RESEARCH ARTICLE OPEN ACCESS

An Optimized System for Fault Tolerant Security Sensitive Distributed Applications

Binu.C.T
Freelancer

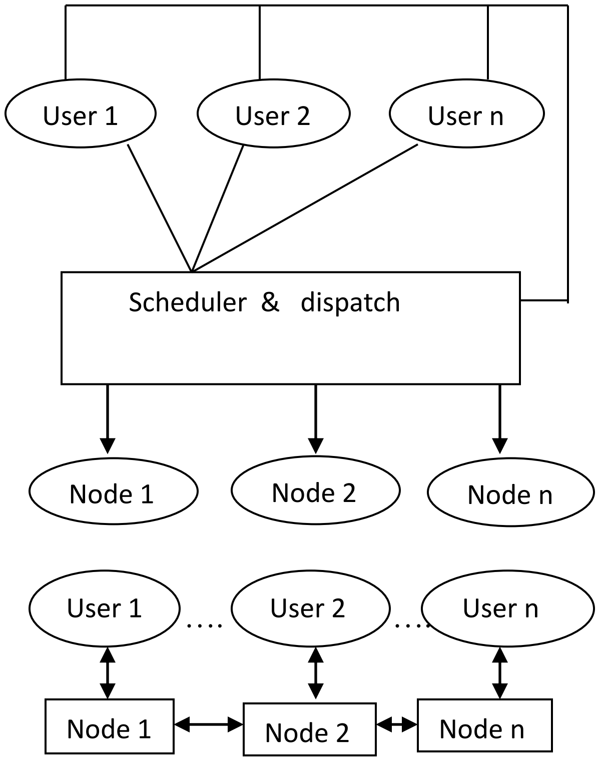
ABSTRACT

It's a challenge to develop a secure trusted distributed system. The necessity of security is very high in distributed computing. It's difficult to develop a scheduling algorithm which cover all the limitations of the system. The proposed system with a scheduling algorithm contain Fault Manager, Trust Manager and security Manager. The empty remote procedure call (RPC) connect with Fault manager to find the fault nodes in the system. Trust Manager with a new trust model helps map trust level in the system. The Security Manger with four levels and each level decides which security algorithms used to build the system. Each machine's ID is encrypted to provide confidentiality and authentication.

Keywords:- Fault tolerant, scheduling algorithm, heterogeneous distributed systems, intrusion, security level

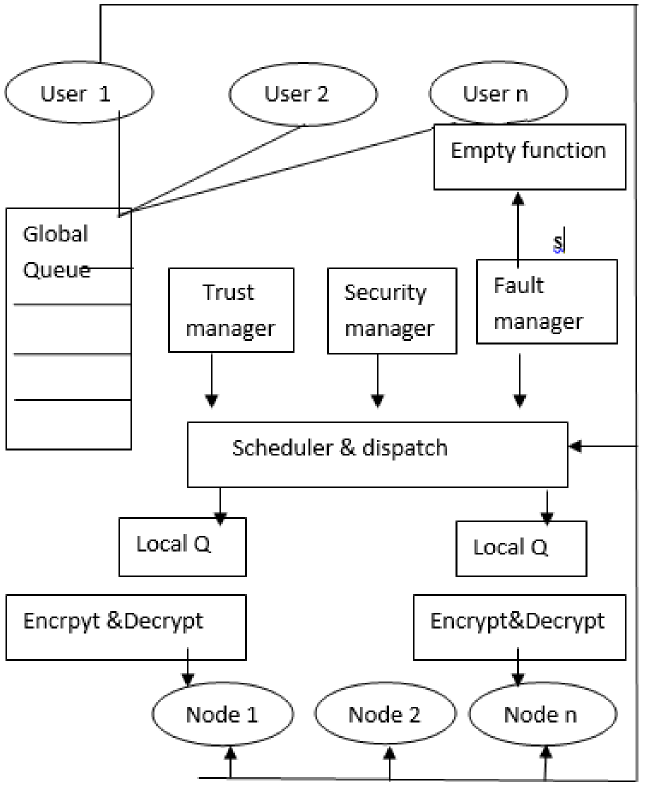
I. INTRODUCTION

5G is the next technology to boost high speed network. It helps to connect a collection of cost-effective, and possibly heterogeneous computers in the form of a computational system such as cloud, Grid, etc. Heterogeneous distributed systems (HDSs) consist of different collection of resources with different capacities and normally interconnected with the high speed networks to meet the requirements of applications. Over the last decade, HDSshave been emerging as popular computing plat forms for compute-intensive applications with various computing needs.Distributed systems are loosely coupled and less important to authentication . Here both the applications and users can cause security threats to the system. The security threats of the system caused by hackers to penetrate distributed systems very easily . Distributed System means connect more than system to do computation. There is lack of computation speed in normal systems. Hats the reasons why we are using distributed computing. There are different types of distributed systems are there named master slave distributed computing and peer to peer distributed computing. Security issue is the main limitation of peer to peer distributed computing. We can protect the system by using master slave distributed computing.



