HIDING SENSITIVE INFORMATION OF STUDENT FOR SECURE STORAGE ON CLOUD

Ankita Khelge[1], Nikita Dhumal[2],

Pratiksha Khopade[3], Mrs. Sonali Dhuttargi[4]

Student Department of IT[1,2,3], Assistant Professor Department of IT[4]

Bharati Vidyapeeth's College of Engineering for Women.

Abstract:

Cloud Computing provides a best way to the user for storing and computing the data. We can use cloud computing to maintain data privacy and confidentiality in the cloud. We have to pay-per-use and it requires an internet connection for work. Due to the lack of data security cloud provides an efficient way to store the data in encrypted form on the cloud. The aim is to prevent misuse of student documents and search the require data as per student requirement. IT application plays an important role in the area in any college organization where we need to secure confidential document. Cloud users are uploading personal or confidential data to the data center of a Cloud. The security analysis and our proposed scheme is secure and efficient. Our aim is to protect the data from unauthorized access. The cloud file might contain some sensitive information and it should not be revealed to others. Hence before sharing, the whole file will be encrypted using ECC/AES algorithm. For decrypting the document, the QR code first needs to be scanned using a cell phone and OTP is used to authentication for downloading and accessing the document. The whole system would be menu-driven and user-friendly. The reason behind why QR code are more useful than a standard barcode is that they can store (and digitally present) much more data, including URL links, geo coordinates, and text.

Keywords: Cloud storage, data integrity auditing, data sharing, sensitive information hiding.

I. BACKGROUND

An ever-increasing number of organizations and people might want to store their information in the cloud. Be that as it may, the information put away in the cloud may be corrupted or lost because of the unavoidable programming bugs, equipment issues and human blunders in the cloud. The information put away in the cloud is consistently shared over various clients in many distributed storage applications, for example, Google Drive. Sensitive information in the context of cloud computing encompasses data from a wide range of different regions/areas and disciplines. To avoid data protection breakdowns

that might result in enormous and costly damages, technical measures and organizational safeguard are need to be deployed using cloud platforms. These shared data stored in the cloud might contain some sensitive information of the user by considering the example of student's sensitive information where these SRs (Student Records) are directly uploaded to the cloud which wants their sensitive information to be shared for admission purposes. The sensitive information contains details of both students and college will be inevitably exposed to the cloud. Sensitive educational records are a typical example of information handled in cloud computing environments, and it is obvious that most individuals will want information related to their education to be secure. Hence, with the evolution of these new cloud technologies in recent times, to protect individuals against surveillance and database disclosure, requirements like data privacy and data protection are increasing. Many remote data integrity auditing schemes have been proposed to verify whether the data is stored correctly in the cloud. In remote data integrity auditing schemes, before uploading them to the cloud the data owner first needs to generate signatures for data blocks. To prove the cloud truly possesses these data blocks in the phase of integrity auditing signatures are used. after the data owner uploads these data blocks along with their corresponding signatures to the cloud.

This paper represents an overview of the research on the security and privacy of sensitive data in cloud computing environments.

II. RELATED WORK

This scheme ensures retrieval and integrity of sensitive data stored on the cloud. In cloud storage scenarios data sharing is an important application. A privacy-preserving shared data integrity auditing scheme is designed by modifying the ring signature for secure cloud storage, to protect the privacy of user identity. A shared data integrity auditing scheme with user revocation by using the proxy re-signature is proposed, to support efficient user Revocation. The aforementioned schemes all rely on Public Key Infrastructure (PKI), which incurs considerable overheads from the complicated certificate management. To simplify certificate management, an identity-based remote data integrity auditing scheme in multi-cloud storage is used. This scheme used the user's identity information such as the user's name or e-mail address to replace the public key. However, all of the existing remote data integrity auditing schemes cannot support data sharing with sensitive information hiding. In this paper, we explore how to achieve data sharing with sensitive information hiding in identity-based integrity auditing for secure Cloud storage.

III. MOTIVATION

To ensure that the Credential information (nothing but Students Documents) of the file is not exposed to the third-party user and all of the Credential information of the file is not expose to the cloud and the shared users.

IV. SYSTEM ARCHITECTURE

Figure shows a detailed flow of Admission process system. It consists of two modules that is

college and student. In this system, the Credential information can be protected and the other information can be published. It makes the file stored in the cloud able to be shared and used by others on the condition that the Credential information is protected, while the remote data integrity audit still able to be efficiently executed.

