Abdul Rahman and Hailes proposed a Trust–Reputation Model [8] based on prior experiences based on trust characteristics from social sciences. F. Azzedin and Maheswaran proposed a Trust Model for Grid Computing Systems [9] which is extension of [8] and [10]. They have insisted on that a direct trust value weighs more than a recommender value. The model lets a newcomer to build trust from scratch by enforcing enhanced security. Here, trust is dynamic, context specific, based on past experiences and spans over a set of values ranging from very trustworthy to very untrustworthy. Farag Azzedin and Muthucumaru proposed a Trust Model [11] for peer to peer computing systems also. In addition to previous model [11], an accuracy measure is associated with each recommendation. Chin Li, V Varadharajan, Yan Wang and V. Pruthi proposed a Trust Management Architecture [12] for enhancing grid security that explores the three dimensional view of trust which includes belief, disbelief and uncertainty. This subjective logic based trust evaluation is based on Dempster-Shafer theory [13]. Z. Liang and W. Shi proposed a PErsonalized Trust Model (PET) [14] for peer to peer resource sharing. PET has accommodated risk assessment which is done to perceive the suddenly spoiling peer. Eigentrust[18] computes a global trust value for a peer by calculating the left principal eigenvector of a matrix of normalized local trust values, thus taking into consideration the entire system's history with each single peer.

9. CONCLUSION

We have presented TUX-TMS: an extensible Reputation based Trust Management system which computes the trustworthiness and reputation of the interacting domains in a grid scenario. The grid domains are dynamic and heterogeneous in nature. The Identity Management System incorporates authentication, authorization, confidentiality, log related and trust related functions. The trust decay factor ensures that the database is maintained up to date by updating when the values are used. TUX-TMS is a secure and reliable system. In addition to developing a theoretical model for TUX, we also conduct a comprehensive performance analysis. Our evaluation results show that both reputation (long-term behavior assessment) and risk (short-term behavior assessment) are important in designing a TUX-Trust Management Model. The results also show that the TUX model is flexible enough for identity and behavior trust by incorporating Audit trail and analysis for identity management. The characteristics of Trust Management Model such as scalability i.e Message, storage and computational overhead, security i.e Fabrication, Masquerading, Collusion, Sybil Attack and reliability have been considered while designing the model and are to be tested. The proposed model is interoperable as we have used web services in developing.

REFERENCES:

[1] P. Resnick, R. Zeckhauser, K. Kuwabara, E Friedman,,"Reputation systems", Communications of the ACM, 43(12): 45-48, December 2000.

[2] Li Xiong, Ling Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities", IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7: 843-857, 2004.

[3] B., Dragovic, E. Kotsovinos, "XenoTrust: Event-based distributed trust management", Second International Workshop on Trust and Privacy in Digital Business, Prague (Czech Republic), 2003.

[4] B. Dragovic, S. Hand, T. Harris, E. Kotsovinos, "Managing trust and reputation in the XenoServer Open Platform", Proceedings of the 1st International Conference on Trust Management, Crete Greece, 2003.

[5] S. Lee, R. Sherwood, B. Bhattacharjee, "Cooperative peer groups in NICE", Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 50, Issue 4 : 523 – 544, March 2006.

[6] S. Song, K. Hwang, M. Macwan, "Fuzzy Trust Integration for Security Enforcement in Grid Computing", NPC 2004, LNCS 3222: 9-21, 2004.

[7] S. Song, K. Hwang., Y.K Kwok, "Trusted Grid Computing with Security Binding and Trust Integration", Journal of Grid Computing, vol. 3, no. 1: 24-34, 2005.

[8] A Abdul Rahman and S. Hailes, "Supporting trust in virtual communities", Proc. of Hawaii Intl Conference on System Sciences, pp:6007, 2000.

[9] Farag Azzedin and Muthucumaru Maheswaran, "Evolving and Managing Trust in Grid Computing Systems", Proceedings of the 2002 IEEE Canadian Conference on Electrical & Computer Engineering, 2002.

[10] N. Damianou, N. Dulay, E. Lupu and M. Sloman, "The Ponder Policy Specification Language", POLICY 2001, LNCS 1995:18-38, 2001.

[11] Farag Azzedin and Muthucumaru Maheswaran), "Trust Modeling for Peer-to- Peer based Computing Systems", Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS'03), pp:99a., 2003.

[12] Ching Lin, Vijay Varadharajan and Yan Wang and Vineet Pruthi "Enhancing Grid Security with Trust Management", Proceedings of the 2004 IEEE International Conference on Services Computing (SCC'04), pp: 303-310, 2004).

[13] Glenn Shafer, "Perspectives on the theory and practice of belief functions", International Journal of Approximate Reasoning 6(3): 445-480, 1992.

[14] Zhengqiang Liang and Wesiong Shi, "PET: A Personalised Trust Model with Reputation and Risk Evaluation for P2P Resource sharing", Proceedings of the 38th Hawaii International Conference on System Sciences, pp.201 .2, 2005.

[15] Shashi, Seema Bawa, "Securing a Grid", International Conference CGCS-2008 (Cluster and Grid Computing Systems), Proceedings of World Academy of Science, Engineering And Technology, Volume 32 ISSN: 2070-3740, pp 7-12, 2008.

[16] Shashi, Seema Bawa, "Evaluating Trust in a Grid Environment", Student Research Symposium, HiPc 2008 (International Conference on High Performance Computing) Bangalore, India, 2008.

[17] Anirban Chakrabarti Grid Computing Security, Springer-Verlag Berlin Heidelberg, 2007.

[18] Sepandar D Kamvar, Mario T Schlosser, Hector Garcia Molina, “The EigenTrust Algorithm for Reputation Management in P2P Networks”, Proceedings of the 12th International conference on World Wide Web, Budapest, Hungary, pp: 640 – 651, 2003.

[19] I. Foster, and C. Kesselman, “The Grid: Blueprint for a New Computing Infrastructure”, San Francisco, CA, USA, Morgan Kaufmann Publishers Inc., 1999.

[20] Grid Interoperability Now Community Group (GIN-CG)(2006). http://forge.ogf.org/sf/projects/gin.

[21] Sarbjeet Singh ans Seema Bawa), “A Privacy, Trust and Policy based Authorization Framework for Services in Distributed Environments”, International Journal of Computer Science, vol. 2 no. 2: 85-92, 2007.

Vitae:

Shashi, is a Research and teaching assistant in the Computer Science and Engineering Department at Thapar University, India. She received her MCA in 2005 from Punjabi university, India, Her research interests include distributed systems, cluster/network/Grid computing. Currently, she is pursuing her Ph.D. with a focus on Trust management and Interoperability in Grids. She is a member of IEEE, ACM and Anita Borg Institute for Women and Technology.

