Bioscene

ISSN: 1539-2422 (P) 2055-1583 (O)

www.explorebioscene.com

Distributed Environment: Security Mechanism Design Structure and Security Implementation for Data Distribution

Jai Pratap Dixit
Assistant Professor
Department of Information Technology
Ambalika Institute of Management and Technology, Lucknow UP, India

Dr. Neelendra Badal
Assistant Professor
Department of Computer Science
Kamla Nehru Institute of Technology Sultanpur, UP, India

Dr. Syed Qamar Abbas
Professor
Department of Computer Science
Ambalika Institute of Management and Technology, Lucknow UP, India

Abstract- *Distributed Environment, can evolve their different behaviors based on their changes in data distribution area. In this paper, we discuss security mechanism design issues and propose security metrics issues also in the context of distributed environment. A key premise with design layouts of distributed environment is that in order to detect their changes, authentication and information must be collected by different approaches of monitoring in environment. How design approaches should be done, what steps should be monitored, and the impact of monitoring may have on the security mechanism of the design issues in target system need for careful consideration. Conversely, the impact of security mechanism design layouts on the securing of data distribution environment. We propose a different design issues in security metrics that can be used to quantify the impact of different monitoring on the distributed security mechanism issues of the target distributed environment.*

Keywords: *Access Authentication, Security Issues, Cryptography, Authentication.*

I. Introduction

Now a days Security aspects in different Distributed Environment plays an important role. It defines that distributed environment such a way mapped with network [3] including client server model. Research has been significantly using different mechanisms with protecting the data with their clients. Partition Technique includes the DBMS redefinition. Data streams clustering technique are highly helpful to handle data and outlier detection.

Distributed system security [21-22] in term of different objectives of database models based on classification, access control, attacks, and system failures. Distributed system is multiple redundant within multiple devices and data transferring between devices with different channels. Cluster Security based on domain knowledge for certification of cluster vulnerabilities. Authentication, cryptographic techniques, access control [6] is many developments towards the generation of secure and trusted distribution environments.

A distributed computer system can be described as a collection of clients and servers communicating by exchange of messages.

- System is running in an open environment
- Need to communicate with other heterogeneous systems

Security issues: Access authorization, one must be authorized to access the distributed computer system: Message security [2]. Passing message confidentially between nodes using some cryptographic techniques: Mutual authentication [4] is a two way authentication both parties authenticate each other's identity suitably

Categories of access authorization are as the following

- Discretionary access control
- Access control matrix (ACM)
- Implemented via access control list or capability list or both.
- Mandatory access control[11]
- Represented as information flow among communicating entities.

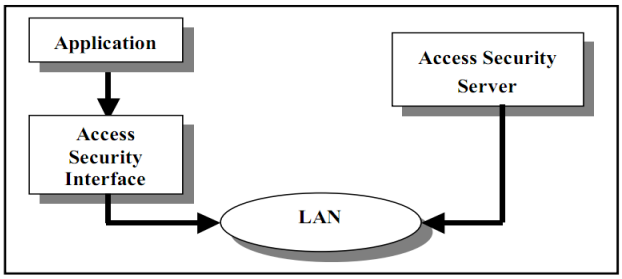

Figure1. Access Procedure

The access security system software may operate at each of the network stations as an independent application (**Fig. 1**).

The various applications will receive the access security services [7] via an access security interface which must be incorporated in each application where these services are required.

II. Security Mechanism

There are the following Security Mechanism used in distributed Environment

- Encryption
- Authentication
- Authorization
- Auditing

Distributed Environment support different Security process depends upon architecture of system. Mechanism of the Security system plays an important role.

III. Globus Architecture Security System

Global Architecture explains the overall security aspects within distributed system (**Fig. 2.**)

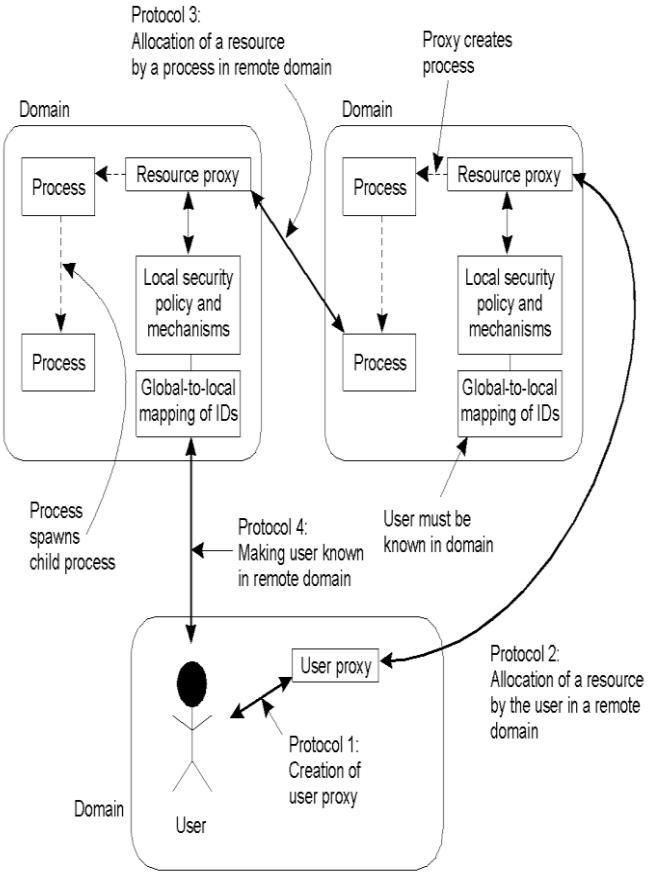

Figure2. The Globus Security Architecture

The environment consists of multiple administrative domains.

