BIOKEY FOR USER AUTHENTICATION AND DATA PROTECTION SYSTEM IN CLOUD

Dr.S.Praveenkumar M.E.,Phd
Assistant Professor
Department of Computer Scienceand Engineering
E.G.S.PillayEngineering college(Autonomous),
Nagapattinam, India
asv.praveen@gmail.com

Duraivelan. P
Department of Computer Science and Engineering
E.G.S.Pillay Engineering college(Autonomous),
Nagapattinam,
duraivelan594@gmail.com

Gurumoorthy. M
Department of Computer Science and Engineering
*E.G.S.Pillay Engineering College(*Autonomous),
Nagapattinam, India
moorthig592@gmail.com

Mohamed Asmin Ali. S
Department of Computer Science and Engineering
E.G.S.Pillay Engineering college(Autonomous),
Nagapattinam, India
mohamedali4372@gmail.com

Abstract

Cloud computing is emerging as the most suitable paradigmfor individuals and organizations to access inexpensive, scalable,ubiquitous, and on-demand computing resources, applications,and data storage services.With the growing popularity of cloud computing, the numberof enterprises and individuals shifting toward the useof cloud has increased rapidly. As a result, a vast amountof important personal information and critical organizationdata, such as personal health records, governmentdocuments, and company finance data, etc., are transmittedacross the Internet and stored in cloud servers.However, outsourcing sensitive data suffers from criticalsecurity threats, privacy, and access control problems. Theseare common concerns of organizations and individuals usingcloud services. When data owners migrate their sensitive datato the cloud, they lose an element of control over their data.With this in mind, this project presents a user-side fingerprint based encrypted file system named ClientCentricFS.Moreover, we propose a Biometric based cryptographic protocol ***BioCRYP*** *that uses symmetric encryption algorithms in order to improve the securityand performance of the personal and shared files that areoutsourced.The key management is conveniently designed. In order to ensure robust data sharing security, the Fingerprint-based encryptionscheme (FBE) is integrated with ClientCentricFS. ClientCentricFS is designed to preserve the integrity of outsourced file dataand file system data structure.*

Keywords:*Biokey,User authentication,Data protection,cloud security,Biometric authentication,Multi-factor authentication,Encryption,Access control,Identity verification,Cybersecurity,Passwordless authentication,Behavioral biometrics,Cloud computing,Privacy protection,Digital identity management,Authentication factors,Two-factor authentication,User identity,Data privacy,Cloud storage security.*

1. INTRODUCTION

Data is one of the most valuable assets that any company can hold. One of the best ways to store these assets is within the cloud.Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centres and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon Web Services (AWS).

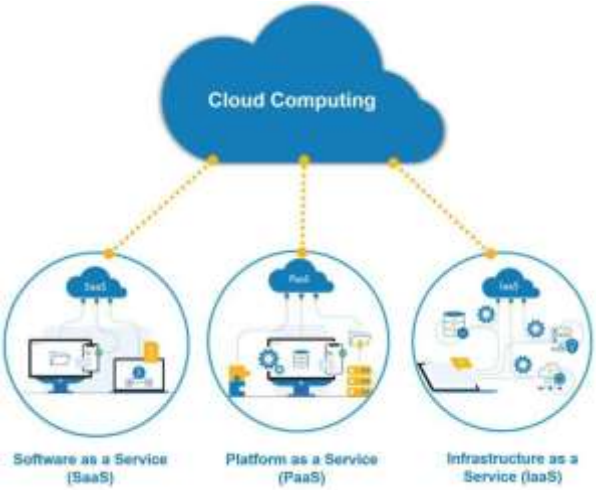


Figure 1.1. Types of Cloud Services

Types of Cloud Services

Cloud computing is not a single piece of technology like a microchip or a cellphone. Rather, it's a system primarily comprised of three services: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).

1. Software-as-a-service (SaaS)

It involves the licensure of a software application to customers. Licenses are typically provided through a pay-as-you-go model or on-demand. This type of system can be found in Microsoft Office's.

2. Infrastructure-as-a-service (IaaS)

Involves a method for delivering everything from operating systems to servers and storage through IP-based connectivity as part of an on-demand service. Clients can avoid the need to purchase software or servers, and instead procure these resources in an outsourced, on-demand service. Popular examples of the IaaS system include IBM Cloud and Microsoft Azure.

