ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com
Journal DOI:10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

AN EFFICIENT SECURITY MANAGEMENT SCHEME FOR DISTRIBUTED NETWORK USING HIERARCHICAL KEY APPROACH WITH ELLIPTICCURVE CRYPTOGRAPHY.

SanvariyaBhadaniya, Vijay Prakash.

Svits, Indore and 452001,india.

Manuscript Info

Manuscript History:

Received: 16 March 2016
Final Accepted: 19 April 2016
Published Online: May 2016

Key words:
ECC(Elliptic Curve Cryptography), administration convention, Cryptosystem, Distributed Framework.

Corresponding Author

SanvariyaBhadaniya.

Abstract

Information access control has turning into a testing issue in distributed storage frameworks. A few procedures have been proposed to accomplish the safe information access control in a trusted distributed storage framework. Elliptic Curve Cryptography is viewed as a standout amongst the most suitable advances for security in distributed storage. In every single existing plan, it is accepted that there is one and only power in the framework in charge of issuing to the clients. On the other hand, in numerous applications, there are various powers co inside in a framework and every power cans freely [1]. Secure and solid gathering correspondence is a dynamic range of exploration. Its notoriety is fuelled by the developing significance of gathering focused and collective properties. The focal exploration test is secure and effective gathering key administration. In this paper, we propose a productive gathering key administration convention in appropriated bunch correspondence. This convention depends on Elliptic Curve Cryptography and diminishes the key length while giving securities at the same level as that of different cryptosystems gives. To the best of our insight, this venture is the first attempt to address the single point bottleneck on both security and execution in cryptography access control plans out in the open cloud storage [2].

Introduction:-

The distributed computing turns into the host issue in industry and the scholarly world with the fast improvement of PC equipment and programming. The distributed computing is the consequence of numerous variables, for example, customary PC innovation and correspondence innovation and business mode in the business. Altogether taking into account the system and has the arrangement of administration for the buyer. The distributed computing framework gives the support of the client and has the character of high versatility and dependability. The asset in the cloud framework is straightforward for the application and the client don't have a clue about the spot of the asset. The clients can get to your applications and information from anyplace. At the point when information has been conveyed it is put away at more areas expanding the danger of unapproved physical access to the information. For instance, in cloud based structural planning, information is repeated and moved habitually so the danger of unapproved information recuperation increments significantly [3]. (E.g. transfer of old hardware, reuse of drives, and reallocation of capacity space).The way that information is recreated relies on upon the administration level a client picks and on the administration gave. That encodes information preceding transferring it to the cloud. The distributed computing changed the style of programming. The information can be put away in the cloud framework and the client can utilize the information in whenever and in anyplace. The information regularly put away in the private or individual framework, for example, PC. The distributed computing can promise the information security and the client don't ensure the information without anyone else's input once more. So the distributed computing must guarantee the security of information put away in the cloud framework. Numerous organizations give the distributed computing stage. [4]

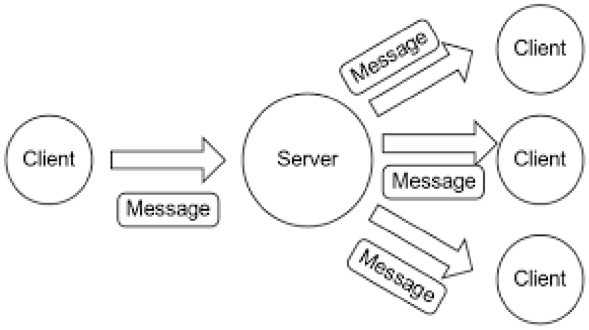


Figure 1:-Key Distribution Approach.

