Journal of Critical Reviews A SURVEY ON BIOMETRIC AUTHENTICATION SYSTEMS IN CLOUD TO COMBAT IDENTITY THEFT

Vanitha Carmel
Vel's Group of Institutions
1 PUBLICATION **8** CITATIONS
SEE PROFILE

Akila D.
Saveetha College of Liberal Arts and Sciences
116 PUBLICATIONS **632** CITATIONS
SEE PROFILE

Multidisciplinary Review Journal

Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 3, 2020

Review Article

A SURVEY ON BIOMETRIC AUTHENTICATION SYSTEMS IN CLOUD TO COMBAT IDENTITY THEFT

V.Vanitha Carmel[1], Dr.D.Akila[2]

[1]Research Scholar, Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Email: vani_carmel@yahoo.com
[2]Associate Professor, Department of Information Technology, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, India. Email : akiindia@yahoo.com

Received: 05.11.2019 *Revised: 10.12.2019* *Accepted: 15.01.2020*

Abstract

Biometrics has by far proven to be an effective solution for many of the security challenges that is prevalent in most of the technical fields in this Digital era. It is the measurement of physical or behavioral traits in humans used for unique identification. Biometricsuses the pattern recognition technology of Digital Image Processing for identifying unique features in humans. Most commonly applied or considered biometric modalities comprise fingerprint impression, facial landmarks, iris anatomy, speech recognition, hand writing detection, hand geometry recognition, Finger vein detection and signature identification. Biometric technology is applied in various fields, Security systems being one among them. This paper presents a thorough survey on how biometrics can be effectively applied to eliminate oneof the cloud security issue, identitytheft. Awide range of biometric authentication system protocols and implementations in cloud environment, especially to combat identity theft have been proposed earlier.

Keywords : Biometrics, Modalities, Pattern Recognition, Identity Theft

DOI: http://dx.doi.org/10.31838/jcr.07.03.97

INTRODUCTION

The process of extorting useful information for analysis, from input images by performing some operations is called the technique of Digital Image Processing. It is a type or sub divisionof signal processing technique where an image is given as input andoutput may be processed image or characteristic features associated with it. Digital Image Processing is an increasingly growing technology and it is the crux of many researcheswithin engineering fields and computer science discipline. Its use is exponentially increasing everyday as it has a wide range of advantages and finds its applications in vast areas.

Image processing mainly includes the following three phases:

- Importing input image through image capturing apparatus;
- Preprocessing, Evaluating and nanomanipulating the input image;
- Giving output,where result will be changed image or analyzedreport that is produced by interpretation of image data.

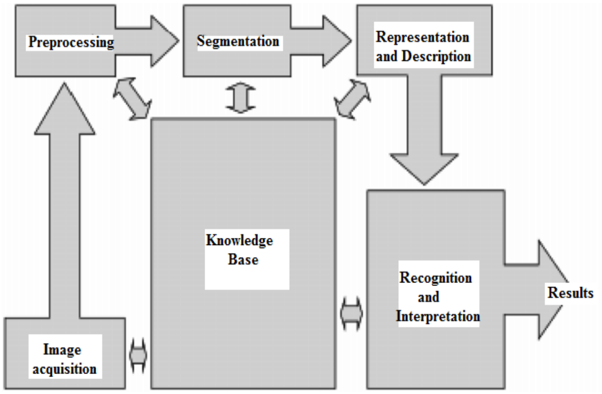

Fig 1: Steps in Digital Image Processing

Some of the areas whereImage Processing is applied extensively are sharpening of image and restoration, Medical Field, Guided Robot vision system,Pattern recognition system and videoprocessing.Pattern recognition technology, which is a major application area of DIP is the discipline for observing, differentiating the patterns of interest, and using it for further decision making. Biometric which refers to the measurement and statistical investigation of people's distinctive physiological and behavioral characteristics uses pattern recognition mechanism to recognize and categorize the individuals, by finding correspondence with the templates stored in the database.

Because of its unique ability to identify individuals ,biometric technology has rapidly become a means to help prevent identity theft and fraud in cloud environment and therefore has found its place among mainstream technologies[12].Biometric authentication is more reliable in detection of duplicate identities than traditional authentication systems which uses passwords and documents for identification[20].Though biometric systems are not completely infallible,the research community is constantly taking significant effort to identify vulnerabilities in cloud security and provide solution to counter them.New algorithms are evolving for protecting biometric template which lessens the concerns about security privacy of the user.

