International Journal of Research in Engineering, Science and Management
Volume 4, Issue 4, April 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

A Major Issue: Data Security in Distributed System Environment

Brinda Jagadeesh[1*], Divya S. Naik[2]

[1,2]Department of Computer Science and Engineering, M. S. Ramaiah Institute of Technology, Bangalore, India

***Abstract*: Data needs to travel from the sender to receiver or might be stored at one place for instance storing the data in one's computer so in both the cases the data confidentiality and data integrity becomes the major concern. If the data isn't sent in bulk then the threats or vulnerabilities are less, but the intruder can try out all the possible way to change the environment of the system where here we consider the data stored in a distributed systems.**

***Keywords*: Data security, distributed system, distributed environment.**

1. Introduction

We here collectively explain about how crucial it is to look at data security in distributed system such that data is unaltered and made unavailable to the intruders by various algorithmic approach. Here some Encryption and Decryption techniques are also addressed.

2. Proposed Methods

The best method among the available processes that ensures security, confidentiality and also aims at low cost maintenance.

The threats addressed by the authors are-Interception, Interruption, Modification and Fabrication.

a) Interception->Unauthorized access to a distributed system.
b) Interruption->When the service is destroyed by intruder.
c) Modification->change of data by an unauthorized party.
d) Fabrication->additional data or work is done such that it is no more in normal state, then it is called fabrication.

Security solution suggested are encryption by Encryption of the key exchange protocol which uses both of Symmetric and Asymmetric cryptographs which is a password based key against security attacks.

Advantages: Authentication using password based authentication can in-turn obtain low cost maintenance.

Disadvantage: Intruder can work on all possible sets of password.

Access and control in distributed system is carried out by protection domain where the protection is defined by objects, access and rights. If there is an request for a process then there is an continuous monitoring of the objects.

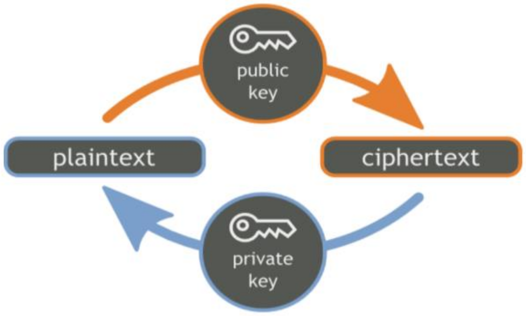
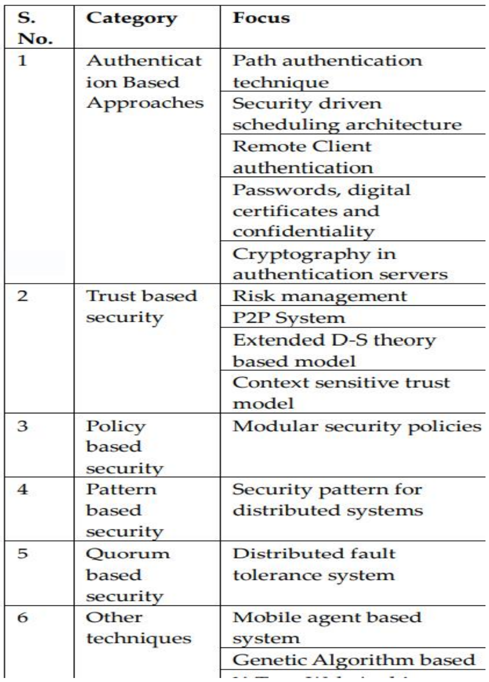


Fig. 1. RSA method

A. Comparative Analysis

Table 1
Comparative analysis



S. No.	Category	Focus
1	Authentication Based Approaches	Path authentication technique
		Security driven scheduling architecture
		Remote Client authentication
		Passwords, digital certificates and confidentiality
		Cryptography in authentication servers
2	Trust based security	Risk management
		P2P System
		Extended D-S theory based model
		Context sensitive trust model
3	Policy based security	Modular security policies
4	Pattern based security	Security pattern for distributed systems
5	Quorum based security	Distributed fault tolerance system
6	Other techniques	Mobile agent based system
		Genetic Algorithm based

The analysis addresses the security issues and challenges as,

i. Should take an approach such a way that its main goal is to provide security.

*Corresponding author: brindaja@gmail.com

ii. Should keep a track of systems activity.
iii. Develop security matrices.
iv. Techniques should be integrated like cryptography method for distributed data communication should be added.
v. Apply middleware in distributed security.
vi. Web services may also be added in security issues.

3. Literature Survey

Jai Pratap Dixit, Dr. Neelendra Badal, Dr. Syed Qamar Abbas-A Novel Approach Of Distributed Security Mechanism Of Data Distribution In Distributed Environment.

The aim of this paper is to,

i. Independently secured data distribution and transformation through mail.
ii. Security during data modification.
iii. Apply and investigate the web services in secure manner with different stakeholders and different number of available data.

