iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5434

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

A Privacy- Sustainable and Secure Biometric Recognition Measure through Cloud Computing Utilizing Block-Chain

Aadithya Aman[1], Badal Sharma[2], Manan V Patel[3], Arjun CS[4], Chaithra B M[5]
[1, 2, 3, 4, 5]*Dept. of Information Science and Engineering, Sapthagiri College of Engineering, Karnataka, India*

Abstract: ***In recent years biometric identification has become more and more common. In the scenario of cloud computing, the owner of the particular databases is encouraged to redistribute the wide scale of biometric data and cloud authentication activities to enable them to reduce the high cost of storage and processing, which, however, presents some sort of malicious threats regarding users' privacy. Via this paper, we attempt to provide a privacy-sustainable and secure framework for outsourcing biometric identification. It encrypts and outsources the data of user's biometrics particularly to the server on cloud. The owner of the database encrypts the data provided by client and therefore transfer it to the cloud to perform a biometric authentication. The cloud conducts operations regarding authentication via the database which is already encrypted and transfers the information to the owner of the database. A detailed security review gives out solid proof that the model proposed by us is quite secure and sustains privacy although attackers can change identification requests and cloud collusion. Results conducted by experiments suggest that the current model achieves greater efficiency in both processesi.e. acknowledgement and preparation as opposed to previous protocols.***

Keywords: Cloud Computing, Security, Block-chain, Biometric Identification, Encryption.

I. INTRODUCTION

One of the most influential ways of identifying a person is biometric authentication. All bio-metric characteristics, for example fingerprints , retina, and eyes, have some essential universality factors (people having their unique fingerprint), uniqueness (the probability of 2 people having the same fingerprint is insignificant) and continuity (the bio-metric characteristics usually stay the same over vast period of time)[1].

These identities have other benefits and drawbacks. Since they simplify the use of biometric characteristics and reliably classify customers, they raise questions about consumer privacy. For example, suppose a user registers themselves using their fingerprint to use other web applications, such as a healthcare system and multiple social networking websites, internet companies may regulate their fingerprint delivery, and discern their personal info such as state of health and documented SNS name. This significantly infringes the privacy of clients. Furthermore, if the fingerprint information of the user is disclosed to the common public, anyone can disguise our user by simply submitting their biometric data, thus validating the entire verification system [2,3]. Since biometric characteristics are exceptional and cannot be altered throughout the lifetime, they cannot be altered and cross-generated once released. Biometric identification has become extremely popular, as it offers a successful approach to determine users. Biometric verification is perceived to be more accurate and easier compared with conventional password-based authentication methods and identification cards. In addition, biometric identification has been used in many fields including biometric characteristics such as fingerprints, iris and facial patterns that can be collected from different sensors. FBI, which is a prominent Database owner that manages the national fingerprint database may want to send out the huge amount of biometric data to the clouds in a biometric identification scheme or model. However, in order to preserve biometric data privacy, the biometric data must be encrypted before it is outsourced to FBI. Whenever an associate of owner such as FBI wants an individual's identity validated, he switches towards the FBI and produces an authentication question using the individual's personal biometric characteristics (e.g., eyes, fingerprints, speaking style, facial frame patterns, etc.). Later on, FBI shall encode the query, and transfers it towards the digital cloud to identify the match to perfection and accuracy. The challenge, then, is to somehow develop a methodology that can effectively and privately conserve biometric authentication in cloud technology. A series of biometric identification approaches that safeguard the security and privacy have been formulated.

A protection problem in cloud computing is a big issue for regulating the unintended client's entry. The biometrics-based authentication process enhances protection. Biometrics-based verification system makes navigating to personal records from any

©IJRASET: All Rights are Reserved

server possible for users. A secure authentication mechanism focused on an Identity [2] to identify the approved user. The system will not increase privacy rates. Most of them, however, concentrate primarily on privacy protection but neglect performance, such as homomorphic encryption and forgetful transmission schemes. These systems, suffering from problems with local machine efficiency, crash once the server size is larger than 10 mb. In addition, Yu and Yuan [4] suggested an efficient biometric recognition system that would protect privacy.