Use of biometrics is increasing each day as our physical modalities like faces, fingerprints,palm vein irises,hand geometry and voices are truly unique,that make them an effectual blockade to cyber criminalstrying to underhandedly impersonate us. They are helpful because unlike names, ID numbers, email addresses, and passwords, they are relatively more distinctive, secret, lasting, steady, difficult to replicate, and—most particularly—physically bound to us, which also happens to be very convenient.

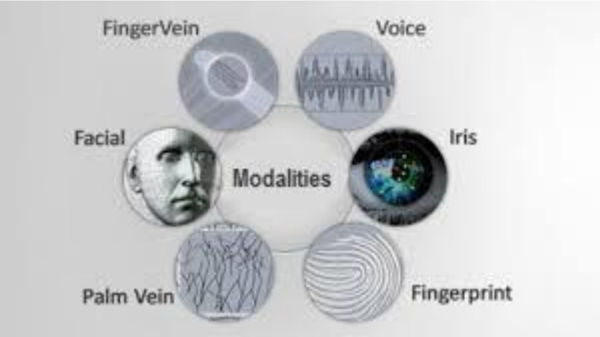

Fig 2: Biometric Modalities

Cloud computing is a computing model which provides on-demand and anywhere, anytime services, especially computer system resources like data storage, computing power and infrastructure to organizations and IT industry. Based on their operational requirements organizations can scale-up or down theservice. Though cloud offers a lot of benefits, it lags in providing security stability which is of great concern. Cloud users are reluctant to store their sensitive and confidential information in cloud due to various security based threats[18].A lot of research has been channelized towards finding effective ways to exterminate security issues from cloud.Centralised and Federated identity is a scheme suggested by studies made by researchers forsafeguarding identity oriented information.

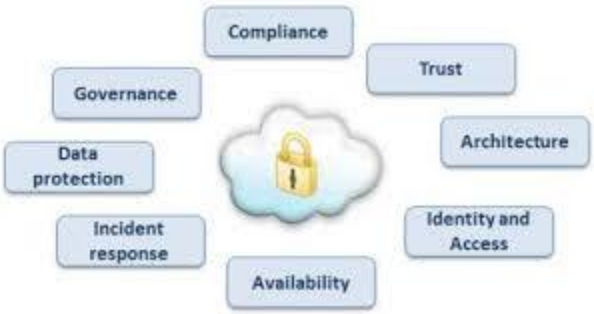

Fig 3 :Cloud Security Issues

LITERATURE REVIEW

The authors in paper [17] havedone a complete analysis of the cloud environment and summarized the currently prevailing security facet in cloud, threats possibilities and mitigations in cloud services with an emphasis on access supervision, identity management, security aspects, and services. Their research evaluates different topics with their generally used mechanisms or techniques, foremost issues related to each mechanism, suggestions and most efficient and robust practices from academic circles and from industry viewpoint.

Table 1:Synopsis of diverse Cloud Mechanisms – Security Aspects and Issues[17].

Topic	Mechanisms/Technique used	Security Aspects	Issues/Attacks
Data Security Threat	Cryptography for secure data communication	The user data is protected through encryption	Brute-Force Attack (Attacker using different password combinations ,eventually hoping to find the correct one)
Resource Availability	Resources accessibility and usability by cloud users	Availability of required resource at right point of time	counterfeit resource usage and Cloud outages due to power loss or network connectivity

Cloud Multitenancy	Hypervisors ,which enables many virtual OS to run on a computer system, VMM (Virtual Machine Monitor)	As resources are shared the need arises for the cyber security	Co-location attacks strategically initiated by adversaries, co-residence where hackers create side channels and extract personal information from VM.
APTs(Advanced Persistent Threat) and Threat from Malicious outsiders	determination of targets in advance and Persistence	cyber security risk	Insight data gathering, surveillance examine assaults, State-supported threatening digital doings, undercover work assault and Hacking

Identity theft is synonym to impersonation or fraud related to identity. Hackers steal personal details of the victims and use it with a malicious intent [1].Most of the time the victims are caught unaware of the situation. Fraudsters usually use such information for monetary gain involving credit, services and merchandise [2]. In some cases the imposters trap the victims in legal issues. According to a survey in USA there has been a gradual increase in identity theft victims each year.

Table 2 :Summary of Services and theattacks Associated with them[17].

