ISSN 2047-3338

Multilayered Cloud Security Model Using Multifactor Session-Long Biometrics Access Control

Karthika Venkatraman[1] and Jihad Qaddour[2]
[1,2]Department of Information Technology, Illinois State University, Normal, United States of America
[1]karthika.v.uni@gmail.com, [2]jqaddour@ilstu.edu

***Abstract*– Cloud computing has tremendously simplified the software industry by enabling companies to offer software, infrastructure and platforms as services with the advantages of maintenance, availability, provisioning time and scalability. As individuals and firms increasingly rely on cloud-based systems to process sensitive data and intellectual property, the security risks surrounding cloud technology have increased by proportion. This paper investigates the vulnerabilities surrounding single point authentication, replay attacks and predictability. Then proposed a multilayered security model using multifactor biometrics authentication for access control. Additional features in the proposed model are to use diverse biometric templates in a randomized way, use strong algorithms for replay protection, session-long authentication with fine-grained biometrics and template updation in database after every successful authentication. Furthermore, the proposed solution approaches security as an ongoing mechanism and extends authentication service to the entire session, as opposed to traditional approaches that offer authentication only at the beginning of a session.**

***Index Terms*– Cloud Security, Multilayer Security Model, Identity Management, Multifactor Biometrics Authentications, Session-Long-Authentication, Fine-Grained Replay and Fine-Grained Multi-Factor Authentication**

I. INTRODUCTION

WITH the increasing number of security issues around user identity, the proposed solution is to use a three-factor authentication using biometric technology with a fine-grained replay protection mechanism.

The three biometric factors recommended to establish user identity are fingerprints, voice recognition and face identification [3] for non-critical applications; And Retina, Iris and fingerprints for critical applications dealing with sensitive data. The next layer of security is to use authentication through biometric data in a randomized way. The randomization algorithm [1] coupled with a True Random Number Generator (TRNG), requests a different combination of biometric input for each login attempt, thus eliminating the predictability in existing mechanisms.

Continuous biometric template updation is a crucial success factor to minimize the possibility of false rejection or false acceptance in this method.

Furthermore, the proposed solution approaches security as an ongoing mechanism and extends authentication service to the entire session, as opposed to traditional approaches that offer authentication only at the beginning of a session. The proposed system captures biometric data on an ongoing basis throughout the session in a fine-grained fashion seamlessly. The proposed solution can be built and offered as Security as a Service (SECaaS) [2].

The next sections in this paper are literary review where an overview of current trends in biometric research is presented, summary of solution to improve authentication with biometric methods, a conclusion and references.

This paper is organized in five sections: Section II is a literature review of cloud access authentication. Section III describes the challenges in existing technologies and provides a rationale for the new model. Section IV describes the proposed new model, its architecture, benefits and challenges. Section V is the final section that offers a summary of future scope.

II. LITERATURE REVIEW

The most popular access control mechanisms in cloud computing include but not limited to discretionary access control, mandatory access control and role-based access control mechanisms. Other methods include attribute-based access control, distributed role-based access control and cloud optimized access control. However, these methods are prone to a variety of issues surrounding convenience, performance, reusability, role assignment, single point of failure, node overhead and authentication failure.

The most recent research surrounding access control encompass a variety of technologies and solutions including fine grained data access control, attribute-based encryption techniques, hierarchical attribute-based solutions, hybrid cryptographic access control models for cloud based EHR systems, two-factor authentication with One-Time-Password, user secret keys and biometric technology for authentication. Review of many research papers are coming as follow:

This is a white paper [4] on using biometric technology in cloud space for enhanced security and access control. This paper describes the role of cloud computing in today's world, its application on various industries, addresses challenges surrounding them and proposes biometric as a solution.