3. Platform-as-a-service (PaaS)

It is considered the most complex of the three layers of cloud-based computing. PaaS shares some similarities with SaaS, the primary difference being that instead of delivering software online; it is actually a platform for creating software that is delivered via the Internet. This model includes platforms like Salesforce.com and Heroku.

Deployment Models

Organizations have several choices for deploying a cloud computing models:

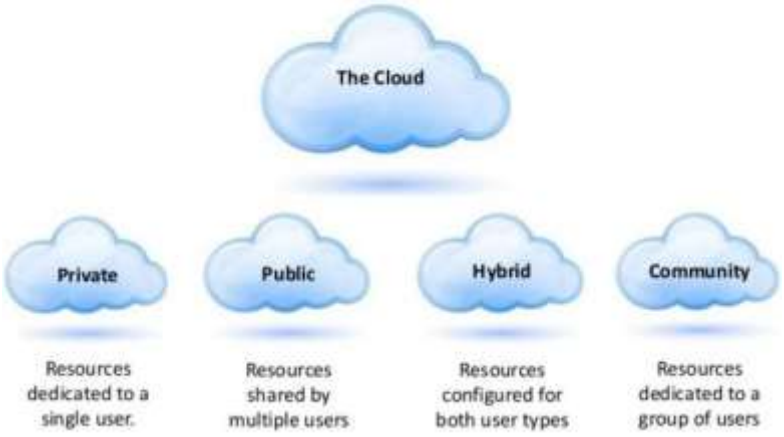


Figure 1.2. Types of Cloud Computing

1. **Public Clouds** - allow resources to be accessed by authorized subscribers.

Public clouds are cloud environments typically created from IT infrastructure not owned by the end user. Some of the largest public cloud providers include Alibaba Cloud, Amazon Web Services (AWS), Google Cloud, IBM Cloud, and Microsoft Azure.

2. **Private Clouds** - restrict resource access to a specific group or organization.

Private clouds are loosely defined as cloud environments solely dedicated to a single end user or group, where the environment usually runs behind that user or group's firewall. All clouds become private clouds when the underlying IT infrastructure is dedicated to a single customer with completely isolated access.

3. **Community Clouds** - allow resources to be shared among two or more organizations. Community clouds are distributed systems created by integrating the services of different cloudsto address the specific needs of an industry, a community, or a business sector.

4. **Hybrid Clouds** - resources are provided by at least two cloud service providers.

A hybrid cloud is a seemingly single IT environment created from multiple environments connected through local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), and/or APIs.

2.RELATED WORK

TITLE: Design and Development of Collaborative Approach for Integrity Auditing and Data Recovery based on Fingerprint Identification for Secure Cloud Storage
AUTHOR: Aachal Wani; Shrikant Sonekar.

The article of this author proposed the Security model for preventing many attacks so we are used Inner most layer as a 3DES (Triple Encryption standard) Cryptography algorithm that is providing 3-key protection as 64-bit and the outer most layer used the MD5 (Message Digest) Algorithm. i. e. Providing 128 – bit protection. As well as we are using Fingerprint Identification as a physical Security that used in third party remote integrity auditing, and remote data integrity auditing is proposed to ensure the uprightness of the information put away in the cloud. Data Storage of cloud services has expanded paces of acknowledgment because of their adaptability and the worry of the security and privacy levels. The large number of integrity and security issues that arise depends on the difference between the customer and the service provider in the sense of an external auditor. The remote data integrity auditing is at this point prepared to be viably executed. In the meantime, the proposed scheme is depending on identity-based cryptography, which works on the convoluted testament the executives. The safety investigation and the exhibition assessment show that the planned property is safe and productive.

TITLE: Web Cloud: Web-Based Cloud Storage for Secure Data Sharing across Platforms
AUTHOR: Shuzhou Sun; Hui Ma; Zishuai Song; Rui Zhang

With more and more data moving to the cloud, security and privacy of user data have raised great concerns. Client-side encryption/decryption seems to be an attractive solution to protect data security. However, the existing solutions encountered three major challenges: low security due to encryption with low-entropy PIN, inconvenient data sharing with traditional encryption algorithms, and poor usability with dedicated software/plugins that require certain types of terminals. This work design and implement Web Cloud, a practical browser-side encryption solution, leveraging modern web technologies. It solves all the above three problems while achieves several additional remarkable features: robust and immediate user revocation, fast data processing with offline encryption and outsourced decryption. Notably, our solution works on any device equipped with a web user agent, including web browsers, mobile and PC applications. We implement Web Cloud based on own Cloud for basic file management utility, and utilize Web Assembly and Web Cryptography API for complex cryptographic operations integration. Finally, comprehensive experiments are conducted with many well-known browsers, Android and PC applications, which indicates that Web Cloud is cross-platform and efficient. As an interesting by-product, the design of Web Cloud naturally embodies a dedicated and practical ciphertext-policy attribute-based key encapsulation mechanism (CP-AB-KEM) scheme, which can be useful in other applications.