- Local operations are subject to a local domain security policy only [10].
- Global operations require the initiator to be known in each domain where the operation is carried out.
- Operations between entities in different domains require mutual authentication [11].
- Global authentication replaces local authentication.
- Controlling access to resources is subject to local security only [8].
- Users can delegate rights to processes.
- A group of processes in the same domain can share credentials.

Distributed Environment Security Challenges

In data distribution, there are the following challenges such as security policy for accessing data, authenticity, security based on time slot selection etc.

Approaches for protection against security threats

- Protection against invalid operations
- Protection against unauthorized invocations
- Protection against unauthorized users

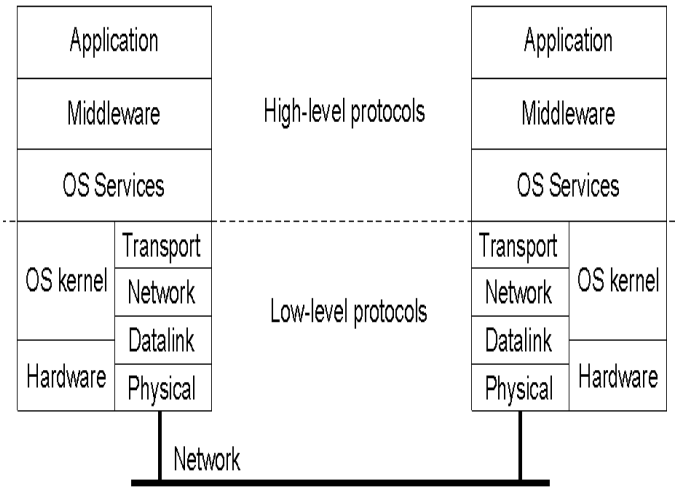

Figure 3 The logical organization of a distributed system into several layers.

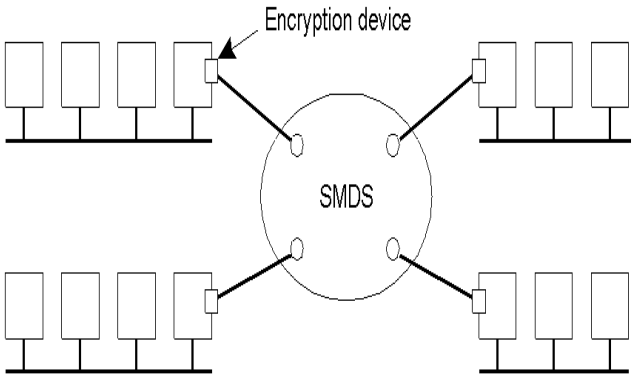

Figure 4.Several sites connected through a wide-area backbone service.

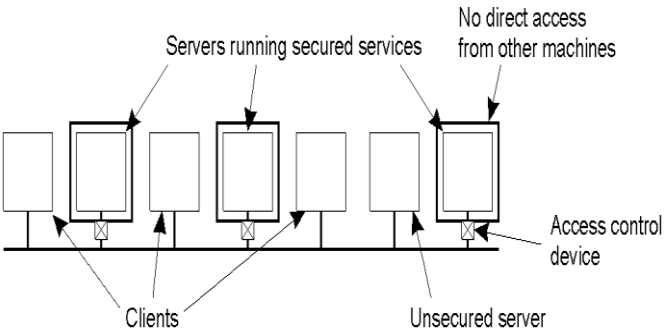

Figure 5 The principle of server running secure services.

IV. Security Mechanism Approaches in Distributed Security

A cryptographic technique uses private key and public key systems. Both provide integrity and authenticity of messages in addition to secrecy, symmetric encryption: private key, asymmetric encryption: private key & public key, Implemented using intricate algorithm like MD5, AEDS, and DES. [12-13]

Distributed authentication protocol: Maintain three basic properties: authenticity, integrity, and freshness.

Mutual authentication protocol*: Characterized* by whether a third-party authentication server is assumed and by how the freshness of messages is guaranteed.