Topic	Issues/Attacks	Mitigations
System Protocols and Standard Sessions	Hijacking(simpler type of hacking), network based attacks(controlled by external devices which are not present in the network), theft of cookies, TLS(Transport Layer Security)vulnerability and attacks	Using secure sessions, using very efficient cum competent antivirus and antimalware software
Web –based Services	Spoofing Attacks to gain illegitimate access, XML Wrapping attacks	Implementing strict safetyguidelines at both the receiver and sender end
Web-basedTechnologies	Web site growth infections, Attacks during session, manipulation attacks(stealthy tweaking of data), malware downloading, browser susceptibility to attacks	Analysis of Vulnerabilities and taking appropriate preventive steps
Availability of Web-based Services	Flooding attacks which makes the server busy and less responsive to legitimate user traffic, DNS reflection which knocks down the internet service pipe and amplification attacks	Regulating the user requests or by increasing the number of servers

With the ever growing cloud technology millions of organizations are moving towards cloud environment to avail its services and lessen their own responsibilities and expenses. But the security issue in cloud eates a major black hole. Identity theft in cloud has been creating a ripple effect and has been causing a vast damage to victims both financial and psychologically. Cloud authentication systems are the entry points for cybercriminals and any deficiency in performance ofit could lead to lethal consequences. Systems using traditional techniques definitely are not a solution for effective authentication systems.

Biometric technology, which uses the physical or behavioral features of an individual for unique identification can be an efficient substitution in place of traditional authentication techniques to exterminate identity theft in cloud environment.

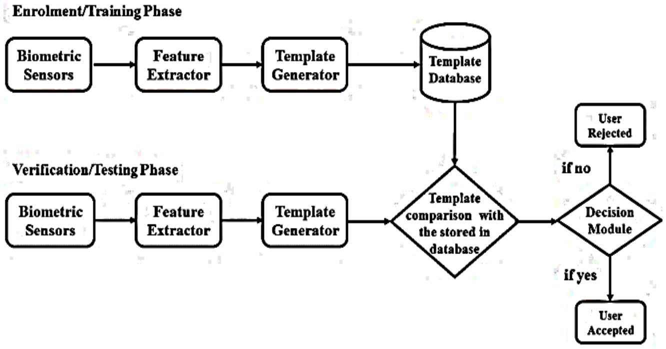

Fig 4: General design for biometric-based system [2]

Biometric uses multiple attributes involving both physical and behavioral traits inhumans for identification. Facerecognition, Finger print recognition, Iris and Retina scanning, Palm vein recognition, Hand geometry and voice recognition belongs to physiological features and signature, keystroke are behavioral characteristics [3][4].

The proposed authentication framework by ShabanaZiyad and A. Kannammal is secured by amalgamating the technique of biometrics along with cryptography [5].Their system structure involves three main phases, Initialization phase followed by Registration phase andVerification phase. Smart cards are created using the details provided by the client as proof. Furthermore at the time of the registration, biometric data are acquired from the client are encrypted and stored in the smart card. Each smart card contains authentication number along with palm vein biometric data and other information. During verification phase the input data from the smart card is compared with the templates in the database and if the matching is found, then handshaking with server is initiated and the user is allowed to access the system.

The insistent rise in identity theft has necessitated the requirement for an extra security priority to be given to personal information. Zahrouni et al have developed an app which acts as an additionallevel of security gateway above the existing banking softwares[6]. A biometric Lock App is proposed which provides extra safety by functioning in tandem with the banking app and ensures a protected use of credit and debit cards. The researchers have employed biometric techniques as the core mechanism in their authentication system. The app helps the user to have a check on their financial transactions by giving suggestions as and when required at all geographic levels. Protecting the vital information is the need of the hour and it is the prime importance in this digital era due to vulnerability of malicious access. The researchers in their work in [7] have done a detailed research on drawbacks in the existing biometric authentication strategies and have come up with a system design which uses the fingerprint, iris anatomy and palm print metrics.RC4 and DWT algorithms have been used for data encryption and information hiding.

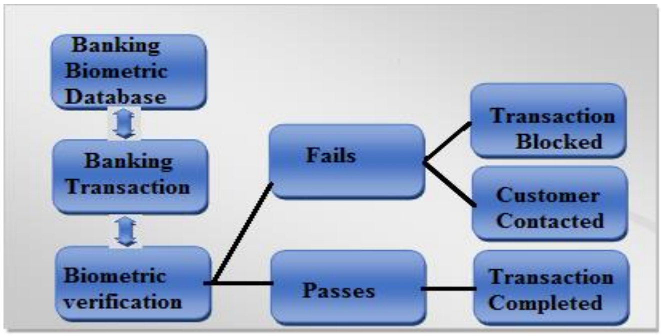

Fig 5:An illustration of banking verification system [6]