TITLE: The Cloud we Share: Access Control on Symmetrically Encrypted Data in Untrusted Clouds
AUTHOR: Alexandros Bakas; Hai-Van Dang; Antonis Michalas; Alexandr Zalitko

Along with the rapid growth of cloud environments, rises the problem of secure data storage-a problem that both businesses and end-users take into consideration before moving their data online. Recently, a lot of solutions have been proposed based either on Symmetric Searchable Encryption (SSE) or Attribute-Based Encryption (ABE). SSE is an encryption technique that offers security against both internal and external attacks. However, since in an SSE scheme, a single key is used to encrypt everything, revoking a user would imply downloading the entire encrypted database and re-encrypt it with a fresh key. On the other hand, in an ABE scheme, the problem of revocation can be addressed. Unfortunately, though, the proposed solutions are based on the properties of the underlying ABE scheme and hence, the revocation costs grow along with the complexity of the policies. To this end, we use these two

cryptographic techniques that squarely fit cloud-based environments to design a hybrid encryption scheme based on ABE and SSE in such a way that we utilize the best out of both of them. Moreover, we exploit the functionalities offered by Intel's SGX to design a revocation mechanism and an access control one, that are agnostic to the cryptographic primitives used in our construction.

TITLE: Efficient Attribute-Based Encryption Outsourcing Scheme with User and Attribute Revocation for Fog-Enabled IoT
AUTHOR: Ling Li; Zheng Wang; Na Li

With the rapid growth of Internet of Things (IoT) applications, fog computing enables the IoT to provide efficient services by extending the cloud computing paradigm to the edge of the network. However, the existing attribute-based encryption schemes rarely focus on user and attribute revocation in fog computing and most of them still impose high computational and storage overhead on resource-limited IoT devices. In this article, we propose an efficient attribute-based encryption outsourcing scheme with user and attribute revocation for fog-enabled IoT. The proposed scheme improves the existing encryption scheme that uses the concept of attribute groups to achieve attribute revocation, making it suitable for fog computing and improving the efficiency of ciphertext update. In addition, it implements a novel method of user revocation in fog computing based on the characteristics of fog computing. In order to reduce the computing and storage burden of IoT devices, the heavy computation operations of encryption and decryption are outsourced to fog nodes and part of secret keys are stored in fog nodes. The security analysis shows that the proposed scheme is secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. The performance analysis shows that the proposed scheme has high revocation efficiency and is efficient enough to be deployed in practical fog computing.

TITLE: Outsourcing Attributed-Based Ranked Searchable Encryption with Revocation for Cloud Storage
AUTHOR: Leyou Zhang; Jian Su; Yi M

With the rapid growth of the cloud computing and strengthening of security requirements, encrypted cloud services are of importance and benefit. For the huge ciphertext data stored in the cloud, many secure searchable methods based on cryptography with keywords are introduced. In all the methods, attribute-based searchable encryption is considered as the truthful and efficient method since it supports the flexible access policy. However, the attribute-based system suffers from two defects when applied in the cloud storage. One of them is that the huge data in the cloud makes the users process all the relevant files related to the certain keyword. For the other side, the users and users' attributes inevitably change frequently. Therefore, attribute revocation is also an important problem in the system. To overcome these drawbacks, an attribute-based ranked searchable encryption scheme with revocation is proposed. We rank the ciphertext documents according to the TF×IDF principle, and then only return the relevant top-k files. Besides the decryption sever, an encryption sever is also introduced. And a large number of computations are outsourced to the encryption server and decryption server, which reduces the computing overhead of the client. In addition, the proposed scheme uses a real-time revocation method to achieve attribute revocation and delegates most of the update tasks to the cloud, which also reduces the calculation overhead of the user side. The performance evaluations show the scheme is feasible and more efficient than the available ones.