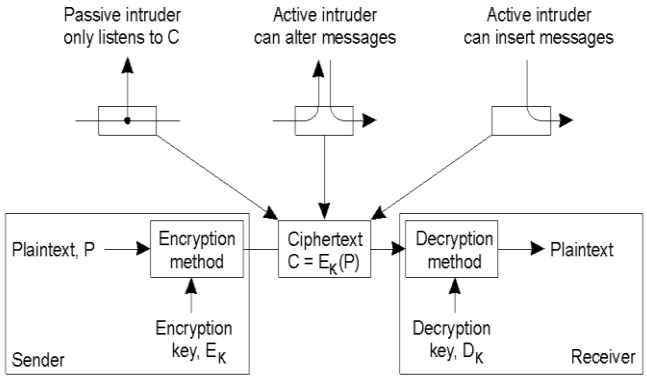

Figure6. Intruders and eavesdroppers in communication

V. Algorithm Procedure

In this approach we use updated algorithm of AES, TDEA and MD5 modified as JNS (Jai, Neelendra, Syed: author's) algorithms. The MD5 algorithm is used hash function producing a 128-bit hash value. It can still be used as a checksum to verify data integrity for implementation[30].

JNS Algorithm Procedure

{// Encryption and Decryption of attached documents and files//}

- Firstly the original text i.e. clear text is converted into bytes and then for the AES algorithm to perform encryption, we need to generate Key, using the derived bytes and the symmetric key.
- Using Memory Stream and Crypto Stream the clear text is encrypted, written to byte array, finally the byte array is converted to base 64 String then returned which is the final outcome i.e. the corresponding encrypted text.
- After that the encrypted text i.e. ciphers text is converted into bytes then similar to the

  Encryption process here too we will generate Key, using the derived bytes and the symmetric key.

- Using Memory Stream and Crypto Stream the cipher text is decrypted, then written to byte array and finally the byte array is converted to Base64String which returned, the decrypted original text.

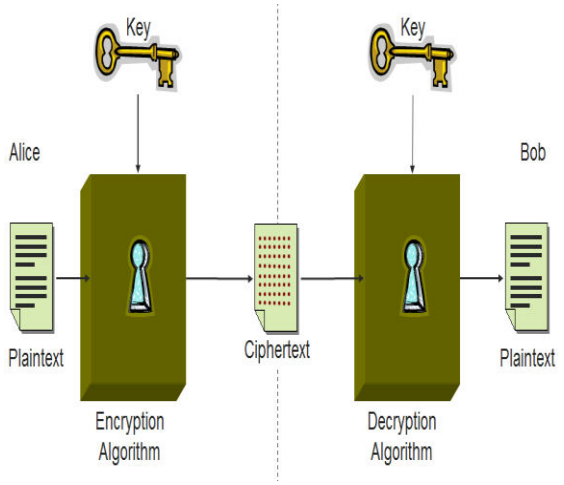

Figure 6(a) Encryption & Decryption Key process

{// Key implementation for encryption and Decryption data//}

- Hashing the encryption and decryption key using MD5.
- Used MD5 hash generator as the result is a 128 bit byte array which is a valid length for the TripleDES encoder.
- Hash functions map binary strings of an arbitrary length to small binary strings of a fixed length. Cryptographic # function has the property which state that computationally infeasible to find two distinct inputs that #function to the same value; that is, hashes of two sets of data should match if the corresponding data also matches. Small changes to the data result in large, unpredictable changes in the hash.
- The hash size for the MD5 algorithm is 128 bits.
- The Compute Hash methods of the MD5 class return the hash as an array of 16 bytes. Some MD5 implementations provide 32-character, hexadecimal / formatted # function. To interoperate with such implementations, format the return value of the Compute Hash methods as a hexadecimal value.

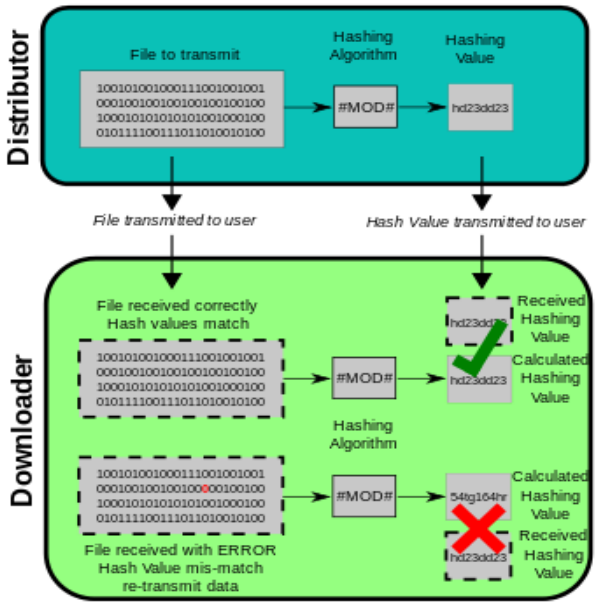

Figure 6(a) MD 5 Key Management

{// encoding and decoding process of data in data distribution //}

- Used to encode and decode the message string.
- TripleDES uses three successive iterations of the DES algorithm. It can use either 2 or 3- 56-bit keys.
- A newer symmetric encryption algorithm, Advanced Encryption Standard (AES), is available. Consider using the AES class and its derived classes instead of the TripleDES class [17] Use TripleDES only for compatibility with legacy applications and data.
- This algo supports to key lengths from 128 bits to 192 bits in increments of 64 bits pattern.
- Decryption and Encryption can be handled in the same way; use Create Decryptor instead of CreateEncryptor. The same key (Key) and initialization vector used to encrypt the file must be used to decrypt it.

