Enhancing Security in Distributed Systems Using Role Based Authentication Scheme

J. Jeyachitra
Research Scholar
Dept. of Computer Applications
School of Information Technology
Madurai Kamaraj University

Dr. K. Iyakutti
Professor
Dept. of Physics and Nanotechnology
SRM University
Chennai

Dr. K. Alagarsamy
Associate Professor
Dept. of Computer Applications
School of Information Technology
Madurai Kamaraj University

Abstract

Designing a distributed system with the uniqueness of consistency and responsibility is a significant issue. Yet one more imperative problem in the distributed system is the process to secluded system which can be attained based on setting the assured access rights, rules or authorization procedures. Security is the challenging task for distributed systems to take care of each and every nodes and packets for an effective data transmission. Several researches made a research on providing security to distributed systems in different levels. Noel De Palma et. Al., presented the design, the completion, and the assessment of a self-protected scheme which targets clustered dispersed applications. The approach is supported with the structural information of the cluster and of the dispersed applications. Even though it provides an easy way to protect the distributed systems from an unauthorized access and attacks, the approach does not support when distributed systems is designed with large number of nodes. To enhance the security of distributed systems, in this work, we plan to implement Role Based Authentication (RBA) scheme. The RBA scheme in distributed system has become the principal model for superior access

IJERT

control as it improves the security measure. It defines the user's limits and capabilities of making changes in distributed system and accessing various areas of the software recursively. While enhancing the security in distributed systems, the lifetime of the network will automatically increase. The experimental performance of RBA Scheme is evaluated with Solar Flare Data Set from UCI repository against existing non-parametric approach for network traffic classification to attain enhanced security and level of protection.

Keywords: Distributed systems, security, role based authentication scheme, principal model.

IJERT

1. INTRODUCTION

Security in computer systems is apprehensive with caring resources from illicit access even as making certain genuine requests can be contented all the time. The current development of computer systems equally in scale and difficulty facades remarkable organization confronts. Policy-based systems organization is a very talented resolution in this situation. It permits the disconnection of the rules that oversee the activities preferences of a scheme from the afforded functionality, and can be modified to grip a huge number of system essentials.

In the precedent two decades there have been numerous progresses in the ground of policy study. Even though the resolution in central systems is well-established, they do not effort virtually additionally in disseminated environments as of scalability, system partitions, and the heterogeneity of the endpoints. This exposition supplies to this attempt by suggesting three techniques to lecture to the difficulty of security strategy description and enforcement in large-scale dispersed systems. To properly implement service and security necessities from users who contain no close information of the fundamental systems, bring in the first dispersed strategy modification resolution that interprets high-level strategies into low-level realize able rules, for which the structure can be completely inferred by entity enforcement points.

Access control is a vital feature of a system's protection, and presents the foundation for all the other devices and measures the structure might operate. The growth of any access control scheme needs the subsequent two notions:

☞ An access control strategy that describes high-level rules consistent with which access control must be synchronized, and

☞ An enforcement method that gears the controls forced by the strategy employing software and/or hardware resolutions.

By specifying the huge number of system fundamentals administered in a dispersed environment, the access control method engaged must be scalable. The conventional method of selling with scalability at the individual level has been delegation of organization and designation of power. Thus it is not possible to preserve a middle policy manager for running all the system devices, which entails the requirement for incorporating and examining policies concerned by numerous policy authors to make sure that they are forever reliable and submissive with the universal security requirements.

IJERT

Network access control is apprehensive with changeable access to confined resource in a transportation network that fulfills with definite security policies. This access control provides the mechanisms for enhancing the lifetime of the network. But when the control on the network is done based on assigning roles for the users involved in the network communication, the system’s security will be high.

The paper is organized as follows. The section 2 describes the related literatures appropriate to the security in distributed systems. Section 3 describes the entire process of RBA scheme for enhancing the security in distributed systems. Section 4 and 5 describes the experimental evaluation and the performance analysis of the proposed RBA scheme and the existing self protection scheme in clustered distributed systems.

2. LITERATURE REVIEW

The complexity of today’s dispersed computing surroundings is such that the presence of bugs and safety holes is statistically inescapable. A very endowed technique to this topic is to perform a self-protected system [1] which refers to the capability of a structure to defend itself next to intrusions, i.e., notice them and scrap them back. The author measured that the hardware surroundings is composed of a collection of machines planned through a local area network with an Internet access by means of a router.