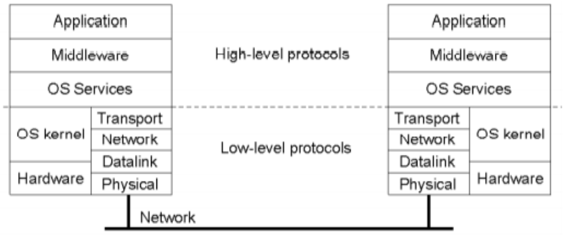


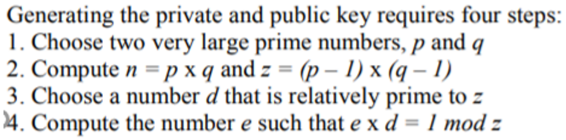
Fig. 2. Layers of security mechanisms

Issues with distributed environment:

i. Automated data security at data segmentation and it's compliment in secured way through Email.
ii. Security at middleware for distribution of data during modification.

A. *Algorithm Approach*

In this method we use updated algorithm of AES, which use specification for encryption of electronic data. Here we conceptually resemble the procedures followed for cryptography.



Generating the private and public key requires four steps:
1. Choose two very large prime numbers, *p* and *q*
2. Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$
3. Choose a number *d* that is relatively prime to *z*
4. Compute the number *e* such that $e \times d = 1 \bmod z$

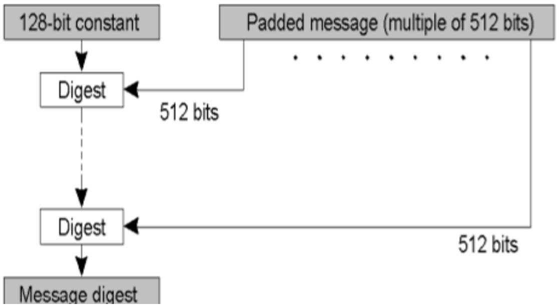


Fig. 3. Message digest process approach

Security at middleware use for data distribution during data compliment version. Generate the compliment approach such that the information is kept a secret within the algorithm to preserve the data.

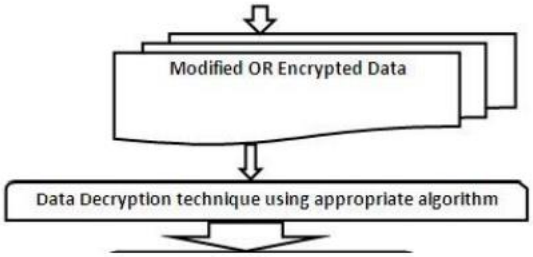
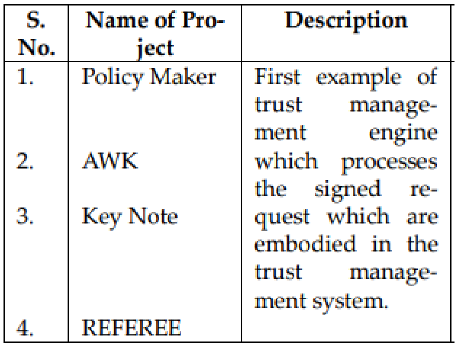

Modified OR Encrypted Data
Data Decryption technique using appropriate algorithm

Fig. 4. Data Modification Security technique

Table 2
List of Ongoing Trust Based Projects



S. No.	Name of Project	Description
1.	Policy Maker	First example of trust management engine which processes the signed request which are embodied in the trust management system.
2.	AWK	
3.	Key Note	
4.	REFEREE	

B. *Proposed Security Framework Based on Trust*

The major characteristics of the distributed system are; concurrency of components. As the distributed systems lack global clock. The rule-based systems the theoretical rules are applied to observe the reliability of the systems.

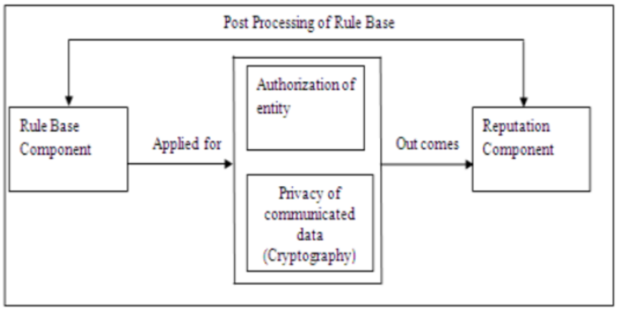


Fig. 5. Proposed security framework based on trust

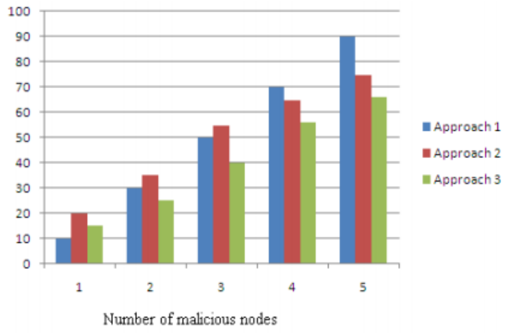


Fig. 6. Number of malicious nodes

The DNA based cryptographic approach mainly follows the rule based method. The application of the rule based is crucial for competitiveness of the distributive computation.

C. Implementation of Security in Distributed Systems

Distributed systems may also contain systems like grid computing environment, cloud environment and so on.

