ISSN No:-2456-2165

Privacy Preserving Methodology for Anonymous Data Sharing

Anugraha.K
M-Tech Student,
Dept. Computer Science and Engineering
IIET, Nellikuzhi, India

George T Vadakkumcheril
Assistant Professor,
Dept. Computer Science and Engineering
IIET, Nellikuzhi, India

Abstract:- Data sharing safety (video, audio, images, etc.) serves an important role in our lives. Protected data sharing is included in my paper, as is maintaining the confidentiality of the sensitive document and the protection of its data sensitivity. The proposed scheme allows data to be used in a variety of ways while still addressing privacy and security concerns. A variety of servers are included in the scheme, which is used to exchange data in a secure manner. A large or small amount of data divided into equal chunks, with each chunk collected by the recipient from several participants. Ordinary individuals can use it to provide info to trusted police without disclosing their names or identities.

Keywords:- *Asymmetric Encryption, Elliptic Curve Cryptography.*

I. INTRODUCTION

The method for anonymous data sharing that maintains anonymity and is mostly used for secure data transfer. The system formerly relied on direct transmission. For safeguarding sender data, many forms of encryption [3] and varying levels of security measures are available. However, the sender is not secure while sending anonymous data. The receiver or data leaker can automatically transfer all of the sender's data. This applications implements generally used encryption and decryption technologies. The system employs a highly efficient algorithm. The intractability of some mathematical problems is the foundation of public-key cryptography. Early public-key systems were built on the assumption that factoring a massive integer with two or more massive prime factors was impossible [1]. The key assumption for elliptic-curve-based protocols is that computing the discrete logarithm of a random elliptic element with respect to a publicly accessible base point is difficult. The total number of discrete integer pairs is used to determine the length of the attribute value. Encryption can help to protect data transmitted, received, and stored by a device while keeping the device's true identity private.

A. Objective

Framework for action of personal data are managed online and encrypted or on always-on servers. It's almost hard to undertake business without your personal data winding up in a networked computer system, hence why learning how to help keep that data private is important. Encryption is the process of converting plain text, such as a text message, into an unreadable format known as cipher text. This improves the security of digital data kept on computer systems or transported across a network like the internet. The text gets changed back to its original form when the receiver reads the message. To decode the information, both the sender and the recipient should have knowledge to a private cipher.Maintaining the Integrity of the Specifications.

B. Scope

This paper focuses on a data sharing system that uses ECC to achieve information inequality and privacy. It is difficult to devise a good method for communicating outsourced data while safeguarding the data owner's identity. To address the aforementioned problem, then propose an anonymous data sharing scheme. It is mostly beneficial to average citizens. A murder witnessed by someone who does not want the victim's identity revealed, for example. He does, however, take pleasure in transmitting intelligence to respected police in the dark. The mechanism facilitates the transmission of such information. A direct transition is not secure for secret data transfer. They can easily be accessed by a third party. As a result of the multiple servers used to transmit files, the participants are unable to recognize their chunks. It also believes that the receiver will be able to receive data without leaking any information. In this circumstance, elliptic curve cryptography is being used. Elliptic Curve is a symmetric encryption approach that encrypts points within an elliptic curve group by applying a variety of the discrete logarithm.

C. Related Works

The administration of data while keeping its use and security strategy is a concern for the cloud owner. A layered architecture was proposed in order to reduce the overhead at the cloud service provider for applying security to each document and then delivering it to the client. This strategy protects the security of the sensitive document as well as the privacy of its sensitive data [5].

The proposed methodology classifications based on the data sensitivities to achieve a balance between privacy protection and usefulness. Create a distributed cloud-based system in which data is classified into four levels of sensitivity: public, confidential, secret and top secret with each level requiring a different level of protection. At the most sensitive levels, such as secret and top secret data, a provision are put in place that identify destination node that

ISSN No:-2456-2165

were generating data leaks. Previously, this system relied on direct transmission. There are many different encryption methods and levels of encryption accessible to secure transmitter data. When transferring anonymous data, however, the sender is not secure. The receiver or data leaker has unrestricted access to all of the sender's information.

II. PROPOSED SYSTEM

The device model consists of a user and several servers, referred to as participants. When a sender sends data to the server, it is broken into several equal-sized chunks and then sent to the participants. The data from multiple participants is collected by the server. Since the data is in an encrypted format, each participant is unable to access their portion of the data. In addition, the server is unable to determine the data owner or the source of the data.

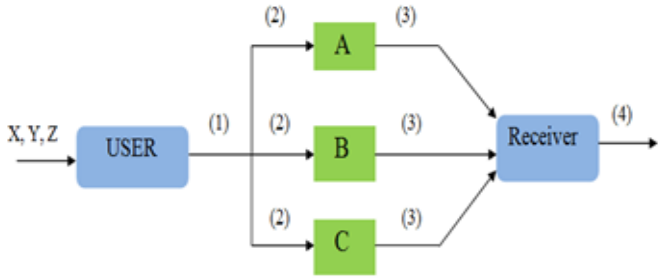

Fig- 1 System model

- Dividing the data (X, Y,Z) into several three equal sized chunks.
- Encrypt the data using ECC and distribute the chunks to participants A, B, and C.
- A, B, and C submit their chunks to the appropriate recipient.
- Finally, the receiver gathers data from several servers and decrypts it.

a) Encryption of data

ECC is a type of encryption used to encrypt data such as audio, video, and photographs. ECC is a versatile encryption method that can be used in place of RSA. It maintains secret key safety for public key encryption using elliptic curve mathematics. Encrypt the data once it has been split into equal-sized chunks. ECC is an asymmetric encryption method, so the public key and private are different.

b) File uploading and splitting

Any type of media, such as video, music, photographs, PDFs, and Word documents, can be added by the user. Files can be broken into equal-sized chunks once they've been uploaded. The chunks are then XORed together. A service provider cannot open the files. This method of communication is more secure.

III. CONCLUSION

The system, it was agreed, must provide safe and secret data transmission. Encryption is a method of transferring data such as video, audio, photos, and other sorts of data without disclosing the identity of the sender. It also thinks the receiver will be able to receive data without disclosing any data. In this case, elliptic curve cryptography is being used. ECC licenses allow for a smaller key size while yet retaining a high level of security. It is harder for hackers to decode than RSA and DSA. This strategy is superior to others since it is more efficient, secure, and powerful.

REFERENCES

[1]. Farzad Salim; Nicholas Paul Sheppard; Reiheneh Safavi-Naini, ”A right management approach to securing data distribution in coalitions” 2010 Fourth International Conference on Network and System Security.

[2]. A. Shabtai, Y. Elovici, and L. Rokach, “A Survey of Data Leakage Detection and Prevention Solutions,” Springer-Verlag NY, 2012, DOI: 10.1007/978-1-4614-2053-8.

[3]. K. Singh, M. Dave, and A. Mohan, “An efficient certificate less encryption for secure data sharing in public clouds,” Natl. Acad. Sci. Lett., vol. 37, no. 4, pp. 351-358, July-Aug. 2014, DOI:10.1007/s40009.

[4]. A. M. Nia, S. Sur-kolay, A. Raghunathan, and N. K. Jha, “Modified AES based algorithm for mpeg video encryption,” IEEE Trans. Emerg. Topics Compute, vol. 4, no. 3, pp. 321-334, Sept. 2016.

[5]. Ishu Gupta, Member, IEEE, Niharika Singh, and Ashutosh Kumar Singh,”Layer based privacy and security architecture for cloud data sharing,” VOL. 15, NO. 2, JUNE 2019