Gaze-based Authentication in Cloud Computing

Ayushi Gahlot
Student
Department of Computer Science Engineering
IMSEC Ghaziabad, India

Umesh Gupta
Assistant Professor
Department of Computer Science Engineering
IMSEC Ghaziabad, India

ABSTRACT
This paper covers the basics of cloud computing, major challenges, need for new security models, and focuses on eye-gaze based authentication technique to secure the critical information stored on cloud. The paper provides an approach for implementation of gaze technology in cloud computing. The gaze-based authentication model involves the concepts of neural networks, Image processing, gaze estimation and feature detection along with the cryptographic concepts.

Keywords
Cloud computing, IaaS, PaaS, SaaS, static, dynamic, gaze estimation, image processing, feature detection, Hough transform.

1. INTRODUCTION
Cloud Computing is a communication model which provides access to a shared pool of configurable IT resources (applications, infrastructure, data storage, servers, networks, etc.) on a network, based on on-demand service. It provides cost effective and easy access to various resources. Cloud computing allows the user to access, manipulate, configure, develop and deploy a wide spectrum of applications online. Cloud computing is platform independent i.e. no additional piece of software needed to be installed. Also, cloud works on on-demand basis, which means that the user can access the resources any time [1].

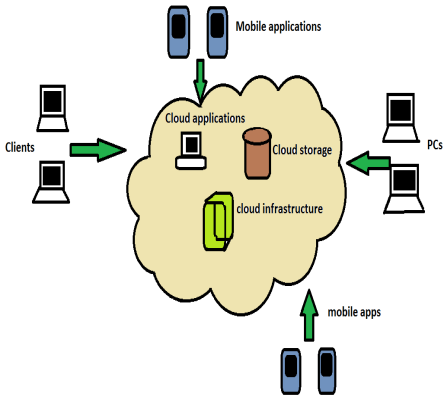

Fig 1: Cloud computing environment

2. BASIC CHARACTERSTICS OF CLOUD

2.1 On-Demand Service
Computing capabilities or resources should be provisioned automatically and the user should be able to access the cloud any time as he wants.

2.2 Broad Network Access
Since the cloud technology is completely web-based, it should be accessible from anywhere and anytime.

2.3 Resource Pooling
The services and resources (physical or virtual) provided by the Cloud Service Provider (CSP) are pooled to serve multiple tenants. This multi-tenant model allows sharing of a single physical instance of hardware, database and infrastructure by multiple consumers.

2.4 Rapid Elasticity
Scaling up and down of resources can be done quickly and flexibly making transformations quick and easy.

2.5 Measured Service
Resources which are allocated to the customer are automatically monitored, controlled and reported. This provides transparency between the consumer and the service provider.

3. CLOUD DEPLOYMENT MODELS
This section of the paper describes the basic cloud deployment models. These deployment models tell about the type of access made to the cloud. Cloud may have following access types: Public, Private, Hybrid, and Community, as shown in fig 2.

3.1 Public Cloud
Public cloud services are made available to the client by a third party service provider via internet, and are easily accessible to the general public.

3.2 Private Cloud
The Public cloud allows the cloud services to be accessible within an organization. Private cloud provides the user as well as the service provider great control over the cloud infrastructure and data storage, making it more secure.

3.3 Community Cloud
The community cloud allows the services and systems to be accessible, used and controlled by a group of organizations, having common interests or goals. It is more secure than a public cloud.

3.4 Hybrid Cloud
A Hybrid cloud is a combination of public cloud and private cloud that are interlinked. In this model, the users keep critical data and services under their control (on private cloud), and the non –critical business information and processing on public cloud.

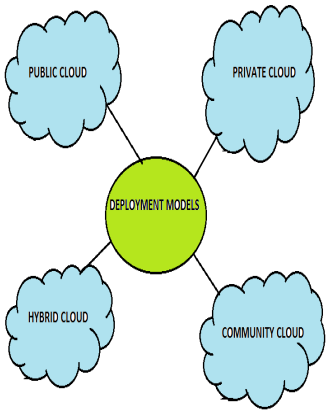

Fig 2: Deployment models of cloud computing

4. CLOUD SERVICE MODELS

This section of the paper explains various basic service models of cloud. Service models are reference models on which cloud computing is based.