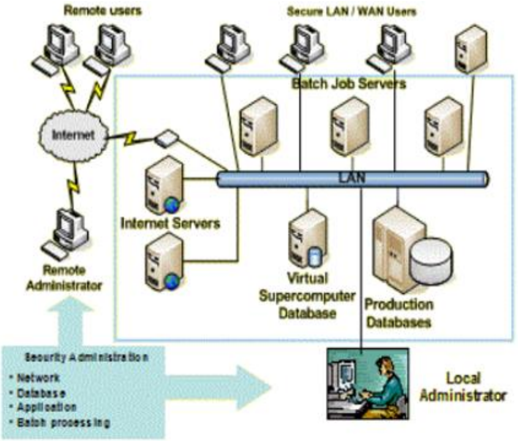


Fig. 7. Computing cluster

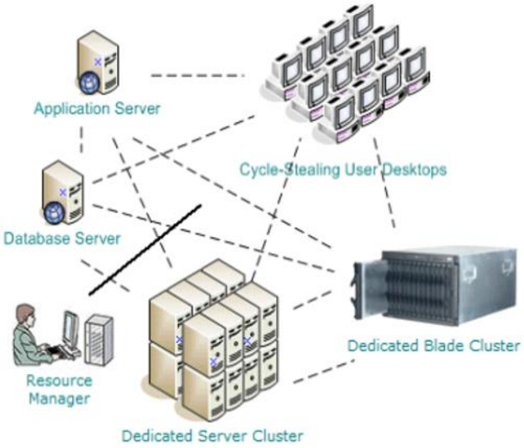


Fig. 8. Grid computing system

Security for Computing Clusters: The most common types of attacks on the clusters are either snooping or node to node attacks.

4. A Survey on Security Services and Mechanisms in Distributed Systems

The designer of the distributed systems should take care the design aspect, security aspect and confidentiality of the subject.

In developing a particular security mechanism, the design and confidentiality of the matter is the main criteria and many approaches such as algorithm approach or encryption or decryption or key exchange method can be implemented based on the number of the systems that are participating in the design.

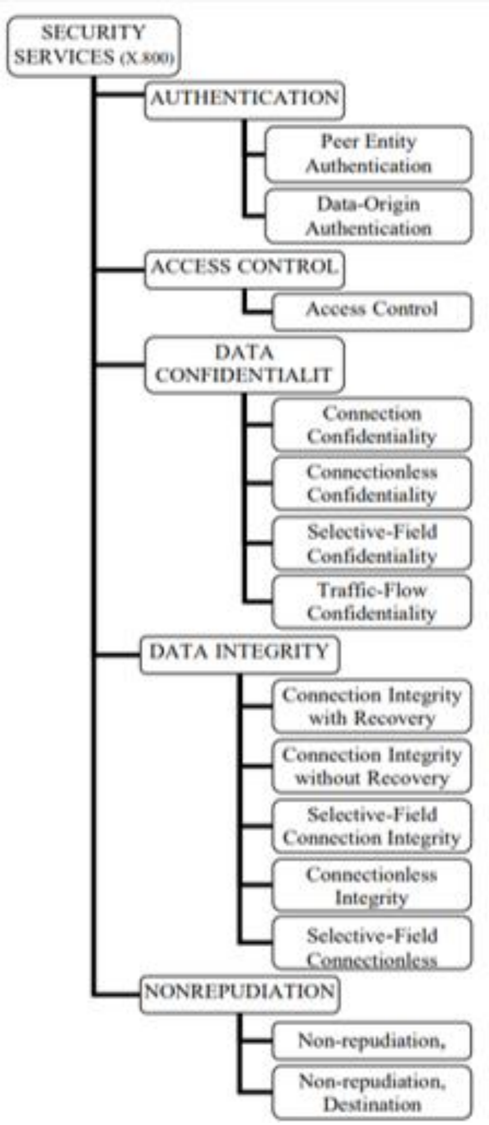

SECURITY SERVICES (X.800)
AUTHENTICATION
Peer Entity Authentication
Data-Origin Authentication
ACCESS CONTROL
Access Control
DATA CONFIDENTIALIT
Connection Confidentiality
Connectionless Confidentiality
Selective-Field Confidentiality
Traffic-Flow Confidentiality
DATA INTEGRITY
Connection Integrity with Recovery
Connection Integrity without Recovery
Selective-Field Connection Integrity
Connectionless Integrity
Selective-Field Connectionless
NONREPUDIATION
Non-repudiation,
Non-repudiation, Destination

Fig. 9. Security services (X.800)

5. Conclusion

Hence, to conclude our discussion we need to pay more attention towards the confidentiality and integrity of the data.

References

[1] Lagarde, Marie-Jeanne. "Security Assessment of Authentication and Authorization Mechanisms in Ethereum, Quorum, Hyperledger Fabric and Corda," 2019.

[2] Prakash, Vijay and Manuj Darbari. "A Review on Security Issues in Distributed Systems." International Journal of Scientific & Engineering Research, 3, no. 9, 2012.

[3] Firdhous, Mohamed. "Implementation of security in distributed systems-a comparative study," 2012.