DATA SECURITY ON VIRTUAL ENVIRONMENT USING ENCRYPTION STANDARDS

Chandini M S[1], Kalyan Simha B[2], Poornashree A S[3], Sreelekha R[4]

[1]*Professor Department of CSE, BITM Ballari*
[2,3,4] *Student Department of CSE, BITM Ballari*

---***---

ABSTRACT - *Cloud Computing is an evolution in computing with a rich family tree. Since the era of the mainframe the industry and computing has evolved in dramatic ways. The concept of cloud computing offers scalable resources dynamically as a service over the internet. The main economic benefits of cloud is that it offers low capital investment and low operational cost. Data security for cloud service encompasses several aspects including secure channels, access controls and encryption. The security in cloud will alternate from higher risk to lower risk and security controls has to be continuously reviewed to support the changes and evolving threat capabilities. There are many data protection approaches used to ensure maximum data protection by reducing risks and threats. The proposed system provides security to data in android devices and also in the cloud environment by adopting cryptographic techniques. We are proposing a simple system that encrypts and decrypts the text files to store and access through cloud. The proposed system enabled trains of information security like confidentiality, integrity and availability of data in cloud computing environment.*

KEY WORDS: Cloud Computing, cryptographic techniques, AES, Encryption, Decryption.

1.INTRODUCTION

Virtual environment is a system that uses remote servers on the internet to store, manage and access the data online rather than local drives. Virtual storage is a system that has more memory which is used to store large or bulk data. Here data security is an important aspect. Cloud storage is an example of virtual environment. Software and databases runs on the cloud server which can be accessed over internet. The storage and computing of data doesn't takes place on the device instead on the servers in the data center, hence users can access data stored in cloud from any device. Data protection in cloud plays a major role. It is the process of securing data in cloud environment without considering any factors like data location, state of data and its management that may be internal or external by third party. Cloud computing is used for efficient and smooth running of business along with infrastructure and software support to computing systems. Various fields such as data storage, education, entertainment, social networking as well as management have great uses of cloud computing. There are many mobile Cloud Computing applications that do not even require a laptop or personal computer to be accessed from. Nowadays companies have moved from building and managing their own data center to storing data in the cloud. The sensitive data in the cloud environment hosts security concerns like data breach, data theft, application vulnerabilities and malware proliferation. Cloud security is a collection of security measures designed to protect the data that includes authentication of devices, access for data and resources. Vulnerabilities in cloud can be seen because of lack of cloud security awareness among operators, customers, managers or technical vulnerabilities.

2.LITERATURE SURVEY

The system for improving Cloud security using biometrics and encryption system collects biometric sample from the user at client side and applies minutiae algorithm that extracts features form biometric sample and verify it in cloud database. If verification is successful the system send login request to server. The cloud authentication server randomly generated OTP and then encrypts the user data using Advanced Encryption Standard and sends encrypted data to user. Using OTP sent by server through HTTP gateway the user can decrypt or convert encrypted data into readable format as mentioned in [1].

Data security in cloud computing is related to virtualization, storage in public cloud and multitenancy. Hypervisor a special function is required to run the OS as virtual machine and can become a primary target if vulnerable. If it gets compromised then whole system can be compromised and hence the data. Another risk in virtualization is the allocation and de-allocation of resources. Usually Clouds implement centralized storage facilities which can be appealing for hackers. Multitenancy is one of the major advantage as well as risk to data in cloud computing. Several authentication techniques are in use to avoid multitenancy issues. Data security in cloud involves more than encryption and depends upon SaaS, PaaS and IaaS. It is difficult to protect the data at rest and issues arising due to data at rest can be resolved by maintaining a private cloud with controlled access. Data in Transmit can be protected by various encryption strategies as mentioned in[2].

Threats in cloud computing environment includes data breach, data loss, account or service traffic hijacking, insecure interface and API's, malicious insiders, insufficient due diligence, shared technology vulnerability, lock-in and acquisition of cloud providers. Attacks in cloud environment includes denial of service, attack on hypervisor, resources freeing attacks, side channel attacks and attacks on confidentiality is mentioned in [3].

As mentioned in[4], the system has been split into four parts namely the system preparation process, Key Establishment Unit that is to the data owner, uploading data to public cloud and downloading data from public cloud. The data owner installs Cloud Management Client application that encrypts data prior uploading the data and decrypts after downloading it from public cloud. This eliminates the problem of data breach and key disclosure risks.