The security of distributed computing is the key import issue in the advancement of distributed computing. The customary security instrument can't ensure the cloud framework totally. The distributed computing application is no limits and versatility and can lead numerous new security issues. The primary security issues incorporate information security, customer information security affirmation, distributed computing stage reliability and distributed computing association. The cloud framework is running in the web and the security issues in the web moreover can be found in the cloud framework. The cloud framework is not unmistakable the standard framework in the PC and it can meet other unprecedented and new security issues. the best stresses over distributed computing are security and assurance [4]. The thought behind distributed computing is comparative: The client can basically utilize capacity, processing power, or exceptionally made advancement situations, without worrying how these work inside. Distributed computing is typically Internet-based registering. The cloud is a similitude for the Internet taking into account how the web is portrayed in PC system charts; which implies it is a reflection concealing the perplexing foundation of the web. It is a style of processing in which IT-related capacities are given "as an administration", permitting clients to get to innovation empowered administrations from the Internet ("in the cloud") without learning of, or control over the advances behind these servers. As the distributed computing framework has more information which might be the private information of client, the information must not be pulverized or snatched [5].

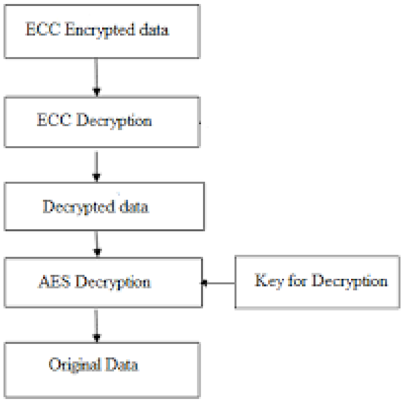


Figure 2:- Execution Process of ECC.

Since the information in the cloud framework might be imperative for the client, the programmer might give careful consideration to get the information. The framework must be secured more painstakingly than the conventional framework. The organization utilizes the cloud framework and stores the information in it. The information can be seen by other individuals who are not individual of organization. The organization must have trust in the distributed computing on the off chance that they need to store the private information in the cloud framework. Administration and security are urgent to processing on the cloud administration supplier's base, if the cloud framework is in firewall or not. [6]

Literature Survey:-

Group communication can benefit from IP multicast to achieve scalable exchange of messages. However, there is a challenge of effectively controlling access to the transmitted data. IP multicast by itself does not provide any mechanisms for preventing non group members to have access to the group communication. Although encryption can be used to protect messages exchanged among group members, distributing the cryptographic keys becomes an issue. Researchers have proposed several different approaches to group key management.

In this proposed approaches [8] can be divided into three main classes: centralized group key management protocols, decentralized architectures and distributed key management protocols. The three classes are described here and an insight given to their features and goals. The area of group key management is then surveyed and proposed solutions are classified according to those characteristics. Group communication applications can use IP multicast to transmit data to all n group members using minimum resources. Efficiency is achieved because data packets need to be transmitting- ted once and they traverse any link between two nodes only once, hence saving bandwidth. This contrasts with unicast based group communication where the sender has to transmit n copies of the same packet. However scalable IP multicast does not provide mechanisms to limit the access to the data being transmitted to authorize group members only. Any multicast-enabled host can send IGMP messages to its neighbour router and request to join a multicast group.

In this paper [9] the security challenge for multicast is in providing an effective method for con- trolling access to the group and its information that is as efficient as the underlying multicast. A primary method of limiting access to information is through encryption and selective distribution of the keys used to encrypt group information. An encryption algorithm takes input data (e.g., a group message) and performs some transformations on it using a cryptographic key. This process generates a ciphered text. There is no easy way to recover the original message from the ciphered text other than by knowing the right key. Applying such a technique, one can run se- cure multicast sessions. The messages are protected by encryption using the chosen key, which in the context of group communication is called the group key. Only those who know the group key are able to recover the original message.