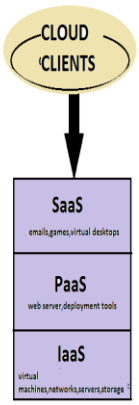

Fig 3: Service models of cloud computing

Cloud can be delivered in following basic models: SaaS, PaaS, and IaaS, as shown in fig 3.

4.1 Software-as-a-Service (SaaS)

This model allows using software applications as a service to the end users. SaaS is software that is owned, controlled, managed, and delivered remotely by one or more service providers via internet, based on the pay-per use service. It provides scalability and transfers the computing load from users to providers.

4.2 Platform-as-a-Service (PaaS)

PaaS provides a runtime environment as a service for applications, development and deployment tools. The user controls the applications that run in that environment, but not the hardware or network infrastructure on which the application runs.

4.3 Infrastructure-as-a-Service (IaaS)

Iaas delivers platform virtualization outsourced service. It allows the user to access fundamental resources such as physical machines, virtual machines, virtual storage, deployed apps, operating system, firewalls, load balancers,etc, but the user can't control the cloud infrastructure.

5. CHALLENGES IN CLOUD COMPUTING

5.1 Security and privacy

Security is the biggest challenge in adopting cloud computing. When using cloud services, the data storage and management is provided by a third party, so it's risky to handover your critical information in hands of someone else.

5.2 Isolation failure

The isolation mechanism of cloud which separates data storage, memory, routing between different users may fail. This will lead to huge risk to the information stored on cloud.

5.3 Locking in

It is a condition of a user to get locked or dependent on a particular Cloud Service Provider, since it is very difficult for a user to switch from one service provider to another.

5.4 Network availability

Due to the always- on nature of cloud, the network services should be all time available to ensure 24*7 access to cloud.

6. NEED FOR NEW CLOUD SECURITY MODELS

Trusting the data on a third party (service provider) is a threat to highly critical information on cloud [2]. The commonly used cryptographic models using manual passwords to provide access to data are failing to protect the data [3]. Once the password is cracked, the information is revealed. Therefore there is a need for stronger authentication. In the present scenario, the mostly used security methods are the cryptography and biometrics. But there is a need for improved authentication since the cryptographic methods rely on passwords (generally static).Even the strongest encryption model can be bypassed if the password is compromised. Strong passwords are generally long and complex, difficult to remember. On the other hand, the multifactor authentication schemes involving use of biometrics [4] have low usability and require additional equipments, and are difficult to implement. There has to be a way out which provides both usability and security, and passwords should be made moreover "dynamic" rather than static [5].

7. EYE- GAZE AUTHENTICATION MODEL

The model overcomes the disadvantages of presently used authentication techniques. The model provides usability of passwords along with multifactor authentication in a single step, using gaze technology (eye- gaze pattern detection and estimation), employing neural networks and image processing techniques .The model uses eye gaze pattern for human-device interaction, that uses inconspicuous eye movements to calculate a person's point of gaze (POG).The model provides increased usability, scalability and high security at minimal expense. The model does not rely on high definition cameras and special lighting conditions; it works in normal conditions and uses the integrated cameras embedded in different devices.

8. INTRODUCTION TO GAZE TECHNOLOGY

Gaze technology is based on eye tracking and gaze estimation of a person's eye. Eye tracking is the process to electronically measure the point-of-gaze (POG) of a person's eye. Eye tracking also measures the motion of an eye relative to the head[6],[7].Gaze technology has wide applications in the field of Human-computer interface (HCI) and biometrics[8].The process of gaze estimation includes feature detection (face and eye region detection), using neural networks and image processing techniques, and pupil (iris) tracking, using an eye tracker.

