IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 13, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

BioKey for User Authentication and Data Protection System in Cloud

A.Mohamed Noordeen [1], A.Mohamed riyas [2] , A.Faizal [3]

Assistant Professor, Department Of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, Tamil Nādu, India [1]

U.G Student, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore Tamil Nādu, India [2,3]

ABSTRACT: Cloud computing is emerging as the most suitable paradigm for 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 number of enterprises and individuals shifting toward the use of cloud has increased rapidly. As a result, a vast amount of important personal information and critical organization data, such as personal health records, government documents, and company finance data, etc., are transmitted across the Internet and stored in cloud servers. However, outsourcing sensitive data suffers from critical security threats, privacy, and access control problems. These are common concerns of organizations and individuals using cloud services. When data owners migrate their sensitive data to 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 Client Centric FS. Moreover, we propose a Biometric based cryptographic protocol **Bio CRYP** that uses symmetric encryption algorithms in order to improve the security and performance of the personal and shared files that are out sourced. The key management is conveniently designed. In order to ensure robust data sharing security, the Fingerprint-based encryption scheme (FBE) is integrated with Client Centric FS. Client Centric FS is designed to preserve the integrity of outsourced file data and file system data structure. Analysis of performance and experimental results show that Client Centric FS is efficient. It can achieve an average throughput of 8.8 MB/sec, and 10.5 MB/sec for writing and reading outsourced files. Security analysis indicates that Client Centric FS is extremely secure and robust against attacks such as brute-force, eavesdropping, man-in-the-middle, and offline-dictionary attacks.

KEYWORDS: Biometric,Client Centric FS,Fingerprint-based encryption(FBE),Robust.

I. 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 centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed bas a cloud provider like Amazon Web Services (AWS).

II. RELATEDWORK

1. Design and Development of Collaborative Approach for Integrity Auditing and Data Recovery based on Fingerprint Identification for Secure Cloud Storage

Author: AachalWani; ShrikantSonekar.
Date of Publication: 13 November 2021
Proposed Methodology

The article of this author proposed the Security model for preventing many attacks so we are used Inner most layer as a 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

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

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.

2. Web Cloud: Web-Based Cloud Storage for Secure Data Sharing across Platforms

Author: Shuzhou Sun; Hui Ma; Zishuai Song; Rui Zhang

Date of Publication: 26 November 2020

Proposed Methodology

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.

3. The Cloud we Share: Access Control on Symmetrically Encrypted Data in Untrusted Clouds

Author:AlexandrosBakas; Hai-Van Dang; AntonisMichalas; AlexandrZalitko

Date of Publication: 17 November 2020

Proposed Methodology

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.

4. Efficient Attribute-Based Encryption Outsourcing Scheme with User and Attribute Revocation for Fog-Enabled IoT

Author: Ling Li; Zheng Wang; Na Li

Date of Publication: 18 September 2020

Proposed Methodology

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.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

III. EXISITING 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 with encryption 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 control and 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 generating the 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. Here user will be able to access the information only when user possesses certain set of attributes that satisfy the policy.

IV. PROPOSED SYSTEM

The proposed system presents a user-side biometric based encrypted file system named ClientCentricFS Moreover, 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.

- **Client Centric Fingerprint Recognition**

Fingerprint biometric is one of the most popular and widely used for authentication. The proposed system uses fingerprint at the matching score level for biometric identification. Convolutional neural networks (CNN) based fingerprint methodology is presented in our work. Input image is enhanced during preprocessing phase. Matching the enhanced fingerprint is done in recognition phase. The overall system performance is enhanced by realizing preprocessing and recognition phases. Performance of the system is evaluated and measured by FAR (False Acceptance Rate) and FRR (False Rejection Rate).