Seema Bawa is a Professor in Computer Science and Engineering Department at Thapar University, India. She holds M.Tech (Computer Science) degree from IIT Kharagpur and Ph.D. from Thapar University (TU), Patiala. Her areas of interests include Parallel and Distributed Computing, Grid Computing, VLSI Testing and Network Management. Prof. Bawa is member of IEEE, ACM, Computer Society of India, and VLSI Society of India.

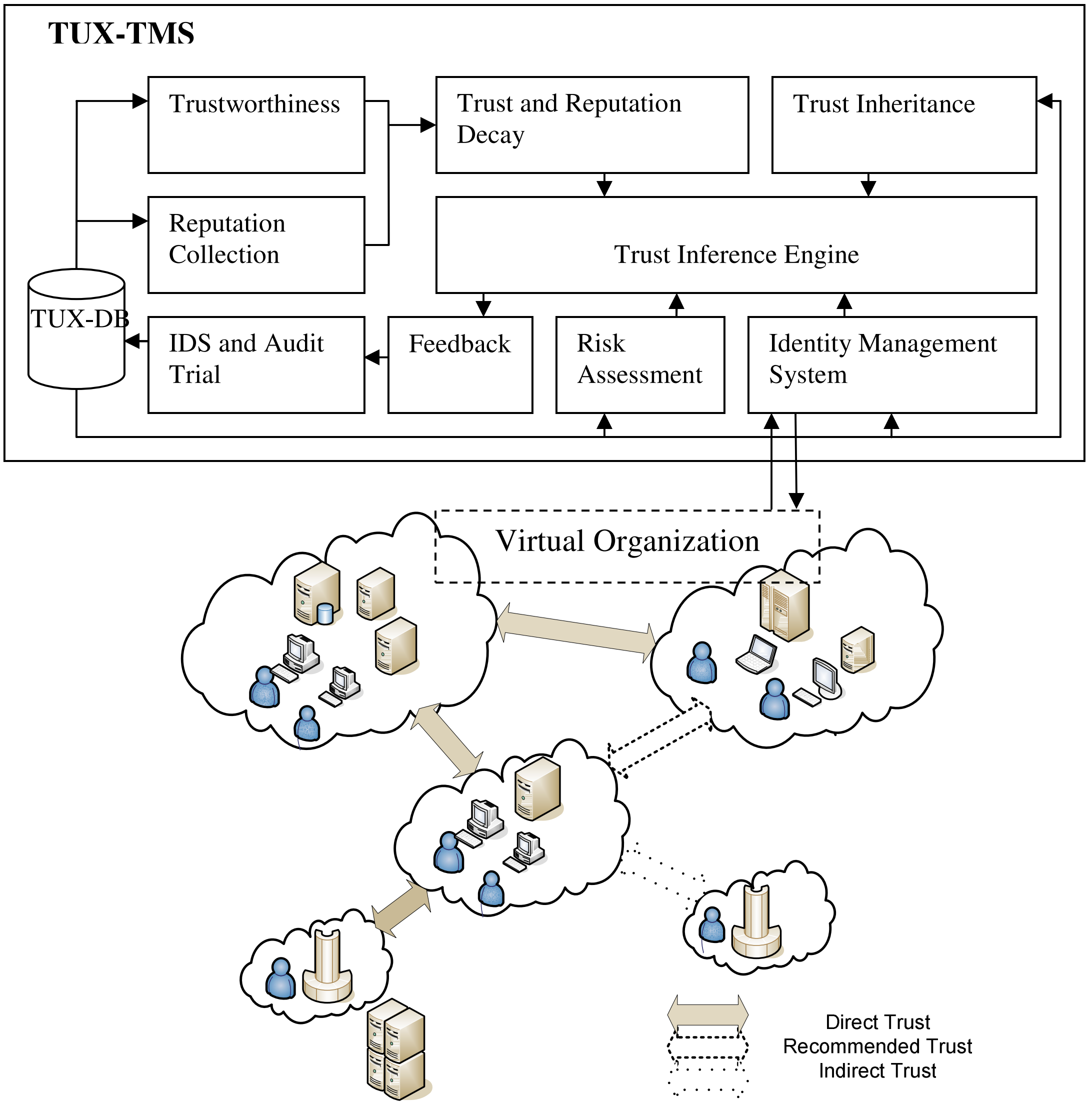

FIGURE1. TUX-TMS Architecture

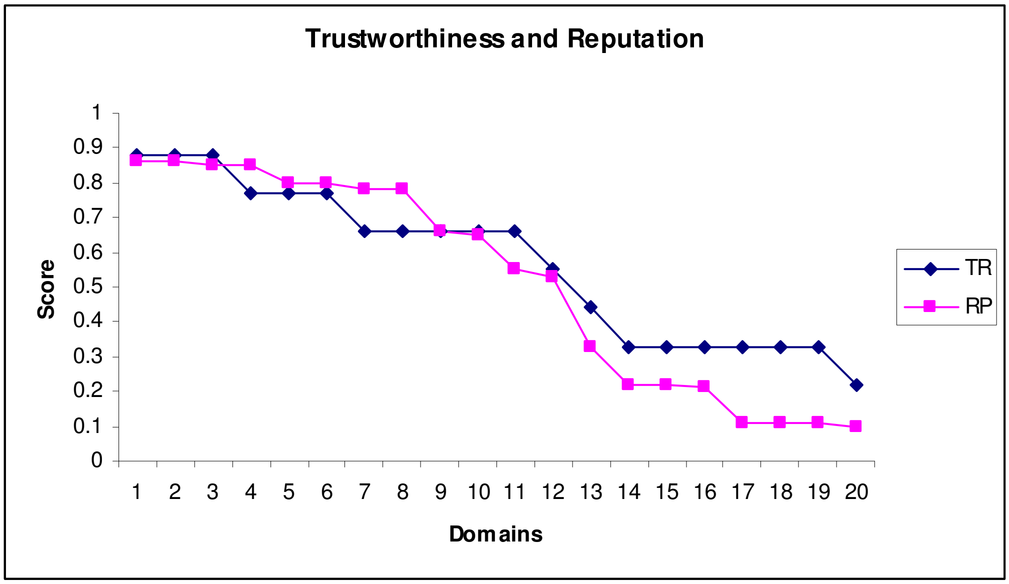

FIGURE2: Trustworthiness and Reputation values without Decay

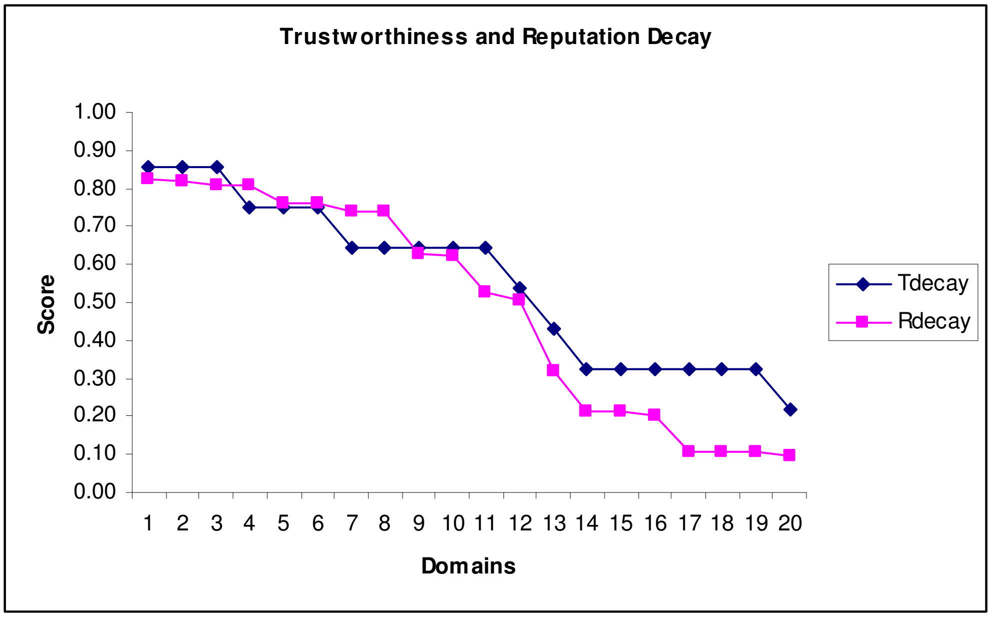

FIGURE 3: Trustworthiness and Reputation values with Decay

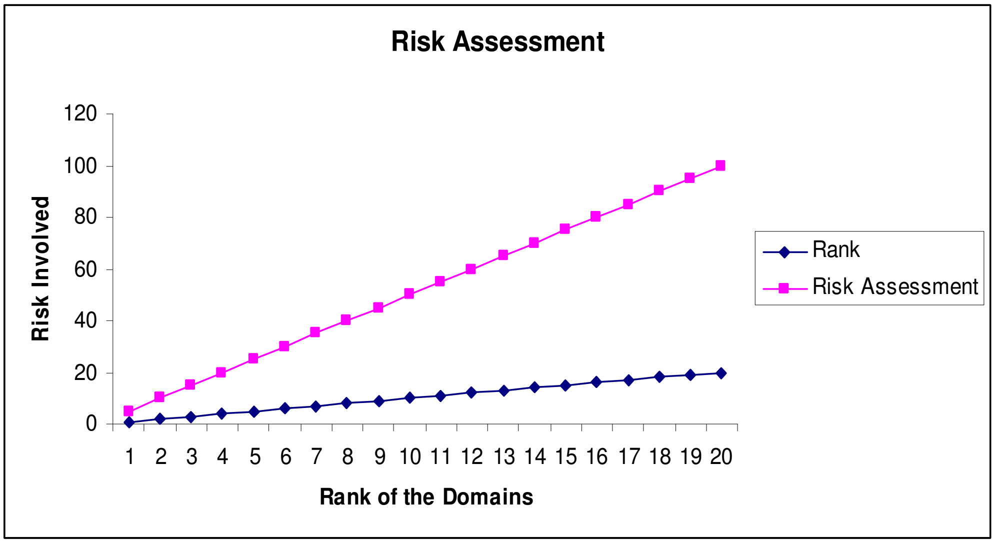

FIGURE 4. Risk Assessment

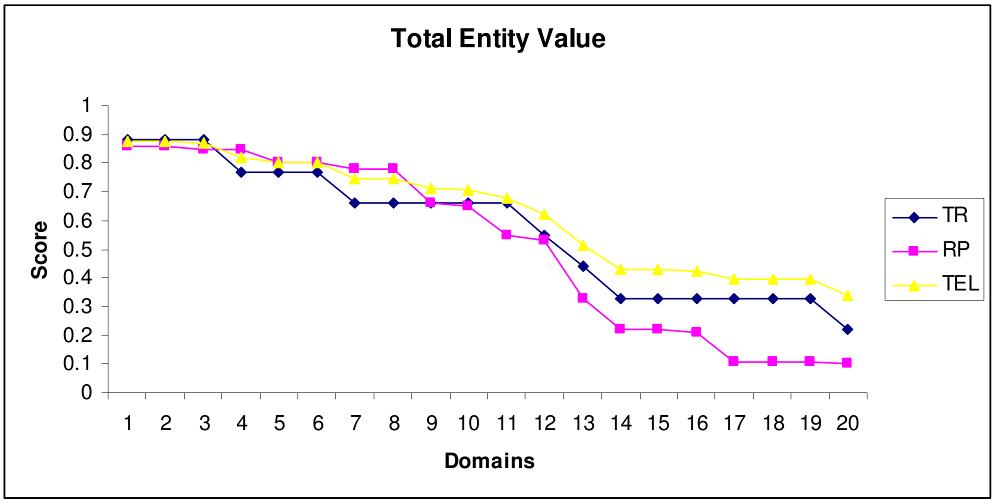

FIGURE 5. Total Entity Value when α=0.5, β=0.3, γ=0.2

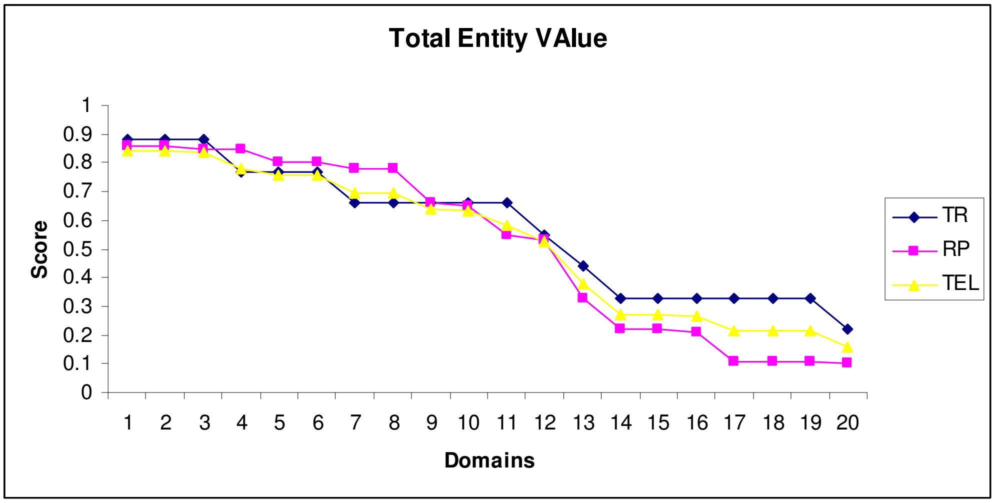

FIGURE 6. Total Entity Value when α=0.7, β=0.3, γ=0

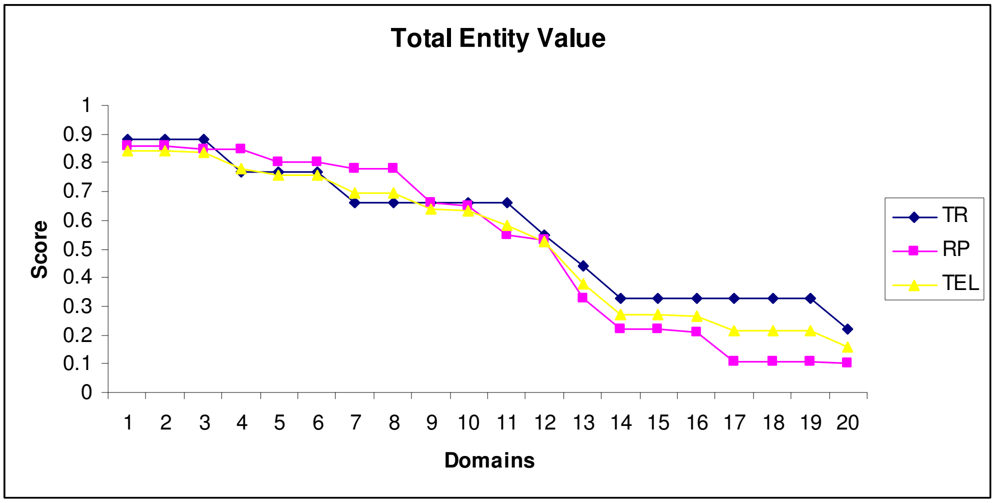

FIGURE 7. Total Entity Value when α=0.5, β=0.5, γ=0

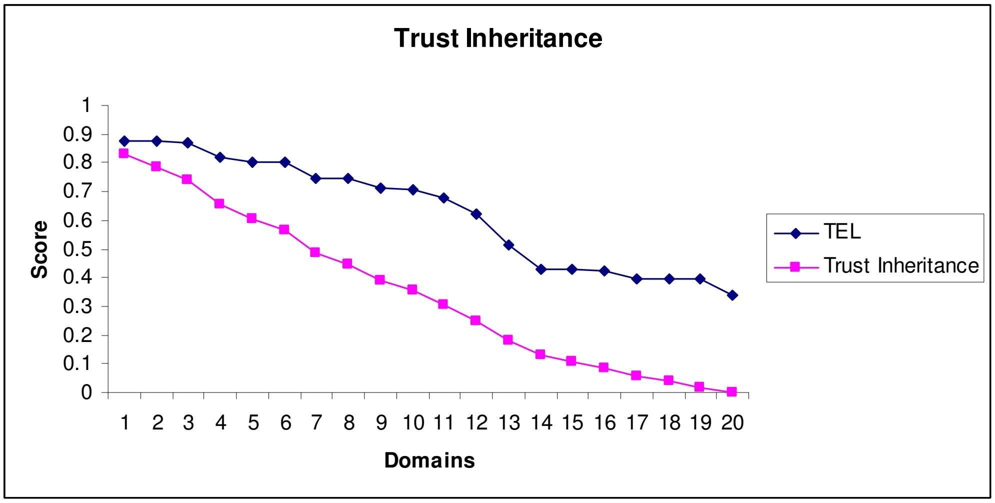

FIGURE 8. Trust Inheritance

Secure Group Communication in Grid Environment

Dr Sudha Sadasivam G sudhasadhasivam@yahoo.com
Professor/Department of Computer Science
PSG College of Technology
Coimbatore – 641 004, India.

Ruckmani V ruckmaniv@yahoo.com
PhD Research Scholar/Department of Computer Science
PSG College of Technology
Coimbatore – 641 004, India.

Anitha Kumari K kesh_chse@yahoo.co.in
ME (SE) Student/Department of Computer Science
PSG College of Technology
Coimbatore – 641 004, India.

ABSTRACT

