Secure Storage & Retrieval Using biometrics

Anoop V Kanavi
Student
Master of Computer Application
Jain (Deemeed-to-be University)
Bangalore, India
anoopk334@gmail.com

Feon Jaison
Assistant Professor
Master of Computer Application
Jain (Deemeed-to-be University)
Bangalore, India
feonm.j@gmail.com

Abstract -- Cloud storage and computing have revolutionized the technology world for more than a decade. Cloud computing and storage have huge advantages over traditional methods. cloud storage and computing are very efficient because they have benefits like cost-effectiveness, faster speed, configuring doesn't take much time, you pay for what you use, around the clock availability, and many more. since cloud storage is cost-effective most database users move to the cloud. this brings us to the issues and challenges with cloud storage and computing. one of the major issues is the privacy of data or information transferred in a virtual environment of the cloud. since the cloud architecture is based on virtualization technology which provides a virtual environment. In recent years biometric authentication has become popular. traditional authentications such as patterns, passwords, ID, aren't enough to stop social engineering attacks like ID Theft. such methods are easy to be forgotten, lost, guessed, brute force, or shared. biometric is more secure because it identifies the individuals by anatomical traits like a fingerprint, iris, face detection, voice, etc. since biometric data is used and stored. the government body which collects citizen details would love to store data is in the cloud to make it cost-effective. In this paper, we are going to talk about the privacy issues and problems of storing data in the cloud and how we can use biometric to achieve confidentiality and integrity.

Keyword: Cloud Security, Biometric authentication,

INTRODUCTION

Cloud storage and cloud computing have become increasingly popular in recent years. With the development of cloud computing and research on virtualization, database owners are motivated to outsource the huge size of data to the cloud to save computational costs and to get rid of expensive storage costs. The cloud computational and storage are cost-effective to the database owners because the cloud service provider offers a lot of resources that are accessible to cloud users. The provided services are computational resources are processing power, power supply, storage disks, software support, and network operational management. The cloud users are also offered with virtualized infrastructure known as Infrastructure-as-a-Service (IaaS). The users will request the required software, hardware, and application to the provider. The virtual environments are hosted and controlled by the cloud provider. This saves a lot of computational cost and maintenance cost. Biometric authentication/identification is increasing day by day. you use biometrics in your phone to login into the device, you have a payment app which you use to your fingerprint to transfer money. in recent day biometric identification has become more reliable and convenient to use compared to the old authentication methods like password, patterns, ID card, etc. biometric authentication has been widely used in different fields by using different types of biometrics like fingerprint, iris, facial recognition, etc. which use different sensors to collect biometric data. In a biometric identification system, the database owner such as the government body who are responsible to manage the citizen data including the fingerprint and iris data. the company may desire to outsource the huge biometric data to cloud servers like IBM, Amazon, to save expensive costs on storage and computation. However, to make sure that your data is secure and safe we have to encrypt the data before sending the data to the outsourced cloud service provider. whenever a user or a citizen wants to access any data, he has to turn to the company and generate an identification query by using the user's biometric data. then, the company encrypts the query and sends it to the cloud to find the close match. The problem is how to design a protocol that gives efficient and privacy-preserving biometric identification in cloud computing.

CLOUD THREATS

Despite possible benefits of cloud computing like rapid disposition, cost-effectiveness, scalability,

