IJCSE International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-3 E-ISSN: 2347-2693

Cloud's Software- Security as a Service(S-SaaS) via Biometrics

Surabhi Shukla[1*], Dharamjeet Kumar[2]

ME (Computer Science), MPCT, RGPV Bhopal, India, surabhishukla1206@gmail.com
[2] MSc (Computer Science), SHIATS Allahabad, India,dharamjeet1987@gmail.com

www.ijcseonline.org

Received: 7 March 2014 Revised: 18 March 2014 Accepted: 26 March 2014 Published: 30 March 2014

Abstract— Cloud computing is considered to be the next generation of information technology framework. It is the next generation computing platforms that can provide dynamic resource pools, virtualization and high availability. The new character brings a lot of new security challenges which have not been taken into account completely in the current cloud computing system. As a consequence, to build a cloud computing data security system is the basis to build cloud computing security system. In this article, the cloud computing technology architecture and the cloud computing data security challenges are the first to be studied and considered, and then the Biometric is raised. At last, the problem definition & resolving strategy has been researched. First of all, user authentication is required to ensure that user data cannot be tampered. Users who pass the authentication can get relative operation on the user data, such as addition, modification, deletion. If the unauthorized user use illegal means to deceive the biometric authentication system, the file entered the system encrypt and privacy defense levels. If key has been got by the intruder. The user data cannot be got valid information even it is obtained through function of privacy protection. It is very important for commercial users of the cloud computing to protect their business secrets.

Keywords- *Cloud Computing,VPN,SLA,QoS, API,Biometrics*

I. INTRODUCTION

A. *Cloud Computing*

The term "cloud", appears to have its origins in network diagrams that represented the internet, or various parts of it, as schematic clouds. The underlying benefit of cloud computing is shared resources, which is supported by the underlying nature of a shared infrastructure environment [8, 25]. Thus, service level agreements span across the cloud and are offered by service providers as a service based agreement rather than a customer based agreement. Measuring, monitoring and reporting on cloud performance are based upon an end user experience or the end users ability to consume resources [22]. The downside of cloud computing, relative to SLAs, is the difficultly in determining root cause for service interruptions due to the complex nature of the environment.

As applications are moved from dedicated hardware into the cloud these applications need to achieve the same or even more demanding levels of service as classical installations [20]. SLAs for cloud services focus on characteristics of the data centre and more recently include characteristics of the network to support end-to-end SLAs.

Any SLA management strategy considers two well-differentiated phases: the negotiation of the contract and the monitoring of its fulfilment in real-time. Thus, SLA Management encompasses the SLA contract definition: basic schema with the QoS (quality of service) parameters; SLA negotiation; SLA monitoring; and SLA enforcement—according to defined policies [21].

Corresponding Author: Dharamjeet, dharamjeet1987@gmail.com

1. Characteristics

- Shared Infrastructure —uses a virtualized software model, enabling the sharing of physical services, storage, and networking capabilities.
- Dynamic Provisioning — this is done automatically using software automation, enabling the expansion and contraction of service capability, as needed.
- Network Access — needs to be accessed across the internet from a broad range of devices such as PCs, laptops, and mobile devices, using standards-based APIs (for example, ones based on HTTP).
- Managed Metering — uses metering for managing and optimizing the service and to provide reporting and billing information. In this way, consumers are billed for services according to how much they have actually used during the billing period.

In short, cloud computing allows for the sharing and scalable deployment of services, as needed, from almost any location, and for which the customer can be billed based on actual usage.

2. Service Models

- Software as a Service (SaaS) —Platform where necessary information for the interaction between the consumer and the service is hosted as part of the service in the cloud.
- Platform as a Service (PaaS) — Consumers purchase access to the platforms, enabling them to deploy their own software and applications in the cloud. The operating systems and network access are not managed by the

consumer, and there might be constraints as to which applications can be deployed.

- Infrastructure as a Service (IaaS) — Consumers control and manage the systems in terms of the operating systems, applications, storage, and network connectivity, but do not themselves control the cloud infrastructure.

3. Deployment Models

- Private Cloud — the cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises.
- Public Cloud — the cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.
- Hybrid Cloud — the cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the requirement to retain some data in an organization, and also the need to offer services in the cloud.

4. Benefits

The following are some of the possible benefits for those who offer cloud computing-based services and applications:

- Cost Savings — Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.

- Scalability/Flexibility — Companies can start with a small deployment and grow to a large deployment fairly rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands.

- Reliability — Services using multiple redundant sites can support business continuity and disaster recovery.

- Maintenance — Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.

- Mobile Accessible — Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

II. SECURITY CHALLENGES WITH CLOUD

User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving. According to survey last year, their arise many threats which took place in cloud[19]. Cloud computing is just a name ambiguous to internet. As previously we denote internet with the cloud type architecture, so that is now only known as the cloud computing but tackles a huge number of problems regarding security. Some threats are mentioned here –

1. Data Breach - Data loss and data leakage are both serious threats to cloud computing, the measures you put in place to mitigate one of these threats can exacerbate the other.

2. Data Loss - Data stored in the cloud can be lost due to reasons other than malicious attackers.

3. Account or Service Traffic Hijacking - Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and password are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites.

4. Insecure Interface and API's - Cloud computing providers expose a set of software interfaces or API's that customers use to manage and interact with cloud services. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

5. Denial of Service - DoS attacks are attacks meant to prevent users of a cloud service from being able to access their data or their applications.

6. Malicious insiders - A malicious insider threat to an organization is a current or former employee, contractor or other business partner who has or had authorized access to an organizations networks system data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality.

7. Abuse of cloud services - One of cloud computing's greatest benefits is that it allows even small organization access to vast amounts of computing power. However, not everyone wants to use this power for good. It might take an attacker year to crack an encryption key using his own limited hardware, but using an array of cloud servers, he might be able to crack it in minutes.

8. Insufficient due diligence - Cloud computing has brought with it a gold rush of sorts, with many organizations rushing into the promise of cost reductions, operational efficiencies and improved security.

9. Shared technology vulnerabilities - Cloud service providers deliver their services in a scalable way by sharing infrastructure, platform and application.

III. BIOMETRICS CONCEPT

"Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual [6]. The application which most people associate with biometrics is security. The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time-of-identification [5]. Identification based on biometric techniques obviates the need to remember a password or carry a token. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user [1, 14, 3]. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic" [2, 4]. Fig (a.).

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

Identification - *One to Many*: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology [11], one can determine matches against a known database.

Verification - *One to One*: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans [23] or can grant access to a bank account at an ATM by using retinal scan.

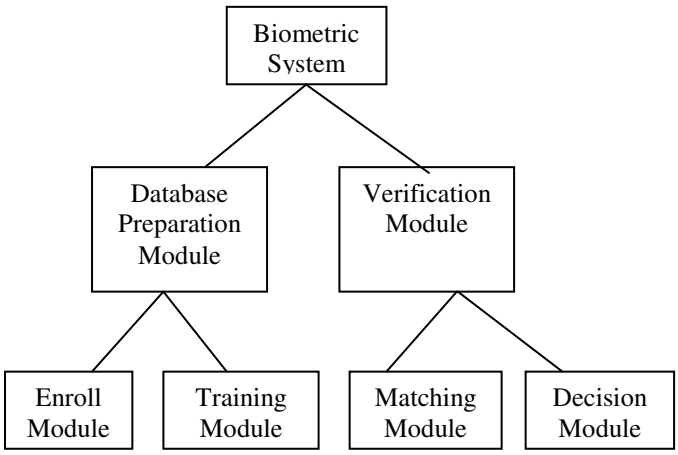


Figure (a.)

Among the various biometric technologies being considered, the attributes which satisfy the above requirements are fingerprint[10], facial features[7], hand geometry[12], voice, iris, retina, vein patterns[9], palm print, DNA, keystroke dynamics[10], ear-shape, odour, signatures etc.

A biometric system can be classified into two modules- (i) Database Preparation Module and (ii) Verification Module. The Database Preparation Module consists of two sub-modules, and they are (a) Enroll Module and (b) Training Module while the other module, Verification module can be divided into two modules (a) Matching Module and (b) Decision Module. Fig (b.)

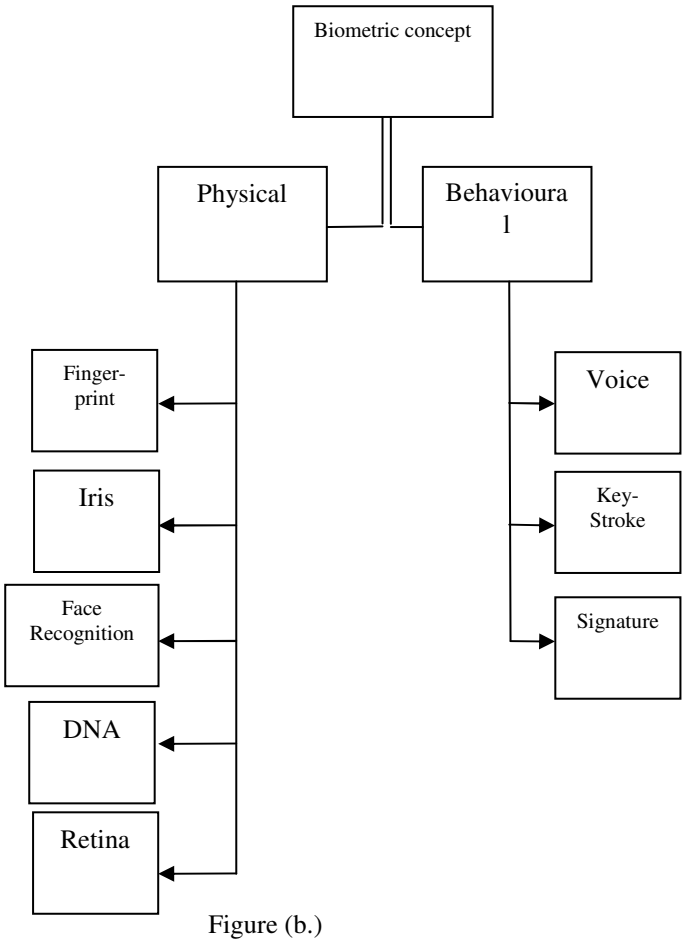


Figure (b.)

IV. PROBLEM DEFINITION AND RESOLVING STRATEGY

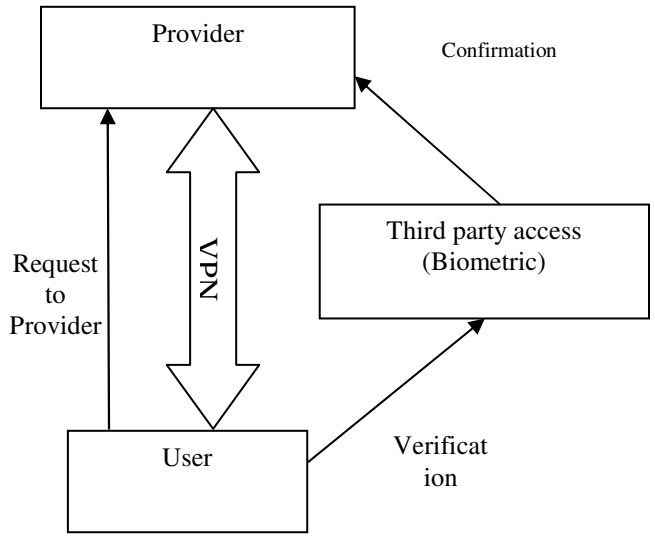
The network representative architecture for cloud data storage, which contains three parts as shown in Users, Cloud Service Provider (CSP) and Third Party Auditor (TPA) [24].Fig(c.)

Users: - Users who have data to be stored and interact with the cloud service provider (CSP) to manage their data on the cloud. They are typically, desktop computers, laptops, tablet computers, mobile phones, etc.

Cloud Service Provider (CSP):- Cloud service provider (CSP) has major resources and expertise in building and managing distributed cloud storage servers. A CSP offers storage or software services to user's available via the Internet.

Third Parity Auditor (TPA):- An optional TPA, who has expertise and capabilities that users may not have, is

monitoring the risk of cloud data storage services on behalf of users.



Figure(c.)

Problem definition

Let us consider a situation in which any malicious attacker attempts to retrieve or update the existing data of a specified user. This can be done either in transmit or in rest. So to avoid these types of attacks the analyst thought that there should be a mediator in between the user and provider, but what if it can mis-guide the mediator too. To overcome this problem we are giving a strategy here below.

Approach

According to our till date knowledge of cloud computing there are three main type of deployment model and those are IaaS, PaaS and SaaS. Many companies are trying to protect data on the cloud either on any deployment model. But we are focusing on SaaS [18]; in this model only User and Provider are basically there. But when we go deep inside the SaaS concept we talk about its security. Now it is not about SaaS it became S-SaaS i.e. Software Security as a Service. In this there is one mediator between user and provider that is known as third party auditor. This third party auditor is the only authority that comes between user and provider to remove or overcome security. Concept of biometric security is hold by third party only.

User is a person who updates his data into the cloud for all time access and from anywhere access [8]. The user who is storing its data in the cloud should be secure enough. The Cloud Service Provider which is giving the facility to user for database storage.

When user needs to retrieve information from the cloud, it should send request to the provider [15]. The provider delivers the requested data to the user. But before giving the data, it should be making sure that the user which is demanding for the database is original or not. For that it will call the third party access which holds the essential characteristic to match the user with the provider's database entries. When the user is found to be original via third party access then a virtual private network is setup between user and provider and all the required data is provided to the user. in our third party access concept we use biometric concept, which is very easier way to recognize that the unique user is demanding for the data or not.

If we come to the start point, then while registering with the provider user gives its essential details to the provider, in that detail we can include biometric information too. Biometric include physical and behavioral concept. Physical and behavioral include, finger-print, face recognition, key-stroke, voice recognition etc. provider should create database of user including biometric properties too, because they will help in identifying the unique user among a number of users or malicious attacker [17]. Biometric information is necessary in case when you want to retrieve your private information then it shall be provided to you only, because this is the responsibility of provider that the user who is storing its information in the cloud should remain safe and secure [24].

V. PROBLEM STRATEGY

With the help of this given figure we can make it very clear that what we actually want to understand you. As we have given our approach of biometric in combination with third party access. According to this flow chart which elaborates our procedure, we will try to make you understand our concept of biometric. Fig (d.)

1. User is ready to retrieve its information from the cloud.
2. User sends request to the provider, to create a VPN.
3. As it is provider's responsibility to safely transmit the data to user, it gives access to third party to check whether it is a correct user or not?
4. Third party then validates the user with the help of biometrics and sends the feedback to provider.
5. If the given feedback of individual user matches with the user database at providers account, then the process will proceed.
6. Process will proceed and a virtual private network will build up between user and provider.
7. The data will be safely transmitted.
8. After fully transmission of data the virtual private network will automatically terminate.
9. Step 5, if the given feedback of individual user doesn't match with the user database at providers account, then it will verify the user once again.
10. While in the case of verification, third party access will send a code to the users mobile; mobile number which is already stored in providers database.
11. If it is a correct user then the step 6-step 8 will take place.
12. Else an error message will be sent to user's account, and the process will be terminated here only.

VI. CONCLUSION

At the end of this paper, we just want to share that if in upcoming time we use biometric concept for data safety will be good enough. As we are using Biometric technique in our

AADHAR card, by which India became the first country world-wide to store its population's data so uniquely. But we just want to accommodate that not only one technique should be used. To be more active and proper in the world of security, we should attempt more than one concept together, so that it can make the security harder to crack.

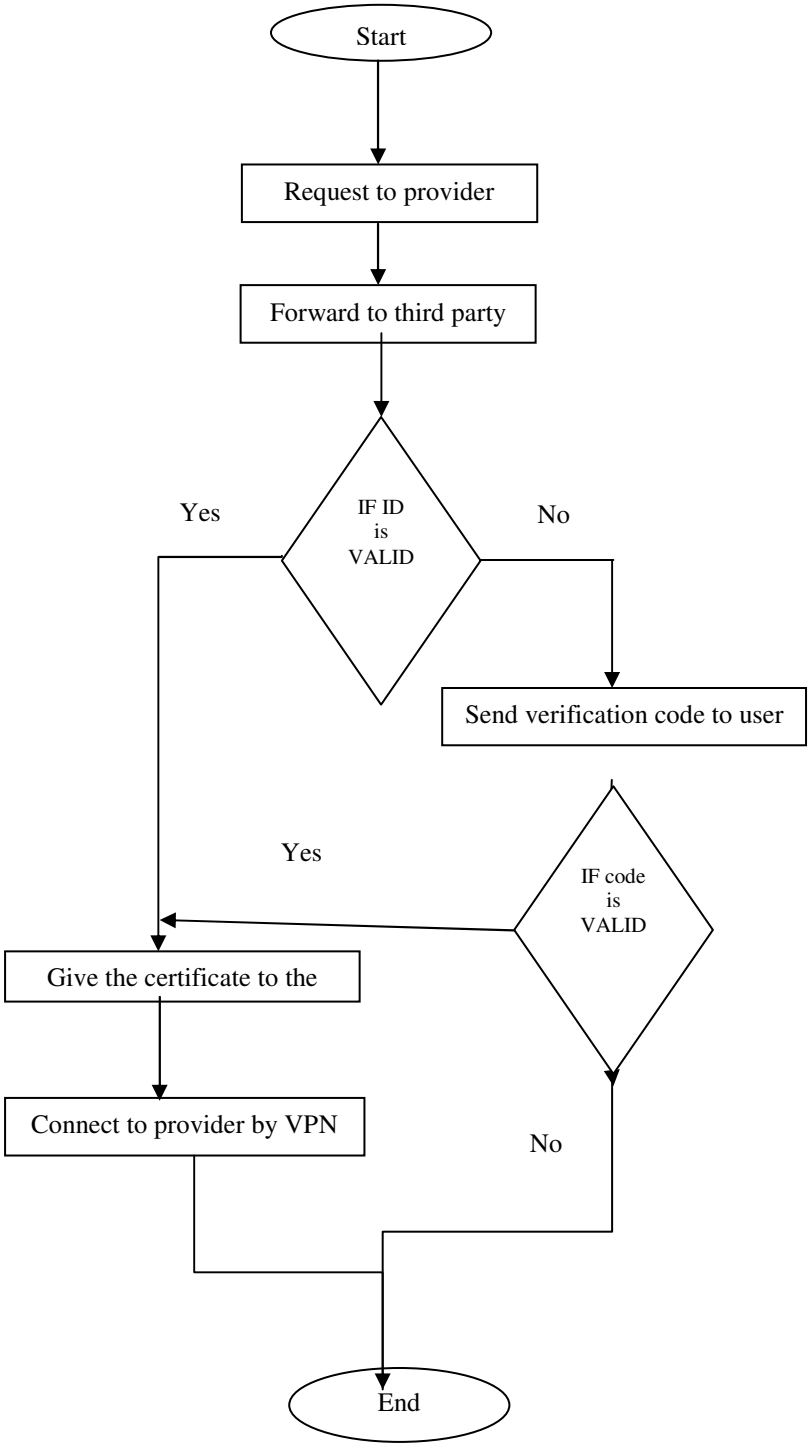


Figure (d.)

VII. REFERENCES

[1] Hataichanok, S., Clarke, N. L., and Furnell, S. M. 2012. Multi-modal Behavioural Biometric Authentication for Mobile Devices. In *Information Security and Privacy Research*, pp. 465-474. Springer Berlin Heidelberg.

[2] Clarke, N. L., and Furnell S. M. 2007. Advanced user authentication for mobile devices. *computers & security* 26, no. 2: 109-119.

[3] Bhattacharyya, D., Rahul R., Farkhod Alisherov A., and Minkyu Ch. 2009. Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology* 2, no. 3 :13-28.

[4] Crawford, H., Karen R., and Tim, S. 2013. A Framework for Continuous, Transparent Mobile Device Authentication." *Computers & Security*.

[5] Briggs, P., Olivier, PL. 2008. Biometric daemons: authentication via electronic pets. In: Proceedings of conference on human factors in computing systems. ACM; p. 2423e32.

[6] Kochetkov, A. 2013. Cloud-based biometric services: just a matter of time." *Biometric Technology Today* 2013, no. 5: 8-11.

[7] Voth, D. 2003. Face recognition technology. *Intelligent Systems, IEEE* 18, no. 3 (): 4-7.

[8] Fernando, N., Seng W. L., and Wenny R. 2013. Mobile cloud computing: A survey. *Future Generation Computer Systems* 29, no. 1 : 84-106.

[9] Wu, K., Jen-Chun L., Tsung-Ming L., Ko-Chin Ch., and Chien-Ping Ch. 2013. A secure palm vein recognition system. *Journal of Systems and Software* 86, no. 11: 2870-2876.

[10] Wang, Xu., Fangxia G., and Jian-feng M. 2012. User authentication via keystroke dynamics based on difference subspace and slope correlation degree. *Digital Signal Processing* 22, no. 5: 707-712.

[11] Gomez-Barrero, M., Javier G., and Julian F. 2013. Efficient Software Attack to Multimodal Biometric Systems and its Application to Face and Iris Fusion. *Pattern Recognition Letters*.

[12] Guo, J., Chih-Hsien H., Yun-Fu L., Jie-Cyun Y., Mei-Hui Ch., and Thanh-Nam L. 2012. Contact-free hand geometry-based identification system. *Expert Systems with Applications* 39, no. 14 : 11728-11736.

[13] Bhatt, Sh., and Santhanam, T. 2013. Keystroke dynamics for biometric authentication—A survey. In *Pattern Recognition, Informatics and Medical Engineering (PRIME), International Conference on*, pp. 17-23. IEEE.

[14] Araujo, L. C, Luiz, S. J., Miguel, G. L., Lee, L. L., and João B. T. Y. 2005. User authentication through typing biometrics features. *Signal Processing, IEEE Transactions on* 53, no. 2: 851-855.

[15] Pursani, M. P. J., and Ramteke, P. L. 2013. Mobile Cloud Computing. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 2, no. 4: pp-1512.

[16] Altinkemer, K., and Tawei W. 2011. Cost and benefit analysis of authentication systems. *Decision Support Systems* 51, no. 3: 394-404.

[17] Khan, A. N., Mat Kiah M. L., Samee U. Kh., and Madani S. A. 2012. Towards secure mobile cloud computing: A survey. *Future Generation Computer Systems*.

[18] Dharamjeet Singh,Surabhi Shukla,"Cloud's SaaS Security by Biometric Concept";International Journal of Computer Science and Engineering 2014; Review r.

[19] www.dialogic.com/12023-cloud-computing-wp

[20] P. Syam Kumar, R. Subramanian and D. Thamizh Selvam." *Ensuring Data Storage Security in Cloud Computing using Sobol Sequence*"; 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[21] 4. NIST/SP800-144.

[22] Kaspersky Internet Security

[23] Mahnoush Babaeizadeh, Majid Bakhfiari, Mohd Aizani Maarof."Keystroke Dynamic Authentication in Mobile Cloud Computing";2014 International Journal of Computer Applications 2014; Volume 90- Number 1.

[24] Zirra Peter Buba, Gregory Maksha Wajiga,"Cryptographic Algoriths for Secure Data Communication";International Journal of Computer Science and Security(IJCSS), Volume(5) :Issue(2) :2011.

[25] Hassan Takabi, James B. D. Joshi, Gail-Joon "Security and Privacy Challenges in Cloud Computing Environments"1540-7993/10/IEEE.

AUTHORS PROFILE

Surabhi Shukla
ME (Computer Science), MPCT,
RGPV Bhopal, India.
surabhishukla1206@gmail.com

Dharamjeet Kumar
MSc (Computer Science),
SHIATS Allahabad,India.
dharamjeet1987@gmail.com