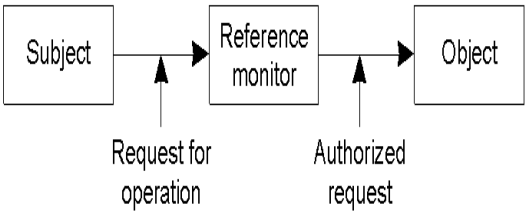

Figure 8 General model of controlling access to objects.

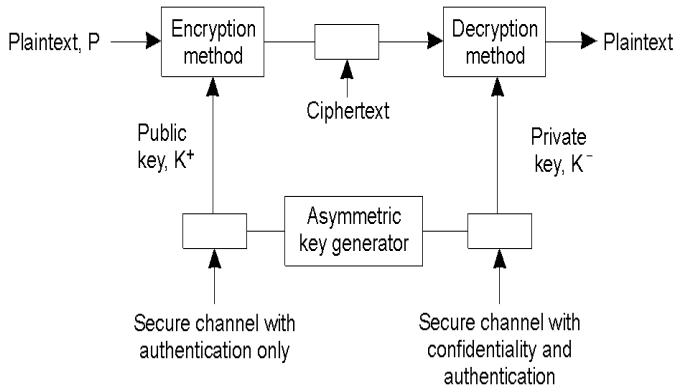

Figure9. Public key distributions in System

VI. Frame Work for Security Mechanism Issues

Design an algorithm for performing the security-mechanism at data partitioned level and transformation of partitioned data. The algorithm should be such that an opponent cannot defeat its purpose. We design a simple schema, tables indexes, constrains with using redefinition procedure [28]. We create different data sets and Outliers detection which helps in clustering for providing new optimistic results

Security mechanisms in middleware for data distribution, its during data modification and data transformation. Generate the modification approaches secret information to be used within the algorithm for securing the data [30].

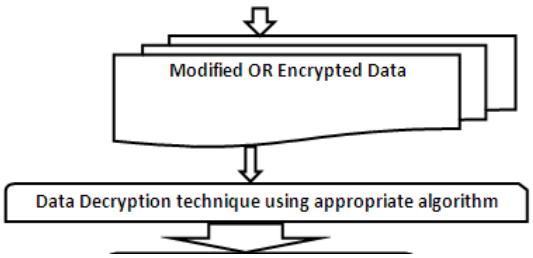

Figure 10 Data Modification Security Technique

Application of data web services [24] in secure manner and it's Monitoring in distributed environment. Develop methods for the distribution and sharing of the secret information. [30]

After modification technique, the data could be used for data mining procedure in distributed environment [5]. And it is very easy to obtain the original data after modification. In the proposed work, the data transformation technique is used for appropriate numerical attributes. Data protection is based on altered or manipulated technique so that data remain even after the procedure [30].

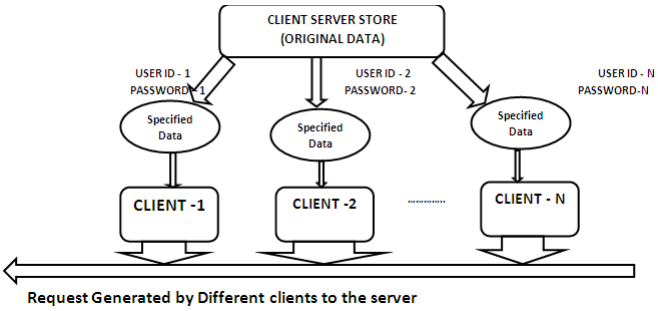

Figure11. Client Site Security Architecture

Specify a mechanism for the client, used by the different principals who make use of the security algorithm for secret information to obtain a particular security mechanism metrics [19-21].
A useful means of classifying security mechanism in terms of event detection, security recovery, authentication, access control, confidentially and Integrity services [18-20-22].
However, it is feasible to prevent the success of this security [26] mechanism, usually by means of encryption (in fig. no-11). Thus, the emphasis in dealing with passive decryption is on prevention rather than detection.

VII. Result

Implementation Work is shown as snaps shots. This research implementation work as online portal **www.jnsdistributedsecurity.com.** Portal provides the user panel and admin panel for data distribution in secure manner.

There are the following steps implemented in Research work.

For admin Login ID jpdixit.iiita@gmail.com Login password: *****, For New Users: First Create their an account in Distributed Environment (Which Implemented)

1. When user created an account they cannot login without admin approval. Firstly admin approved it than user can login the system.
2. At the time of use registration user decide two passwords, one is for login, second one for accessing file and E-mail data.