3.EXISTING SYSTEM

Identity Based Encryption (IBE):

IBE is a public key encryption schema. Where the public key consists of some information about the key holder like email address. The admin / key-authority issues a private/secret key which is tied to the pubic key. The owner of the public key can only decrypt then encrypted message.

Role Based Access Control (RBAC):

In this approach the access is granted to a specific role rather than individuals. Any individual who is assigned this role will automatically inherit the privileges assigned the role.

Attribute Based Access Control (ABAC):

It is a relatively newer and simpler to implement than RBAC. In this paradigm if a user has a set of attributes which satisfy the object they want to access, then they can retrieve that object.

Attribute Based Encryption (ABE):

ABE is an encryption schema which can perform a fine-grained access control withencryption where a user with certain attributes can read the data or parts of the data which the attributes grant access to. When compared with other schemas ABE has a complex access controland decryption process. The public is generally hosted in the cloud which can be accessed by the users in the cloud to create their private keys. Using attributes, we can make use of both IBE and RBAC algorithms using ABE. This motivated me to pursue a study based around ABE schemas.

Cypher text Policy Attribute based Encryption:

Ciphertext policy-based encryption scheme is a public key encryption scheme where the

public keys are generated by taking implicit parameters from the elliptic curve. While generatingthe private keys it considers the policy. To encrypt the data, it mainly requires the attributes of users which were specified in the form of access tree structure, we call it as policy. Suppose owner who is uploading the information will specify the policy as "3 of 3" it indicates at least 3 attributes of the user who are trying to access the information should be satisfied.

DISADVANTAGES :

- Inherent key escrow: Private key is known to PrivateKey Generator (PKG).
- For sending private key requires secure channel.
- The lack of impressibility seems to limit its applicability to larger systems.
- Difficulty in user revocation.

4.PROPOSED SYSTEM

The proposed system presents a user-side biometric based encrypted file system named Client Centric FS More over, we propose a hybrid cryptographic scheme that combines Fingerprint based user authentication and biometric encryption algorithms in order to improve the security and performance of the personal and shared files that are outsourced. Biometric encryption is used to encrypt the contents of outsourced files in the CCFS. The goals of the proposed ClientCentricFS are twofold. First, design a cryptographic layer that effectively encrypts all files that are outsourced to the cloud storage in a highly secure and transparent manner. Second, enable a secure data sharing of cloud storage at the granularity of individual files with the proposed CCFS.

Client Centric File System

It's a client-centric solution, which means that it contains the master copies of all the data files which are stored inside the cloud.Files are directly synchronized to storage gateways in every location in real-time for allocation.File locking and file sharing are also frequently managed in the client centric file system, allowing multiple users to access similar files from the cache without requiring to download the content from the cloud every time.

User-centric security management enables data owner to apply different security application settings to different data user roles. Data owner can create several user roles, assign an appropriate user role to each user, and define different application settings to the devices owned by users with different roles.Depending on the role of this employee in the company, Data owner can expand or limit the rights of this person to change application settings.

ADVANTAGES :

- By using biometrics, anyone can keep their data as secret and private.
- Our scheme efficiently generates strong keys (256 bits) from fingerprint biometrics.
- enhances the security strength and reduces space for key storage.
- Secure Biometric Lock System for Files.

5.Methodology

1. Cloud Server Web App:

The cloud server stores the encrypted data and provides keyword search services. When a search user submits a trapdoor, the cloud server would check to see whether the keyword in the trapdoor matches with the keyword in the

index ciphertext.

1. Data Owner Login
2. Encrypted File upload
3. File Manipulation
4. Access Control Policy
5. Logout

2. Cloud Client Web App

CC web app runs locally on our device or pc allows to access files from all our devices. It's easy to use and integrates seamlessly between data and the cloud. CC web app technology meets the latest standards and encrypts both files and filenames with AES and Fingerprint key length.

Client-side encryption is the act of encrypting data before sending it to. The client downloads the encrypted object from Cloud Server. Using the material description from the object's metadata, the client determines which user Fingerprint Key to use to decrypt the data key. The client uses that Fingerprint Key to decrypt the data and then uses the data key to decrypt the object.