A Grid is a collection of resources that are available for an application to perform tasks. Grid resources are heterogeneous, geographically distributed and belong to different administrative domains. Hence security is a major concern in a grid system. Authentication, message integrity and confidentiality are the major concerns in grid security. Our proposed approach uses a authentication protocol in order to improve the authentication service in grid environment. Secure group communication is brought about by effective key distribution to authenticated users of the channels serviced by resources. The proposed approach facilitates reduced computation and efficient group communication. It also ensures efficient rekeying for each communication session. The security protocol has been implemented and tested using Globus middleware.

Keywords: authentication, grid computing, grid security, multicasting, encryption.

1. INTRODUCTION

Grid protocols and technologies are being adopted in academic, government, and industrial organizations. Grid computing facilitates remote access to high–end resources for computation and data intensive jobs. Researchers can access heterogeneous and geographically distributed hardware and software resources efficiently. Two important requirements in grid include the formation of virtual organizations (VO) dynamically and establishment of secure communication between the grid entities. A VO is a dynamic group of individuals, groups, or organizations that have common rules for resource sharing [1].

Security in computational grids encompasses authentication, authorization, non-repudiation, integrity, confidentiality and auditing. To avoid the illegal users from visiting the grid resources strong mutual authentication between grid entities should be guaranteed. Password-based authentication is extensively used because of its simplicity. Authorization allows a specific permission for a particular user on a specified resource (channels). Confidentiality of information in a VO should also be ensured [4]. The necessity for secure