In this research [10] the group may require that membership changes cause the group key to be refreshed. Changing the group key prevents a new member from decoding messages exchanged before it joined the group. If a new key is distributed to the group when a new member joins, the new member cannot decipher previous messages even if it has recorded earlier messages encrypted with the old key. Additionally, changing the group key prevents a leaving or expelled group member from accessing the group communication (if it keeps receiving the messages). If the key is changed as soon as a member leaves, that member will not be able to decipher group messages encrypted with the new key. However, distributing the group key to valid members is a complex problem. Al- though rekeying a group before the join of a new member is trivial (send the new group key to the old group members encrypted with the old group key), rekeying the group after a member leaves is far more complicated. The old key cannot be used to distribute a new one, because the leaving member knows the old key. There- fore, a group key distributor must provide another scalable mechanism to rekey the group. A simple scheme for rekeying a group with n members has the key distribution centre (KDC) assigning a secret key to each member of the group.

The idea in [11] Group key management is a difficult task in implementing large and dynamic secure multicast. In this paper, a new scheme is proposed in the basis of in-depth analysis of the requirements of the secure multicast and group key management. The scheme is based on the multicast group security architecture and multicast security group key management architecture proposed by IETF. This scheme constructs group key based on pairings and distributes the group key using HASH function polynomial, and manages group key making use of the dynamic layering GCKS. The scheme is better in security, lower in computation cost and communication cost. The analysis comparison proves that the scheme has strong scalability and efficiency.

The concept in [12] fault-tolerant, scalable and reliable communication services have become critical in modern computing. An important and popular trend is to convert traditional centralized services (e.g., file sharing, authentication, web, and mail) into distributed services spread across multiple systems and networks. Many of these newly distributed and other inherently collaborative applications (e.g., conferencing, white-boards, shared instruments, and command-and-control systems) need secure communication. However, experience shows that security mechanisms for collaborative and dynamic peer groups tend to be both expensive and unexpectedly complex. In that regard, dynamic peer groups are very different from non-collaborative, centrally managed, one-to-man y (or few-to-man y) broadcast groups such as those encountered in Internet multicast. Dynamic Peer Groups (DPGs) are common in man y layers of the network protocol stack and man y application areas of modern computing. Examples of DPGs include replicated servers (such as database, web, time), audio and video conferencing and, more generally, applications supporting collaborative work. In contrast to large multicast groups, DPGs tend to be relatively small in size, on the order of hundred members. Larger groups are harder to control on a peer basis and are often organized in a hierarchy .DPGs typically assume a many-to-many (or, equivalently many-to-many) communication pattern rather than one-to-many pattern common of larger hierarchical groups. Despite their relatively small number, group members in a DPG may be spread throughout the Internet and must be able to deal with arbitrary partitions due to network failures, congestion, and hostile attacks. In essence, a group can be split into a number of disconnected partitions each of which must persist and function as an independent peer group. Security requirements in collaborative DPGs present several interesting research challenges. In this paper, we focus on services.

Problem Statement:-

In existing framework, Cryptographic strategies were connected to get to control for remote stockpiling frameworks. The information proprietors scramble records by utilizing the symmetric encryption approach with substance keys and afterward utilize each client's open key to encode the substance keys. It requires every information proprietor to be online constantly. A few routines convey the key administration and appropriation from the information proprietors to the remote server under the supposition that the server is trusted or semi-trusted. System testing is the stage of implementation, which aimed at ensuring that system works accurately and efficiently before the live operation commence. Testing is the process of executing a program with the intent of finding an error. A good test case is one that has a high probability of finding an error. A successful test is one that answers a yet undiscovered error.[13]

Downsides of the current framework:-

- ❖ The key administration is exceptionally confused when there are an extensive number of information proprietors and clients in the framework.
- ❖ The key dispersion is not helpful in the circumstance of client powerfully framework.
- ❖ The server is can't be trusted by the information proprietors in distributed storage frameworks.
- ❖ It can't be connected to get to control for distributed storage framework.