Traditional system applies authentication in either one mode or multiple modes. Single- sign-on (SSO) is a technique which uses traditional methods and allows the user to gain entry into the system by entering their identity information only once , but can avail and access the service at various levels[8] [9][10].Shruthi and MahendraVerma proposed an enhanced SSO based authentication system which is based on multi-factor concept[10].The whole process is eased for user convenience and the system is efficient compared to existing modules which is deficient in protection of cookies, security of cached data,protection of tempory storage ,solely dependent on credentials for authentication etc. The authors have suggested continuous bit sequence oriented certificates using more management schemes. Therefore the system is a completely protected one offering security against malicious manipulations.

In a federated environment, Trusted computing and multi tenancy can help solve trust and security issues[8][9].In their research work presented by EghbalGhazizadeh et al the integrated concept of trusted computing which would offer improved security,federated identity management for signal authentication and OpenlO Web Single-Sign on(Web SSO) has been proposed to resolve identity theft crisis in cloud[9].The scheme is a unique model, as it has not been so far offered in SSO in web or federated identity.

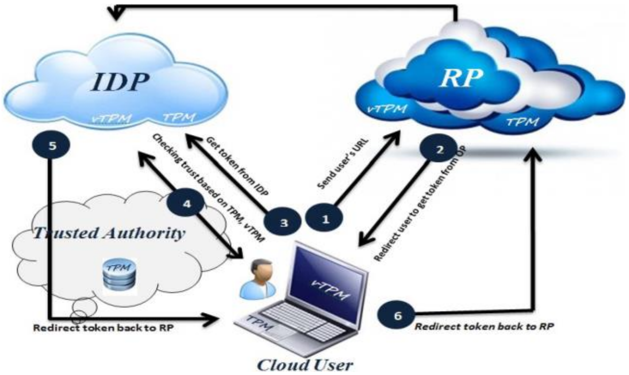
IDP
vTPM
TPM
RP
vTPM
TPM
5
4
3
1
2
6
Checking trust based on TPM, vTPM
Get token from IDP
Send user's URL
Redirect user to get token from OP
Trusted Authority
TPM
vTPM
TPM
Redirect token back to RP
Redirect token back to RP
Cloud User

Fig 6: Proposed OpenID[9] architectural model to mitigate identity theft crisis

The cloud services provided by service providers are diverse in nature and often federated which are beneficial to the cloud users. Without a proper Authentication process, the providers as well as the users will be at loss as third parties would easily gain entry and carry out some undesirable act. Mohamed Ibrahim Beer et al have analyzed the vulnerabilities in federated identity when it is implemented into inter and intra-organizational computing environment[8].An Adaptive architectural model for security has been put forth for identity federation management in which Public Key Infrastructure(PKI) is used that complies to security standards and specification of SOA(Service Oriented Architecture).

The authors of paper[11] have done a case study on protocol designed by Amin et al for authentication in cloud environment. They have elaborated on intricacies and security weaknesses existing in the protocol and have suggested a scheme as a solution. The researchers have designed a authentication protocol which uses BAN (Burrows-Abadi-Needham) logic and a heuristic analysishave been done to substantiate the efficiency of their protocol. The authors claim their protocol has excellent functionality compared to other available protocols.

Florian Obergrusberger et al have proposed biometric observer principle and have implemented a specific prototype to protect the procedure of biometric features enrollment(registration) in cloud atmosphere[13].Primarily the strategy uses the aspects of Web of Trust. The whole process of authentication, from initial stage of creating a biometric template to the final phase of authentication is supervised by an observer or supervisor ensuring the legitimacy of the system. A reliable and all-inclusive trust model ensures dependability and trustworthiness of the biometric identities stored in the system database.

Insurance and finance industry are the worst sufferers due to identity theft. The study by Chandramohan et al have focused on the privacy issues involving intellectual and confidential information belonging to insurance and finance sectors[14].Through their study, the researchers have tried to assure the CR(cloud users/Requesters) that their data stored in cloud is safe and secure .The technique, Privacy Preserving Model to Prevent Digital Data Loss in Cloud(PPM-DDLC) has been projected for securing data in cloud.

Continual authentication proves to be suitable for handling a range of security issues. The concept of continuous authentication is used to avoid security threats like illegal identity sharing, insider threat, lopeholes in forensic analysis etc.Online examination impersonation fraud falls in former category. The approach stated by IssaTraore et al has the concept of continuous authentication being implemented in online examination platform[15].The authors have created a framework which acts as a shield in an online exam and it includes features like video streaming of exam environment and exam management services. Multiple biometric modalities is evaluated using offline datasets.