3. PROPOSED METHODOLOGY

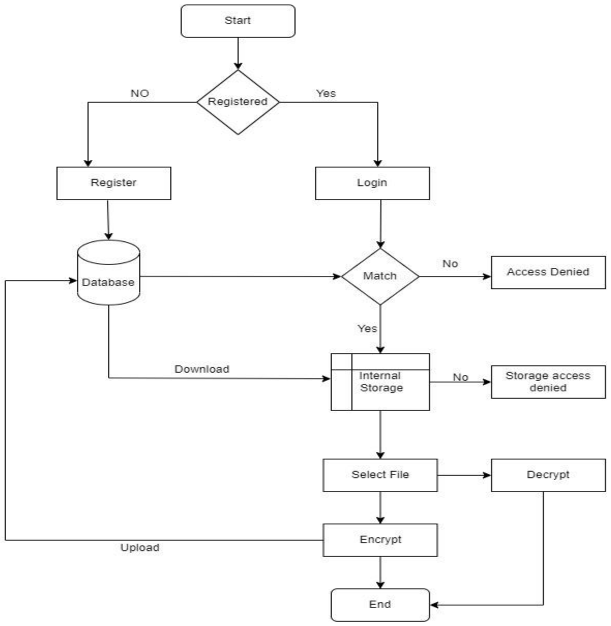


Fig 3.1 Flowchart

- **Registration:** The application needs to identify the user to save their data in the cloud. To enable this, we use firebase authentication that provides backend services. Custom authentication of firebase makes authentication easy for the users. The user has to provide username and set a new password to register for the first time. The password must contain minimum of 6 characters and has to be matched with confirmation field provided. As the user registers the credentials will be stored in the firebase that helps for future login. If any of the field is left empty an appropriate toast is displayed to the user. If the user is already registered, they can move directly to login frame by clicking on 'Have Account? Login' button in register page. Registered user can be checked in the firebase console.

- **Login:** It allows a user to gain access to the application when they enter valid details. The login screen consists of two text fields - one for entering username and other for password. If either of the text fields are empty then an appropriate error is displayed to the user. The registered user has to provide valid credentials for logging into the application. Otherwise, login will be failed. Only registered users can login in to the application. When any of the registered user forgets password in that case the application provides a way to reset the password. When user clicks on 'forgot password' the application ask the user for mail id and check that user in firebase. If existing user, a mail is sent to respective user that contains a link to reset the password. After changing the password user can easily login intothe application.

- **Encryption:** After login, the user has to select the doc file to be encrypted. If the field is left empty an appropriate message is displayed to the user. Storage permissions need to be granted by the user before selecting a file from internal storage. AES algorithm will be applied to selected file and encryption takes place. The encrypted file will be stored in the internal storage with .txt extension.

- **Decryption:** After the user encrypts a file, if the file is to be decrypted then the user should select the required encrypted file from the list. AES algorithm will be applied to the selected file and decryption takes place. The decrypted file will be stored in the internal storage with .txt extension.

4. Cryptographic Techniques

Enhancing data security in cloud is the main concern and there are two distinct encryption methods like symmetric and assymetric techniques that provides a solution. Symmetric encryption method is also called as secret key algorithm or private key cryptography that requires sender and receiver to have access to a same key where both have to ensure that key is stored securely. Assymetric encryption technique is also called as public key cryptography that uses two keys for encryption(public and private key). Public key is freely available to anyone, whereas the private key remains with the intended recipients only, who need it to decrypt the message.

AES, RSA, Triple DES, Blowfish and Twofish are some of the cryptographic algorithms.

The proposed system uses AES to ensure data security in virtual environment.

AES: The Advanced Encryption Standard (AES) is a trusted standard algorithm that is extremely efficient in 128-bit form and also uses 192 and 256-bit keys for encryption purpose. It is defined as go to standard for encrypting data in private sector as it is invulnerable to all types of attacks except brute force. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. One round consists of several steps that include substitution, transposition and mixing of the input plaintext to transform it into final ciphertext. The first step in the AES encryption cipher is substitution of data using a substitution table followed by shifts in data rows. The third step is concerned with mixing columns and the last transformation is performed on each column using a different part of the encryption key.

Triple DES: Triple DES is a symmetric key block cipher that is successor to Data Encryption Standard (DES) algorithm which applies DES algorithm three times to every data block.

RSA: RSA is a public-key encryption asymmetric algorithm which was invented by Rivest, Shamir and Adleman. This algorithm is frequently used to secure connection between VPN clients and servers as well as seen in web browsers, email and other communication medium.