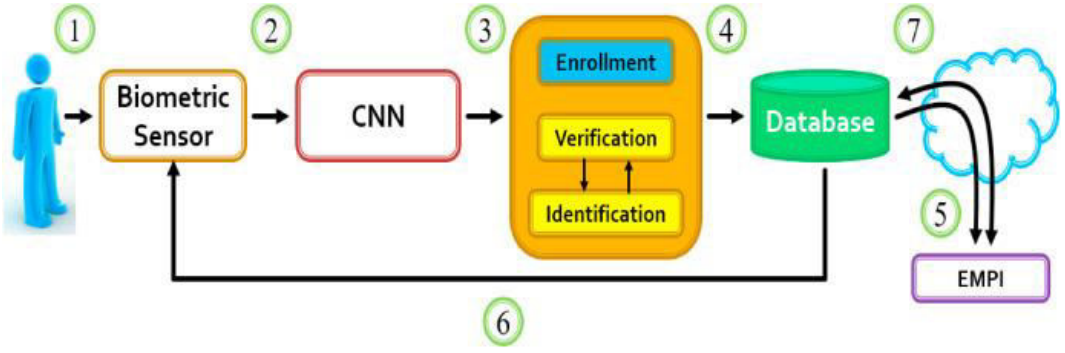


Figure 3.1. CNN Fingerprint Authentication

- **Client Centric Fingerprint Enrollment**

Enrolment mode is a phase of learning to gather biometric data about whom to recognize. The images are collected from a single biometric trait in the enrolment phase and are processed to obtain a clear image as well as to correct distortions and to obtain the region of interest for extracting features. The feature extraction module extracts the details from the pre-processed image. The feature vector is created by extracting specific features from the image function and storing them in a database.

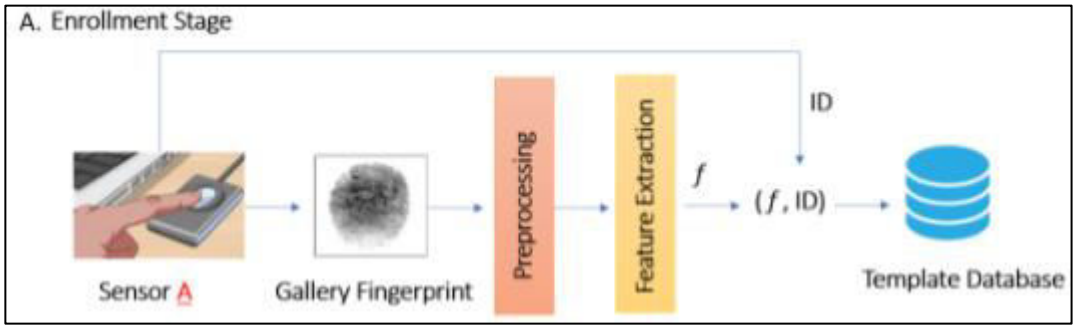
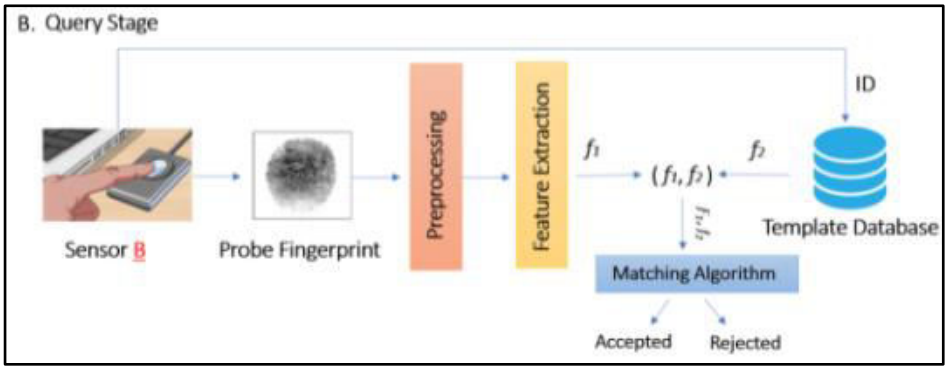


Figure 3.2 Fingerprint Enrollment

- **Client Centric Fingerprint Authentication**

In the query stage, a fingerprint is captured using sensor B, it is pre-processed using the same method and the features are extracted using the same descriptor used in the enrollment stage. Then the similarity between features S1 of the query

fingerprint captured from sensor B and the features S2 retrieved from the template database by the user ID is calculated to decide whether there is a "match" or "non-match";



Finger 3.3 Fingerprint Authentication

Symmetric Key Encryption

Symmetric encryption uses a common secret key for both encryption and decryption. Private key encryption is best suited to be used in trusted work groups. It is fast and efficient, and properly secures large files. The leading private key encryption is DES (Data Encryption Standard). DES was adopted as a federal standard in 1977. It has been extensively used and is considered to be strong encryption. Other types of private key encryption include: Triple-DES, IDEA, RC4, MD5, Blowfish and Triple Blowfish. Secret-key, single-key, shared-key, one-key, and private-key encryption are other words for symmetric-key cryptography.

- **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.