Anomaly disruption appreciation tries to blot imbalanced behavior of the system by probing the normal actions of the organization (in its place of attacks). The system can be routed and any disobedience is marked. Previous work [2] represented and recognized events appropriateness at the altitude of structure calls. Current processes of anomaly-based appreciation can be recognized in [3].

Expansion of secured and reliant dispersed systems is a serious research subjects. The paper [4] is a bequest processing the summarization of effort accepted out in this area in addition to recognizing novel research lines. Numerous techniques concerning security features in dispersed systems have been conferred, like substantiation based techniques, improvement of reliant based representations, access control based approaches, etc. A summarization of these issues is given in conclusion section.

As part of the safety inside dispersed systems, a variety of services and resources require defense from illegal use. Remote substantiation is the most normally used technique to decide the individuality of a distant client. The paper [5] examined a systematic technique for validating clients by three issues, specifically password, smart card, and biometrics. A general and safe structure is presented to improve two-factor substantiation to three-factor certification.

IJERT

The paper [6] presented an sufficiency and safety assessment of electric power allocation schemes with dispersed generation. For this achievement, bulk power system sufficiency and safety assessment ideas are modified to allocation scheme applications. But the assessment does not hold up mutual discrete-continuous reproduction representation which imitates the allocation system action. In [7], the authors presented a simulations-based expression of a mixture electricity market that unites the dispersed competitive compensation of decentralized markets with the system safety guarantees of central markets.

The author in [8] proposed a threshold proxy re-encryption system and combines it with a decentralized removal system such that a safe dispersed storage space system is devised. The distributed storage space system not only ropes safe and vigorous data storage and repossession, but the data in the storage space servers does not hold up with the user with no data back to the database. In [9], the author presented CAMRIT, a Control-based Adaptive Middleware structure for Real-time security service in distributed embedded systems. The paper [10] presented a federation proofs-based substantiation procedure (GUPA) to speak to the security subject for numerous readers and tags immediate classification in disseminated RFID syst ems. The dispersed creation (DG) has turn out to be a necessary and crucial part of such sharing systems from both an ecological and an energy safety viewpoint [11]. But the sharing systems do not give appropriate secure load balancing over the network.

IJERT

To enhance the security in distributed systems, Role Based Authentication (RBA) scheme is presented in distributed system has become the principal model for superior access control as it improves the security measure. The RBA scheme assigns set of roles to the users in distributed system by setting the limits and the capabilities of the system.

3. PROPOSED METHODOLOGY

In this work the proposal of the Role Based Authentication Scheme is implemented mainly for Security purpose developed at the distributed systems. The RBA scheme works based on deployment of commercial different software applications that considerably enlarges the user’s limits and capabilities and accessing various areas of the software recursively. The RBA incorporates the ease of use of existing online security self-clustering approach. RBA scheme is a superior model for access control which has existed as a concept for security measure. It has been so deviously stated that the discernment of access control has been around for a very long time, both deliberately and unintentionally. The architecture diagram of the proposed RBA scheme is defined in fig 1.

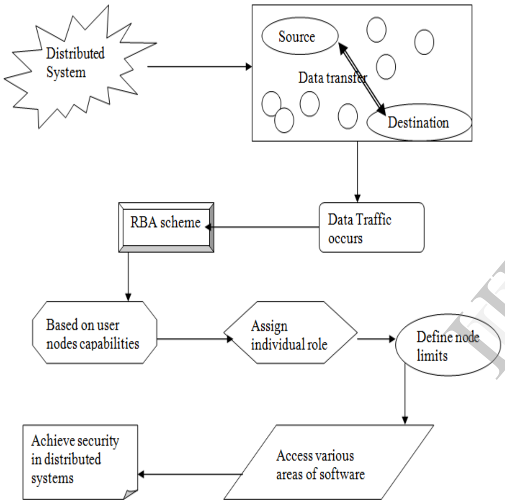

Fig 1 Architecture diagram of the proposed RBA scheme

From fig 1 it is being observed that the security of the distributed systems is achieved based on the role based authentication scheme. The RBA scheme assigns an individual role to each of the nodes in the network based on its task in the network system. The assignment of the role is done based on identifying the capabilities of the users and the nodes and assign limits to the nodes task to avoid the network traffic. BY assigning the limits, the systems have the ability to access various areas of the software recursively.

The security measures are normally discussed while constructing the distributed system which are used to protect the network from third party attacks. It provides numerous set of security access and managing users in distributed system. The framework of RBA scheme systematically identifies the RBA implementations standards.