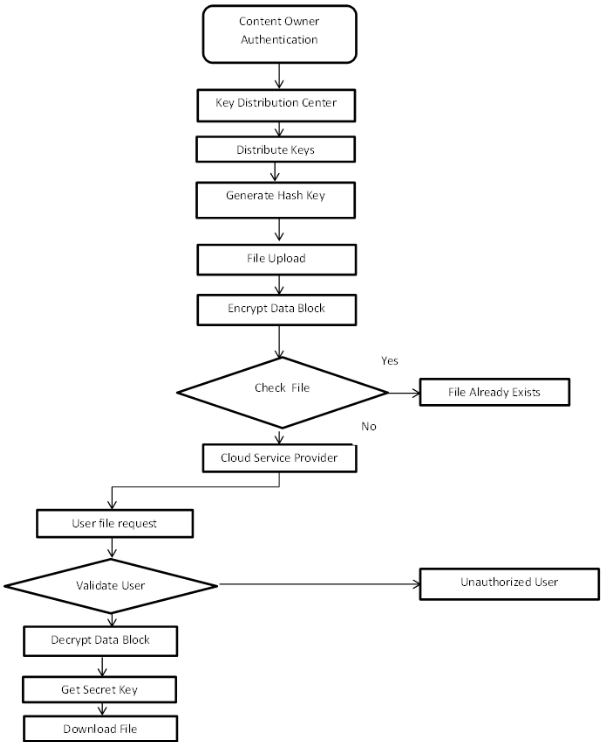
Proposed Solution:-

When we talk about the problem of to defeat all the above issue we propose a proficient gathering key administration convention in appropriated bunch correspondence. This convention depends on Elliptic Curve Cryptography and diminishes the key length while giving securities at the same level as that of different cryptosystems gives. We give the abnormal state security and stay away from the replication of document in the cloud administration supplier. In proposed framework, we utilize hash capacity to create key for the record .By utilizing hash capacity to dodge the duplication in cloud. After that we apply cryptographic procedure for security reason. We utilizing ECC calculation for encryption and unscrambling process.

Utility of the framework:-

- ❖ Avoid duplication in cloud.
- ❖ Increase the security level.
- ❖ High effective.
- ❖ ECC calculation gives top of the line

Cloud computing is often confused with grid computing (a form of distributed computing whereby a "super and virtual computer" is composed of a cluster of networked, loosely-coupled computers, working together to perform very large tasks), utility computing (the packaging of computing resources, such as computation and storage are provided as a measured service that have to be paid similar to a traditional public utility such as electricity) and autonomic computing (computer systems capable of self-management). Many cloud computing deployments are powered by grids, have autonomic characteristics and are billed like utilities, but cloud computing can be seen as a natural next step from the grid-utility model.



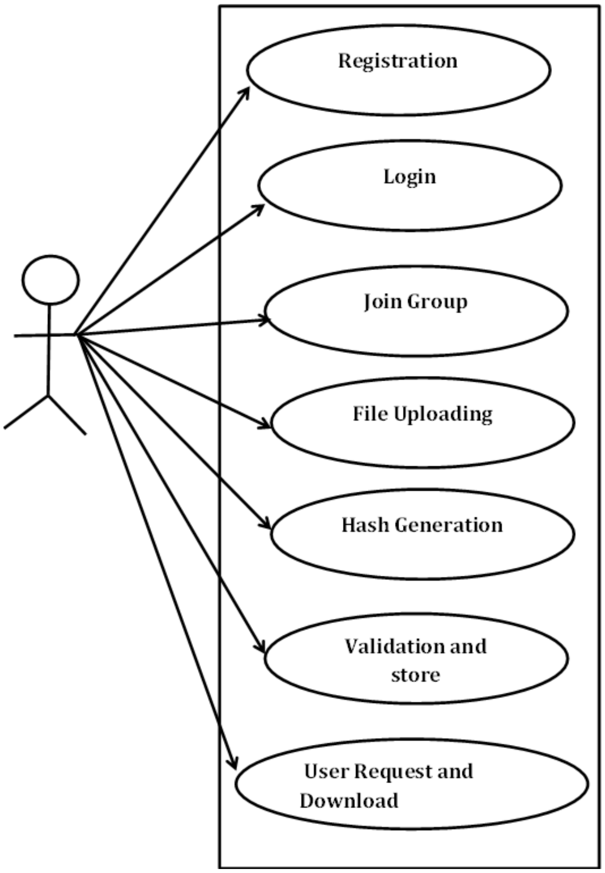


Figure 3:- Work Flow of Proposed System.