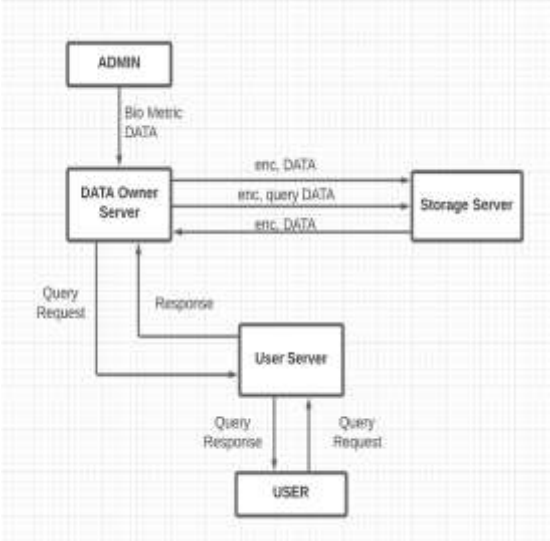
pervasiveness, and no. of distinct features, it possesses a no. of challenges like High-Performance Computing, trust, consistency, competence, management of danger, consistency, and plenty of more. Although, data security is taken into account one in all the first challenges in cloud computing. it's yet not answerable that in what ways data may be kept secure from malevolent users. Each cloud disposition model has distinct levels of knowledge privacy, the general public cloud has less data discretion associated with other clouds. The private cloud is taken into account more protected as compared to others but it's more costly. Procurement of the facilities provided by that of personal clouds is problematic because it is unaffordable by both low and middle-class organizations. the only real public clouds face data confidentiality, safety, and accessibility matters. Hence, the conception of multi-clouds is more useful because it provides better considerable safety and cloud services accessibility. These also are called inner clouds. Foremost data protection challenges in cloud computing are associated with resources sharing on the net accessing virtualization and dispersed technology. The storage service is considered a fundamental service offered by clouds. All amenities are acquiescently accessible for entire users. Different organizations and govt. might use the cloud for storing sensitive info. the info is stored anywhere globally, despite saving data and info on the server of a corporation, it's stored in a cloud's server which might then be shared in any parts of the planet. because of its centralized position, it becomes easier for malicious users to illegally access this data. Enhancements in user's data ultimately increased the protection risks and crimes especially cyber-crimes. Reports of the IDC survey indicated that data safety risks are rated 88 percent.

PROBLEM STATEMENT

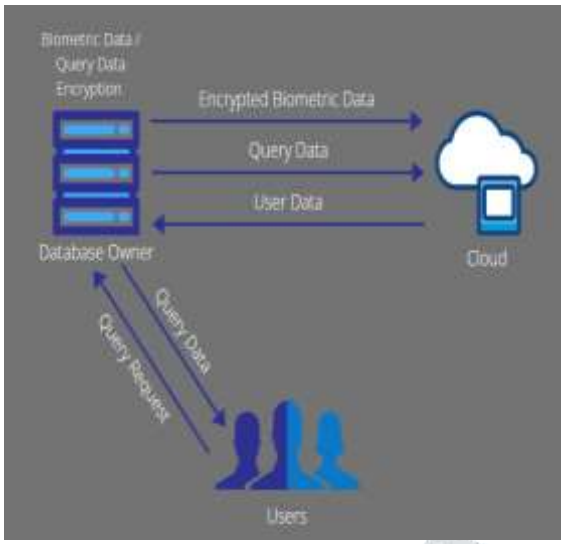
Most of the cloud service provider doesn't encrypt their data in the cloud and many users don't encrypt the data before uploading to the cloud. there are around 1500 data breaches every year, which questions the privacy of the user data stored in the cloud. Some companies encrypt the data in the cloud but the chances of decrypting the are slim but not zero. In 2018, The chairman of the Telecom Regulatory Authority of India (TRAI) R S Sharma disclosed his Aadhaar number on the microblogging site and challenged Twitter users to show how the information could be used to harm him. The chairman was Denying the data breach on UIDAI. within 7 hours hackers posted a screenshot of sending rs.1 to Mr. Sharma via the Aadhaar-enabled payment service using apps such as BHIM and Paytm. the hackers later went on sharing Mr. Sharma's mobile no DOB, Residential address, phone no, PAN no, Bank details, etc. In Kerala, there was a similar case where the government was trying to outsource the data to a non-governmental agency. This might have led to a severe data breach with Hugh security ramifications. the data had confidential information of the Kerala police, it even had the criminal case and criminal records. which could have been accessed by the third-party agency. But this was stopped by officers and opposition leaders. Due to Covid Pandemic people sitting at home tried to make money through stocks. At end of FY20, there were around 40.8 million new Demat accounts opened. There are few companies that offer complete online trading. among them is Upstocks. Upstocks had a data breach in April 2021 releasing details like Aadhaar, PAN card, and Bank account number. Mobikwik is a mobile wallet and payments app. In April 2021 they had data leaked and the data was available on the dark web. the data set was around 8.2TB in size. the data included information like KYC documents, Aadhaar cards, Credit card details, mobile phone numbers linked to MobiKwik wallet.