3. When admin approved users can access the data distribution as secure manner.

4. Admin can create a Separate security password for data.

5. All file converted into ZIP format.

6. Users can send any data to registered users.

7. Encryption and Decryption algorithm updated MD5,
   Triple - DES & AES Algorithms as JNS Algorithm.

8. Admin can only show the encrypted data

9. E-mail selection only via check box selection

10. Trying to security of the documents as time duration as particular date

11. No one can access documents on server

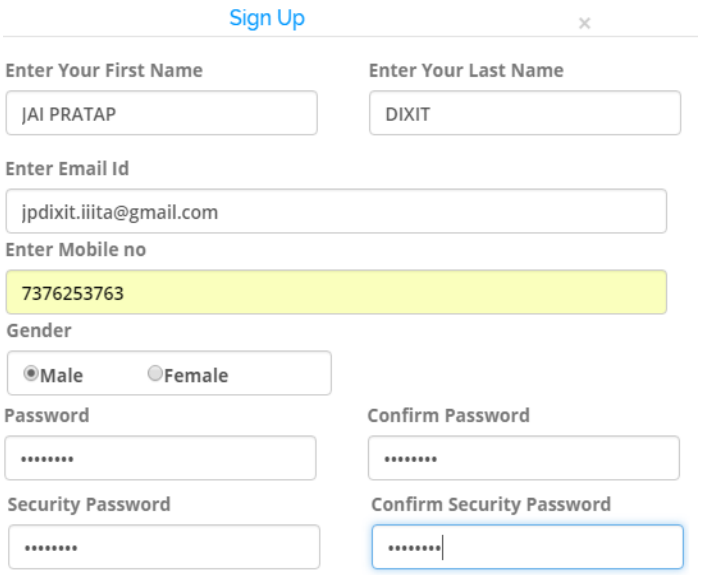

Figure12 Registration Form

Describe (**Figure 12**) the login process with different security password one is used for login and others one is used for the secureencrypted file accessing.

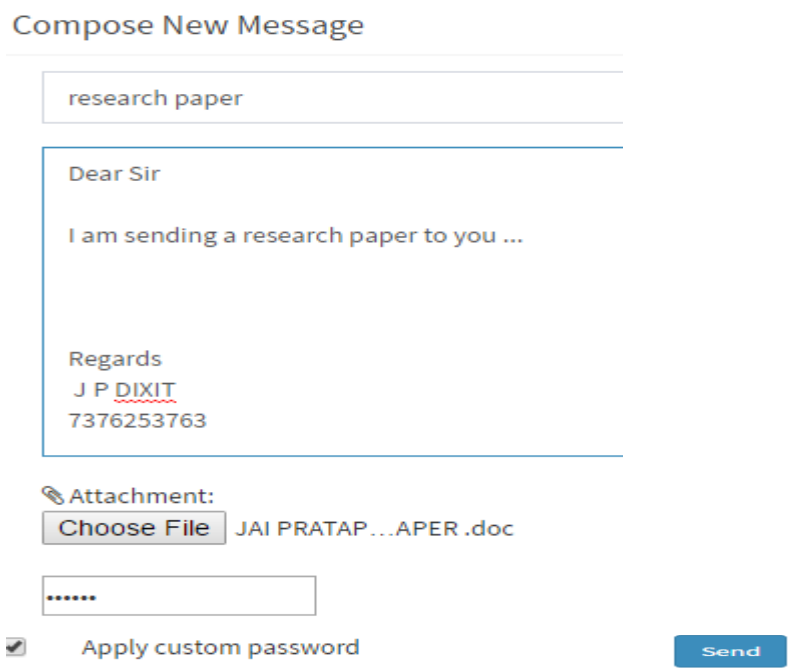

Figure 13 Message writing

Message writing(**Figure 13)** with secure password refers to the custom password by admin.

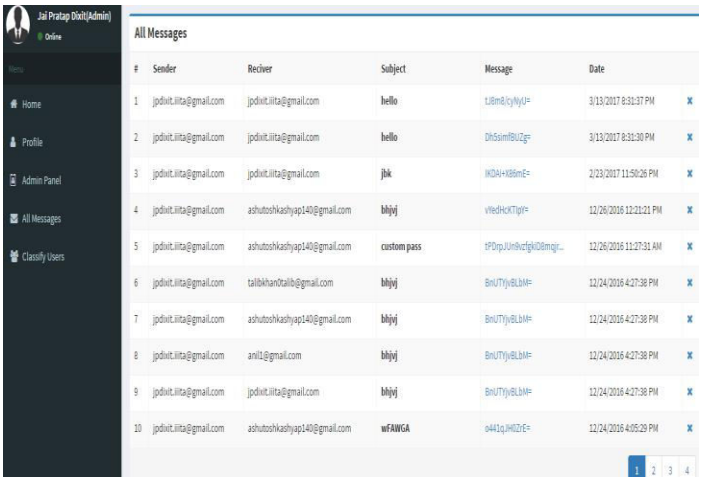

Figure 14 *Message* Description Details

Encrypted message data (**Figure 14)** are recorded by algorithm automatically. Which cannot be accessed by server hackers?