Figure 4:- Proposed Use-Case Concept.

Acknowledgements:-

This research work is self-financed but recommended from the SVITS so as to enhance the key distribution problem with present techniques in distributed network using this method. Thus, the authors thank the anonymous reviewers for their valuable comments, which strengthened the paper. The authors also wish to acknowledge institute administration for their support & motivation during this research. They also like to give thanks to VIJAY PRAKASH for discussion regarding the approach adapted for this paper.

References:-

1. Jiang and Hu, “A Survey of Group Key Management,” IEEE International Conference on Computer Science and Software Engineering, Vol. 3, pp. 994-1002, December 12-14, 2014.
2. Shen, Huang and Chen, “A Time-Bound Hierarchical Access Control for Multicast Systems” Proceedings of IEEE International Conference on Machine Learning and Cybernetics, Xian, Vol. 2, pp. 543-548, July 15-17, 2012.
3. Kim, Perrig andTsudik, “Tree-based Group Key Agreement,” ACM Transactions on Information and System Security, Vol. 7, Issue 1, pp. 60-94,February 2004.
4. Panja, Madria and Bhargave, “Energy and Communication Efficient Group Key Management Protocol for Hierarchical Sensor Networks,” IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Taichung, Taiwan, Vol. 1, pp. 8-15, June 05-07, 2006.
5. Zhang, Li, Chen, Tao and Yang, “EDKAS: An Efficient Distributed Key Agreement Scheme using One-Way Function Trees for Dynamic Collaborative Groups,” IEEE Multi-conference on Computational Engineering in Systems Applications, Beijing, China, pp. 1215-1222, October 2006.
6. Mortazavi, Kato, “An Efficient Distributed Group Key Management using Hierarchical Approach with Diffie-Hellman and Symmetric Algorithm: DHSA,” IEEE International Symposium on Computer Networks and Distributed Systems, pp. 49-54, February, 23-24 2011.

7. Zeng, Xia and Su, “A New Group Key Management Scheme based on DMST for Wireless Sensor Networks,” 6th IEEE International Conference on Mobile Adhoc and Sensor Systems, Macau, China, pp. 989-994, October 12-15, 2006.
8. S. Maria Celestin Vigila and K. Muneeswaran, ―Implementation of text Based cryptosystem using elliptic curve cryptography‖, IEEE, 2009.
9. D. Sravana Kumar, CH. Suneetha and A. Chandrasekhar, ―Encryption of data using Elliptic Curve over Finite Field‖, IJDPS, Vol. 3, No. 1, 2012.
10. R. RajaramRamasamy, M. AmuthaPrabakar, M. Indra Devi and M.Suguna, ―Knapsack based ECC encryption and decryption‖, International Journal of Network Security, Vol. 9, No. 3, PP. 218-226,Nov. 2009.
11. Padma Bh, D. Chandravathi and P. PrapoornaRoja, ―Encoding and Decoding of a Message int the Implementation of Elliptic Curve Cryptography using Koblitz‘s method‖, IJCSE, Vol. 02, No. 05, 2010.
12. William Stallings, Cryptography and Network Security, Prentice Hall, 5th Edition, 2010.
13. VivekKapoor, Vivek Sonny Abraham and Ramesh Singh, ―Elliptic Curve Cryptography‖, ACM Ubiquity, vol. 0, Issue 20, May 20-26, 2008.
14. Darren Hankerson, Julio Lopez Hernandez and Alfred Menezes, ―Software implementation of Elliptic Curve Cryptography over Binary Fields‖, Cryptographic Hardware and Embedded Systems — CHES 2000, Lecture Notes in Computer Science Volume 1965, 2000, pp 1-24.