They built three systems in particular, and established a practical protocol to achieve fingerprint trait defence reliability. In their system, the database holder oversees cloud-matched identification functions to boost performance. Nevertheless, Zhu [5] figured out that a malicious client and cloud-initiated manipulation attack would breach the Yu and Yuan protocol. Wangetal[6] suggested the Cloud-BI-II strategy that used arbitrary diagonal equations for biometric categorization. Yet, their work has been considered ineffective in [7] and [8]. In this paper we suggest an accurate and privacy-sustainable biometric authentication model which can endure the consumers and cloud manipulation assault.

II. LITERATURE SURVEY

Biometric based identification systems have made headlines to a lot of development in data security, data privacy alongside a range of methods including block-chain and cloud computing among many others.

A. Identity Management in the Age of Blockchain 3.0

For virtually any contact that happens online since the advent of the Internet, identification has been a significant feature. In this paper, by reflecting from the scenarios of two of the world 's largest biometric ID systems: India's Unique Identification System and China's Sesame Credit Social Identity System, we highlight and discuss existing limitations of unified IdM [13] systems.IdM is a 'safety discipline' that allows the correct people to access the proper resources at the right time, for the appropriate reasons. Conventional IdM systems like passports or driving licenses are dissociated as the documents can be easily forged, expensive, time-consuming to process and trustless.And from the other contrary, internet - based IdM systems, such as Facebook, run a federated identity scheme that can authenticate the identity of users across systems to decide whether access is allowed or not. This paper examines self-souverain identity through groundbreaking block-chain 3.0 application. They then define some core features of block-chain technology to resolve the challenges faced by centralized IdM services and pose opportunities to promote HCI experiments around de-centralized IdM services to stimulate discussion in the workshops.

1) Demerits

a) These have struggled to evolve from the traditional web forms used for more than two decades to authenticate the identity of the users online.

b) These are particularly vulnerable to data breaches, and these centralized IdM services models pose specific risks and challenges – in the form of reputational and prospective financial harm to both the company / organization and increased mistrust in its operation.

c) Fraudulently filling the online form, to lie to someone else, is fairly easy.

B. Portable Trust: biometric-based authentication and block-chain storage for self-sovereign identity systems

They conceived a mobile biometricdriven authentication system focused solely on local processing. Their Android open source solution examines existing smartphones' ability to collect, process and match fingerprints using their built-in hardware only. Their architecture [14] is specifically designed to run locally and autonomously, allowing fingerprint readers to have no cloud service, server or approved hardware access. It involves three main phases, starting with the acquisition of fingerprints using the smartphone camera, followed by a processing pipeline to obtain minutiae features and a final stage to match other locally stored fingerprints, based on the descriptors Focused FAST and Rotated BRIEF. They obtained a mean matching accuracy of 55 percent, with a thumb finger limit of 67 percent. Their ability to capture and process a fingerprint [14] in a few seconds using a smartphone makes this research accessible in a broad range of contexts, such as remote regions offline. This work is specifically designed to be a key building block for a solution to self-sustainable identity and to integrate with their permission less blockchain for identity and key attest.

1) Demerits

a) The processing of a typical finger-print consumes a lot of time as compared to other existing systems.

b) The machine provides a mean matching accuracy of 55 percent for the left-hand thumb with a maximum of 67 percent and a minimum of 35 percent for the left pinky finger which is considered low.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

C. Virtualization in Cloud Computing

Virtualization technology is a part of the foundations for Cloud computing technology. Late in the Sixties when applications were multiplexed on very expensive mainframes, a technology was required that allowed resource utilization to the full extent possible, and virtualization technology thus emerged. Virtualization uses VMM in the multiplexing of hardware resources, server consolidation and running of multiple OS instances simultaneously, so that VMM can take control of the running guest OS flows. VMM is a thin software layer which runs conventionally on a computer's hardware. This may also run on the operating machine over a host OS.

VMM is responsible for the management of VMs, and does not allow direct contact with the host hardware. Guest OSs running on VMs communicate through the VMMs only with host device resources. The VMM usually runs at some of the most protected level and is considered a reliable component, whereas the guest operating system is considered untrusted and, thus, runs in user mode. Later, as modern technology progresses in processor capacities, bus speed, storage space, memory, and reduces the costs of dedicated servers.

1) Demerits

a) Not every system or server can run in an environment of virtualization. That means a individual or organization can operate properly using a hybrid system.

b) It can carry a high implementation expense.

c) Biometric encryption in cloud computing does not solve security concerns, but secures biometric data against most security issues.