1. Data Owner
2. Register/Login
3. Erroll DO Fingerprint
4. Biometric Symmetric Key Generation
5. Add user
6. Generate Login Credential
7. Share Login Credential
8. Enrol DU Fingerprint
9. Upload Normal file to CCFS
10. Biometric Authentication
11. Encrypt File using Bio Key
12. Upload Encrypted File to Cloud Server
13. Data User
14. Login
15. Biometric Authentication
16. Encrypt/Decrypt File
17. Logout

3. Fingerprint Module Integration

Communication between the module and the host system can be done via wirelessly through IoT using MQTT protocol. The module embeds algorithms for the capture, extraction and matching of fingerprints. Embedded biometric API includes matcher and fingerprint extractor features.

1. DCNN Fingerprint Recognition

2. 1 Fingerprint Biometric Acquisition

The first challenge facing a finger scan system is to acquire a high-quality image of the fingerprint. Image quality is measured by dots per inch (DPI)- more DPI means a high-resolution image. The lowest DPI generally found is the 300 to 350 DPI range. There is seven patterns of papillary ridge i.e. Loop, Arch, Whorl, Tented Arch, Double Loop, Central Pocked Loop and Accidental.

3. DCNN Fingerprint Classification

CNN was used as a trainable deep neural network. The fingerprint image of size 227×227 pixels was used to extract the CNNfeatures, which were used to train the CNN architecture. The structure consisted of a series of convoluted layers followed by a poolinglayer. Each layer was defined for a specific computation. The designed network started with an input layer which indicated the size andtype of the input data. The fully connected layer was the output layer, which used to perform the data classification. This proposedCNN architecture was constructed by the following layers.Convolutional layers: The convolutional layer applied convolutional filters to the input images in this step. A

set of mathematical functions was performed on each image to produce a single value in the output feature map. The outputs were submitted to an activation function for introducing nonlinearities into the model. One of the most used activation functions used in this experiment was ReLU rectifier linear function, which can be mathematically expressed as, f(x)=max (0, x), where x is the neuron input. A smooth approximation to the rectifier is the analytic function, f(x)=ln (1 + e^x), which is also called the soft plus function.

Pooling layers. Pooling layer is another basic part in the CNN architecture. This layer summarised the features within a feature map extracted by the convolution layer using the average function or max-pooling, which were used to reduce the dimensions of the feature map. Therefore, the network had to learn reduced number of parameters and subsequently reduced the computational time. Max pooling algorithm extracted subregions of the feature map and keeps only their maximum value.

Fully connected layers. Classification was performed by this layer on the features extracted by the convolutional layers and down sampled by the pooling layers. In this layer, every node is fully connected to all activations in the preceding layer.

Input layer: It takes the pre-processed fingerprint image. An image size of 227×227 where width 227 pixel and height 227 pixel were considered for this layer.

Two combinations of convolutional and pooling layers: First convolutional layer contained padding 0 and a stride of 4, with a total of 96 filters having a size of 11×11. On the other hand, the second convolutional layer contained 256 filters of size 5 × 5, padding 2 and stride 1. Both layers were followed by a ReLU rectifier function. A max-pooling layer having window with a size of 3 × 3 and stride 2 was placed after each convolutional layer.

Three convolutional layers and a pooling layer: The third, fourth and fifth convolutional layers were followed by ReLU function containing 384, 384, 256 filters respectively. A max pooling layer with a size of 3 × 3 and stride 2 was arranged after the three convolutional layers.

Fully connected layer and an output layer: Among the three fully connected layers, first and second layers contained 4096 neurons each. The output layer denoted by the third fully connected layer could be triggered by a SoftMax regression function. Each layer of a CNN produced a response, or activation, to an input image. However, only a few layers within a CNN were suitable for image feature extraction. The layers at the beginning of the network captured basic image features, such as edges and blobs, which were subsequently processed by the deeper network layers combining the early features to form a higher-level image feature. Recognition tasks can be made easier by the higher-level features as they combined all the primitive features into a richer image representation. In the proposed system, the features were gathered from the fully connected layer

4. Fingerprint Symmetric Cryptography

Our proposed approach has three components, namely, template generation, key generation and key regeneration. A string of binary number as cryptographic key is extracted from fingerprint template and this key is used to encrypt a message. During decryption process, the user is able to generate that cryptographic key from a fresh fingerprint instance to decrypt the encrypted message.

