Ilkogretim Online - Elementary Education Online, 2020; Vol 19 (Issue 2): pp. 1888-1893
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2020.02.696773

Group Communication With Secure Process Based On Identity Crypto System

G.Malathi [1] , D.Evangeline Nesa Priya [2]

[1]Assistant Professor, Department Of Computer Science And Engineering Sri Sairam Institute Of Technology, Chennai

[2]Assistant Professor, Department Of Information Technology Thangavelu Engineering College, Chennai

ABSTRACT

The Group communication for applications like board-meeting, group discussions and teleconferencing is very critical . Collaborative and distributed application are used for the multi-party interactive computation with Secure group communication . In general, group communications involve over open networks. Group Key Agreement (GKA) is a special key approach to manage a set of secure group keys and group dynamics. To establish a common secret key between the users ,the Conventional and unconventional GKA protocols are used . The members from the group can securely exchange message using the shared key. Asymmetric Group Key Agreement (AGKA) a group of members to establish a public group encryptionkey dynamically providing a different secret decryption key in a identity basedcryptosystem with group communication.

1. INTRODUCTION

The Big Data allows efficiencies in terms of cost, productivity, and innovation within an organization. This process does not come without its flaws. Data analysis often requires multiple parts of Organization to work in collaboration and create new and innovative processes to deliver the desired outcome. HDFS stores extremely large files containing record- oriented data and that data can be used for references. It does not split large data files. The size of the files and the number of replications are not configurable but it can be duplicated and used by theusers..

1. OVERVIEW OF THEPROJECT

Organizations today are confronted with the challenge and the opportunity of data growing at unprecedented rates. This data comes from numerous sources such as
– ERP systems, Web services, Data Warehouses, Website logs Social Media, Mobile devices, Sensors, etc. - in various forms - Structured, Semi- structured and Unstructured. It does not splitlargedatafiles.Thesizeofthefiles and the number of replications arenot

2. OBJECTIVE OFPROJECT

Big Data is the growing field with rapidly changing data and related values. Big Data analytics has the potential to provide great insights and opportunities to organizations in the areas of consumer

behavior, marketing, fraud detection and customer service. With the right technical architecture, true real-time decisions are configurable but used in various places. The use and adoption of Big Data within Organization processes is beneficial and allows efficiencies in terms of cost, productivity, and innovation. It does not split large datafiles. The size of the files and the number of replications are not configurable. To reduce productivity, cost and innovation within an organization Big data is used.

enabled providing organizations with heightened agility. While most organizations recognize the importance and benefits of Big Data analytics, there are challenges arising from the nature of Big Data analytics and limitations of existing technologies that need to be considered for improvingpurpose.

3. SCOPE OF THEPROJECT

Without any hacking information , this paper provides a group communication between the members present in the particular group.An intruder can't simply eavesdrop a group communication because web socket protocol was proposed without key escrow. By knowing the group encryption key and decryption key, any entity can encrypt or decrypt the messages to the group members. Application such as in military areas it can be used in an effective manner.

1. PROBLEMSTATEMENT

The organization is responsible for storing the data and retrieving the data that are stored in a common place. In all the branches they can store and retrieve the data. The data will stored in the common database.Thevalues will be retrieved/used by using MapReducealgorithm. The secret keys whichare

1. DOMAININTRODUCTION

Database Systems and Knowledgebase Systems share many common principles and simulates the ideas of key exchanging andinteraction between these two related fields of interest. With the useof

2. SYSTEMANALYSIS

2.1 EXISTING PROJECT

In the existing system, Static members is having the same group communication.It may become inefficient because the sender may change the key frequently. Group Key Agreement protocol requires two or more rounds to establish a secret key.User priority will be analyzed only

DISADVANTAGES

used by the group members are leaked, then the previously established secrets will be exposed to the attacker. Therefore the protocol is no longer secure and can be hacked easily. The attackers will intrude the data easily and security is very less.All users have to stay online to finish the protocol before they can receive any encrypted contents.
DKE, the paper mainly concentrate on identify, investigate and analyze the underlying principles in the design concepts and effective use of these systems. The original result has been published with new items inknowledge engineering and the interfaceofthetwofields.

through the session concept. A trusted third party people are used to generate keys for the members in the group is not available. The estimation is hard because we don't know who will send encrypted messages to the group members. All users have to stay online to finish the protocol before they can receive any encryptedcontents.