IJERT
IJERT

System model

The presentation of the distributed systems is as follows. Assume a set of number of nodes N which are associated by a network where every node in the network comprises a set of resources. Each task arrived to a set of nodes could either arrived from outside or from other nodes in the network. All nodes in the network should assign the same average arrival rate of tasks from the network. Identify the set of users for requistion of nodes and packets in the distributed network.

☞ Nodes of the distributed system are efficiently sorted from 1 to N, where N is the total number of nodes in the distributed system. Assign id to each set of node in the system.

☞ Associate the nodes using the broadcast network and the processing gap of communication for two nodes is the same.

☞ Each node in the network has utility task T referrred as T_n.

☞ Identify the number of users in the network

☞ Set some tasks to each of the user in the network for an effective communication

☞ Analyze the users' transmission and the packet delivery to the destination node in the network.

Role based authentication scheme in Distributed systems

A role-based authentication is a scheme which controls the system access to authoritative users. Within a network, roles are assigned based on the users' utilities and their appropriate tasks. To achieve the defined operations for the users in the network, specific roles are assigned. Users with particular roles and role assignments obtain the appropriate section permissions to achieve reliable data transmission in the distributed systems. Managing the individual user turn out to be an issue of assigning proper roles to the user's report; this make simpler the process of adding a new user node, or moving the node to another set of classified network. The essential view of RBA scheme is that the access permissions are assigned based on the user roles, and users are directorially allocated to proper roles. RBA scheme make sure that only approved set of users are provided access to definite data or resources. In RBAC, a role is a task in the framework of a distributed system with a related semantics concerning its ability and task.

IJERT

There are some crucial rules are defined for RBA scheme which is defined as:

☞ Assigning role to user

☞ Authorizing the role

☞ Permission authorization

The first rule describes the process of assigning the certain limits to the set of user nodes in the network. The second rule describes the process of defining the cross boundaries amongst the nodes in the network. So, the user node should not cross the specific boundary assigned into it. The third rule describes the boundary limit depicts that it will allow only the nodes which has an authorization to perform the distinct operations in the distributed systems. Through the RBA scheme, the entire distributed systems are well administered with the set of user policies and node authentication for packet transmission.

Enhancing security in distributed system using RBA

The distributed system is fully designed with each set of individual users with the roles as independent with each other. The task of the individual set of nodes are assigned with the administrative roles comprises the associations to other roles. These relationships comprise the procedures among the user related roles and when and how they can process common set of resources. Thus, the RBA scheme in distributed system framework recognizes for a role position (Fig 2):

i) Access control and policies related to the individual set of users,

ii) Form a communication network among each set of user roles in the network

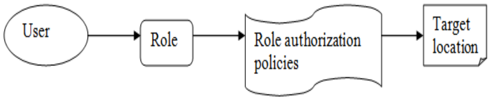

Fig 2 user role assignment

Based on different set of user roles, it granted access to the set of lists which are maintained in the distributed systems. The lists are,

☞ Resource list which maintains a set of resources into which only the authorized set of users can access

☞ Service list maintains a list of services in which the user roles are defined and accessed.

☞ User role list maintains a list of resources and services into which the user roles have granted access.

The assignment of user role relation sustains all the associations between users and roles and it consists of

☞ user name,

☞ Number of data packets,

IJERT

- ☞ the actual role and
- ☞ the assigned role.

Where the user name represent the name of the user, the total numebr of data packets which are ready to send thorught the network, actual role describes the assigned limits of the resource utilization in the network, assigned role describes the required resources needed to process the specified tasks.

When more numebr of data requesting the same set of resourcesw in the distributed system,t he data traffic occurs. With the traffic engineering principles, the data traffic are organized and analyzed. To secure the data in the data traffic, the assigned user roles will analyze the data traffic and its limits and redundancies in the traffic queue. This is identified based on each user role in the specified agent.

Consider a distributed systems which has a set of nodes N= {n1, n2,..,nn} with a set of resources as R = {r1, r2,…, rn}. If more number of nodes requests the same set of resources in a resource pool, then there a situation with data traffic occurs. That time with the implementation of traffic engineering principle, the traffic is organized. But there is a chance of data in the traffic gets unauthorized access from the unauthorized users. For that, a role has been assigned to all set of users who are all roaming around the network. The users in the distributed systems are assigned with the set of individual roles to protect the data in the traffic roles are assigned as supervisor, analyzer, Evaluator.