Blowfish: Blowfish is a symmetric key block cipher that was designed to replace DES. It was created by Bruce Schneier that uses single encryption key to encrypt/decrypt and provides a good encryption rate.

Twofish: Twofish is a successor to Blowfish which is a symmetric key block cipher with a block size of 128 bits and with a variable key length. It uses a single key that converts plain text to cipher text that cannot be understood before decoding. This algorithm uses pre computed and key dependent substitution boxes.

4.RESULT AND DISCUSSION

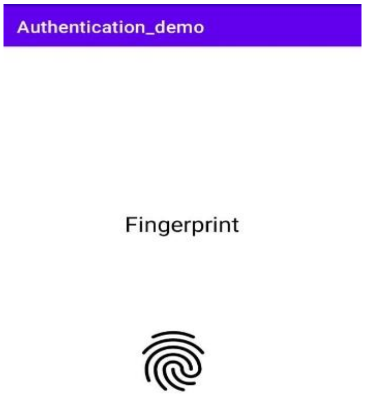


Fig 4.1: Fingerprint

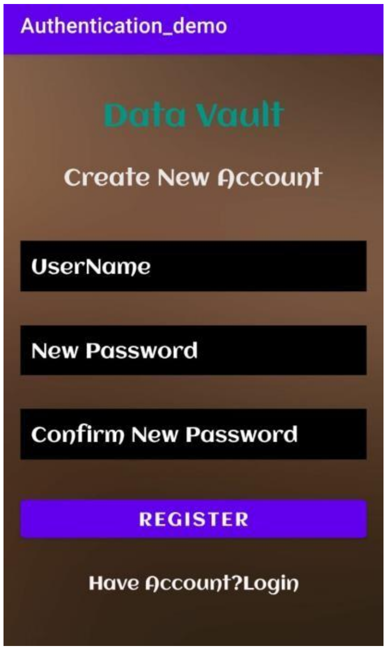


Fig 4.2: Registration

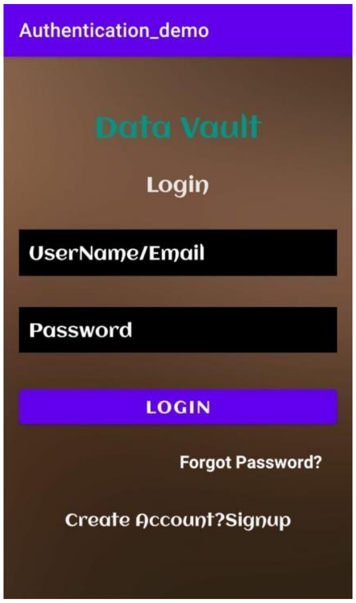


Fig 4.3: Login

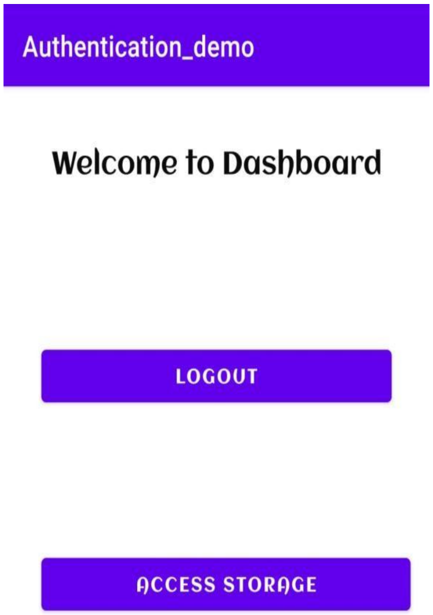
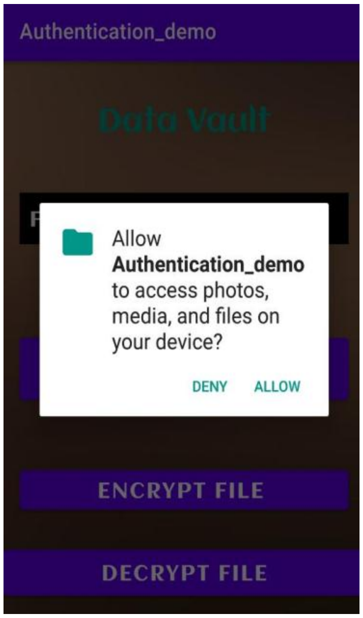
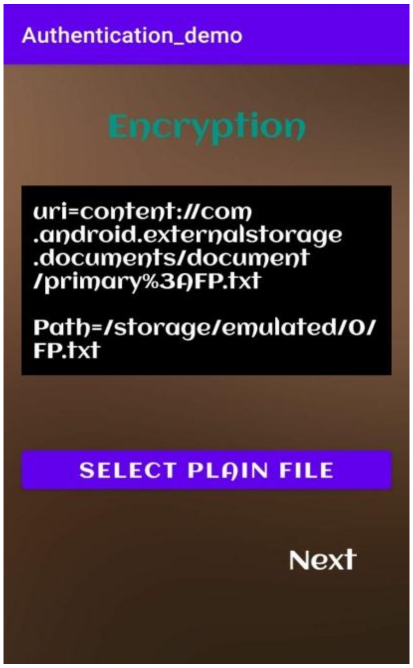