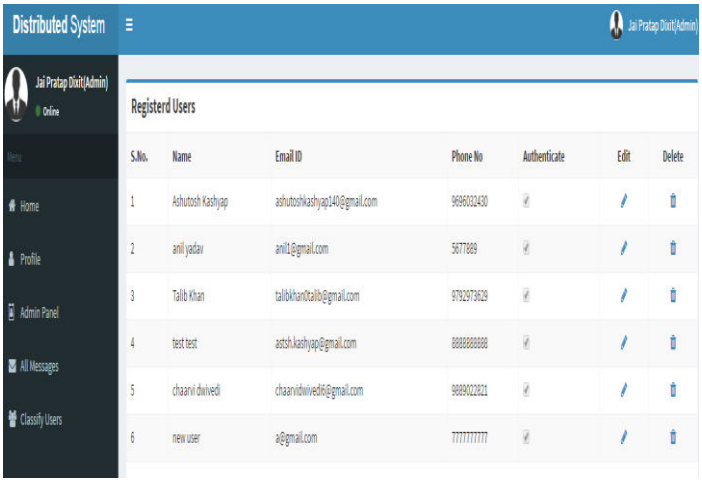

Figure 15 Admin panel for user authentication

Via admin panel admin can authenticate the person in the system for authorized users (**Figure 15**)

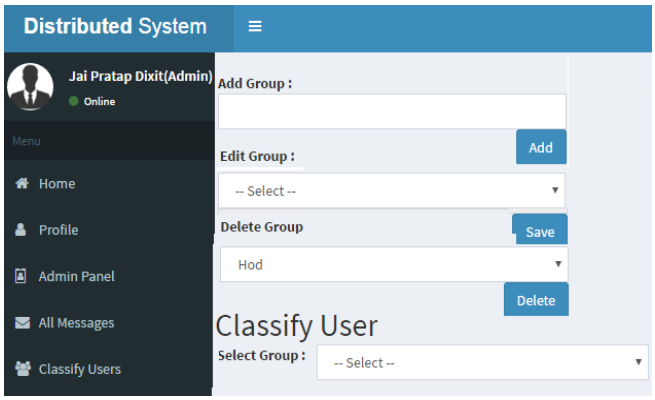

Figure 16 Group Creation in Security System

Admin can classified the different users as category within distributed system (**Figure 16**)

Users sending a message

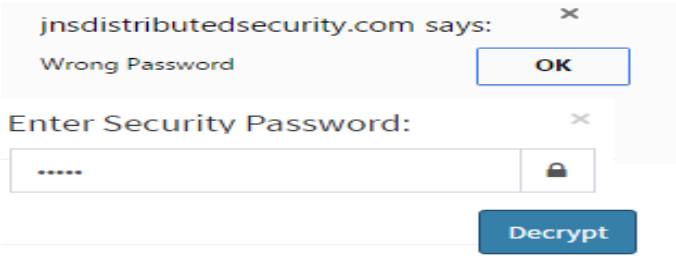

Figure17 Security Password Verification

When user opens an E-mail it asked a password for decryption of messages as (**Figure 17)**

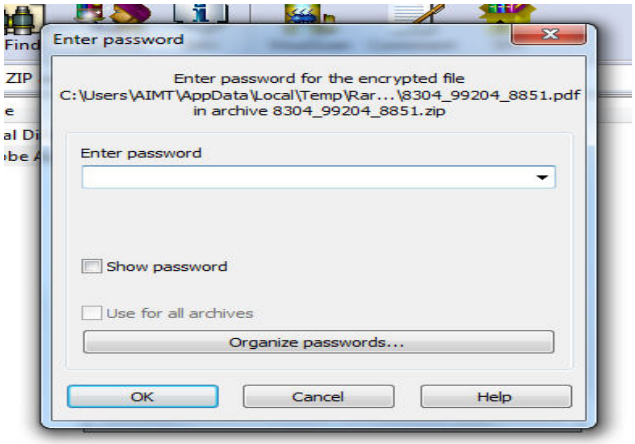

Figure 18 Security Password

In above diagram (**Figure 18)** all encrypted file become converted into a zip format and also asked for the secure password for accessing a file.

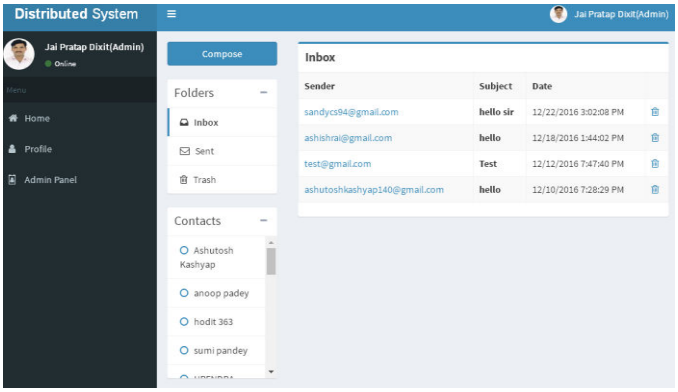

Figure19 *Admin Pannel*

For sending an E-mail client choose an appropriate E-mails for data distribution as **Figure 19**.