The supervisor user role will supervise the distributed system by identifying the entry of any new node/ unauthorized access in to the data transfer. The analyzer user role will analyze the user requests waiting in the queue which leads to data traffic. The Evaluator user role will evaluates the user requests present in the queue and directs the requests to the appropriate target location in the distributed systems. Based on these set of user roles in the distributed systems, the security for data packets is achieved.

At first, the supervisor supervises the set of users and the requests in the network. After supervising the set of resources in the

IJERT

system, it will check whether the resources are accessed and processed with the assigned tasks or not. If it processed well, the supervisor set the resources assigned value as positive. If it does not process well, then the negative state of the resource assignment is set.

Then the analyzer analyzes the set of assigned tasks and actual roles of users in the system. It will check with the distributed systems based on the set of assignment of tasks and the users. Based on the examination of set of assigned tasks for the respective user role, the implementation of the tasks with the user is assigned with it. Then the evaluator evaluates the data packets of the assigned set of users. So, based on the diverse set of user roles, the user requests in the traffic is analyzed and processed. The below algorithm describes the process of RBA scheme in distributed systems for effective data transfer.

// Algorithm

```
Assign U as a set of users
NewU is the new user and ExisU is the existing user
R is the role assigned to the user
L is the limit given to the users U for security purpose
Perm is the permission given to the set of users U
Begin
        If NewU enters into the network
            Identify the L assigned to the user
            If (L=1)
                Continue to process
                Exit
            Else
                Abort the user requests
        End If
        For each users U
            Identify the R (U)
        End For
        If R (U) has authorized set of packets
            Permit the user to its assigned limits
        Else
            Check with the limits of the actual assigned tasks
        End If
End
```

IJERT

At first, the RBA algorithm check the user's needed things that is number of resources it needed to access the network. Then the RBA scheme examines the limits and capabilities of the user based on which it will allow the nodes to access the set of resources in the resource pool. If the user properly provided the limits to the distinct user, then the RBA scheme permits the user to obtain permission for accessing the nodes and data packets in the distributed systems.

EXPERIMENTAL EVALAUTION

Experimental evaluation is done to estimate the performance of the proposed Role Based Authentication (RBA) scheme in distributed system. Experiments are conducted with the Solar Flare Data Set from UCI repository against existing non-parametric approach for the process of enahncing the load distribution system.

The description of solar flare data set is defined as follows (Table 1):

The solar flare database contains 3 potential classes, one for the number of times a certain type of solar flare occurred in a 24 hour period. Each instance represents captured features for 1 active region on the sun. The total number of instances used here are 323 and second set of data instances are measured to be 1066. The total number of attributes used here are 13 with 3 set of class attributes.

Table 1 Details of solar flare dataset

Dataset name	No. of instances	Total no. of attributes	No. of class attributes
Solar flare dataset	323, 1066	10	3

IJERT

The values of the attribute information are described in the subsequent table (table 2).

Attribute	Values
Code for class	(A,B,C,D,E,F,H)
Code for largest spot size	(X,R,S,A,H,K)
Code for spot distribution	(X,O,I,C)
Activity	1-reduced, 2-unchanged
Evolution	1-decay, 2 – no growth, 3 - growth
24 hour flare activity code	1-nothing as big as an m1, 2- one M1
Historically complex	1-yes, 2- No
Area	1-small, 2- large
Area of the largest spot	1 = < =5, 2 = >5

Table 2 Attribute description

From all these predictors three set of flare classes are predicted, which are represented in the last three columns.

C - Common flares - Class flares production in 24 hours;
M - Moderate flares - Class flares production in 24 hours;
X - Severe flares - Class flares production in 24 hours;

With these set, the experiments are conducted to estimate the performance of the proposed quality engineering scheme. The performance of the proposed Role Based Authentication (RBA) scheme in distributed system is measured in terms of enhanced security and level of protection.

IJERT

Enhanced security is measured in terms of rate at which the set of users are entered into the network under the control of authentication and access control in distributed systems. Security in the distributed systems attains high in rate since the RBA scheme provides the limits and capabilities of the user for providing the secure route path over the network.

Risk reduction rate measures the rate of risks obtained while transmitting the packet data provided by the RBA scheme and to measure the effective communication among the nodes in the network. The protection level describes the process of measuring the level of security in each node in the network.