communication between grid entities has motivated the development of the Grid Security Infrastructure (GSI). GSI provides integrity, protection, confidentiality and authentication for sensitive information transferred over the network in addition to the facilities to securely traverse the distinct organizations that are part of collaboration [2]. Authentication is done by exchanging proxy credentials and authorization by mapping to a grid map file. Grid technologies have adopted the use of X.509 identity certificates to support user authentication. GSI is built on top of the Transport Layer Security (TLS) protocol. Both TLS and GSI operate at the transport layer. They require an ordered reliable transport connection, so typically they are implemented over Transmission Control Protocol (TCP). This approach is not suitable for web service-based technologies on the grid. Simple Object Access Protocol (SOAP) protocol [13] is used by the emerging Open Grid Service Architecture (OGSA). This necessitates for support message layer security using XML digital signature standard and the extensible markup language (XML) encryption standard [14]. Enhancements of SOAP messaging to provide message integrity and confidentiality are standardized in Organization for Advancement of Structured Information Standards (OASIS). The WS-secure conversation specification [15] describes how two entities can authenticate each other at the message layer. Grid middleware like Globus Toolkit™ Version 4.0, pyGridWare and Open Grid Services Infrastructure (OGSI).NET/Web Services Resource Framework (WSRF).NET (Wasson et al., 2004) use WS-secure conversation based on TLS authentication handshake in the SOAP message layer. Globus Toolkit [3] provides security services for authentication, authorization, management of user credentials and user information.