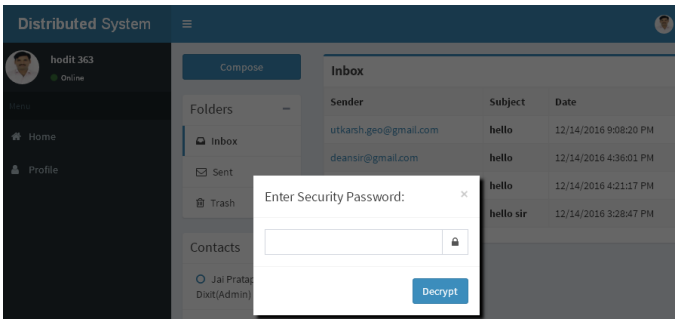

Figure20 Security Check Encryption

A secure password asked at the time of E-mail opening for message as above diagram in (**Figure 20)**

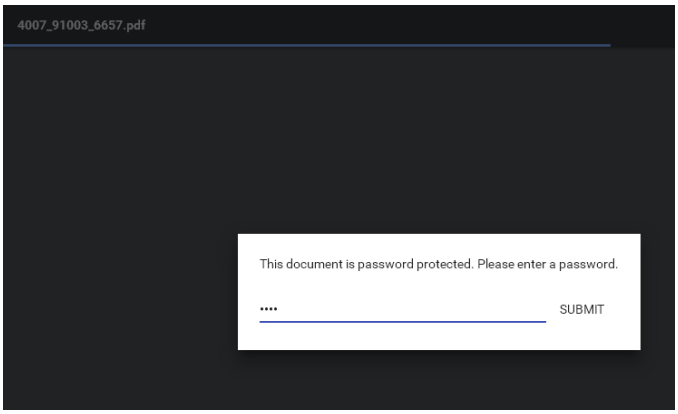

Figure 21 Security Check Password

This **Figure 21** describe the file accessing secure password for particular file . it may be users or admin password as per sending critiera for data distribution for secure communication.

Figure 22 Time slot base secure mechanism

Data can be secure by the time duration access for data distribution. It provides by the admin of the system. **(Figure 22)**

VIII. Conclusion and Future Scope

Here, we Implemented the proposed research work design scheme based on the a novel approach of data distribution security mechanism in distributed environment data partitioned level and its transformation of partitioned data in secure manner, middle ware security mechanism in data distribution. During data modification and data transformation using efficient algorithm in security system for implementation. Also provide a proposal for application of data web services in secure manner and it's monitoring in distributed environment.

The previous security mechanism was discussed the security challenges will be implemented in future using appropriate security mechanism.

Current encryption algorithm are sometimes expensive to execute and can be decrypted with some known information. A more efficient and secure algorithm is needed to achieve the security goal.
Techniques to identify the eavesdropper in the communication network quickly and correctly. The intelligent agent is a good practice whereas it must introduce a third party monitor to the distributed computing system. Monitor can be a potential secure issue in terms of system attack.
As cloud computing has been widely used in recent years, the security issue becomes a harder problem since more computers in scattered locations join the system. Challenging work is proposed to ensure the safe communication among these endpoints. Data can be secure by the time duration access for data distribution.

Acknowledgement

I acknowledge my great gratitude and immense respect to Dr. Neelendra Badal [Assistant Professor- Department of CSE, Kamla Nehru National Institute of Technology, and Sultanpur] and Dr. S Q Abbas [Professor- Department of CSE, Ambalika Institute of Management and Technology] for their encouragement, inspiration and insightful suggestions. I would like to gratitude to Dr Alok Mishra for his valuable support and guidance.

References

[1] H. Hamdi, M. Mosbah, "A DSL framework for policy based Security of distributed systems", 3rd IEEE International Conference on Secure Software Integration and Reliability Improvements, pp. 150-158, 2009 Article (CrossRef Link)

[2] Adi Armoni, "Data Security Management in Distributed Computer Systems", Informing Science, Volume 5, 2002. Article (CrossRef Link)

[3] K. Boudaoud; N. Agoulmine; J.N De Souza, Distributed Network Security Management Using Intelligent Agents",2004. Article (CrossRef Link)

[4] Mirtaheri S.L, Khaneghah E.M, Sharifi M, Azgomi M.A; "The influence of efficient message passing mechanisms on high performance distributed scientific computing", Parallel and distributed Processing with Applications IEEE: 663-668, 2008. Article (CrossRef Link)

[5] Naqvi, S.; Riguidel, M., "Security architecture for heterogeneous distributed Computing systems", security technology, 38th international conference, IEEE Explore 2004. Article (CrossRef Link)

[6] Edara, U.R.; Subramanian, N.; Dwivedi, M.; Sinha, A., "A system for security assessment grid environment", 2010 IEEE 4th international conference, pages:1—6, 2010. Article (CrossRef Link)

[7] Vijayarani Mining, Dr.A.Tamilarasi "Data Transformation Technique for Protecting Private Information in Privacy Preserving Data Mining", Advanced Computing: An International Journal (ACIJ), Vol.1,No.1, November 2010 Article (CrossRef Link)

[8] Domingo-Ferrer, J & Mateo-Sanz, J. M. (2002), "Practical data- Oriented micro aggregation for statistical disclosure control", IEEE Transactions on Knowledge and Data Engineering, vol. 14, no. 1, pp. 189-201, 2002.Article (CrossRef Link)

[9] Samarati, P (2001), "Protecting respondents' identities in Microdata release", IEEE Transactions on Knowledge and Data Engineering, 13(6):1010-1027. 2001.Article (CrossRef Link)

[10] Mayur Sawant, Kishor Kinage, Pooja Pilankar, Nikhil Chaudhari "Database Partitioning: A Review Paper" International Journal Of Innovative Technology and Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue- 5, October 2013.Article (CrossRef Link)