With cloud-enabled Bring Your Own Device (BYOD) policies becoming increasingly pervasive each day, the possibilities of data breaches, fraud and cyberattacks on mission-critical workloads have become endless. The convenience of virtual desktops is juxtaposed with unique risks, with access control being the most prominent of all. Mobile devices on the other hand, have additional risks of unsupported devices resulting in uncontrolled data flow. Implementing security solutions on endpoints not administered by the service present a challenge in imposing security policies.

Certain industries, such as banking, health sciences and e-commerce are more vulnerable to security threats than others are and demand more robust security frameworks. Furthermore, applications relying heavily on additional PINs and passwords only make them inconvenient. To make it worse, these password-based security measures do not help the systems uniquely identify end-users.

Biometrics offer a viable solution to tackle identity related issues as it is unique to individuals, cannot be copied and cannot be shared. Biometrics when offered in cloud as a service makes it fast, efficient, doable and can be offered on demand. Additionally, biometric as a service is not network centric, it is scalable, and ensures sovereignty. Other advantages of this approach is its usage of multi-factor authentication under Fast Identity Online (FIDO) and is established by an alliance of major companies, consolidating the advantages of biometrics, Near Field Communication(NFC) and Universal Serial Bus (USB) tokens while making existing devices and systems interoperable.

SECaas [9] focus primarily on security services delivered in cloud environments on demand. SECaas makes better quality services available to customers in cloud and offers variety features available immediately as opposed to on-premises services. This minimizes the provisioning time and makes maintenance simpler as is it done by the service provider. It also brings down the total cost on security services as the billing is done as per usage.

SECaas providers offer a range of Identity and Access Management (IAM) services including centralized directory services, access management services, identity management services, identity federation services, role-based access control services, user access certification services, privileged user and access management, separation of duties services and reporting services.

The proposed architecture features IAMaas in public cloud, where two key components IAM manager and IAM core perform policy administration and IAM services respectively. Through IAMaas, the user gains access to protected resources such as devices, data, applications, services and Configuration Service Providers (CSP).

The implementation of this architecture features the web server (Windows OS) in public cloud. The IAM core and IAM manager in a different VM that includes a MySQL database which stores user credentials in an encrypted format. When user establishes his credentials, a token is generated and is passed on to user through a protected network (devices, data and server). This is offered as a cloud service and can be availed through a range of devices.

This paper offers a cursory view of how SECaas is implemented in the present-day scenario with an emphasis on Biometric Identity Management.

The patented method in [10] incorporates multipoint verification of user identity through biometric methods. The first step of biometric authentication happens in the client side through speech recognition, which ensures early detection of intrusion attempt, saving time and efforts of server side authentication. After the successful client-side authentication, the server-side authentication is incorporated using a string of algorithms for analyzing speech data. The advantage of this method is usage of two different sets of algorithms in server and client sides ensuring multiple layers of protection against intrusion. The reliance on multiple algorithms to analyze the same data also improves the quality of its outcomes.

The method in [11] presents a biometric based approach for remote access of devices based on a code stored in the device. The first step in this approach is to validate bio data by matching it against a benchmark (code) stored in the mobile device. Once a match is detected and user is authenticated, the code is then sent to a remote device. The remote device in turn provides the access codes to lock/unlock the device remotely.

This method emphasizes the possibility of using handheld devices to obtain biometric data and use it for access control.

This technique in [12] generates an asymmetric private key based on parts of biometric data. This private key is then used in part upon a user password. The resulting private key is used as a digital signature for the electronic message.

This private key is meant for one time use and will not be saved anywhere. A new private key is regenerated inputting both a new instance of biometric reading as well as a new instance of the password.

The paper [8] focuses on the issues related to the service delivery model of cloud computing. The paper describes the various security issues of cloud computing with respect to its service delivery model SaaS. In addition, the paper describes the security issues facing Software as a Service (SaaS) delivery model and few solutions that partially address them.

III. OBSERVED CHALLENGES IN CURRENT RESEARCH AND SOLUTIONS

TABLE I. Cons and Solutions

Cons	Solutions
The existing research work in biometrics does offer several hybrid models, taking advantage of multi-factor authentication for identity management. These models are either client-server-based approaches or not adequately adapted for cloud based/ SOA systems [5], [11], [7].	Security as a Service with biometrics
The second disadvantage in current research is that, they do not take advantage of existing hand-held smart devices to	The usage of smartphones, smart watches & fit bits can bring down the cost and provisioning time of biometric authentication.

capture biometric data and leverage it for identity management in cloud space adequately [13].	
The current approaches in the industry view authentication as a one-time process at the beginning of a session [8].	They do not offer continuous validation throughout the session. Continuous identity assessment comes with advantages of intrusion detection.
The current models use one specific type of biometric data or a specific combination of biometric data that does not change anytime during the security lifecycle [8].	Multifactor biometric authentication using randomized algorithms would offer a better solution.
Inadequate usage of biometric data to implement fine-grained authentication [8].	Incorporate biometrics for seamless fine-grained authentication.
Multiple User Ids and passwords makes it difficult for an end-user to manage/remember [15].	Biometrics is a solution.
Different identity management solutions have different nuances and software often run into incompatibility issues [8].	Biometrics as a unilateral solution.
Existing authentication policies are often inadequate to address diverse requirements of applications and access modes.	Multifactor authentication with scalability for application needs.
Even though an end-user is prompted to type in the credentials over a secure tunnel, a risk always remains of either the user being forced to sign in under duress, or a brute force, man-in-the-middle kind of attack.	Use of algorithms to verify the freshness of attacks and authentication from multiple sources.
Session management policies are often difficult to enforce/implement	Seamless session management with fine grained authentication.
Even when an organization wants to move its applications to a pure cloud-based infrastructure, federation of the identity management system becomes very challenging, sometimes stalling vital projects, and adding to maintenance and operational cost.	Reliable security solutions and encryption.
Identity management system do not have adequate means to differentiate between a real human being trying to access his/her personal data, and an auto-bot trying to guess credentials for a real user, and a back-end service account which used to schedule/automate batch jobs.	Biometrics, with replay protection can make the distinction clear.
While password expiry is mandated for any real person, password expiry can be very challenging process when it comes to handling service/unmanned accounts.	Biometric passwords can be made to renew periodically, especially when data surrounding vein patterns etc.. tend to change over time.
Authentication is traditionally perceived as a one-time activity, with a session expiry/timeout indicating the end of the session life.	Session-long fine-grained authentication.

As a result, the solution to various identity management problems is often linear and based on discrete variables. However, interaction between humans and computers are closer to continuous variables, and it follows an ever-changing, ever-evolving pattern that should be correctly imbibed within an access control mechanism.

IV. NEW MODEL AND ADVANTAGES

The abundance of cloud-based applications spanning across industries such as banking, E-commerce, health services and defense offer the convenience of high-end technology with reduced provisioning time and usage-based charges.

However, the multi-tenant nature of cloud space presents a plethora of security vulnerabilities, of which authentication is one. The rate at which companies migrate their existing products to cloud space, also demands that the security features be developed in proportion. The lack of a holistic identity management strategy, which also deploys certain degree of unpredictability to combat ever-evolving attack methods are something to be fulfilled to make cloud space more secure for future use.

Unfortunately, in a number of cases, this means a new system with very high development costs, deployment costs and provisioning time. A truly holistic identity management strategy should translate to a product in such a way that it can be used in conjunction with existing systems, without creating a need for additional hardware or infrastructure.

Keeping the above factors and current limitations in mind, one can say that:

- Authentication or authentication should not be treated as a separate process than the user work-flow within an application.
- Much as living objects learn to identify another living being/element, an identity manager service in the cloud must be able to recognize a user in the most intuitive manner, while consciously avoiding Type-1/Type-2 errors.
- A security model/identity management service should be able to evolve based on the type of user and their comfort level.
- A true cloud-based service must be easy to configure against any type of application, legacy or cloud-based.
- A true cloud-based solution must act as the single source of truth for any user, irrespective of the different type of applications he/she might need access to.
- A true cloud-based Identity Management (IDM) solution must accept multiple kinds of inputs (fingerprint/facial recognition/retinal scan/voice recognition/regular password) from the end-user, depending on the device being, and should have consistent performance and characteristics irrespective of the mode of authentication being used.
- Irrespective of the kind of authentication input, it should provide a universal window/terminal for login purpose that should work consistently and predictably in both devices and desktop-based application.
- A cloud-based IDM solution should also allow an application to check the user's identity/authenticity in between a session in a non-intrusive way so as to sustain

a legitimate session in a secure way without disturbing the user.

- A true cloud-based service should be able to allow federation with any application, and provide backward compatibility for legacy applications
- Should be inherently elastic and scalable
- It should be accessibility-compliant

V. NEW STRATEGY FOR BIOMETRICS AS A SERVICE IN IDENTITY MANAGEMENT

The proposed new model offers biometric identity management as a service. It uses multiple templates of biometric data to establish the identity of users; Two randomized biometric factors from three {Fingerprint, face recognition, voice recognition} for less critical applications; Three biometric factors from a set of templates {fingerprints, face recognition, voice recognition, retina, iris} for crucial mission-critical applications dealing with sensitive or classified user data [4], [6].

After successful authentication, once the session is established, the service still verifies the identity of the user in a fine-grained fashion at randomized intervals of time, without any efforts from the end-user. In other words, use the front camera in the handheld device or automatic verification of fingerprints from touchscreens.

Usage of randomized combinations of biometric inputs, enhance security through unpredictability. The second time, user tries to login to the system, the system requests for a different combination of biometric data to establish credentials (e.g., {left thumb fingerprint, right forefinger fingerprint and voice}, {voice, face, right thumb fingerprint}). Furthermore, the randomization should be used in such a way that, a user is not requested for same combination of data twice in a row. This minimizes the probability of hacking attempts being successful.

TABLE II. Key Features

Key Features
• Multifactor biometric authentication for authentication in cloud systems • Fine grained authentication implementation throughout the session for prevention of session hijacking • Randomization of biometric inputs • Continuous biometric template updation • To be implemented as a service (SECaas in cloud)

The biometric security as it presents numerous advantages also leaves the users with a unique set of challenges. What if the biometric data is stolen? What if biometric data is intercepted by another way? Here are the key success factors for use of biometric in software applications.

TABLE III. Success Factors

Success factors
1. Safety of biometric templates – The database should be strongly encrypted with a key of length 128 along with other security measures of data center in place 2. Replay protection – Reliable algorithms to ensure the freshness of biometric data 3. Encryption at rest and in transmission 4. Tuning for Accuracy – False acceptance vs. False rejection 5. Efficiency 6. Availability – Backup and recovery methods should be applied as appropriate and have traditional authentication method as a failover process.

VI. ARCHITECTURE OF PROPOSED MODEL

The architecture of the proposed model follows a multilayered security model for biometric security in cloud. The process begins by requesting users for multiple forms of biometric input with the combination being randomized for each user. If the credentials are authentic, the system creates a new session for the user. Else, validates if the user has exceeded limits for trials. If the number of unsuccessful attempts is within limits, then the system allows user to re-enter credentials with a new combination of biometric data. Upon successful authentication, the session begins, and the system authenticates users through fine-grained authentication throughout the session at regular intervals of time without the user ever having to re-renter credentials until the end of the session.

If the user credentials are found to be invalid anytime during the session, the session is terminated immediately, and the login attempt is logged in audit trail.

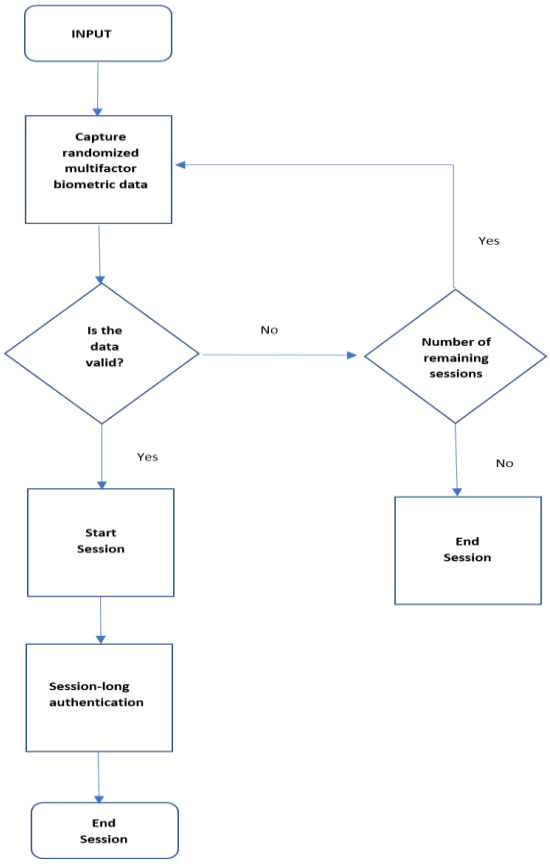

Fig. 1. Example of a ONE-COLUMN figure caption

A. Choices of biometric templates

Successful implementation of biometrics as a service by Frost and Sullivan [4], shows the way for viability of biometrics in cloud, while the implementation model used by [4] covers all success factors for implementing biometric access control in cloud. The following are the types of biometric data most commonly used in software industry today.

1. Fingerprint verification
2. Hand geometry
3. Retinal scan
4. Iris scan
5. Voice verification
6. Signature verification
7. Facial recognition
8. Palm print
9. Vein pattern
10. Ear, body shape
11. Odor
12. Gait

The data published by [38] and [39] show that fingerprint recognition, iris and retina are the most reliable biometric data today with iris being the most reliable of all of them [38]. Therefore, this is the ideal combination of inputs recommended for critical applications in defense, medical and finance industries dealing with sensitive data. It is to be noted that retina scanning is already a standard in defense implementations across the globe. However, due to implementation costs associated with retina and iris scanners, this may not be implementable for less-sensitive day-to-day applications.

For applications where the sensitivity of data is comparatively less, more inexpensive implementation models can be used using moderately reliable biometric data, such as face and voice recognition [38], [39].

B. Tuning

One of the key success factors for biometric authentication in cloud is its capability to identify false data. The concern that the attackers can falsify biometric data such as fingerprints, photographs from other sources and using them for authentication is among the leading concerns in biometrics.

Usage of strong algorithms to verify freshness of the data can provide enhanced replay protection. So can usage of advanced watermarking techniques for biometric data [40-43].

The next success factor is to balance false recognition with false acceptance. Using stricter algorithms for recognition can lead to scenarios of false rejection. On the other hand, using lenient algorithms in favor of convenience leads to false acceptance. Strong normalization techniques, neural networks-based approaches and speech coding algorithms should be incorporated to strike a balance between two [44], [45].

Finally, certain facets of biometric data are subject to change in course of time (e.g., the dimensions of facial appearance, vein pattern). Therefore, it is essential that the biometric templates are kept up to date. Every time we take a sample of biometric value, we have a new template available after validation. Updating template database after every successful validation of biometric data.

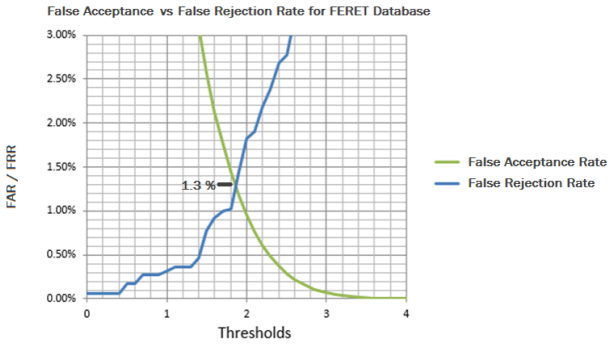

Fig. 2. Balancing False Acceptance and False Rejection [46]

The above diagram depicts a normalized implementation balancing false acceptance and false rejection rates.

C. Considerations for mobile applications

Face detection with the front-camera, finger-print recognition and voice recognition features with Artificial Intelligence in existing phones are all excellent choice for session-long authentication process for mobile-based applications. This eliminates the possibility of session hijacking. This feature is highly recommended for applications with high criticality and can be readily utilized with existing hardware in mobile devices.

D. Considerations for desktop applications

Camera that typically ships with laptops or a dedicated high-resolution web camera, voice recognition features with existing AI software and fingerprint scanners are the best choices for session-long authentication. In addition, typing speed and device location could be factored in to enhance accuracy.

VII. PROPOSED IMPLEMENTATION MODEL WITH MICRO SERVICES ARCHITECTURE

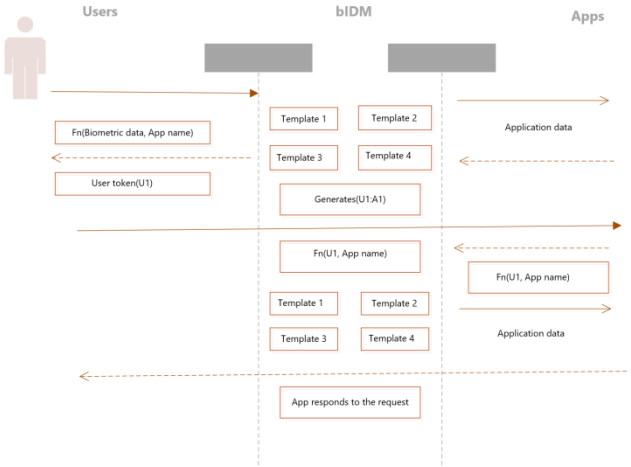

Fig. 3. Proposed implementation model

The proposed model is developed as a service and could be implemented through micro-services with java or an equivalent language. This new service could be built on top of existing cloud architectures as an additional new layer.

In this new model, the user sends a combination of biometric data {quintet} along with app identifier to Biometric Identity Management (bIDM). Then bIDM verifies the biometric data and determines id data quality is above the p-value. The bIDM, then generates a unique user token and application token pair for the session.

bIDM returns the user token to user with the token set to expire within a finite time limit. Then when the user makes a call to the application with user token, the application passes on the user token to bIDM. The bIDM in turn, verifies the user token and application token combination and allows a pass-through. Once the timer expires, the bIDM, expires the token pair. Once token expires, the fine-grained authentication takes over till the end of the session. In case of data anomaly or when the user attempts to sign in again after successful log off, the above-mentioned process is followed again.

Here is an algorithm that proposes one way of implementation with a True Random Number Generator(TRNG). The TRNG generates a random number (m), which represents the template number from 1 to n.

Step 1: Start

Step 2: Register new user with biometric templates Saved_Templates = {template1, template2, template3, template4…templaten}

Step 3: Registration successful

Step 4: Initiate authentication to Sign In

Step 5: Use a TRNG to generate a random number m

Step 6: Pick the template from 1 to n, based on m (e.g., if the random generator generates a number m=3, then template 3 would be picked to establish identity.)

Step 7: Request the user to input the template identified by TRNG

Step 8: Verify if the user input matches the template in the system

Step 9: If there is a match, repeat processes 5 to 8 again. Else, end session and not allow users to attempt authentication for the next z seconds (z =30-60 min) from the same IP address.

Step 10: If there is a match, initiate session and set the session-length to x seconds. Else, end session and not allow users to attempt authentication for the next z seconds from the same IP address.

Step 11: Authenticate session every y seconds

Step 12: If the session has reached its length, repeat steps 4 to 10. Else, end session and not allow users to attempt authentication for the next z seconds from the same IP address.

Step 13: End

It is a good practice to use TRNG that uses real entropy, such as external temperature, pressure etc. for implementation. Some of the widely used TRNGs include Fortuna, CryptGenRandom, Yarrow and /dev/random.

VIII. CONCLUSION

In this paper, we have proposed an authentication method that strengthens security, while effectively addressing session-hijacks, which is one of the biggest security concerns today. The multilayer authentication method proposed in this paper, uses a set of biometric authentication templates to identify a user. The authentication service randomizes the authentication process by enabling applications to use a different biometric template each time of authentication. The randomization is achieved here through a True Random Number Generator which decides which template should be used at the time of initial authentication and would be repeated twice for different tempale. This obscurity significantly increases the time and effort required by an attacker to gain unauthorized access. An additional layer of security, is the session-long fine-grained authentication. In the unlikely event that the initial authentication is taken over, the session-long authentication can detect session-hijacks subsequently, thereby rendering protection to the entire session. Furthermore, after each unsuccessful authentication attempt, there is a lock-out period which prevents the user from reattempting authentication immediately after. This mechanism prevents attackers from using automated tools reattempt authentication.

Finally, as a future research, biometrics can be combined with artificial intelligence, leading to self-governing authentication methods.

REFERENCES

[1]. S. Zhong, A practical key management scheme for access control in a user hierarchy. Science Direct. 2002.

[2]. M. Hussain, H. Abdulsalam. SECaaS: security as a service for cloud-based applications. Second Kuwait Conference on e-Services and e-Systems. 2011.

[3]. R.P.Koster, A.Hermanus, M.Akkermans, B.Rijnsoever,"Biometric authentication and identification",US 8572397 B2. 2013

[4]. Frost and Sullivan, "Biometrics as a service",Fijutsu,2016.

[5]. K.Punithasurya, J.S.Priya,"Analysis of Different Access Control Mechanism in Cloud". International Journal of Applied Information Systems, Foundation of Computer Science FCS, 2012.

[6]. C. Hahn and J. Hur,"Towards Privacy-Preserving Biometric Identification in Cloud Computing", 2016.

[7]. M. Haghighat, S. Zonouz, M.Abdel-Mottaleb,"Trustworthy cloud-based and cross-enterprise biometric identification"[ScienceDirect. 2015].

[8]. Rashmi, Dr.G.Sahoo and Dr.S.Mehfuz,"Securing Software as a Service Model of Cloud Computing:Issues and Solutions"[International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.4, August2013. DOI : 10.5121/ijccsa.2013.34011].

[9]. D.H.Sharma, C.A. Dhote and M.Potey,"Identity and Access Management as Security-as-a-Service from Clouds", International Conference on Communication, Computing and Virtualization, 2016.

[10]. T.R Mozer, "Biometric client-server security system and method". US Patent7, 487, 089 B2. 2009.

[11]. John Cronin. Smartphone fingerprint pass-through system. Patent application publication. US 2015/0358315 A1. 2015.
[12]. A.A Albahdal, T. E Boult, "Secure biometric cloud storage system", Patent US 9166796 B2, 2014.
[13]. N. Meghanathan, "Review of access control models for cloud computing", ICCSEA, SPPR, CSIA, WimoA – 2013.
[14]. R. Nandakumar, K. Prasanth," Biometric Encryption to Enhance Confidentiality in Cloud Computing",CiiT. 2015.
[15]. ISACA, Security as a sevice:Business Benefits. 2013
[16]. Y.Kadam,"Security Issues in Cloud Computing A Transparent View",International Journal of Computer Science Emerging Technology. 2011; 316–22.
[17]. M.A.Vouk, "Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology. 2008; 235–46.
[18]. Cloud computing. 2013,Available from: http://en.wikipedia.org/cloud_computing
[19]. D.Catteddu, G.Hogben,"Cloud Computing:- Benefits, risks and recommendations for information security",Web Application Security. 2009; 7–17.
[20]. F.Sabahi,"Cloud Computing Security Threats and Responses", 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN).
[21]. J.H.Choi1, S.H.Lee, M.K.Kim,"Integrated user authentication method using BAC (Brokerage Authentication Center) in Multi-clouds",Indian Journal of Science and Technology,2015; 8(25):1–7.
[22]. S.Lee, I.Ong, H.T.Lim and H.J. Lee, "Two factor authentication for Cloud computing",International Journal of KIMICS. 2010; 427–32.
[23]. A.K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition", IEEE Trans Circuits Systems. Video Technology. 2004; 4–20.
[24]. N.K. Ratha, J.H. Connell, R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal. 2001; 614–34.
[25]. NIST SP 500-292."Cloud Computing Reference Architecture: An Overview", National Institute of Standards and Technology. 2011; 3–4.
[26]. "CSA Top threats working group. The notorious nine"-2013. CSA(cloud security alliance). 2013; 8–21.
[27]. J.Y.Lee,"A study on the use of secure data in cloud storage for collaboration",Indian Journal of Science and Technology. 2015; 33–6.
[28]. L.O.Gorman, A.Labs, B.Ridge,"Comparing Passwords, Tokens, and Biometrics for User Authentication", Proceedings of the IEEE. 2003; 21–40.
[29]. A.K.Jain, K.Nandakumar, A.Nagar,"Biometric template security. EURASIP Journal of Advances in Signal Processing", 2008; 1–17.
[30]. Israeli biometric data hacked. 2013. Available from: http://www.natlawreview.com/article/israeli-biometric-data-hacked
[31]. "British biometric passport hacked",2013. Available from: http://www.theinquirer.net/inquirer/news/1009515/british-biometricpassport.
[32]. M.Upmanyu, A.M.Namboodiri, K.Srinanthan, C.V.Jawahar," Blind authentication: A secure crypto biometric verification protocol", IEEE Transactions on Information Forensics and Security. 2010; 255.
[33]. D.T.Rajanbabu, C.Raj,"Multilevel encryption and decryption tool for secure administrator login over the network. Indian Journal of Science and Technology", 2014; 8–14.
[34]. R.Rivest, A.Shamir, L.Adleman,"A method for obtaining digital signatures and public-key cryptosystems",Communications of the ACM. 1978; 120–6.
[35]. S.Kavinhariharasudhan et al,"Double encryption based secure biometric authentication system",International Journal of Engineering Trends and Technology.2012; 64–70.
[36]. RSA Algorithm. 2013. Available from: https://simple.wikipedia.org/wiki/RSA_(algorithm)
[37]. AES. 2013. Available from: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[38]. SANS Institute, Biometrics: An in depth examination,2003
[39]. Biometric comparison guide, https://epic.org/privacy/surveillance/spotlight/1005/irid_guide
[40]. Y. Ueshiege, K. Sakurai,"A proposal of one-time -biometric authentication",unpublished
[41]. Biometric template security. http://dl.acm.org/citation.cfm?id=1387883.
[42]. S.Y.Chiou, "Secure method for biometric-based recognition with integrated cryptographic functions",unpublished
[43]. R.Islam, S.Sayeed and A.Samraj,"Biometric template protection using watermarking with hidden password encryption".
[44]. M.Vatsa, R.Singh and A.Noore,"Reducing the false rejection rate of iris recognition using textural and topological features"
[45]. "Normalizations and selection of speech segments for speaker recognition scoring", http://ieeexplore.ieee.org/document/196655/appliedrecognition.com.
[46]. appliedrecognition.com