Wei Jiea et al. [5] have proposed a scalable GIS architecture for information management in a large scale Grid Virtual Organization (VO) with facilities to capture resource information for an administrative domain. The framework also incorporates security policies for authentication and authorization control of the GIS at both the site and the VO layers. Haibo Chena et al. [6] have applied trusted computing technologies in order to attain resource virtualization to ensure behavior conformity and platform virtualization for operating systems. Yuri Demchenko [7] has analyzed identity management in VOs and usage of Web Service (WS)-Federation and WS-Security standards. G. Laccetti and G. Schmid [8] have introduced a unified approach for access control of grid resources. (PKI) Public Key Infrastructure and (PMI) Privilege Management Infrastructure infrastructures were utilized at the grid layer after authentication and authorization procedures. Xukai Zoua et al. [9] have proposed an elegant Dual-Level Key Management (DLKM) mechanism using Access Control Polynomial (ACP) and one-way functions. The first level provided flexible and secure group communication whereas the second level offered hierarchical access control. Li Hongweia et al. [10] 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. Being certificate-free, the authentication protocol aligned well with the demands of grid computing. Yan Zhenga et al [11] use identity-based signature (IBS) scheme for grid authentication. Hai-yan Wanga. C and Ru-chuan Wanga [12] have proposed a grid authentication mechanism, which was on the basis of combined public key (CPK) employing elliptic curve cryptography (ECC).

Once the grid entities are authenticated, key distribution occurs between the grid entities to ensure secure communication. Some existing key distribution schemes include manual key distribution, hierarchal trees and secure lock. Manual key distribution lacks forward and backward secrecies, whereas hierarchical model requires more footprints. Secure lock method is computation intensive. The proposed system encrypts session keys thereby reducing computational costs, communication costs, and key storage footprint. Although the method is simple, it ensures good accuracy. The proposed work aims at authenticating the users and allocating channel resources to the users based on the availability of the resource and security weights. It ensures both user and resource authentication. Then encryption key to ensure secure communication among these members is distributed among the channel members. The message digest of the information to be transferred is encrypted for confidentiality using the key and then transferred to authenticated grid entities.

Reconcilable key management mechanism is proposed by Li [16] in which the key management middleware in grid can dynamically call the optimum rekeying algorithm and rekeying interval is based on the rates that the group members join and leave.

Li [18] proposed an authenticated encryption mechanism for group communication in term of the basic theories of threshold signature and basic characteristics of group communication in grid. In this mechanism, each member in the signing group can verify the identity of the signer, and the verifying group keeps only private key.

A scalable service scheme for secure group communication using digital signatures to provide integrity and source authentication is proposed by Li [17] . In this approach, Huffman binary tree is used to distribute keys in VO and complete binary tree is used to manage keys in administrative domain. Sudha [20] proposed to use tree-based approach for secure group key generation and establishment of communication among domains in a VO using trust relationships.

The proposed work aims at authenticating the users and allocating channel resources to the users based on the availability of the resource and security weights. Then encryption key to ensure secure communication among these members is distributed among the channel members. Digest of the information to be transferred is formed and then it is encrypted for confidentiality and then transferred to its peers. The remaining of the paper is organized as follows: Section 2 is constituted by the proposed authentication and channel distribution mechanism. Section 3 discusses about the analysis done so far. Section 4 discusses about implementation results and Section 5 concludes the paper.

2. PROPOSED SYSTEM ARCHITECTURE

The components of the system depicted in figure 1 are described as follows..
1) Registration component to register the legitimate users/managers of the channel.
2) Join/leave component to take care of authentication of the channel users.
3) Key generation system that generates the encryption key randomly.
4) Key distribution system that distributes the keys to the authenticated members of the channel.
5) Channel to distribute the encrypted information among the group members.

When legitimate entities (users and resources) register to the channel, the encrypted hash value of their passwords is stored in the authentication server. The proposed approach initially authenticates the user by matching its encrypted hash value with that stored in the authentication file. If authenticated, a random key is generated and distributed among the members in the channel or group. The message digest of the message to be transferred is encrypted and multicast to the group through the channel.. The receivers then decrypt and decode to get the original message (figure 2)