length. The Fault is the another issue in the distributed computing. The entire system collapse when the machine called node fails. So fault tolerance is another area tocover.The remote procedure call in the distributed computing helps to connect the master system with the nodes. The function names are residing in the slave system and the master system contains the definition. The request and acknowledge is a good technology to find the fault nodes in the system. But its takes more computation time and memory.We propose, design and evaluate a fault tolerant security sensitive scheduling system, which mainly includes, aTrust Manager, Fault Manager, Empty Function, Security Manager, Schedule Queue, Scheduler and Dispatch,Encrypt and Decrypt ID installed in HDSs. I have created a trust model formulated using a mathematical equation to calculate the trust level of each nodes in HDSs. I believe that the coordination of fault manager, trust manager and security manager with scheduler would provide a best system. The task in the system are of two types named dependent and independent task. This paper consider dependent tasks.

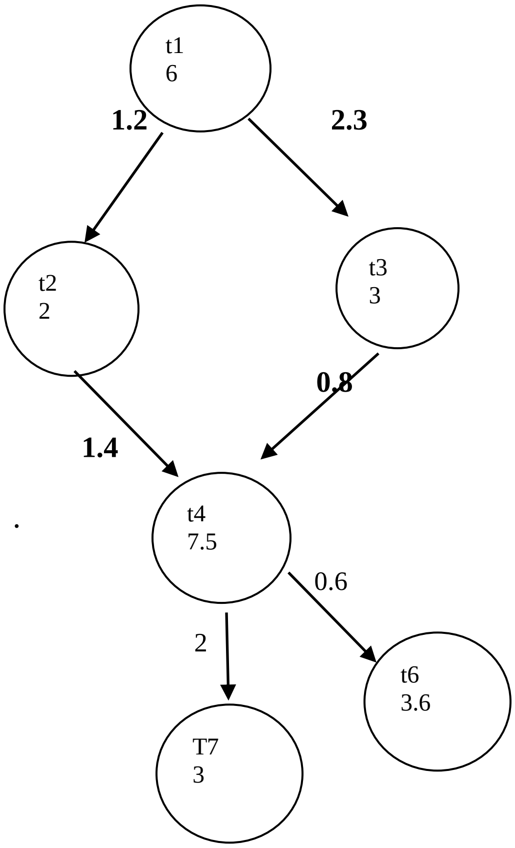
II. SYSTEM ARCHITECTURE



Optimized Fault tolerant Security Sensitive Distributed Architecture

Fault Tolerant Security Sensitive Scheduling Architecture

I propose fault tolerant securitysensitive scheduling architecture which includes the modules such as Trust Manager, Fault Manager, Empty Function, and Security Manager as depicted in Fig. 1. Trust Manager Module is used to find trust of each node in the system. Security threatsmainly include: individual malicious peers, malicious collectives, malicious collectives with camouflage, malicious spies, Sybil attack, man in the middle attack, partially malicious collectives and malicious pre-trusted peers.



(a)Inter dependent task& (b) Inter dependent processor

III. SECURITY AND TRUST

Definition of Trust

Def: Trust is a firm belief that the node do the task in right way at right time.

Trust Manager uses Trust Level of each node and connect it with Security Sensitivity.

Security Sensitivity SS=Cos (TL)

If TL=90 (Highest Trust Level value) then
SS=0
If TL=0 then
SS=1
Each node has priority similar to task priority.

If Trust level value is 45 have the highest priority
TL=46 have node priority 2
TL=44 have node priority 3
TL=47 have node priority 4
TL=43 have node priority 5 and so on

Definition of Security

Def: Security means intruders and their activities are blocked in the system.

Security Manager

It provides three types security services such as Confidentiality, Authentication and Integrity. I divide the nodes in the system into two groups. Group Family and Group Friends

D. 30% of the nodes are in Group Family and remaining 70% of nodes in group Friends. Family group have the higher priority than Friends.

E. We initialize TL=45 when a new node is entering into the system and dynamically updating its values.The value increasing after each computation without failure.The TL value decreases after each failure.

Tan inverse(x) is the equation to connect the Trust Level value.

Tan(45)=1

There are different types of faults named Operating system failure, Network failure, System failure etc. These faults cause failure of the system. There is the purpose of Fault Manager. The Fault Manager dynamically update the fault variable of each node to identify the fault. The Empty function in the system is called to each node. Itreturns the value zero to indicate that there is no fault. Otherwise it returns the value one to indicate that there is fault. When the Fault Manager identify the fault, itsends the scheduler to assign the task to high security machine.