When then the previously established secrets will be exposed to the attacker and the protocol is no longer secure , the secret are leaked.

2.2 PROPOSEDPROJECT

The main objective of thispaper is to provide secured communication for the group of members. More than one-round/single user IBAAGKA protocol is proposed BAAGKA protocol enables a groupof

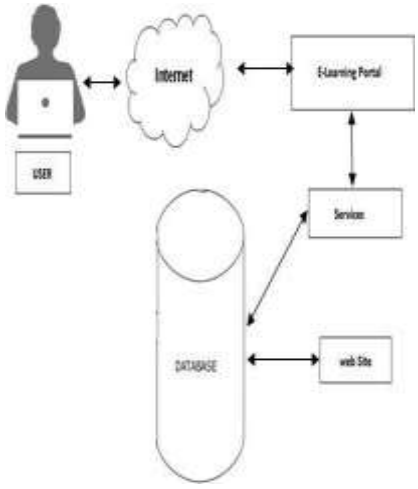
user may join or leave the group. It provides communication efficiently. This system is key escrow free. An

3. SYSTEMARCHITECTURE

All users have to stay online to finish the protocol before they can receive any encrypted contents. Security is less, because the active and passive attackers intrude the data easily.
users to establish a common encryption key and their respective decryption keys. Dynamic

member are allowed in group communications. Group member can only view Attachment file. It does not suffer from the key escrow problem.

attacker cannot break the secrecy of previous protocol runs even if the attacker obtains all the members long- term private keys.



4. SYSTEMIMPLEMENT ATION

4.1 USERMODULE

In this module, the user side login will be authenticated and session is maintained. User registration must be needed in this module. The user login and registration is common for both the Server and Client. To begin the secure communication between the clients, initially server-side must runthe application. This feature helps group of people to share or exchange informationin

.

4.2 ADMINMODULE

In this module,theAdmin side login will be authenticated and session ismaintained. HeretheAdminrolewillbeIPconfigurations are provided to group members. So that unauthorizedpersonscan'tabletoenterintothe group. Admin can able to view the member of the group that are created. In case if members of group need to be update, the admin can able to make thechanges.

5. CONCLUSION

The main concept of thepaperis to provide secured communication forthe

6. FUTUREENHANCEMENT

In future, the group admin can mute a single person chat in a group to avoid unwanted Circumstances. Based on the user requirement it is possible to
. a group of members without loss of data. All the member in the group can able to interact with each other. Members in a group are allowed to join or leave the group. Information which is shared within the group member is securely maintained by using the encryption and decryption process.

group of members was achieved. IBAAGKA protocol enables a group of users to establish a common encryption key and their respective decryption keys. Dynamic member are allowed in group communications.

It offers secrecy and known-key security, and it does not suffer from the key escrow problem. the group admin can mute a single person chat in a group to avoid unwanted circumstances. Based on the user requirement it is possible to implement the video communication for my web application. implement the video communication for my web application.

REFERENCES

- M. H. Au, J. K. Liu,W. Susilo, andJ.

  Zhou, "Realizing fully secure unrestrictedID-based ring signature in the standard model based on HIBE,"IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1909– 1922,Dec. 2013.

- M. Bellare and P. Rogaway, "Entity authentication and keydistribution," inProc. 13th Annu. Int. Cryptol. Conf. (CRYPTO), 1994, pp.232–249.

- D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT), 2005,pp.440–456.

- D. Boneh and A. Silverberg,"Applications ofmultilinear forms to cryptography,"

  Contemp. Math., vol. 324, no. 1, pp. 71– 90,2002.

- M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," in Proc. Workshop Theory Appl. Cryptograph. Techn. (EUROCRYPT), 1995, pp.275–286.

- L. Chen and C. Kudla, "Identity based authenticated key agreement protocols from

pairings," in Proc. 16th IEEE Comput. Security Found. Workshop (CSFW), Jun./Jul. 2003, pp.219–233.

- L. Chen, Z. Cheng, and N. P. Smart, "Identity-based key agreement protocols from pairings," Int. J. Inf. Security, vol. 6, no. 4, pp. 213– 241,2007.