D. Block-chain based Identity Management with Mobile Device.

Block-chain is a powerful and distributed transaction network that requires a centralized, stable, open, and consensus-based record keeping framework.

It was applicable to situations such as smart city, supply cShain, storage and exchanging of medical data and so on. Many works have been done to improve the performance of such systems and their security. There is however a lack of identity linking mechanism when a human being is engaged in the respective test environment, i.e. when one is engaged in an action, his / her identification in the actual world should be properly represented in the block chain network.

We propose Block-ID [15], a novel identity management system for individuals that leverages biometric authentication and trusted computing technologies, to fill this gap. We also build a prototype to demonstrate its functional viability. They suggest Block-ID, which helps by creating online identity from government issued IDs to accurately link personal information to the block-chain based transaction network.

Attached to a mobile device is this wireless identifier. Block-ID leverages user authentication based on biometrics, and trust computing technologies to ensure that the information stored in the block chain represents the truth correctly. Theoretically, the Block-ID can be applied with trust computing technology to any biometrically enabled mobile device.

1) Demerits

a) The secret key's confidentiality and honesty depend on the smart-phone. When an attacker can breach the privacy policy and steal the password that is stored on the device, the attacker will use that to communicate directly with the block chain.

b) The digital identity used in the block chain is connected to the individual, identification provided by his / her government, mobile, and biometric information about him / her. If there is no retention of the binding attribute, the digital identity may not represent the correct details of the person who uses it.

III. EXISTING MODEL USING ONTOLOGY

We propose a fingerprint identification scheme to preserve privacy. For biometric authentication, our scheme utilizes a symmetric homomorphic encryption algorithm, does achieving both protection and performance. In order to save storage costs and increase performance, we require the server to offload most computations to a cloud so that fingerprints are protected.

In addition, most computations are transferred to a third-party organization from a server to leverage their resources. There is, however, a pay-off between efficiency and privacy,i.e., they will presume the server has the permission to access the database of fingerprints.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

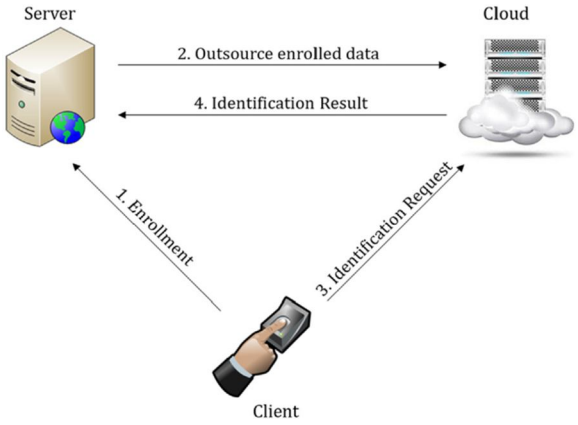


Figure 1: The system model of the existing scheme.

We stress that considering the irrevocability of biometric data, such an assumption must be alleviated for example, a malicious employee with access to the fingerprint database could sell a copy of the data to another, or the server may be hacked, thereby making the data unrecoverable.

A. Threat model

We believe attackers are residing outside of the network and trying to eavesdrop data sent from a client [11]. Such intruders are aimed at acquiring the raw biometric data of a victim, the fingerprint in this case. The attackers can then bypass the recognition process and get to the data server successfully. Biometric features, as described earlier, are unable to be revoked when leaked. Hence it is essential to protect biometric data from attackers. We describe the cloud as an honest yet suspicious organization, meaning that it conducts properly in most cases yet attempts to harvest the fingerprint data of the biometric information.

Virtualization poses certain security issues. These security concerns have moved into cloud environments which effects the confidentiality of biometric data. It also overcomes many security weaknesses associated with biometric data confidentiality in Cloud computing. Using biometric encryption reinforces this confidentiality. However, biometric encryption does not address security problems in cloud computing, but secures biometric data against several of these security challenges [12]. There is no work relevant to biometric encryption studied in cloud computing until this moment. However, biometric encryption in Cloud computing are going to be implemented in the future. And biometric encryption for biometric data can also be implemented and tested in cloud computing.