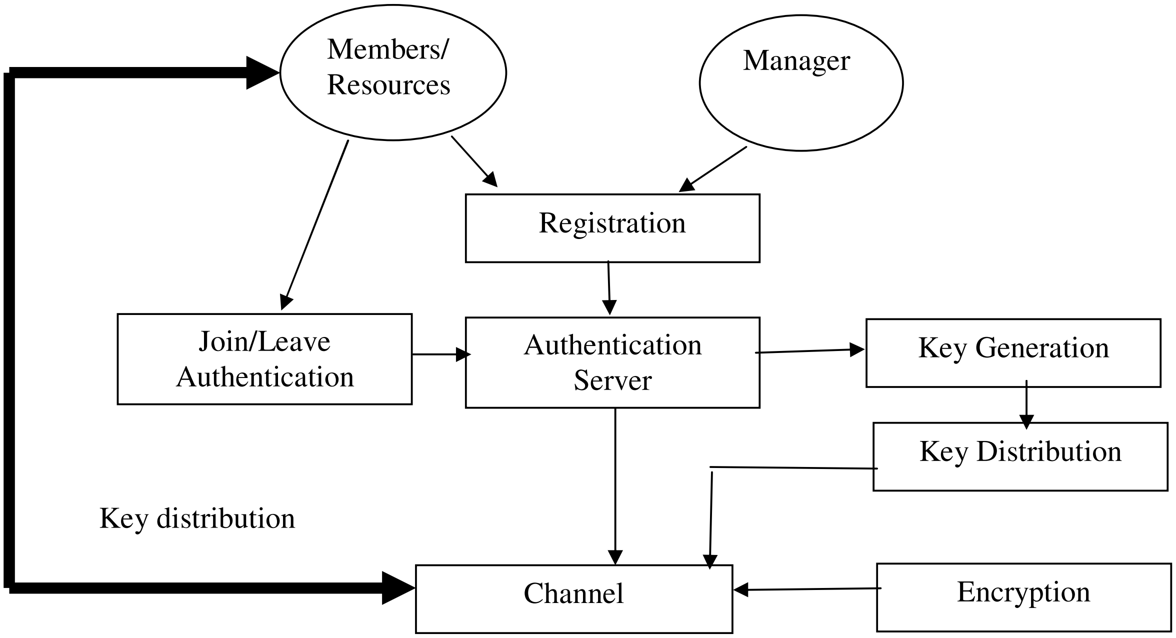

FIGURE 1: System Architecture

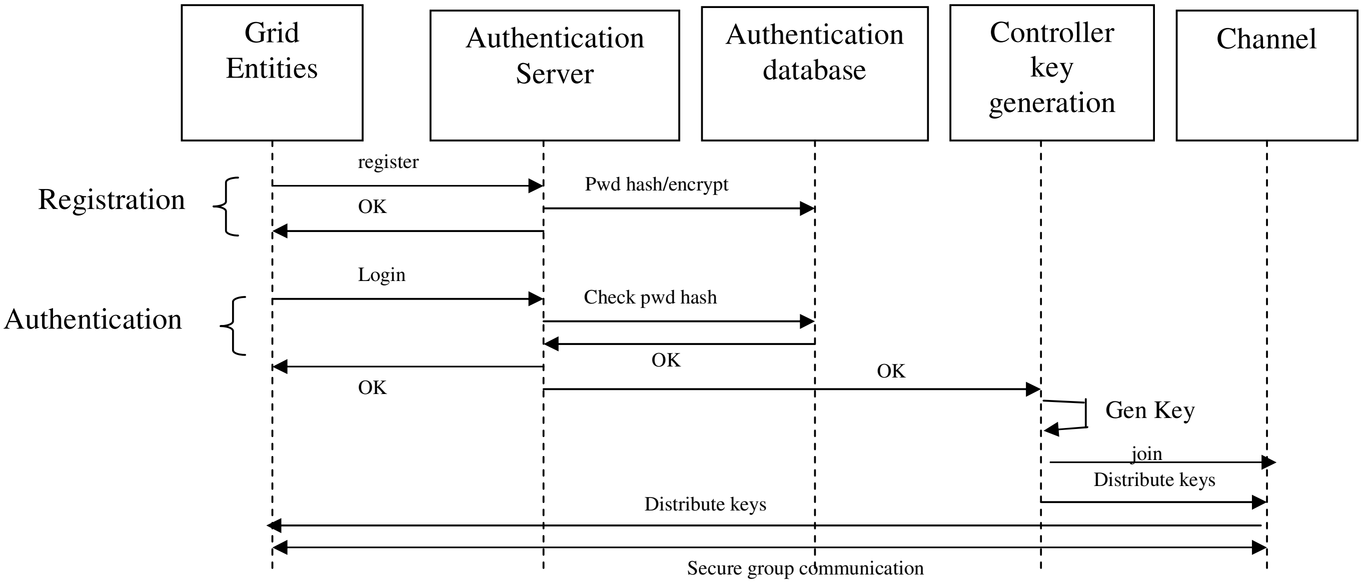

FIGURE 2: Process of secure group communication

The entire process consists of two major activities – authentication and key distribution for secure group communication. These activities are described in the following paragraphs.

2.1. Authentication Process:

The block diagram illustrating the registration process of the users is depicted in the Figure 3. Users who require services from the VO register using their username and password. The hash value of the password is calculated using Message Digest (MD5) algorithm and the encrypted password is stored in the authentication file.

The user who wants the services of VO has to login 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 hash value of the password and compares it with the decrypted value maintained in the authentication file. If the user is a valid user then the authentication server allows the user to join the channel and distributes the encryption key to the user.

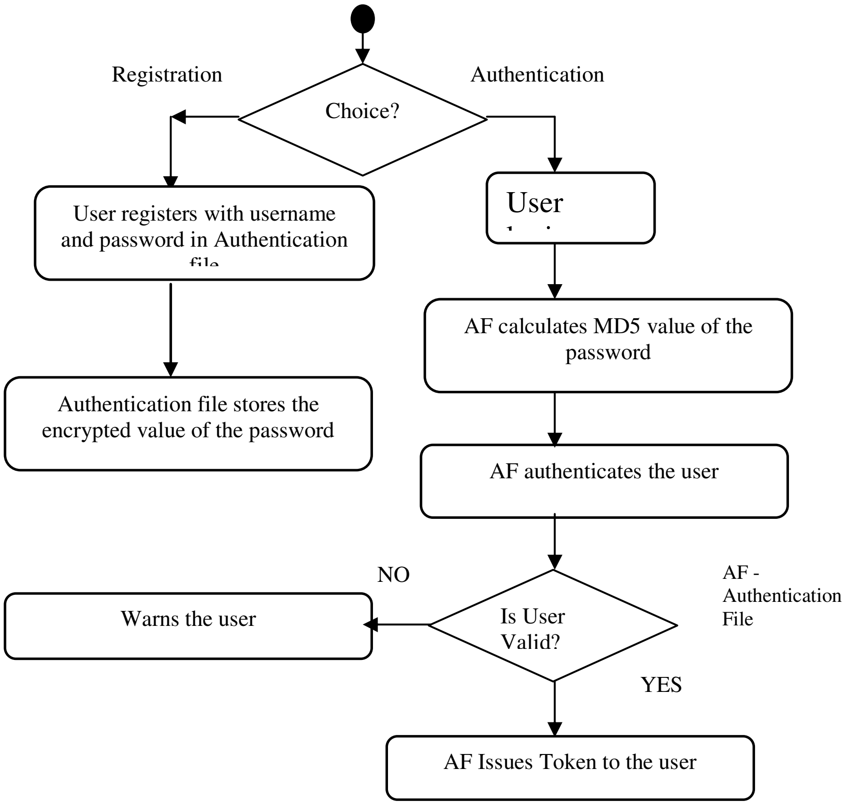
Registration
Authentication
Choice?
User registers with username and password in Authentication file
User
AF calculates MD5 value of the password
Authentication file stores the encrypted value of the password
AF authenticates the user
NO
AF - Authentication File
Warns the user
Is User Valid?
YES
AF Issues Token to the user

FIGURE 3: Authentication Scheme

2.2. Key Distribution And Secure Group Communication:

Confidentiality in information transfer in a distributed system is enabled by encrypting the information. Keys should be distributed securely among the members of the group. In existing approaches, each member shares a secret key with the group controller. If the information is to be transferred to ‘n’ members, ‘n’ encryptions followed by ‘n’ unicasts are needed. The computational complexity of the existing approach is overcome by using encoded session keys. Hence the proposed approach uses only an encoding followed by a multicast operation. This leads to reduced computation and provides efficient group communication. Further, the proposed approach ensures dynamic and secure group communication, forward secrecy and backward secrecy. The encoded key is used to manage member join, leave operations and for group communication. The security of the communication is achieved using one-way hash function to maintain integrity and encryption for confidentiality. Since a key is maintained for each channel/group, secure group communication is facilitated. The computation time of the key distribution is fast when compared to the key distribution by traditional algorithms like AES.

MD5 is used to generate the message digest. MD5 verifies data integrity by creating a 128-bit message digest from a message of arbitrary length. It can be used for digital signature applications, where a large file must be compressed in a secure manner before being encrypted using a public-key system. Steps in MD5 approach is listed as follows.

1) Arbitrary length message is padded with a '1' followed by '0's, so that its length is congruent to 448, modulo 512.
2) Then the length of the message (64 bits) is appended to it.
3) The MD5 algorithm uses four 32-bit state variables. They are initialized with constant values. These variables are sliced and diced to form the message digest.
4) 512-bit message blocks are used to modify the state in 4 rounds. Each round has 16 similar operations based on a non-linear function *F*, modular addition, and left rotation. Function F is different for each round. At the end of 4 rounds, the message digest is formed from the state variables. The message digest is then encrypted using Data Encryption Standard (DES) algorithm [19] and transmitted to its peer group member.