Fig 4.4 Dashboard



Allow **Authentication_demo** to access photos, media, and files on your device?

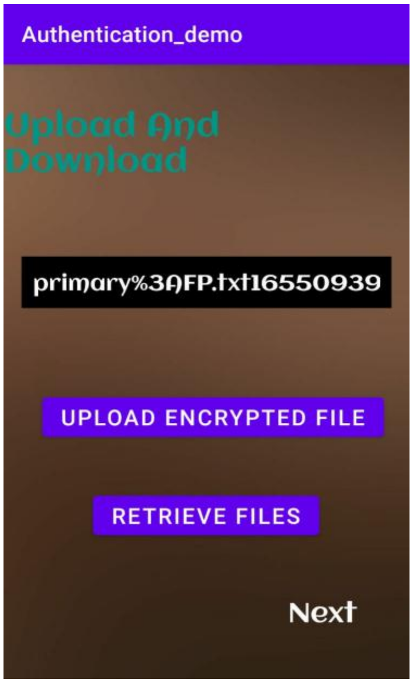
Fig 4.5: Storage Permissions



uri=content://com.android.externalstorage.documents/document/primary%3AFP.txt

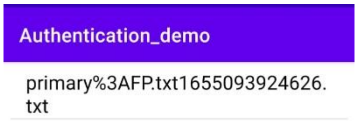
Path=/storage/emulated/0/FP.txt

Fig 4.6: Encryption



primary%3AFP.txt16550939

Fig 4.7: Upload and Download



primary%3AFP.txt1655093924626.txt

Fig 4.8: List of uploaded files

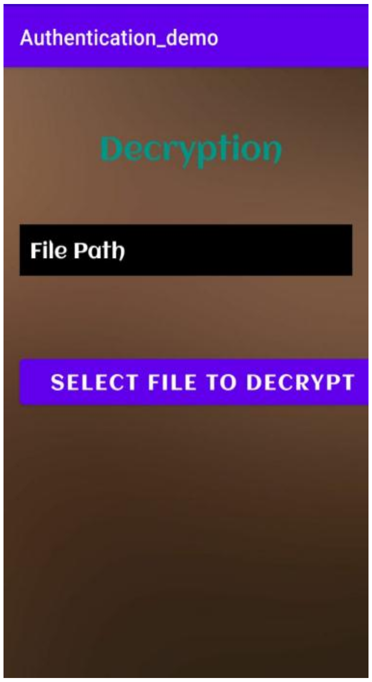


Fig 4.9: Decryption

5. CONCLUSION

In a fast-paced growing digital world it is crucial to protect digital information from manipulation and unauthorized access. Cloud is the latest technology that has immense benefits and there are areas of concern related to security and privacy that are unanswered and open. In consequence, we are developing an application that provides security in cloud by using cryptography and authentication techniques.

REFERENCES

1. Md. Alamgir Hossain & Md. Abdullah Al Hasan (2020): Improving cloud data security through hybrid verification technique based on biometrics and encryption system, International Journal of Computers and Applications, DOI: 10.1080/1206212X.2020.1809177

2. Albugmi, Ahmed & Alassafi, Madini & Walters, Robert & Wills, Gary. (2016). Data Security in Cloud Computing. 10.1109/FGCT.2016.7605062.

3. E. Datta and N. Goyal, “Security attack mitigation framework for the cloud”, 2014 Reliability and Maintainability Symposium, 2014, pp. 1-6, doi: 10.1109/RAMS.2014.6798457.

4. Celiktas, Baris & Celikbilek, Ibrahim & Ozdemir, Enver. (2019). A Higher Level Security Protocol for Cloud Computing. 97-101. 10.1109/UBMK.2019.8907019.