B. Demerits of Existing System

1) User lose some control.
2) Risk of exposing confidential data.
3) Synchronizing the deliverables.
4) Hidden costs.
5) Data Privacy at risk.

IV. PROPOSED SYSTEM DESIGN

We propose an effective and privacy-conserving biometric identification with block-chain scheme that can resist the users and cloud collusion attack. We analyze the biometric identification scheme and demonstrate that it is highly appropriate and that under the proposed level-3 attack there is no security vulnerability. In particular, we show that by colluding with the cloud, the attacker cannot recover their hidden keys, and then decrypt all users' biometric traits.

As seen in Fig.2, the program includes three types of entities: the owner of the database, the users and the cloud. The owner of the database maintains a large amount of biometric data that is encrypted and forwarded to the cloud for storage. If a user decides to recognize him / her, the owner of the database is sent a query request. The database owner produces a cipher-text for the biometric characteristic after receiving the request and then transmits the cipher-text for identification to the cloud.

©IJRASET: All Rights are Reserved

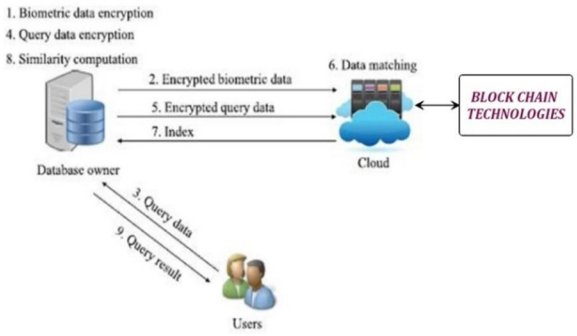


Figure 2: The Proposed System

The cloud server determines the best fit for the encrypted query and returns the associated index to the owner of the database. Finally, the owner of the database computes the similarity between the query data and thus the index-related biometric data, and returns the query result to the user.

A. Design goal

Our goal is triple. Firstly, fingerprint data will not be exposed to all people, including the server and the cloud, during registration and identification. Next, the scheme proposed should be able to screen out malicious clients who send random values much like the Finger Codes of legitimate clients. Finally, the computing and communication recognition should be effective.

We have introduced the proposed scheme for evaluating the actual results. To analyze the practicality of the proposed scheme in cloud computing, we programmed our proposed framework using the Java Unix instance language in Amazon's EC2 cloud [9]. We are setting up five databases with different sizes To develop a realistic biometrical identification scheme. The Amazon EC2 cloud consists of a single instance node with the 2.5 GHz E5-2670v2 CPU and 1 GB ram from Intel. Linux runs with low I / O performance at the cloud example. Yuan et al. [10] 's scheme is, to the best of our knowledge, the most recent and quickest among the current schemes. Therefore, to compare with our scheme we implemented this biometric identification scheme.

B. Enhanced security using Block -chain Technology

A block chain is basically a centralized record store or a public ledger with all transactions or digital events executed and exchanged by participating parties. That public ledger transaction is varied by consensus of a plurality of network participants. And, once entered, it can never delete the knowledge. The block-chain includes a certain and variable record of every transaction that has been made. To use a simple example, it is simpler to steal a cookie from a jar of cookies, which is kept in a secluded place than stealing the cookie from a jar of cookies held in a marketplace, where thousands of people watch.

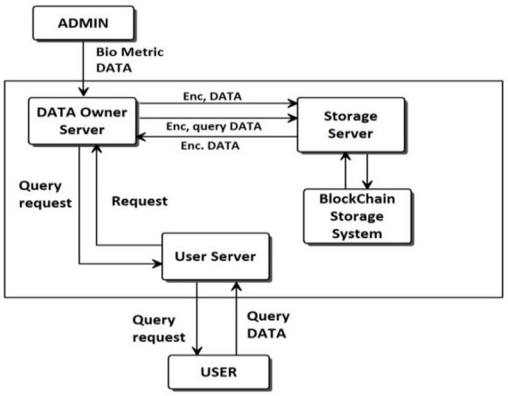


Figure 3: Proposed System Architecture

In the report, it distinguishes between multiple types of block-chain and explains the two biggest platforms, namely Bit coin. While introducing these two platforms, we explain the most important technology and algorithms as proof of the concept of work used.