RESULTS AND DISCUSSION

RBA scheme in distributed system is compared with the existing self protection scheme in distributed systems in measuring the rate of security, level of protection and efficiency. The below table and graph describes the performance of the proposed RBA Scheme in distributed systems and existing self protection scheme in clustered distributed systems.

Number of users	Security (%)	
	Proposed RBA scheme	Existing self protection scheme
25	56	45
50	63	49
75	69	54
100	72	61

125	78	68
150	82	73

Table 5.1 number of users vs. security

The security of the users' data is measured based on the number of users in the distributed systems. The value of the proposed RBA scheme is compared with the existing self protection scheme is illustrated in table 5.1.

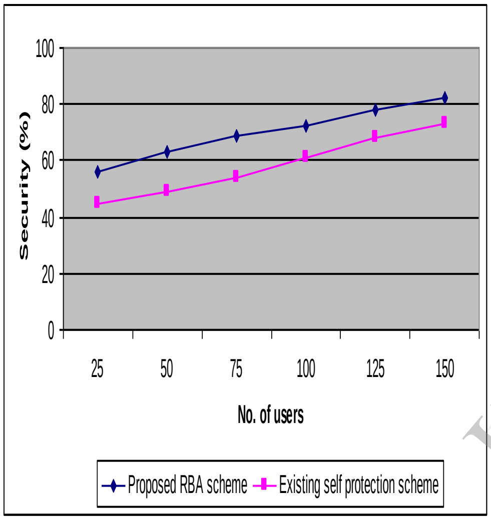

fig 5.1 number of users vs. security

Fig 5.1 describes the security level of the users and their appropriate data in the distributed systems. Compared to the existing self protection scheme, the proposed RBA scheme provides high level of security. Since the RBA scheme assigns role for the set of users involved in the distributed systems, the limits are known to all the participants. The participants in the distributed system do not exceed the boundaries assigned to it. So the chance of loss of packets in the distributed systems is less. But the existing self protection scheme mitigates only the configuration of the security components of the system. The variance in the security level is 10-13% high in the proposed RBA scheme.

IJERT

Number of users	Risk reduction rate (%)	
	Proposed RBA scheme	Existing self protection scheme
25	45	65
50	53	69
75	58	73
100	64	76
125	70	79
150	75	82

The risk reduction rate is measured based on the number of users in the distributed systems. The value of the proposed RBA scheme is compared with the existing self protection scheme is illustrated in table 5.2.

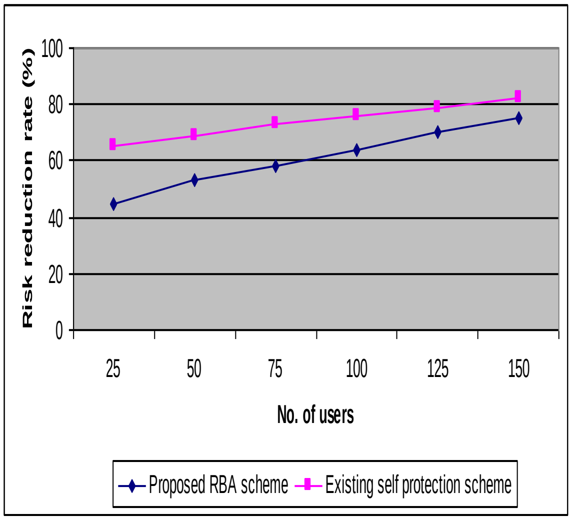

Fig 5.2 number of users vs. risk reduction rate

Fig 5.2 describes the risk reduction rate measured based on the number of users in the distributed systems. Compared to the existing self protection scheme, the proposed RBA scheme provides less risk reduction rate. Since the security in the RBA scheme is high, the chance of occurrence of risk while transferring the data is less. Because, each users in the distributed system is assigned with an authenticated role for the purpose of transferring the data from source to destination, so the assigned role users checked with the appropriate data transfer information. The variance in the risk reduction rate is 8-11% less in the proposed RBA scheme.

Number of users	Efficiency (%)	
	Proposed RBA scheme	Existing self protection scheme
10	62	25
20	66	31
30	72	36
40	77	42
50	82	46
60	85	52

Table 5.3 number of users vs. efficiency

The efficiency of the security appliance is measured based on the number of users involved in the distributed systems. The value of the proposed RBA scheme is compared with the existing self protection scheme is illustrated in table 5.3.