Parameter	ECC	RSA
Year of proposed	2005	1977
Computational Overhead	Roughly 10 times than that of RSA can be saved	More than ECC
Key Size	System parameter and key pair are shorter for the ECC	System parameter and key pair larger for RSA
Bandwidth Saving	ECC offer considerable bandwidth saving over RSA	Much less bandwidth saving than ECC
Key generation	Faster	Slower
Encryption	Much faster than RSA	At good speed but slower than ECC
Decryption	Slower than RSA	Faster than ECC
Small Device Efficiency	Much more efficient	Less efficient than ECC
Scalability	Optimal scalability	Not optimal

Encryption Technique: To encrypt the data using encryption. This process will continue at the time of file upload. For this, we are using the AES (Advanced Encryption Standard) algorithm.

Decryption Technique: Here in this process we are performing decryption at the time of file download to get data in original form.

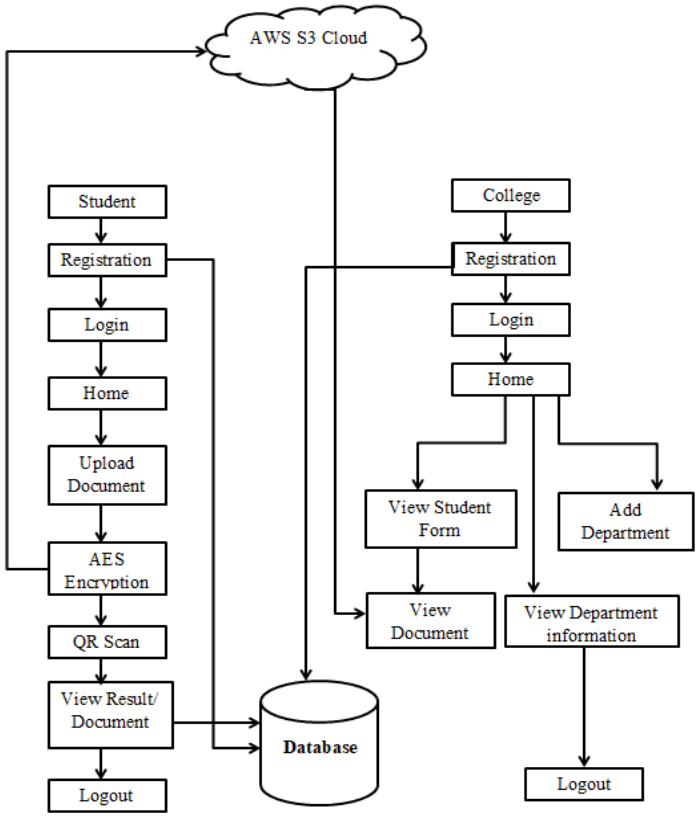

Fig. 1 System Overview

[4] ECC (Elliptic curve cryptography): In this algorithm, we are generating a signature for file to save the data confidentiality. That signature will be linked to the file.

Table No. 1 (Comparison between ECC and RSA)

From above comparison table we get to know that ECC is better than RSA. Hence instead of RSA we are implementing ECC.

Parameter	AES	3DES	Blowfish
Key length	128,192 OR 256 Bits	168(K3),112 (K1, K2)	32-448 Bits
Cipher type	Symmetric block cipher	Symmetric block cipher	Symmetric cipher algorithm
Block size	128,192, 256 bits	64 bits	64 bits
Develped	2000	1978	1993
Securiy	Considered secure	One only weak which is exit in DES	Vulnerable
Possible keys	2^{128} ,2^{192},2^{256}	2^{168},2^{112}	2^{32},2^{448}
Round	10(128 bit), 12(192 bit), 14(256 bit)	48	16
keys	single	Single	public

Table No.2 (Comparison between AES, 3DES, Blowfish)

From above comparison it is clear that AES is better for encryption due to its key length and AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 64-bit key of DES and blowfish.

CONCLUSION: In this paper, we are proposing a system to protect the Credential information of the student. In this paper, we proposed an identity-based data integrity scheme for secure cloud storage, which supports data sharing with Credential information hiding. Our scheme makes the file stored in the cloud able to be shared and used by others on the condition that the Credential information is hidden, while the remote data integrity auditing is still able to be efficiently executed

REFERENCE:

[1] Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage Wenting Shen, Jing Qin, Jia Yu, Rong Hao, and Jiankun Hu Senior Member, IEEE, VOL. 14, NO. 2, FEBRUARY 2019

[2] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy preserving secure cloud auditing scheme for group users via the third party medium," Journal of Network and Computer Applications, vol. 82,pp. 56–64, 2017.

[3] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Trans. Inf.Forensics Security, vol. 11, no. 6, pp. 1362–1375, Jun. 2016.

[4]Chaitanya Varma, "A Study of the ECC, RSA and the Diffie-Hellman Algorithms in Network Security," IEEE Conference 2018.