[11] Wen Qi, Jie Song and Yu-bin Bao, "Near-uniform Range Partition Approach for Increased Partitioning in Large Database" , IEEE, 978-1 -4244-5265-1/10, 2010.Article (CrossRef Link)

[12] Jie Song and Yubin Bao, "NPA: Increased Partitioning Approach For Massive Data in Real-time Data Warehouse", IEEE, 978-1 – 4244-7585-8/10, 2010.Article (CrossRef Link)

[13] Eugene Wu and Samuel Madden, "Partitioning Techniques for Fine-grained Indexing", IEEE 978-1 -4244-8960-2/11, 2011 Article (CrossRef Link)

[14] Dr. S. Vijayarani1, Ms. P. Jothi "Hierarchical and Partitioning Clustering Algorithms for Detecting Outliers in Data Streams" International Journal of Advanced Research in Computer and Communication Engineering, ISSN 2278-1021 /: 2319-5940 Vol. 3, Issue 4, April 2014 Article (CrossRef Link)

[15] Yogita, Durga Toshniwal, "Clustering Techniques for Streaming Data–A Survey" in proc. of the IEEE 2012. Article (CrossRef Link)

[16] Dr. S. Vijayarani , Ms.P.Jothi, "Partitioning Clustering Algorithms for Data Stream Outlier Detection" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 4, April 2014 Article (CrossRef Link)

[17] Sudipto Guha, Adam Meyerson, Nine Mishra and Rajeev Motwani, "Clustering Data Streams: Theory and practice, "IEEE Transactions on Knowledge and Data Engineering, vol. 15, no.3, pp. 515-528, May / June, 2003.Article (CrossRef Link)

[18] George Coulouris, Jean Dollimore and Tim Kindberg, "Distributed System –Concept and Design", 4th ed. London England: Addison –Wesley, 2005 Article (CrossRef Link)

[19] Andrew S Tenenbaum and Maarten van Steen, "Distributed System: Principle and Paradigms", 2nd ed. Upper Saddle River, NJ, USA: Pearson Higher Education, 2007 Article (CrossRef Link)

[20] Firdhous "Implementation of Security in Distributed system –A Comparative Study" International Journal of computer System Vol,2, No. 2, 2011 Article (CrossRef Link)

[21] Yuchong Hu, Yinlong Xu, Xiaozhao Wang, Cheng Zhan, and Pei Li, "Cooprative Recovery of Distributed Storage System From Multiple Losses with network Coding ", IEEE Jouranal On Selected Area in Communications, Vol.28, no. 2, pp.268- 267, Feb 2010.Article (CrossRef Link)

[22] Wei Li and Rayford B Vaughn, "Cluster Security Research Involving the Modeling of Network Exploitations Using Exploitation Graphs", in 6th IEEE International Symposium on Cluster Computing and the Grid Workshop, Singapore, 2006, pp26-36.Article (CrossRef Link)

[23] Ragib Hassan Suvda Myagmar, Adam J Lee, and William Yurcik, "Toward a threat model for storage system", in Proceeding of the 2005 ACM Workshop on storage security and Survivability, USA, 2005
Article (CrossRef Link)

[24] Theodoros K Dikaliotis, Alexandros G Dimakis, and Tracey Ho, "Security in Distributed storage system by communicating a logarithmic number of bits", in IEEE, ISIT, Austin, TX, USA, 2010 pp. 1948-1952 Article (CrossRef Link)

[25] Vijay Prakash, Manuj Darbari "A Review on Security Issues in Distributed Systems" International Journal of Scientific & Engineering Research Volume 3, Issue 9, September-2012 1ISSN 2229-5518 , Article (CrossRef Link)

[26] M. Shehab, A. Ghafoor, E. Bertino, "Secure collaboration in a Mediator free distributed environment", IEEE Transactions on Parallel and Distributed Systems, vol. 19, no.10, pp.1338-1351, 2010.Article (CrossRef Link)

[27] S. Pallickara, J. Ekanayake, G. Fox, "A scalable approach for the secure and authorized tracking of the availability of Entities in distributed systems", IEEE International Parallel and Distributed Processing symposium, pp.1-10, 2007Article (CrossRef Link)

[28] T. Xiaoyong, K. Li, Z. Zong, B. Veradale, "A novel security-Driven scheduling algorithms for precedence-constrained tasks in heterogeneous distributed systems", IEEE Transactions on Computers, vol 60, no.7, 2011, pp.1017-1029.Article (CrossRef Link)

[29] X. Huang, Y. Xiang, A. Chonka, J. Zhou, R.H Deng, "A Generic framework for three factor authentication: Preserving Security and privacy in distributed systems", IEEE Transactions on Parallel and Distributed Systems, vol. 222, no.8 2011, pp.1390-1397.Article (CrossRef Link)

[30] Dixit J .P, Badal Neelendra, Abbas S.Q. "A Novel
Approach: Distributed Security Mechanism of Data Distribution in Distributed Environment" in International Journal of Applied Engineering Research ISSN 0973-4562 (2017) pp. 2115-2122 Article (CrossRef Link)