©IJRASET: All Rights are Reserved

C. Advantages of Proposed System:

1) *Security:* The privacy of biometric data should be protected during identification processes. Attackers and the semi-honest cloud should not learn the sensitive information about it.

2) *Efficiency:* The computing costs on both the owner and user side of the database should be as small as possible. Most biometrical identification operations should be performed in the cloud to gain high efficiency.

3) Reduce workload and enhance productivity.

4) Better flexibility and speed.

V. CONCLUSION

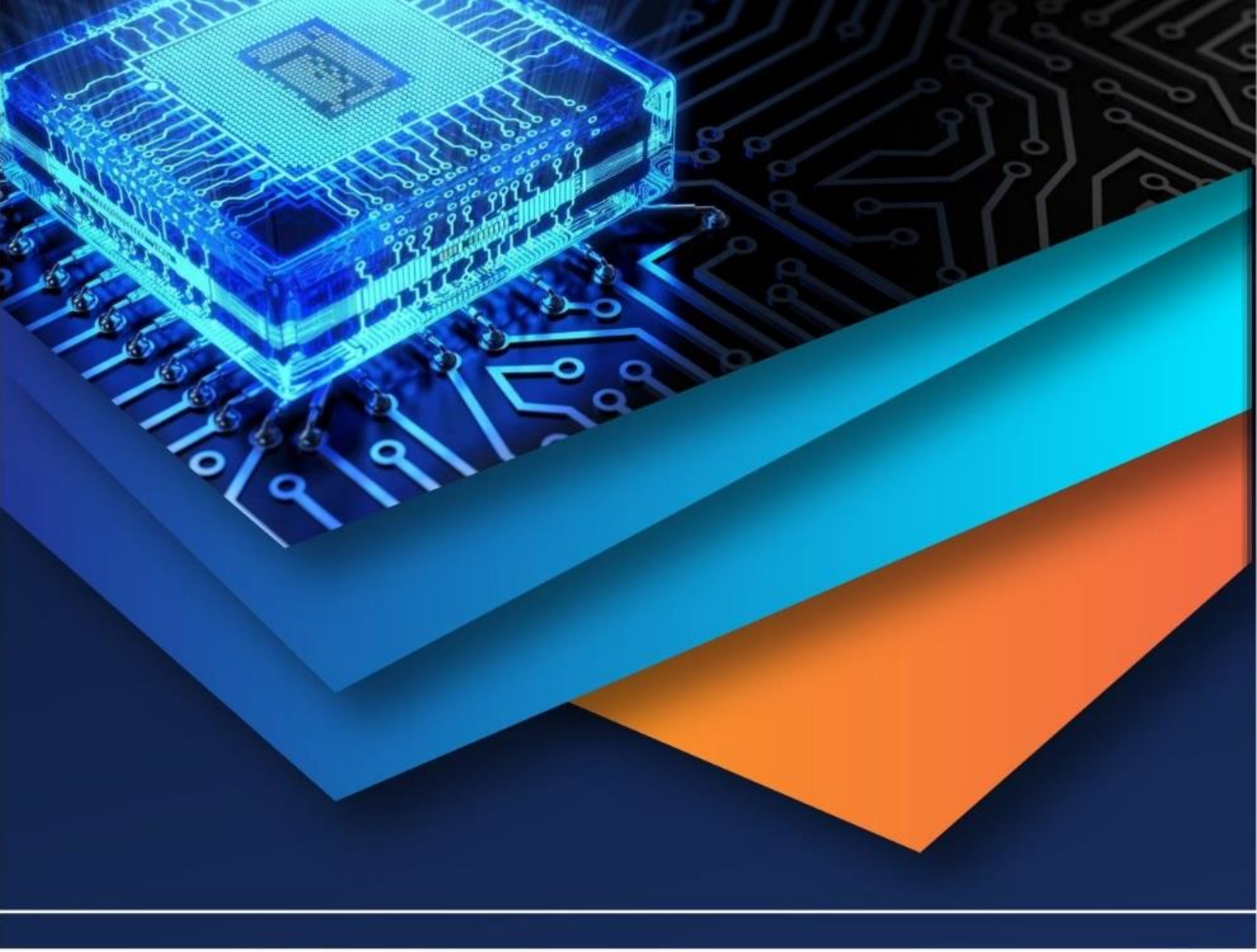
In conclusion, we proposed an effective and privacy-conserving scheme in cloud computing for biometric authentication. In contrast to previous studies, we do not require any individuals to access customer biometric data except the client. The security analysis shows not to reveal the biometric data to the server and cloud. We effectively outsource the biometric identification of clients to the cloud by leveraging the additively homomorphic encryption.