1. Bio KeyGen

The proposed Model takes as input the given JPEG/JPG image and gives as output a 64-bit key. The key generated is input to the parity drop table DES key generator. The entire focus of the project is the second block i.e 64-bit key generator from the Input image. The 64-bit key generator block is further divided into sub-blocks portraying in details the inner working of the block. The input JPEG/JPG is converted to binary image. The binary images with only two levels of interest. The black pixels that denote ridges and the white pixels that denote valleys are employed by almost all minutiae extraction algorithms. A grey level image is translated into a binary image in the process of binarization, by which the contrast between the ridges and valleys in a fingerprint image is improved. Thinning process is performed to reduce thickness of lines. Thinning is a morphological operation that is used to remove selected foreground pixels from binary images. It is particularly used for skeletonization. It is used to tidy up the output of edge detectors by reducing all lines to single pixel thickness.After the fingerprint ridge thinning marking minutia points is relatively easy. For each 3X3 window, if the central pixel is 1 and has exactly 3 one-value neighbours, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 One-value neighbour, then the central pixel is a ridge ending. The false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. These false minutiae might impact the accuracy and genuine of the finger code generated from a given fingerprint image. These false minutiae are removed. The set of minutiae set generated is of greater size. This set need to be reduced to derive a 64-bit set. The original minutiae set is recursively reduced until a 64-bit key is obtained.

2. Data Owner

Data owner utilizes the cloud to store his private data. Before outsourcing the data to cloud, the data owner encrypts the potential keyword as index, and then uploads them to the cloud server. To achieve access control, the data owner encrypts the index with an access policy which describes the right the access the sensitive data. So that, in the encryption phase, an access policy is specified and embedded into the ciphertext to realize fine-grained access control.

3. Fingerprint Authentication

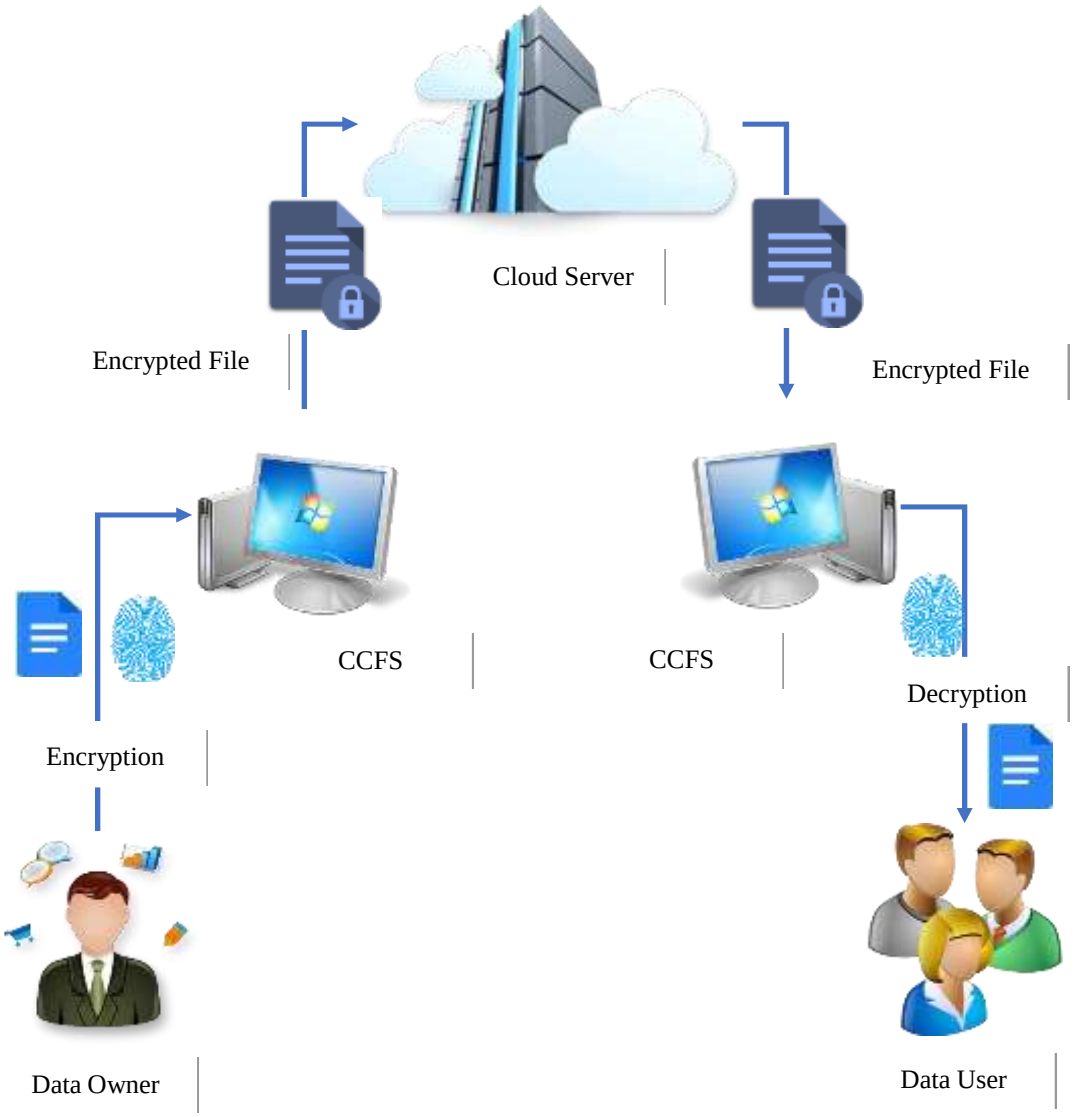
The feature matching step is the most critical step in a fingerprint recognition system. In this step the similarity between two images is measured, and by calculating the correlation between these images, the decision is given. This project proposed a method for measuring the similarity between two fingerprint images. One of the images is considered to be the input image that should be verified and another image is the one which is stored in the system database. By using this method, the difference between two mentioned images can be measured. The smaller the difference between the two images indicates more similarity