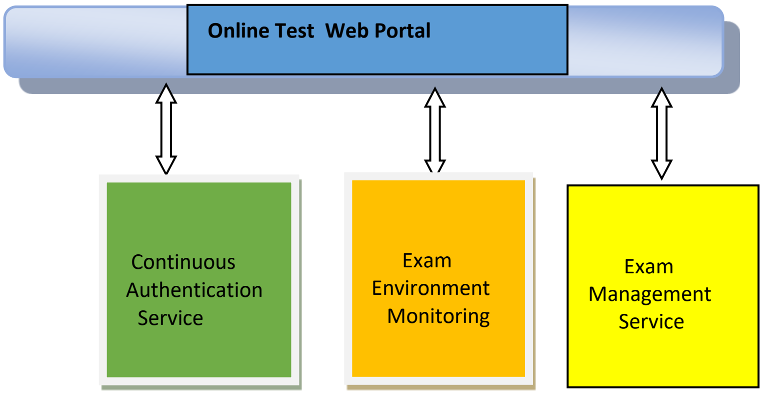
Online Test Web Portal
Continuous Authentication Service
Exam Environment Monitoring
Exam Management Service

Fig 7:ExamShield high-level architecture

Table 3: Summary of some of the Cloud based authentication systems along with mechanism used

Authors	**Proposed Scheme/Topic**	**Mechanism used**
ShabanaZiyad and A. Kannammal[5]	A Multifactor Biometric Authentication for the Cloud	Smart card technology, Palm vein and Fingerprint biometrics, Encryption
LamjedZahrouni et al[6]	Preventing Identity Theft Using Biometrics Based Authentication System	Biometric Lock App using face and fingerprint biometrics which acts as Extra layer of security upon existing banking application
Malathi.R and JebersonRetnaRaj.R[7]	An Integrated Approach of Physical Biometric Authentication System	Fingerprint, iris recognition and palm print metrics are used for identification.RC4 and DWT algorithms has been used for data encryption and information hiding.
Mohamed Ibrahim et al[8]	Adaptive Security architectural model for protecting identity federation in service oriented computing	Public Key Infrastructure (PKI) for secure access control, mutual authentication (Two way authentication),secure OTA(over the air)updation along with other securityTechnologies
EghbalGhazizadeh et al [9]	A Trust Based Model for Federated Identity Architecture to Mitigate Identity Theft	TPM(Trusted platform module), Virtual TPM, OpenID protocol which try support the tasks of authentication, authorization and identity federation.
ShrutiBawaskar and MahendraVerma[10]	Enhanced SSO based Multi-Factor Authentication for Web Security	Bit sequence based certificate,Cryptography,SSO technology,smart cards.

Chenyu Wang et al[11]	An Enhanced user Authentication protocol Based on Elliptic Curve Cryptosystem in Cloud Computing Environment	Public Key algorithm to defy offline dictionary guessing attack ,Elliptic Curve cryptosystem
Florian Obergrusberger[13]	Biometric Identity Trust :Toward Secure Biometric Enrollment in Web Environment	Biometric observer(four-eyes principle), which enables a protection scheme which is efficient as well as flexible and trust metrics to analyze the trust level of a node.
ChandramohanDhasarathan[14]	A Secure Data Privacy Preservation for On-demand Cloud Service	Privacy Preserving Model to Prevent Digital Data Loss in Cloud (PPM-DDLC) for securing the data in cloud. Continual authentication for handling a range of security issues.
IssaTraore et al[15]	Ensuring Online Exam Integrity Through Continuous Biometric Authentication[15]	Mouse dynamics(based on user interaction with mouse), keystroke dynamics(based on users rhythm of typing keys on keyboard) and facial examination are used for identification through continuous authentication scheme.
Eari Ryan M.Aleluya and CelessamaeT.Vicente [16]	FacetureID:Face and hand Gesture Multi-factor Authentication using Deep Learning	A MFA(Multi Factor Authentication) based system which does Face verification using Deep CNN-Convolution Neural Network, Handwriting scrutiny using Leap Motion tracking and OTP
AnkitChoudhary et al[18]	Fog Computing:Mitigating insider Data Theft attacks in the cloud	Decoy Technology is applied to identify fraudulent insiders.
K Sarat Chand and Dr. B Kezia Rani [21]	Biometric Authentication using SaaS in Cloud Computing	AES for encryption and AMBA for matching process with database template
Ali Z et al [22]	Edge-centric multimodal authentication system using encrypted biometric templates	Mel-frequency cepstral coefficients and perceptual linear prediction coefficients is used for Speech recognition. Facial Recognition is done determining eigenfaces
Kumari S et al [24]	Design of a provably secure biometrics-based multi-cloud-server authentication scheme[24]	ECC (elliptic curve cryptography) and Biohashing Is used for authentication
Zhu D et al [25]	A Quantum Identity Authentication Protocol Based on Optical Transmission & Face Recognition	optical transmission, quantum key concept and facial recognition. One-time pad scheme for facial feature point encryption