- **Client Centric DES Symmetric Key Encryption and Decryption**

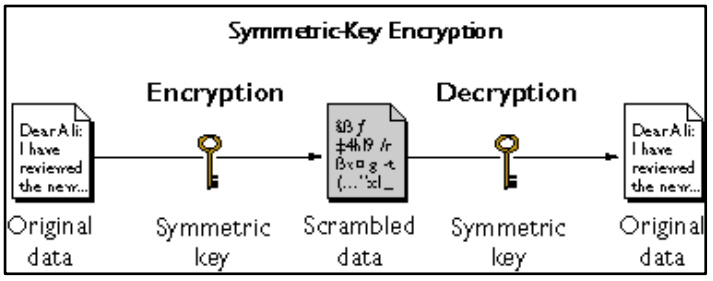


Figure 3.4 DES Symmetric Key Encryption and Decryption

Client-side biometric encryption is the cryptographic technique of encrypting data on the sender's side, before it is transmitted to a server such as a cloud storage service. Client-side encryption features an encryption key that is not available to the service provider, making it difficult or impossible for service providers to decrypt hosted data. Client-side encryption allows for the creation of applications whose providers cannot access the data its users have stored, thus offering a high level of privacy

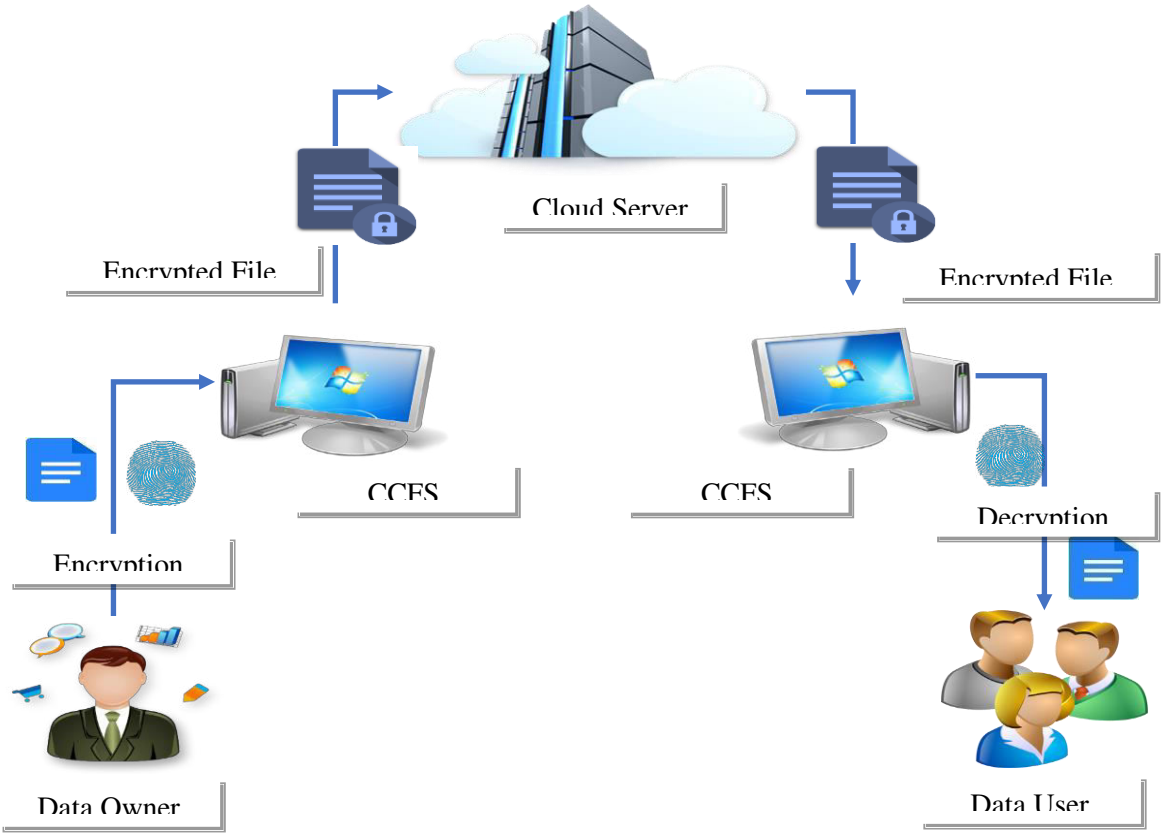
|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

V. OVERALL ARCHITECTURE



VI. METHODOLOGY

1.Biometric is the alternate to maintain the privacy of key by protecting it with users biometric from unauthorized access.
2.In this protocol, a cryptographic key is linked with users fingerprint data.
3.A string of binary number as cryptographic key is extracted from fingerprint template and this key is used to encrypt a data.
4.Decryption process, the user is able to generate that cryptographic key from a fresh fingerprint instance to decrypt the encrypted message.

VII. CONCLUSON

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 Bio Key. CCFS does not introduce dependencies to the asymmetric encryption ciphers, but rather proposes a Biometric Symmetric encryption scheme that combines Fingerprint and Bio Key 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

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

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.

REFERENCES

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.

INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details