4. Fingerprint based Encryption.

The algorithm takes Fingerprint key PK, attribute policy T and message Mas input and outputs ciphertext C.

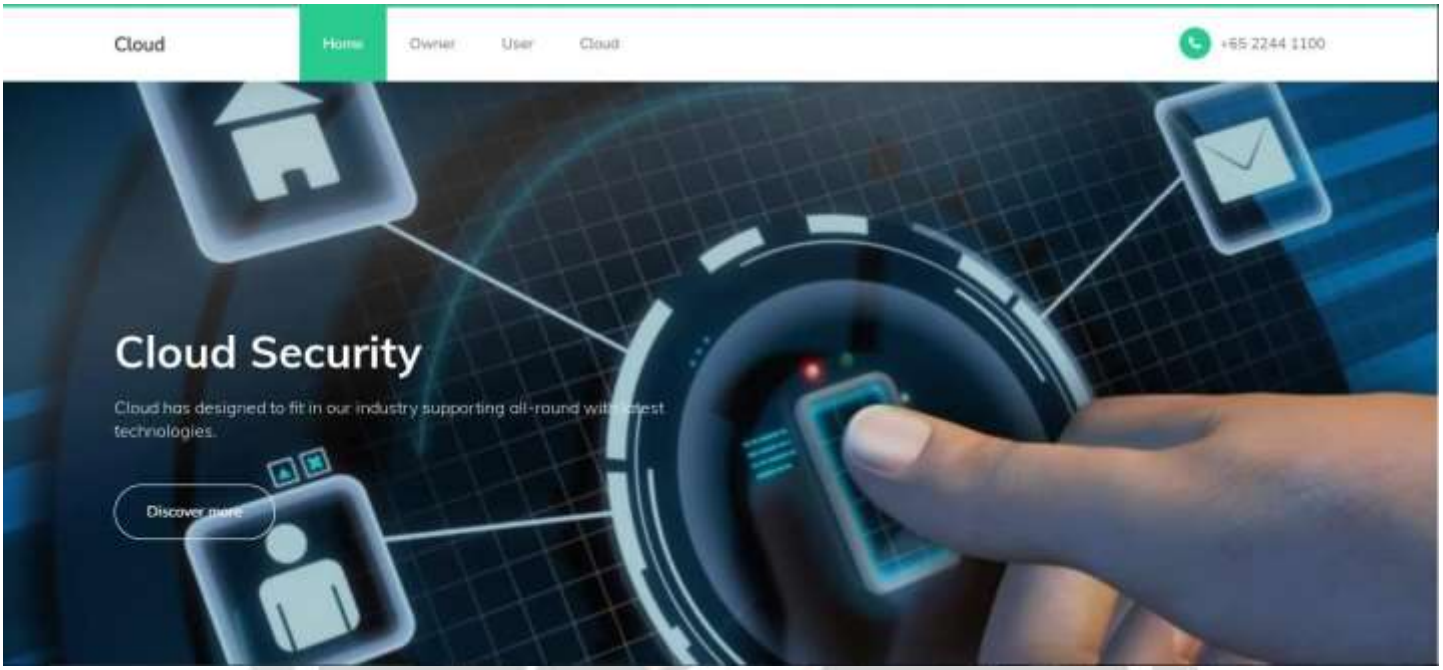
5. Fingerprint based Decryption

The algorithm takes the Fingerprint key PK and ciphertext C as inputs. Only if access control policy W matches the user attribute policy T, the algorithm outputs plaintext M.