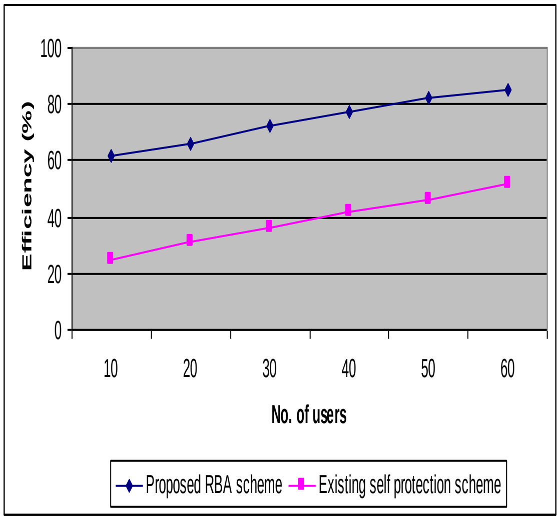

Fig 5.3 number of users vs. efficiency

IJERT

Fig 5.3 describes the efficiency of the security appliance is measured based on the number of users involved in the distributed systems. Compared to the existing self protection scheme, the proposed RBA scheme provides high efficiency. Because the RBA scheme provides high level of protection to the users by assigning individual role and lessens the risk of entering unauthorized access to the users. The variance is 17-20% high in the proposed RBA scheme.

Finally, it is being observed that the RBA scheme provides high level of security by implementing the Role Based Authentication Scheme (RBA) in terms of assigning roles to the users for the purpose of secure data transfer in distributed systems.

CONCLUSION

In this paper, we presented the role based authentication scheme that provides the active distributed system environment and assignment of limits and capabilities to a user of the database. The RBA scheme vigorously amends the role and permission assignment supported with the environment and the access pattern of the user and mechanically checks with the user should persist its processes to database or not. Alternatively, it also checks that the secure data transfer among the specified route path over the distributed system. Compared to the existing self protection scheme, the proposed RBA scheme is evaluated in terms of security level, risk reduction rate and efficiency. The performance results revealed that the proposed RBA scheme provides high level of security and efficiency by lessening the occurrence of risk done by unauthorized users in the distributed system.

IJERT

REFERENCES

[1] Noel De Palma, Daniel Hagimont, Fabienne Boyer, and Laurent Broto, ‘Self-Protection in a Clustered Distributed System’, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 2, FEBRUARY 2012

[2] D. Mutz, F. Valeur, C. Kruegel, and G. Vigna, “Anomalous System Call Detection,” ACM Trans. Information and System Security, vol. 9, no. 1, pp. 61-93, Feb. 2006.

[3] S. Sicard, F. Boyer, and N. De Palma, "Using Components for Architecture-Based Management: The Self-Repair Case," Proc. Int'l Conf. Software Eng., 2008

[4] Vijay Prakash, Manuj Darbari, "A Review on Security Issues in Distributed Systems", International Journal of Scientific & Engineering Research Volume 3, Issue 9, September-2012

[5] Xinyi Huang et. Al., "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems", IEEE Transactions on Parallel and Distributed Systems, (Volume:22 , Issue: 8) , 2011

[6] Issicaba, D. et. Al., "Adequacy and Security Evaluation of Distribution Systems With Distributed Generation", IEEE Transactions on (Volume:27 , Issue: 3) Power Systems, 2012

[7] Ilic, M. et. Al., "Transmission pricing of distributed multilateral energy transactions to ensure system security and guide economic dispatch", IEEE Transactions on (Volume:18 , Issue: 2) Power Systems, 2003.

[8] Hsiao-Ying Lin et. Al., "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", IEEE Transactions on (Volume:23 , Issue: 6) Parallel and Distributed Systems, 2012.

[9] Xiaorui Wang et. Al., "Control-Based Adaptive Middleware for Real-Time Image Transmission over Bandwidth-Constrained Networks", IEEE Transactions on (Volume:19 , Issue: 6) Parallel and Distributed Systems, 2008

[10] Hong Liu et. Al., "Grouping-Proofs-Based Authentication Protocol for Distributed RFID Systems", IEEE Transactions on (Volume:24 , Issue: 7) Parallel and Distributed Systems, 2013

[11] Miyoung Kim et. Al., "Design of the Optimal ULTC Parameters in Distribution System With Distributed Generations", IEEE Transactions on (Volume:24 , Issue: 1) Power Systems, 2009.

IJERT