3. ANALYSIS

The analysis of the work has been done under the following heads:

3.1. Md5 Analysis:

The probability of two messages having the same message digest is on the order of 2^64 operations. The probability of coming up with any message having a given message digest is on the order of 2^128 operations. This ensures uniqueness of the message digest.

3.2. Replay attack:

Usually replay attack is called as 'man in the middle' attack. Adversary stays in between the user and the file and hacks the user credentials when the user contacts file. As key matching between the users is checked before file transfer and the information is encrypted before transfer, the probability of this attack is minimized.

3.3. Guessing attack:

Guessing attack is nothing but the adversaries just contacts the files 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 approach uses random generation of key, it is more difficult to guess the password.

3.4. Stolen-verifier attack:

Instead of storing the original password, the verifier of the password is stored. As the encrypted hash value of the password is stored, the proposed protocol is also more robust against the attack.

.

4. RESULTS AND DISCUSSIONS

Sl. No	Username	Password	Hash value
1	user1	admin	4c56ff4ce4aaf9573aa5dff913df913d
2	user2	Test2	Dfg45f4ce4aaf9573aa5dff913df913e
3	user3	test5	dddd6ffsdfdfdffffff913df997art567fg
4	user4	test8	4c56ff4ce4aaf9573aa5dff913df913d
5	user5	test10	sfggce4aaf9573aa5dff913df913fget

TABLE 1: Authentication File with unique hash value of passwords

The proposed authentication and distribution of channels has been implemented and tested on Globus middleware. It 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 using their username and password (Table 1). The authentication server stores the encrypted hash values of the passwords. As the hash values of the passwords are different, it ensures uniqueness.

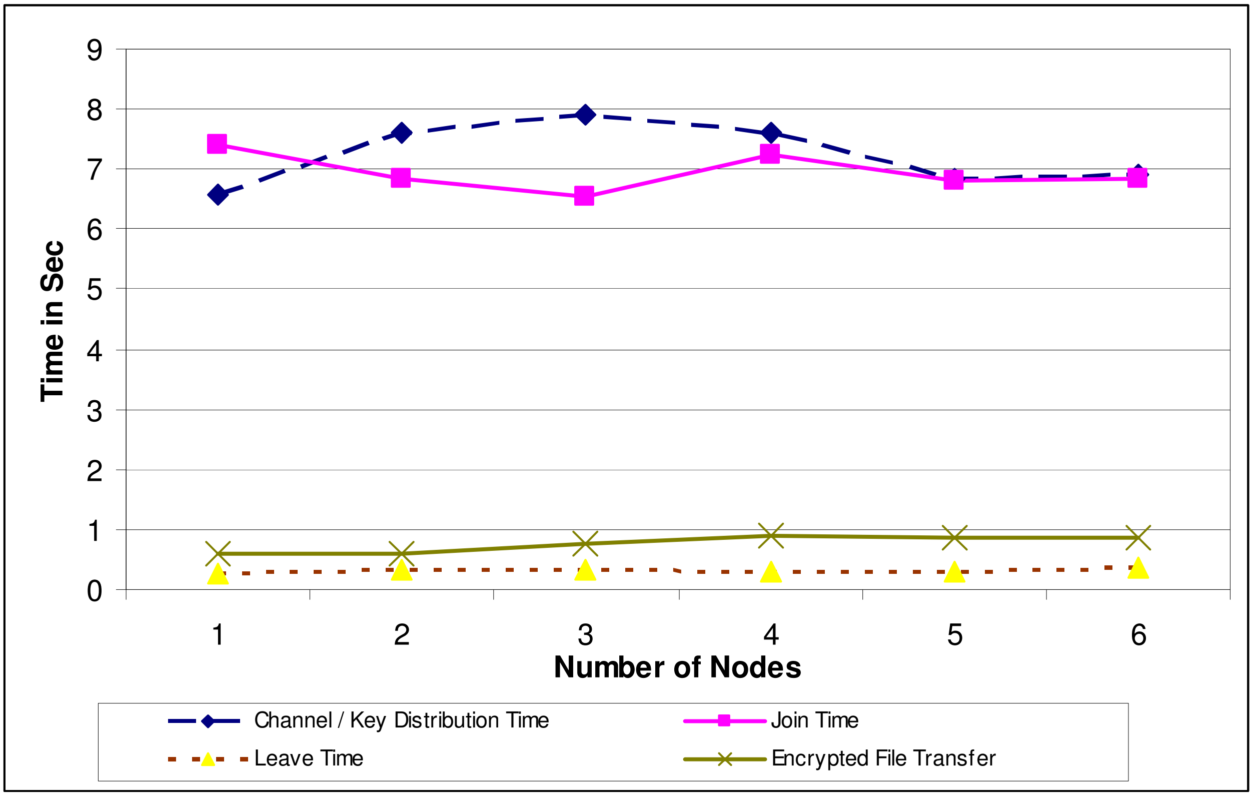

FIGURE 4: Experimental Results

Users join in the distributed channels across multiple machines in the grid. Once authenticated, key distribution and secure file transfer takes place. Figure 4 shows that the key distribution time and time for node join/leave remains almost a constant, irrespective of the number of nodes, incontrast to the hierarchical approach. Once the user joins the channel, secure file transfer occurs by encryption the information and multicasting it to the group members. Hence file transfer time also remains a constant in contrast to the unicast approach.

5. CONCLUSION

Grid Computing enables virtual organizations, to share geographically distributed resources. This paper proposes an effective approach for authentication and key distribution to ensure secure group communication in the grid environment. As the interpreted and distinct form of user credentials are maintained in the authentication files, there is very less chance to reveal the user credentials to the adversary. The implementation of our authentication protocol showed its effective performance in pinpointing the adversaries and paving the way to valid users to access resources in the VO by establishing as efficient computational channel distribution. Finally it is worth fit to host this scheme as a service in globus , also this basic scheme simply reduces computation complexity by replacing cryptographic encryption and decryption operations. Computation complexity further reduced by using algorithms like SHA , RIPEMD , IDEA .

6. REFERENCES

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

[2] 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.

[3] I.Foster, “Globus Toolkit Version 4: Software for Service-Oriented Systems,” in the proceedings of the IFIP International Conference on Network and Parallel Computing, vol .1 ,pp. 11-33, 2004.

[4] 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.

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

[6]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.

[7]Yuri Demchenko, “Virtual organizations in computer grids and identity management”, Information Security Technical Report, vol.9, no. 1,pp.59-76, January-March 2004.

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

[9]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.

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

[11]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.

[12]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.

[13]Gudgin, M., Hadley, M., Mendelsohn, N., Moreau, J-J. and Nielsen, H.F. (2003) SOAP Version 1.2 Part 1: Messaging Framework. W3C Recommendation, Available at http://www.w3.org/TR/soap12-part1/ (accessed on June 2003).