PROPOSED SYSTEM

The idea is to solve the problem of privacy. To do this we can make an efficient and privacy-preserving identity verification method that will stop the attack launched by the users and the cloud. we analyse the identification method and its show security weakness under level 3 attack. specifically, we demonstrate that a hacker can retrieve a secret key by intercepting the cloud network and can decrypt the biometric data that is stored in the database. Three kinds of endpoints are involved during this system that's the database manager, data users, and therefore the cloud. The database manager holds a huge quantity of biometric data which is encrypted and transmitted to the cloud for storage. when a user tries to log in or tries to retrieve data from the database, the user has to send a request query to the database manager. The manager hashes the biometric value sent by the user to the cloud to verify the biometric hash value that is stored in the cloud. The cloud software will analyse which stores hash value is close to the hashed query and returns the data to the database manager. the database manager checks the query data



and biometric data and check the index and sends the user the requested data.



IMPLEMENTATION

when the user shares his information with the database owner. The collected data will be encrypted in the database before sending it to the cloud. The collected details like biometric will be hashed and encrypted before storing in the cloud. Once all the data is encrypted and stored in the cloud. The user can access the stored data by using his fingerprint for biometric authentication and send a query. the database owner will take the biometric data and hashes it and matches the data with the stored biometric hash data in the cloud and retrieve the query data. Since the data is being encrypted at the endpoint even is if the data is stolen by the attackers. They will have stolen encrypted data. which will hard to decrypt all the data hence becoming useless.

Advantages of Proposed Systems

- Reduce workload and enhance productivity
- Better flexibility and speed
- It is Efficient since Computational costs should be as low as possible.
- Better Security During the identification process, the privacy of biometric data should be protected.

CONCLUSION

This paper proposes an efficient and privacy-oriented biometric authentication in cloud computing. the proposed biometric authentication system is a very secure and new upcoming strategy in secure cloud computing. to achieve privacy, we design and analyze a new method of authenticating in a cloud system. the analysis shows that the proposed method will protect from potential attack. It provides higher security from attackers, therefore, protects the privacy of the user who stores their data. this system achieves all the three triads of security integrity, confidentiality, and accessibility.

REFERENCE

[1] Using Multi-Clouds to Ensure Security in Cloud Computing. Mohammed A. AlZain, Ben Soh, Eric Pardede.

[2] An Efficient and Privacy Preserving Biometric Authentication Scheme in Cloud Computing. LIEHUANG ZHU, XIMENG LIU.

[3] Biometric Authentication System Security and User Privacy. Anil K. Jain, Karthik Nandakumar.

[4] An Efficient and Privacy Preserving Biometric Authentication Scheme. Dr.V. Naresh, T. Gopi Venkata Ajay, T. Naga Sai Reddy, M. Srinivas.

[5] Challenges and threats in cloud security. Gnana Chaitanya, Chagarlamudi.

[6] Classification of Data to Enhance Data Security in Cloud Computing. Kumar Pal Singh, Dr. Vinay Rishiwal, Prof. (Dr.) Pramod Kumar.

[7] Cloud Data Security while using Third Party Auditor. Ashish Bhagat, Ravi Kant Sahu.

[8] Two Factor Authentication Access Control for Web Based. Chandana c, Vanishree M L,Dr. Kavitha K S, Dr. Kavitha C.

[9] A Survey on Cloud Storage. Jiyi WU, Jianqing FU, Zhijie LIN, Jianlin ZHANG.

[10] Cloud Computing & Security Issue. Manisha Thakur, Dr. Neeru Bhardwaj.