.

Multi-Factor Authentication (MFA) is the current trend which is emerging rapidly.MFAis a combination of more than one factors like i)inherence(biometric characteristics of the user) ,ii)possession(something the user has) and iii)knowledge (something the user knows), for authentication. Though there are many systems which is based on MFA,none has explored the following combination of face recognition ,OTP (One Time Password) and Hand gesture recognition as claimed by the author[16].The study has proved the efficiency of their strategy which has a novel authentication technique called Faceture ID. This study has three very useful contributions: i) Pre-trained Deep Convolution Neural Network based sample gallery set for face verification, ii) Handwriting identification using Leap motion controller, which tracks the movement of hand and finger using LED's with infrared technology and CNN(Convolution Neural Network for categorization, and iii) MFA scheme with a combination of face, hand gesture and OTP. Decoy documents can be used to trick the illegitimate access by an malicious insider in organization [18].In their research,the authors have proposed observation knowledge access patterns by identifying user behavior and thoroughly scrutinizing it to detect malicious activity of an insider to illegimatelyaccess someone's documents in Cloud.

To overcome the risks involved in using the traditional methods like passwords and PINs for securing data Sarat and Kezia [21] have proposed a Biometric system for authentication and they claim it to be more unique and very efficient in controlling data breach in cloud computing. In their system the researchers have used AES(Advanced encryption standard algorithm) for encrypting the biometric data obtained from the user at the time of registration and have devised AMBA(Advanced Minutiae Base Algorithm) for comparing user data with that of the templates in the database during the verification or matching makingprocess.

Biometric information is subjected to privacy protection law as it is very sensitive in nature. To deal with the data security issues, a multi-modal biometric system for authentication has been proposed by Ali Z et al[22].Their work targets the edge-centric cloud computing. Portable personal devices are used for the encryption of biometric data,thus optimizing the use of cloud recourses. A novel encryption method has been devised in the system. The edges in the proposed system transmit the encrypted data containing speech and facial features to cloud for processing. The cloud takes care of the process of decryption and then acknowledging an individual in case of being an authorized user. Speech recognition is done using the concepts of Mel-frequency cepstral coefficients and perceptual linear prediction coefficients. Facial Recognition is done determiningeigenfaces.Finally a majority voting scheme is used for identifying the user.The researchers claim their work to be more reliable due to the effectiveness of their encryption algorithm.

In this paper[23],the authors have proposed a privacy preserving biometric system with data encrypted and stored in the database located in the cloud. The correctness of the identification system is achieved first and secondly the privacy of very sensitive biometric information and secret values of keys is captured and preserved confidentially. The identification security system has been tested for efficiency against *Level-II* and *Level-III*attacks.

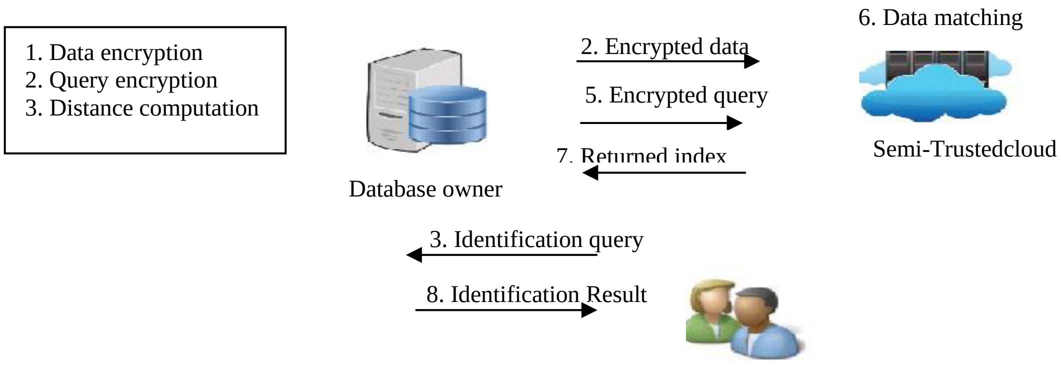

Fig 8:Architecture of the cloud-based biometric-identification system[23].