[14] Eastlake, D. and Reagle, J. (Eds.) (2002) XML Encryption Syntax and Processing. W3C Recommendation, available at http://www.w3.org/TR/xmlenc-core/ (accessed on December 2002).

[15] Della-Libera, G. et al. (2002) Web Services Secure Conversation Language (WS-Secure Conversation). Version 1.0, available at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobspec/html/ws-secureconversation.asp (accessed on 2002).

[16] Li1, Y., Xu, X., Wan, J., Jin, H. and Han, Z. (2008) 'Aeolus: reconcilable key management mechanism for secure group communication in grid', 2008 IEEE Asia-Pacific Services Computing Conference.

[17] Li, Y., Jin, H., Zou, D., Chen, J. and Han, Z. (2007) 'A scalable service scheme for secure group communication in grid', 31st Annual International Computer Software and Applications Conference (COMPSAC 2007).

[18] Li, Y., Jin, H., Zou, D., Liu, S. and Han, Z. (2008) 'An authenticated encryption mechanism for secure group communication in grid', 2008 International Conference on Internet Computing in Science and Engineering.

[19] William M. Daley, Raymond G. Kammer,"DES", U.S. DEPARTMENT OF sCOMMERCE published in FIPS October 25, 1999.

[20] Sudha, G, Geetha J, "Secure communication between grid domains based on trust relationships and group keys", accepted in Int. J. Communication Networks and Distributed Systems, 2010.

[21] G Geethakumari, Dr Atul Negi, Dr V N Sastry ," RB-GDM: A Role-Based Grid Delegation Model", 2008 International Journal of Computer Science and Security (IJCSS) ,Volume :2 Issue: 1, Pages 61-72.

CALL FOR PAPERS

Journal: International Journal of Security (IJS)
Volume: 4 **Issue:** 1
ISSN:1985-2320
URL: http://www.cscjournals.org/csc/description.php?JCode=IJS

About IJS

Information Security is an important aspect of protecting the information society from a wide variety of threats. The International Journal of Security (IJS) presents publications and research that builds on computer security and cryptography and also reaches out to other branches of the information sciences. Our aim is to provide research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems.

IJS provides a platform to computer security experts, practitioners, executives, information security managers, academics, security consultants and graduate students to publish original, innovative and time-critical articles and other information describing research and good practices of important technical work in information security, whether theoretical, applicable, or related to implementation. It is also a platform for the sharing of ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community. We welcome contributions towards the precise understanding of security policies through modeling, as well as the design and analysis of mechanisms for enforcing them, and the architectural principles of software and hardware system implementing them.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJS.

IJS List of Topics

The realm of International Journal of Security (IJS) extends, but not limited, to the following:

- Anonymity
- Anonymity and pseudonymity
- Attacks, security mechanisms, and security service
- Code security, including mobile code security
- Authorisation
- Biometrics
- Cellular/wireless/mobile/satellite networks securi
- Authentication
- Public key cryptography and key management
- Confidentiality, privacy, integrity, authenticatio
- Cryptography and cryptanalysis
- Data confidentiality issues
- Data integrity issues
- Data recovery
- Database security
- Denial of service
- Denial of service attacks and countermeasures
- Dependability and reliability
- Design or analysis of security protocols
- Distributed access control
- Distributed and parallel systems security
- Electronic commerce
- Formal security analyses
- Fraudulent usage
- Information flow
- Information hiding and watermarking
- Intellectual property protection
- Intrusion detection
- Key management
- Multicast security
- Network and Internet security
- Network forensics
- Network security performance evaluation
- Non-repudiation
- Peer-to-peer security
- Prevention of traffic analysis
- Privacy protection
- Computer forensics
- Revocation of malicious parties
- Risk assessment and management
- Secure location determination
- Secure PHY/MAC/routing protocols
- Secure routing protocols
- Security group communications
- Security in ad hoc networks
- Security in cellular networks (2G, 2.5G, 3G, B3G,
- Security in communications
- Security in content-delivery networks
- Security in distributed systems
- Security in domain name service
- Security in e-mail
- Security in high-speed networks
- Security in integrated networks
- Security in integrated wireless networks
- Security in internet and WWW
- Security in IP networks
- Security in mobile IP
- Security in optical systems and networks
- Security in peer-to-peer networks
- Security in satellite networks
- Security in sensor networks
- Security in VoIP
- Security in wired and wireless integrated networks
- Security in Wired Networks
- Security in wireless communications
- Security in wireless internet
- Security in wireless LANs (IEEE 802.11 WLAN, WiFi,
- Security in wireless MANs (IEEE 802.16 and WiMAX)
- Security in wireless PANs (Bluetooth and
- Security policies

IEEE 802.

- Security specification techniques
- Security standards
- Tradeoff analysis between performance and security
- Trust establishment
- Viruses worms and other malicious code
- WLAN and Bluetooth security

CFP SCHEDULE

Volume: 4
Issue: 2
Paper Submission: March 31 2010
Author Notification: May 1 2010
Issue Publication: May 2010

CALL FOR EDITORS/REVIEWERS

CSC Journals is in process of appointing Editorial Board Members for ***International Journal of Computer Security (IJS)***. CSC Journals would like to invite interested candidates to join **IJS** network of professionals/researchers for the positions of Editor-in-Chief, Associate Editor-in-Chief, Editorial Board Members and Reviewers.

The invitation encourages interested professionals to contribute into CSC research network by joining as a part of editorial board members and reviewers for scientific peer-reviewed journals. All journals use an online, electronic submission process. The Editor is responsible for the timely and substantive output of the journal, including the solicitation of manuscripts, supervision of the peer review process and the final selection of articles for publication. Responsibilities also include implementing the journal's editorial policies, maintaining high professional standards for published content, ensuring the integrity of the journal, guiding manuscripts through the review process, overseeing revisions, and planning special issues along with the editorial team.

A complete list of journals can be found at http://www.cscjournals.org/csc/byjournal.php. Interested candidates may apply for the following positions through http://www.cscjournals.org/csc/login.php.

Please remember that it is through the effort of volunteers such as yourself that CSC Journals continues to grow and flourish. Your help with reviewing the issues written by prospective authors would be very much appreciated.

Feel free to contact us at coordinator@cscjournals.org if you have any queries.

Contact Information

Computer Science Journals Sdn BhD
M-3-19, Plaza Damas Sri Hartamas
50480, Kuala Lumpur MALAYSIA

Phone: +603 6207 1607
+603 2782 6991
Fax: +603 6207 1697

BRANCH OFFICE 1
Suite 5.04 Level 5, 365 Little Collins Street,
MELBOURNE 3000, Victoria, AUSTRALIA

Fax: +613 8677 1132

BRANCH OFFICE 2
Office no. 8, Saad Arcad, DHA Main Bulevard
Lahore, PAKISTAN

EMAIL SUPPORT
Head CSC Press: coordinator@cscjournals.org
CSC Press: cscpress@cscjournals.org
Info: info@cscjournals.org

COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA