Multifactor Biometric Authentication for Cloud Computing

Jihad Qaddour
School of Information Technology
Illinois State University
Normal, Illinois, USA
jqaddou@ilstu.edu

***Abstract*—Cloud Computing is a fast-growing technology, which can do everything from running applications to storing data off-site. It means a person can save his work around the globe, retrieve, update, delete and use the data/information stored in the cloud from anywhere in the world at any time. The popularity of cloud in the business world has resulted in its data centers growing at an unprecedented rate. While there are so many benefits, there are always risks involved with sharing resources, which leads to privacy and security concerns. Therefore, usage of Cloud Computing is still not at par with businesses particularly; businesses who have critical data that they cannot afford to lose or have stolen. This paper investigates issues and challenges related to the authentication security of cloud computing. Further, in this paper, a new solution is proposed to enhance user authentication in Cloud Computing using biometrics with multifactor authentication techniques.**

Keywords-Cloud Computing; Security; Security threats; Biometric; Multi-factor authentication.

I. INTRODUCTION

In the modern world, the Internet is growing at an exponential pace. With this pace, many new technologies came into existence and caught the attention of people from different backgrounds, as well as industries. One of the most popular tools is Cloud Computing (CC), which is growing at an unprecedented rate. Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, application, and services) that can be rapidly provisioned and released with minimal management efforts or services provider interaction [11][15]. Cloud Computing is a way to store any data, such as images, videos, codes, and sensitive data on a remote location other than the local device. Before Cloud Computing came into existence, people used to save their data on their local drives, where the data was not always accessible. This was one of the main drawbacks, which drove the development of a technology that gives access to data at any place and that can be saved other than on local drives. In addition, CC is a service that is provided by some vendors to users offering options for storing, updating, deletion of data, and developing different applications. Moreover, the data will be stored at the remote location, which gives users an option to retrieve and share data at any time and any place. Every action has a reaction, and similarly, when a new technology comes into existence, it has some benefits as well as drawbacks. It is affected by downtime, security and privacy issues, it is vulnerable to attacks, and it has a limitation of control and security. However, CC also helps in minimizing the infrastructure cost, as it is cheaper than the cost incurred in the infrastructure upgrades. It also eliminates the requirement of upgrading infrastructure related to storage.

In the paper, the focus is on the authentication in Cloud Computing and security issues that may arise or exist during authentication. It is organized into four sections: Section II talks about the Cloud Computing concept, Section III addresses literature review, Section IV talks about the research methodology, and Section IV concludes our work.

II. CLOUD COMPUTING CONCEPT

Cloud Computing has various features and the National Institute of Standards and Technology (NIST) defined the most essential five characteristics of Cloud Computing (CC) [15].

A. Essential characteristics of Cloud Computing

1. Broad network access and shared infrastructure

CC provides access to thin or thick client platforms (for example, mobile phone, laptops, and others) through standard mechanisms. As a part of doing business, cloud providers invest in and build the infrastructure necessary to offer software, platforms or infrastructure as a service to multiple consumers. Capabilities are available through shared networks with multitenant customers. Provider's resources are pooled to serve multiple consumers using a multi-tenant model.

2. On-demand self-service

With on-demand self-service, the cloud consumer will be able to purchase and use cloud services as the need arises. Moreover, a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. To make this possible, a cloud provider must obviously have the infrastructure in place to handle consumers' requests. Most likely, this infrastructure will be virtualized, so different consumers can use the same-pooled hardware.

 ISBN: 978-1-61208-625-5

3. Elastic and scalable

Capabilities can be elastically provisioned and released to scale rapidly outward and inward commensurate with demand. It allows providers to add or remove features, without interruption and, at runtime, to handle the load variation. From a consumer point of view is to have the ability to expand and reduce resources according to their specific service requirement. This service capability provides an elastic and scalable Information technology (IT) resource. Consumers pay for only the IT services they use. Although no IT service is infinitely scalable, the cloud service provides the ability to meet the consumer's IT needs creates the perception that the service is infinitely scalable and increases its value. In the consumption-based pricing model, providers charge the consumer per units consumed. For example, cloud vendors may charge for the service by the hour or gigabytes stored per month.

4. Dynamic and virtualized

The need to leverage the infrastructure across as many consumers as possible typically drives cloud vendors to create a more agile and efficient infrastructure that can move consumer workloads, lower overheads and increase service quality. Many vendors choose server virtualization to create this dynamic infrastructure.

5. Measured Services

CC automatically controls and optimizes resources used by leveraging a metering capability at some level of abstraction appropriate to the type of service [11].

B. *Cloud Computing Deployment Models*

In addition, researchers have categorized four basic cloud deployment models for delivery purpose and they are as shown in Figure 1 [11]:

a. Public Cloud

Public cloud infrastructure is made available to the public and is owned by organizations selling the cloud service that are responsible for infrastructure, maintenance, controlling the data, and for the operation of CC. Examples of the public cloud include Google App Engine, Microsoft Azure, and Amazon EC2 [11]. All major components are outside the enterprise firewall, located in a multi-tenant infrastructure and access the cloud through a secure IP.

b. Private Clouds

This cloud infrastructure is operated solely by the internal IT of the organization; the organization may choose to manage the CC in-house or contract it to a third party. The computing infrastructure may exist on premises or off premises. Examples of a private cloud include hospitals and universities.

c. Community Cloud

The community cloud shares the characteristics of both the public and private cloud. It has restricted access to the private cloud and shares its resources with many organizations like the public cloud. A good example is a healthcare industry cloud. The infrastructure is a composition of two or more clouds (private and public). Community cloud involves sharing of computing infrastructure between organizations of the same community. For example, all government organizations within the state of California may share computing infrastructure in the cloud to manage data related to citizens residing in California.

d. Hybrid Cloud

The hybrid cloud infrastructure is a composition of two or more clouds (public, private, or community). This is very attractive to smaller businesses for which the security is an important concern. Hybrid Cloud Organizations may host critical applications on private clouds and applications with relatively fewer security concerns on the public cloud. A related term is cloud bursting. In the cloud, bursting, organizations use their own computing infrastructure for normal usage but access the cloud for high/peak load requirements. This ensures that a sudden increase in computing requirements is handled gracefully [4].

C. *Cloud Service Models*

NIST defined three types of services for the cloud model

a. Software as a Service (SaaS)
b. Platform as a Service (PaaS)
c. Infrastructure as a Service (IaaS)

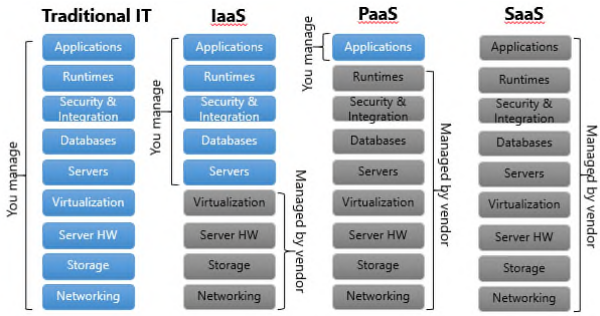

Figure 1. Cloud service model

a. Software as a Service (SaaS)

SaaS is an ever-increasingly popular option for software distribution. The Cloud Provider (CP) provides service to customers in the form of software, specifically application software running on and accessible in the cloud. The applications are accessible from various client devices through simple interfaces such as web browser. Some examples of services are Google Gmail, Microsoft 365, and Cisco WebEx [11].

b. Platform as a Service (PaaS)

PaaS cloud provides service to the customer in the form of a platform on which the customer's application can run. A PaaS cloud provides useful software building blocks and a number of development tools that assist in deploying new applications. In effect, PaaS is an operating system in the cloud. For example. Google PaaS offers to build and host web applications on the Google infrastructure.

 ISBN: 978-1-61208-625-5

c. Infrastructure as a Service (IaaS)

With IaaS, the customer has access to the resources of underlying cloud infrastructure. IaaS cloud provides virtual machines and other abstracted hardware and operating systems. IaaS offers customers processing, storage, networks, and other fundamental computing resources so that the customer can deploy and run arbitrary software. Some examples of IaaS are Amazon Elastic Compute Cloud (Amazon EC2), Microsoft Windows Azure, Google Compute Engine (GCE) [9][11].

III. LITERATURE REVIEW

Cloud Computing overgrows many computing paradigms like grid computing, global computing, and Internet computing in various aspects of on-demand self-service, broad network access and shared infrastructure, elasticity and scalability, guaranteed QoS (Quality of Service), and autonomous system and virtualization [13][14], etc. A few states of the art techniques that contribute to Cloud Computing are:

Wang et al. [1] proposed in their paper a new Cloud Computing model named as a hybrid model with respect to authentication and data security. In that article, a number of methods were discussed in regards to assure data security to protect user data. Authentication for the data based on public key infrastructure, virtualization, and single encryption are some methods discussed in their paper. Hemalatha et al. [2] did a comparative analysis of security issues and encryption techniques in cloud computing. The author of the article discussed the two delivery models for addressing the issues in Cloud Computing and they are cloud classification and encryption mechanisms. In addition, to assure the privacy and security of data over a cloud, authors did a comparative study based on encryption techniques. Xin et al. [3] discussed user authentication and unauthorized user access. They did their research on data security model based on multiple dimensions and proposed a three-layer defense model. In that model, each layer has their own role to perform.

R. Massod et al. [6] did their research on implementing Honey encryption to address brute force attack. A brute force attack is done to get the user password or Personal Identification Number (PIN) by the trial-and-error method. For doing this, an automated software is used which can generate many consecutive guesses. Brute force attack can be of two type. The first is when a security analyst is testing an organization's network security. This type of attack helps the analyst to point the gaps from where any attack for data is possible. The second one is when a criminal uses brute force attack to get encrypted data. The Honey Encryption (HE) technique is used with Secure Repository Manager (SRM) who creates a secure repository at server and client systems. With every attack using the wrong cipher key, HE will yield a fake plain-text or honey messages. This message may seem legitimate but will be incorrect. This way the attackers will have a bunch of fake plain-texts all looking like actual text. So even if the attacker has the actual text they will have to narrow it down from the haystack of false texts.

After implementing honey encryption, it is almost impossible to get any information or data of any user from the server, because of honeypots. Use of honeypots is useful as it generates new words named as honey words that looks like the valid data but difficult to differentiate between the original data and the data with honey words, which is invalid. If the data is of large size, then a large number of chunks are used to secure the data, and if the data is small, then a small number of chunks are used. SRM first encrypts the data before uploading the data to the cloud then performs other functionalities to provide the security and privacy of the encrypted data [4].

Hang et al. [5] proposed a public key encryption method for integrity and authentication issues in cloud computing. While data in transit over an internet, which is a type of unsecured circuit, an unauthorized person, may access the data, which is the main security issue in Cloud Computing services. It is the cloud provider's responsibility to provide the security and integrity of the data to the end user. Therefore, they use a public key to encrypt as well to decryption the data. In a public key encryption method, the only way to set back the data to its original form and make it understandable is to encrypt or decrypt the data with two secret keys (private key and public key). The private key remains with its respective owner as confidential and a public key is available to everyone through a directory or public repository. Private and public keys are related mathematically in a specific way; if the data is encrypted using a public key, it decrypts only with its corresponding private key. On the other hand, if data is encrypted using the private key, then it should only be decrypted by the corresponding public key to make the data intelligible. Public key encryption is implemented in the cloud as:

- The user uses its own private key to encrypt the data.
- Cloud Computing infrastructure units, tools for virtualization, and all other elements in the system have their own keys.
- To perform the authentication, all elements of the system uses private and public key at first place.
- All events occurred in the cloud have their own unique key. Therefore, public key encryption method assures the safe and secure exchange of data over the cloud.
- It is also advisable to the cloud provider that they can design features of the public key infrastructure, which is helpful to improve the security of data over the cloud.
- Data moving in or out should be encrypted or decrypted to assure the security.
- A hardware security model should be used to store the keys and performing decryption and encryption of data to make it intelligible for the intended user and unintelligible for the others.

Akashdeep et al. [16] reviewed the multifactor authentication technique to address the security issues in the

 ISBN: 978-1-61208-625-5

Cloud Computing system that users are facing. They put forward an idea using of at least two separate identifiers for the validation of information instead of using one identifier that is an ID and password, which helps in enhancing security to get an access by introducing numerous barriers for the user. Using this technique will reduce the chances for any hacker to get access to the system by using stolen passwords to have any critical data that he is not intended to retrieve. To assure the safety and security of user data stored in the cloud, use firewalls, multifactor validation, and load balancers to withstand data center infrastructure and security system technique from the hackers and other security threats. Multi-factor authentication technique provides the user with access passwords/keys to gain access to the cloud system. If the user is unable to provide the password or keys correctly, then IDS system will alert about the issue.

He et al. [8] likewise presents new security issues because the information administration and proprietorship are isolated, and the administration is worked on a virtualized stage. In his paper, a novel Dynamic Secure Interconnection (DSI) mechanism is proposed to disengage the distributed computing framework into a few elements of dynamic virtual trust zones with various security approaches actualized for various clients in order to improve security.

There are three different types of components in DSI, namely, DSI clients, DSI server and virtual bridges. The DSI server is the focal controller for taking care of the administration and security approaches. At the point when a VM is introduced, it is associated with the DSI server to enroll and begin to work within the framework. At the point when the VM state changes, e.g. suspend, restart, float or eliminate, it will educate DSI server to redesign the VM state. Therefore, the DSI server keeps up all VM properties what's more, states, for example, the virtual MAC (vMAC) and virtual IP (VIP) locations of VMs, the VM proprietor, the relating virtual scaffold, the ongoing VM state, and so forth.

Likewise, DSI server keeps up the VM correspondence conventions, strategies, and exercises. On the off chance that VMs remain inside the same network, they can converse with each other utilizing vMAC and VIP. On the off chance, that VMs remain in the various nearby system, particularly behind network gadgets, vIP based passages will be set up to associate VMs. In the meantime, suitable activity control approaches will be actualized amid the association bootstrapping stage, for example, encryption calculations, key administration convention, and movement redirection. The DSI clients are a large number of VMs. The properties of each DSI client includes vMAC and vIP addresses, VM state, VM owner, corresponding virtual bridge, host, and its own virtual trust zone ID. Virtual bridges are in charge of performing and implementing the communication protocols and policies. The communication between two DSI clients is performed in a peer-to-peer mode [8].

IV. BIOMETRICS ENHANCED CLOUD SECURITY

Literature survey and reviews point out the researcher's addressed problems related to cloud security and privacy issues. Researchers proposed some solutions regarding the security issues in a Cloud Computing system, which addresses some problems. However, there is still need to do more research in the Cloud Computing area to guarantee security and privacy of end-user data. Usage of Cloud Computing is still not at par with businesses particularly; businesses such as financial institutions which have critical data that they cannot afford to lose or have stolen.

Implementation of biometric features (fingerprint scanning, iris scan) will turn into a helpful tool for protecting the data from threats like identity threat, shared technology issues and many more. The proposed solution with a multifactor biometric feature enhances the security one level ahead than the previous solutions proposed by other researchers. Multifactor authentication is responsible to provide authentication to access with the public and private key provided to the user by the cloud provider. If by chance an unauthorized person gets the keys to access the cloud of another user, without biometric access (unique to a user that cannot be stolen by anyone), a person with bad intentions would not be able to gain access.

The biometric feature is not new in the market. It is used in many organizations for employee registration or attendance, in visa formalities. This biometric feature also serves as a beneficial and unique feature to attract corporations and organizations to convince them to use the cloud system to process and store their data on the cloud system.

The implementation of the proposal of biometrics with multifactor authentication in this paper is unique and different from other researchers.

There have been many developments in the field of biometrics, which means things are more reliable and costs are down. Biometrics offer high-level identification management security operations that have several advantages over traditional means and now they are available to you at lower costs. Currently, the new smartphones and laptops have the feature of scanning fingerprint to unlock phones and applications and taking a picture of the iris. For the systems that lack the feature of biometric scannings, such as older desktops, cheap instruments are available in the market to add. In addition, some major banks have added the option of using fingerprint technology as the login password for the user as it is hard to remember the complex password, which is hard to hack. Biometric log-ins mean a person can be directly connected to a particular action or an event. In other words, biometrics creates a clear, definable audit trail of transactions or activities. This is especially handy in case of security breaches because you know exactly who is responsible for it. As a result, you get true and complete accountability, which cannot be duplicated [17].

In general, there are four biometric types of physical qualities that are utilized or can be utilized as a part of end user verification:

 ISBN: 978-1-61208-625-5

- Unique mark examines (fingerprint scanning), which have been being used for a long time by law implementation and other government organizations and is viewed as a solid, extraordinary identifier.
- Retina or iris checks, which have been utilized to affirm a user's identity by examining the course of action of veins in the retina or examples of shading in the iris.
- Voice acknowledgment, which utilizes a voice print that investigations how a user says a specific word or arrangement of words extraordinary to that person.
- Facial acknowledgment, which utilizes one of kind facial elements to distinguish a person.

The biometrics feature is undoubtedly a more effective method for verification than the more regular methods used for authentication like passwords, smart cards, or a mix of the two. Conceivably, the user would not need to recall secret and complex passwords to get to data. Additionally, passwords have lapse dates that require a new task of passwords and more work for technical employees hired for support. Organizations, enterprises, and medicinal suppliers have found that too often clients forget their passwords, and attempting to explore through a process consisting of multiple steps to get the required data.

Biometric technology also ensures the data security and assures that there will be no manipulation done by any other employee under any circumstances. In addition, it binds the person to be at the place when needed, no other person can take his or her place as the unique physical attribute is used for verification, which cannot be hacked, stolen or copied by others.

V. MULTIFACTOR BIOMETRIC AUTHENTICATION IN CLOUD COMPUTING

The multifactor two-layer authentication is presented as follows:

1. Registration Phase: Client registers with the cloud application by providing all biometric information required for authenticating the users
2. Login Phase: Client uses login form to access the cloud application and its services. This accepts username and password.
3. True Random Number Generator (TRNG) phase: Use TRNG to generate a random number from 1-4
4. Biometric authentication Phase: Once the TRNG number generated, the client will be requested to provide the biometric identity identified by TRNG.
5. Full access phase: once the client provides the biometric identity, it will be compared with the stored user's biometric information. The client will have full access if it is matched, otherwise will be granted basic access, which is accessing not sensitive and valuable data. Figure 3 shows the algorithm steps for successful authentication.

The new proposed methodology is shown in Figure 2.

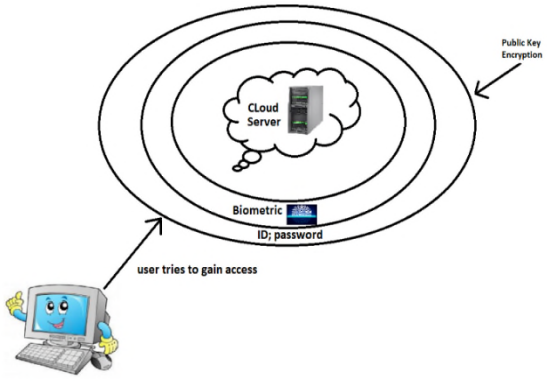

Figure 2. Biometric with multifactor authentication technique

A. Advantages

Advantages of this method include that there are two levels of access. The first level is a basic level to access basic data using the regular user id and pw. In the second level, the user has to provide one of his biometric identities based on true random generators to be able to access all sensitive data or to configure his cloud. This method is better suited for customers with more sensitive and valuable data. By using this case, malicious intrusion and brute force attack will become worthless at the very first step, such as the first layer of authentication because biometric identity is unique for everyone. By using biometrics, it would take care of remembering additional passwords or carry extra badges, documents, or ID cards. Moreover, using biometric technology with public key encryption makes the methodology more secure and better protected.

B. Disadvantages

The drawback of this method includes that users have to use better equipment, which is capable of providing biometric identities. These technologies are available and affordable.

C. Algorithm

The following graph shows the process and algorithm for implementing the multifactor biometric authentication model.

Here is an algorithm that proposes for multifactor biometric authentication implementation with a True Random Number Generator (TRNG) to access the cloud computing.

- Proposed Algorithm

Step 1: Start
Step 2: Register new user with biometric templates Saved Templates = {template1, template2, template3, template4}
Step 3: Registration successful
Step 4: Initiate authentication to Sign In using ID & PW
Step 5: Use a TRNG to generate a random number m
Step 6: Pick the template from 1 to 4, based on m
Step 7: Request the user to input the template identified by TRNG

 ISBN: 978-1-61208-625-5

Step 8: Verify if the user input matches the template in the system
Step 9: If there is a match, the user will have full access to the cloud
Step 10: End

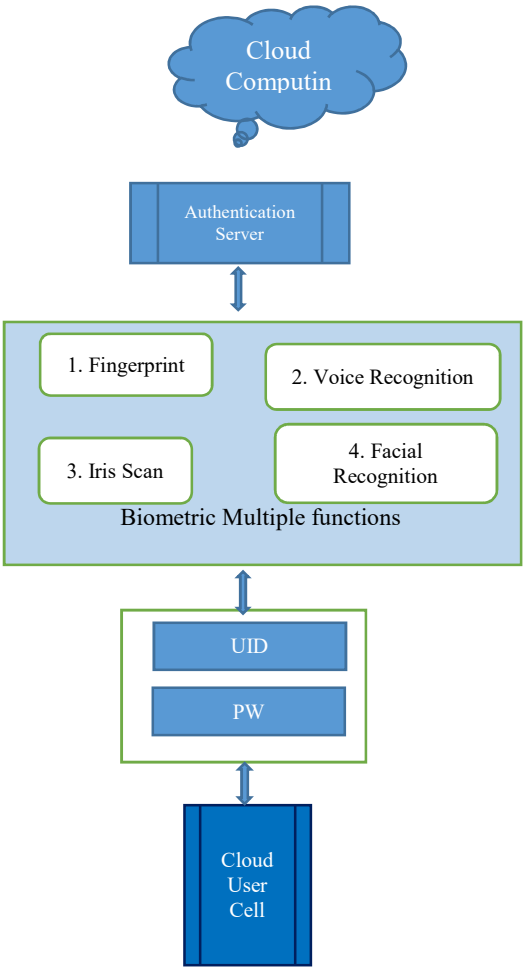

Figure 3. Multifactor biometric authentication

VI. CONCLUSION

We proposed a new multilayer authentication methodology with biometric authentication. The new methodology is introduced using biometric technology with multifactor authentication technique in addition to public key encryption. The model comprises two level authentication. The first level to access the basic data by using the classical user id and pw, but for accessing sensitive data and configuring the cloud, biometric identity is required. This will add an additional layer of security for customer sensitive data and configuration. Therefore, based on the sensitivity of the customer's data, one or two layer's authentications will be required.

Cloud Computing is the technology in the modern era which is widely used by users irrespective of their professions. Cloud is for everyone, which means there is no need to have a specific level of education to be eligible for using the cloud. It eliminates the dependability of data stored at one location that cannot be accessible from anywhere, anytime. With multifactor biometric authentication to the cloud, users can access data from any place at any time, location independent. In addition, it helps in reducing the cost of infrastructure if any upgrade of hardware is required, which has new device purchasing cost, installation cost, maintenance cost.

This methodology helps in avoiding security issues like a malicious intrusion and brute force attack, which are the major threats that need to be addressed first. This methodology works as a catalyst for convincing businesses/ to use the cloud in their organization for the critical data too. By using multifactor biometric authentication, it would take care of remembering more passwords, carry extra badges, documents, or ID cards to access sensitive data.

For future research, with all the available solutions in the cloud, more research is still required to make accessing data automated and transparent to the user. This method is a subject for my second paper and future research including the conversance of cloud NFV and other technologies.

REFERENCES

[1] J. K. Wang and X. Jia, "Data Security and Authentication in hybrid Cloud Computing model," IEEE Global High Tech Congress on Electronics (GHTCE), November 2012, pp. 117-120.

[2] N. Hemalatha, A. Jenis, A. C. Donald, and L. Arockiam, "A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing," International Journal of Computer Applications, 96 (16), 2014.

[3] Z. Xin, L. Song-qing, and L. Nai-wen, "Research on Cloud Computing data security model based on multi-dimensional," IEEE International Symposium on information technology in medicine and education (ITME), 2012, pp. 897-900.

[4] M. Ahmed and M. A. Hossain, "Cloud Computing and security issues in the cloud, International Journal of Network Security & Its Applications, 6(1), 25, 2014.

[5] F. Hang, and L. Zhao, "Supporting end-user service composition a systematic review of current activities and tools" IEEE International Conference on Web Services (ICWS), June 2015, pp. 479-486.

[6] R. Masood and M. Aslam, "Innovative approach ensuring security and privacy in cloud computing" Pakistan Journal of Science, 68(1) 2016.

[7] A. Juels, and T. Ristenpart, "Honey encryption: Encryption beyond the brute-force barrier," IEEE Security & Privacy, 12(4), 2014, pp. 59-62.

[8] L. He, F. Huang, J. Zhang, B. Liu, C. Chen, Z. Zhang, and W. Lu, "Dynamic secure interconnection for security enhancement in cloud computing," International Journal of Computers Communications & Control, 11(3), 2016, pp. 348-357.

[9] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust management of services in cloud environments: Obstacles and solutions," ACM Computing Surveys (CSUR), 46(1), 12, 2013.

[10] https://www.alertlogic.com/blog/top-5-cloud-security-issues-for-2018//

[11] W. Stallings, "Foundation of Modern Networking SDN, NFV, QoE, IoT, and Cloud," Addison Wesly, 2016.

[12] ITU-T Y.3500, "Cloud computing- overview and vocabulary," August 2014.

[13] L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, "Scientific cloud computing: early definition and experience," 10th

 ISBN: 978-1-61208-625-5

IEEE Int. Conference on High-Performance Computing and Communications, Dalian, China, Sep. 2008, pp. 825-830, ISBN: 978-0-7695-3352-0.

[14] A. B. Angadi and K. C.Gull, "Security issues with possible solutions in cloud computing- a survey," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 2, February 2013, ISSN: 2278 – 1323.

[15] P. Mell and T. Grance, "The NIST definition of cloud computing," http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf Accessed [12/4/2018]2011.

[16] B. Akashdeep, G. Subrahmanyam, V. Avasthi, and H. Sastry, "Review of solutions for securing end user data over cloud applications," International Journal of Advanced Computer Research, Vol 6 (27), June 2016 pp. 222-229.

[17] http://www.m2sys.com/blog/biometric-hardware/advantages-biometric-identification-management-system/ [Accessed 4-2018]

 ISBN: 978-1-61208-625-5