The authors proposed biohashing technique which has zero EER(Equal Error rates) and ECC(elliptic curve cryptography)for the purpose of authentication, in the multi-server based cloud service environment.Biohashing and ECCare considered to be very competent in handling the security of biometric data in the authenticationprocess [24]. The scheme has four phases, as follows: System Initialization phase, User-registration phase, Logging-in phase, Authentication and agreement of key phaseand change of password phase.

In this paper[25], authentication protocol using quantum identity has been put forth .It is based on optical transmission and facial feature recognition. The proposed scheme integrates optical transmission, quantum key and facial recognition. Nine key facial features in the image is recognized through face identification technologyand quantum key is acquired by optical transmission[28]. The face key features obtainedare encrypted and decrypted using one-time pad encryption scheme.The protocol intends to ensure user information confidentiality and authenticity at initial stage of user registration and later, during the authentication stage, achieving a high degree of efficiency in securing the system against security attacks[27].

Security of templates in the database is vital to the reliability of a biometric system. In this paper [26] minutiae descriptors is used to improve the operating efficiency of matching process and securityof fuzzy vault of fingerprint minutiae. Experimental results obtained based on fingerprint database in public domain shows considerable reduction in FAR(False Accept Rate) without affecting GAR(Genuine Accept Rate).

CONCLUSION

Biometric technology is considered to be a solution for security challenges in various fields. IdentityTheft, a major threat in cloud computing can be prevented through anappropriate biometric authentication system. This paper provides a state-of-art survey on the diverse authentication systems available in cloud environment to combat Identity theft. Many of the research works have made significant effort to provide an efficient authentication system which guarantees security against data theft. Contribution of each of the work has been discussed and strategies employed by the researchers have been explored in this paper.

REFERENCES

1. Margaret Rouse,“Identity Theft”, https://searchsecurity.techtarget.com/definition/identity-theft ,Jan 2020.
2. National Security Agency,CyberSeurity Information, Cybersecurity Requirements Center (CRC),Cybersecurity_Requests@Nsa.Gov
3. A. M. Hussein,H.M. Abbas,M.S.M. Mostafa.”Biometric-based Authentication Techniques for Securing Cloud Computing Data - A Survey”,Researchgate.net,International Journal of Computer Applications (0975 – 8887) Volume 179 – No.23, February 2018
4. G.Naveed, R.Batool, “Biometric Authentication in Cloud Computing”, JBMBS, Vol.6(5),2015.
5. S.Ziyad and A. Kannammal,” A Multifactor Biometric Authenticationfor the Cloud”, Springer India, Computational Intelligence, Cyber Security and Computational Models, Advances in Intelligent Systems and Computing 246, 2014.
6. L.Zahrouni, D.Blackwood, S.Rizvi and J.Gualdoni,” Preventing Identity Theft Using Biometrics Based Authentication System”, IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies, 2017.
7. R.Malathiand R. Jeberson Retna Raj, “An Integrated Approach of Physical Biometric Authentication System”, International Conference on Computational Modeling and Security, Procedia Computer Science 85 (2016) 820 – 826,2016.
8. M.I.Beer Mohamed, M.F.Hassan, S.Safdar , M.Q.Saleem, “Adaptive Security architectural model for protecting identity federation in service oriented computing”, Journal of King Saud University – Computer and Information Sciences. 2019, pp.1-13.
9. E.Ghazizadeh,M.Zamani,J.AbManan,R.Khaleghparast and A.Taherian,” A Trust Based Model for Federated Identity Architecture to Mitigate Identity Theft”,IEEEInternational Conference for Internet Technology and Secured Transactions.97B-1-90B320-0B/7/2012.
10. S.Bawaskar and M.Verma, “Enhanced SSO based Multi-Factor Authentication for Web Security”,International Journal of Computer Science and Information Technologies, Vol. 7 (2) , 2016, 960-966, 2016.
11. C.Wang,K.Ding,B.Li,Y.Zhao,G.Xu,Y.Guo and P.Wang,”An Enhanced user Authentication Protocol Base on Elliptic Curve Cryptosystem in Cloud Computing Environment”,HindawiWireless Communications and Mobile Computing , Article ID 3048697, 2018.
12. D.Meva and K.Popat,” Cloud Computing and Biometrics”,International Journal for Research in Applied Science & Engineering Technology,Volume 6 Issue I, January 2018.
13. F.Obergrusberger,B.Baloglu,J. Sanger and C.Senk,” Biometric Identity Trust :Toward Secure Biometric Enrollment in Web Environment”,MYousif,LSchubert(Eds):Cloudcomp,LNICST 112, pp. 124–133, 2013.
14. C.Dhasarathan, V.Thirumal , D.ponnurangam,”A Secure Data Privacy Preservation for On-demand Cloud Service”, Journal of King Saud University-Engineering Sciences,volume 29,Issue 2,pages 144-150, 2017.