Confidentiality means make the information secrete. Authentication means whether the user have right to access the information. Integrity means whether the information is correct.There are three levels of security with three types of security services.The three levels is based on Trust Level(TL/) value.The TL value 0 to 30 constitute Level1 Security.TL value 31 to 60 constitute level 2 Security .Finally TL value 61 to 90 constitute Level 3 Security.Each level have three types of security services named confidentiality,authentication and integrity.Three high secure confidentiality algorithms for each security level.Similarlly Three high secure authentication algorithms for each security level.Finally three high secure integrity algorithms for each security level.

Three Confidentiality Algorithms

- DES (Data Encryption Standard) — Uses an encryption key that is 56 bits long. This is the weakest of the three algorithms.
- 3DES (Triple-DES) — An encryption algorithm based on DES that uses DES to encrypt the data three times.
- AES (Advanced Encryption Standard) — The strongest encryption algorithm available. Fireware can use AES encryption keys of these lengths: 128, 192, or 256 bits.

Three Authentication Algorithms:

HMAC-MD5

MD5 produces a 128-bit (16 byte) message digest, which makes it faster than SHA1 or SHA2. This is the least secure algorithm.

HMAC-SHA1

SHA1 produces a 160-bit (20 byte) message digest. Although slower than MD5, this larger digest size makes it stronger against brute force attacks.

HMAC-SHA2

Three Integrity Algorithms:

Diffie-Hellman Key Exchange Algorithm

The Diffie-Hellman (DH) key exchange algorithm is a method used to make a shared encryption key available to two entities without an exchange of the key. The encryption key for the two devices is used as a symmetric key for encrypting data. Only the two parties involved in the DH key exchange can deduce the shared key, and the key is never sent over the wire.

A Diffie-Hellman *key group* is a group of integers used for the Diffie-Hellman key exchange. Fireware can use DH groups 1, 2, 5, 14, 15, 19, and 20.

AH(Authentication Header)

Defined in RFC 2402, AH is a protocol that you can use in manual BOVPN Phase 2 VPN negotiations. To provide security, AH adds authentication information to the IP datagram. Most VPN tunnels do not use AH because it does not provide encryption.

ESP(Encapsulating Security Payload)

Defined in RFC 2406, ESP provides authentication and encryption of data. ESP takes the original payload of a data packet and replaces it with encrypted data. It adds integrity checks to make sure that the data is not altered in transit, and that the data came from the proper source. We recommend that you use ESP in BOVPN Phase 2 negotiations because ESP is more secure than AH. Mobile VPN with IPSec always uses ESP.

VI. NODE ID ENCRYPT AND DECRYPT

Each node's ID is encrypted and send to each node from the master machine. The node decrypt and use for its own purpose. It makes more security to the distributed computing.

```
1. Compute the task priority(TP) till reach final task
2. Empty task has assigned highest priority
3.Sort the tasks into a scheduling list by
    non-increasing order oftask priority(TP)
4. While the scheduling list is not empty do
5. Remove eachtask $t_i$from the scheduling list
6.The variable Fault is initialized to zero
    6. for each node $p_j ϵ P$ do
    7. Compute BFT($t_{i,}p_j$)
    8.If empty task returns the fault variable as zero
    9.If verify pj from family group
    10.Assign task ti to the node pj ϵ P with BFT of ti
11.elsefamily group is empty then select Pj from Friends group
12.End
13.Else if fault=1
14. Compute BFT($t_{i,}p_j$)
15.Assign task ti to highest secure node
  16.End
```

The total time complexity of the Security Sensitive algorithm is :

$$O(n^2)+n\log(n)+\log(n)$$

VII. CONCLUSIONS

We believe that the fault tolerant security sensitive scheduling algorithm meets the security requirements of the system and providebetter performances

Future studies in this domain to rework the algorithm to improve the performance

We thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCE

[1] Tang Xiaoyong,Kenli Li,Zeng Zeng,Bharadwaj Veeravalli A Novel Security-Driven Scheduling Algorithm for Precedence Constr-ained Tasks in Heterogeneous Distributed Systems, IEEE Transactions on ComputersJuly 2011

[2] G. Theodorakopoulos and J.S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 318-328, Feb. 2006.

[3] T. Xie, X. Qin, and A. Sung, "SAREC: A Security-Aware Scheduling Strategy for Real-Time Application on Clusters," Proc. Int'l Conf. Parallel Processing (ICPP '05), pp. 5-12, 2005.

[4] Hyungsoo Jung, Hyuck Han, Hoen YYeom ,SooyongKang, Athanasia:A user transparent and fault tolerant Parallel Applications ACM/IEEE SC05

BINU C.T have completed Master of Engineering from S.A Engineering college Chennai. He have 3 years of experience in teaching and 2 years of experience as software Test Engineer. He would like to persue Phd in computer Science & Engineering