6.Experimental Result

The Experimental result shows the overall performance of the proposed system. Here Fingerprint based user authentication and biometric encryption algorithms in order to improve the security and performance of the personal and shared files that are outsourced are implemented using PHP as front end and MySQL as backend software.



The above figure is interface of a Biokey for user authentication and data protection system in cloud

7.CONCLUSION

In this project, Client Centric FS is introduced. CCFS is a user-side fingerprint based encrypted fille system that is implemented to secure outsourced files to cloud storage systems. It can enforce a secure file system mount over the cloud synchronized directory to perform a transparent encryption on per-file basis using BioKey. CCFS does not introduce dependencies to the asymmetric encryption ciphers, but rather proposes a Biometric Symmetric encryption scheme that combines Fingerprint and BioKey is used to encrypt files for the outsourced personal and shared files. In addition, CCFS uses the IBE scheme to facilitate the outsourced file sharing accessible only by authorized users with appropriate secret keys. CCFS can guarantee the integrity of the outsourced data files and the file system data structure against tampering and deletion attacks. The performance of the proposed CCFS on different file sizes has been quantitatively evaluated on representative hardware and file sizes. The results show that CCFS is reasonably efficient. With a block size of 4 KB, CCFS could achieve an average throughput of 8.8 MB/sec, and 10.5 MB/sec, respectively, for writing and reading outsourced files. Security analysis show that the proposed CCFS is highly secure, and it can effectively resist attacks, such as brute-force, eavesdropping, man-in-the-middle, offline dictionary, and collusion attacks on outsourced files.

8.REFERENCE

1. G. Fawkes, Report: Data Breach in Biometric Security Platform Affecting Millions of Users, 2019, [online] Available: https://www.vpnmentor.com/blog/report-biostar2-leak/.

2. B. Carl, Report: Retail-Focused Used Electronics Business Leaks Customers' IDS & Fingerprints in Data

Breach, 2020, [online] Available: https://www.websiteplanet.com/blog/tronicsxchange-breach-report/.

3. O. Goldreich, Foundations of Cryptography: Basic Applications, Cambridge, U.K.:Cambridge Univ. Press, vol. 2, 2009.
4. M. Upmanyu, A. M. Namboodiri, K. Srinathan and C. V. Jawahar, "Blind authentication: A secure crypto-biometric verification protocol", IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 255-268, Jun. 2010.
5. M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama and T. Koshiba, "Packed homomorphic encryption based on ideal lattices and its application to biometrics", Proc. Int. Conf. Availability Rel. Secur., pp. 55-74, 2013.
6. H. Chun, Y. Elmehdwi, F. Li, P. Bhattacharya and W. Jiang, "Outsourceable two-party privacy-preserving biometric authentication", Proc. 9th ACM Symp. Inf. Comput. Commun. Secur., pp. 401-412, Jun. 2014.
7. J. H. Cheon, H. Chung, M. Kim and K.-W. Lee, "Ghostshell: Secure biometric authentication using integrity-based homomorphic evaluations", IACR Cryptol. ePrint Arch., vol. 4, pp. 484, May 2016.
8. J.-H. Im, J. Choi, D. Nyang and M.-K. Lee, "Privacy-preserving palm print authentication using homomorphic encryption", Proc. IEEE 14th Int. Conf. Dependable Autonomic Secure Comput. 14th Int. Conf. Pervas. Intell. Comput. 2nd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech), pp. 878-881, Aug. 2016.
9. S. F. Shahandashti, R. Safavi-Naini and N. A. Safa, "Reconciling user privacy and implicit authentication for mobile devices", Comput. Secur., vol. 53, pp. 215-233, Sep. 2015.
10. J. Sedenka, S. Govindarajan, P. Gasti and K. S. Balagani, "Secure outsourced biometric authentication with performance evaluation on smartphones", IEEE Trans. Inf. Forensics Security, vol. 10, no. 2, pp. 384-396, Feb. 2014.