15. I.Traore,Y.Nakkabi,S.Saad,B.Sayed,J.D.Ardigo and P.M.de FariaQuinan, ”Ensuring Online Exam Integrity Through Continuous Biometric Authentication”,Springer International Publishing ,2017.
16. R.M.Aleluya and C.T.Vicente,”Faceture ID: Face and hand Gesture Multi-factor Authentication using Deep Learning”, International Conference on Computer Science and Computational Intelligence, 135 (2018) 147–154 , 2018.
17. I,Indu,P.MRubeshAnand and V.Bhaskar,”Identity and Access management in Cloud Environment :Mechanisms and Challenges”,ElsevierEngineering Science and Technology, an International Journal 21 (2018) 574–588, 2018.
18. A.Choudhary,T.Nikam,R.Singh and Y.kawle,”Fog Computing:Mitigating insider Data Theft attacks in the cloud”,International Journal of Advance Research,Ideas and Innovations In Technology, Volume 4, Issue 2,2018.
19. G.R Mettu and A.Patil,”Data Breaches as top Security concerns in Cloud Computing”,International Journal of Pure and Applied Mathematics,119(14):19-27,2018.
20. A.K.Jain and K.Nandakumar,“Biometric Authentication: System Security and User Privacy “,IEEE Published by the IEEE Computer Society ,0018-9162/12,Nov2012
21. K Sarat Chand and Dr. B Kezia Rani,”Biometric Authentication using SaaS in Cloud Computing”,
22. International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 02, Feb-2018.
23. Z.Ali,M.S.Hossain,G.Muhammad,I.Ullah,H.Abachi, andA.Alamri,” Edge-centric multimodal authentication system using encrypted biometric templates”,Elsevier Future Generation Computer Systems,2018.
24. C.Zhang,L. Zhuand C.Xu ,” PTBI: An efficient privacy-preserving biometric identification based on perturbed term in the cloud”, Information Sciences 409, 56-67,2017.
25. S.Kumari,X.Li,F.Wu,A.KDas,K.K.RChoo and J Shen,” Design of a provably secure biometrics-based multi-cloud-server authentication scheme”, Future Generation Computer Systems, 68, 320-330,2017.
26. D.Zhu,X.Li,R.We,J.Wu, andL.Song,” A Quantum Identity Authentication Protocol Based on Optical Transmission & Face Recognition”, International Journal of Online Engineering (iJOE), 14(04), 58-69,2018.
27. A.Nagar,K.Nandakumarand A.K Jain,” A hybrid biometric cryptosystem for securing fingerprint minutiae templates”, Pattern Recognition Letters31 (2010) 733–741.
28. C. Sudha, **D. Akila,** “Detection Of AES Algorithm for Data Security on Credit Card Transaction”, International Journal of Recent Technology and Engineering (IJRTE) Volume-7, Issue-5C, February 2019,pp.283-287
29. Dr. Jafar A. Alzubi, Dr. Omar A. Alzubi, Dr.G.Suseendran, **Dr.D.Akila**“+A novel Chaotic map encryption methodology for image cryptography and secret Communication with steganography- **International Journal of Recent Technology and Engineering,** Vol.8(1C2), May 2019, pp.1122-1128
30. Gupta V, Puri R, Gupta S, Jain S, Rao GK. "Tamarind Kernel Gum: An Upcoming Natural Polysaccharide." Systematic Reviews in Pharmacy 1.1 (2010), 50-54. Print. doi:10.4103/0975-8453.59512
31. Ayub, S.G., Ayub, T., Khan, S.N., Dar, R., Andrabi, K.I.Reduced nitrate level in individuals with hypertension and diabetes(2011) Journal of Cardiovascular Disease Research, 2 (3), pp. 172-176.
DOI: 10.4103/0975-3583.85264