It is particularly suitable for cloud computing Delegation-based business applications. In this paper, we introduced a controllable privacy protecting search scheme that allows a cloud storage owner to handle their cloud data's lifetime and search rights with ease. In the journal version of the paper, we will provide more explanations and comparisons on the proposed scheme and will demonstrate the security of the proposed scheme through formal evidence. Our further research will be dedicated to the development of complex access control and search privileges.

REFERENCES

[1] Jain, L. Hong, and S. Pankanti, ‘‘Biometric identification,’’ Commun. ACM, vol. 43, no. 2, pp. 90–98, 2000.
[2] R. Allen, P. Sankar, and S. Prabhakar, ‘‘Fingerprint identification technology,’’ in Biometric Systems. London, U.K.: Springer, 2005, pp. 22–61.
[3] J. de Mira, Jr., H. V. Neto, E. B. Neves, and F. K. Schneider, ‘‘Biometric oriented iris identification based on mathematical morphology,’’ J. Signal Process. Syst., vol. 80, no. 2, pp. 181–195, 2015.
[4] J.Yuan and S.Yu,‘‘Efficient privacy-preserving biometric identification in cloud computing,’’ in Proc. IEEE INFOCOM, Apr. 2013, pp. 2652–2660.
[5] Y. Zhu, T. Takagi, and R. Hu, ‘‘Security analysis of collusion-resistant nearest neighbor query scheme on encrypted cloud data,’’ IEICE Trans. Inf. Syst., vol. E97.D, no. 2, pp. 326–330, 2014.
[6] Q.Wang,S.Hu,K.Ren,M.He,M.Du,and Z.Wang,‘‘CloudBI:Practical privacy-preserving outsourcing of biometric identification in the cloud,’’ in Proc. Eur. Symp. Res. Comput. Secur., 2015, pp. 186–205.
[7] Y. Zhu, Z. Wang, and J. Wang, ‘‘Collusion-resisting secure nearest neighbor query over encrypted data in cloud,’’ in Proc. IEEE/ACM 24th Int. Symp. Quality Ser. (IWQoS), Jun. 2016, pp. 1–6.
[8] S.Pan,S.Yan,andW.Zhu,‘‘Securityanalysisonprivacy-preservingcloud aided biometric identification schemes,’’ in Proc. Australasian Conf. Inf. Secur. Privacy, 2016, pp. 446–453.
[9] X. Hei and X. Du, ‘‘Biometric-based two-level secure access control for implantable medical devices during emergencies,’’ in Proc. IEEE INFOCOM, Apr. 2011, pp. 346–350.
[10] M. Barni et al., ‘‘Privacy-preserving fingercode authentication,’’ in Proc. 12th ACM Workshop Multimedia Secur., 2010, pp. 231–240.
[11] H. Delfs, H. Knebl, and H. Knebl, Introduction to Cryptography. Berlin, Germany: Springer, 2002.
[12] K. Liu, C. Giannella, and H. Kargupta, ‘‘An attacker’s view of distance preserving maps for privacy preserving data mining,’’ in Knowledge Discovery in Databases: PKDD (Lecture Notes in Computer Science). Heidelberg, Germany: Springer, 2006, pp. 297–308.
[13] Identity Management in the Age of Blockchain 3.0 Arthi Kanchana Manohar , Jo Briggs Northumbria University Newcastle Upon Tyne, UK
[14] Portable Trust: biometric-based authentication and blockchain storage for self-sovereign identity systems J.S. Hammudoglu, J. Sparreboom, J.I. Rauhamaa, J.K. Faber, L.C. Guerchi, I.P. Samiotis, S.P. Rao and J.A. Pouwelse (course supervisor). Computer Science department, Delft University of Technology, The Netherlands.
[15] Blockchain-based Identity Management with Mobile Device Zhimin Gao, Lei Xu,Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, Weidon gShi Department of Computer Science,University of Houston Houston,Texas

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)