9. GAZE ESTIMATION PROCESS:

Step1: Building a database:
The first step is to collect and compile a database that contains images from a diverse population of users. These images are used for pattern matching during image processing.

Step 2: Image Acquisition
The real time video images are captured from the integrated camera of the device, and are passed for processing and recognition phases [7], [9].

Step 3: Facial Feature detection
The model uses Haar cascades [10] for rapid and accurate detection of face and eye regions. Haar features refer to the two- dimensional images extracted by calculating the integral or sum of the image intensities, within the rectangular sections of the image having varied intensities. There are parameters called classifiers (or cascades) which are ordered through AdaBoost machine learning algorithm [11]. The weights for classifiers are set according to the false acceptance rate measured by AdaBoost training set. The feature detection algorithm proceeds as: A special Haar cascade for face detection is passed along with a scaled image (640x480p) to detect face. The feature detection algorithm returns the rectangular areas of the image that are identified by the cascaded face filter, and the best match is selected [12].

Step4: Eye Detection
In this step, the face image is subdivided into half vertical and half horizontal portions, creating a mask, so that only a part of the image close to the eye is needed to be processed, speeding up the process. Now, for eye detection, same matching algorithm is used which was used for face detection. A special eye Haar cascade is applied to the input image to detect eye region. After eye detection, the image is again cropped and passed further for pupil (iris) tracking. Hough transform, (which is a computer vision algorithm) for pupil detection is given by:

$$H(\Omega) = \sum_{i=1}^{N} p(Xi, \Omega)$$

$$\text{Where } p(Xi, \Omega) = \begin{cases} 1 & , \forall (X, \Omega): f\{X, \epsilon\} = 0 \ \cap T_{\Omega} \neq 0 \\ & 0; \text{otherwise} \end{cases}$$

where X_i represent feature points in image space, $f(X, \epsilon) = 0$ represents parametric constraint equations, T_{Ω} represents accumulators unit in parameter space with center Ω.

Since the pupil is round, the expression is given by:

$(x - a)^2 + (y - b)^2 = r^2$ where (a, b) is the center with radius r.

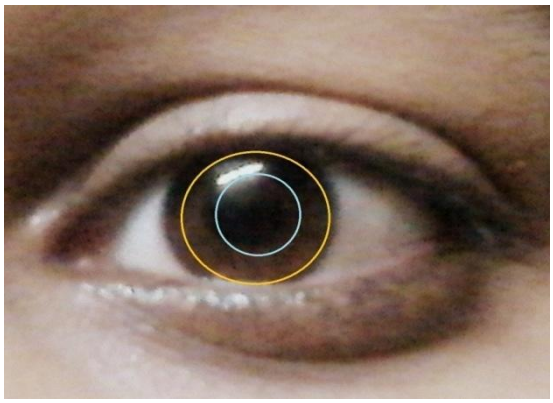

Fig:4: Eye detection(Person 'A')

Step 5: Pupil tracking:
The image passed has to be segmented before pupil can be tracked. Segmentation is a process (in image processing) which refers to separation or division of pixels corresponding to a specific object, in order to identify the object (pupil).

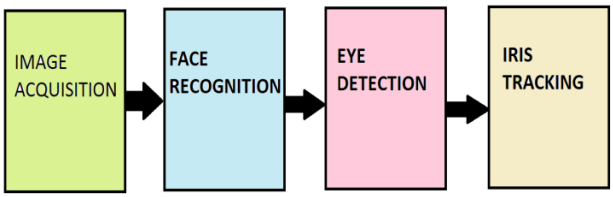

Fig 5: Gaze estimation process

10. WORKING OF EYE-GAZE AUTHENTICATION MODEL (in cloud)

In cloud computing environment, the user accessing the cloud database has to enter a PIN and go through an authentication procedure of gaze estimation, and is granted access only if he is passes the check. The gaze-based authentication check in cloud computing proceeds as shown in fig 6.

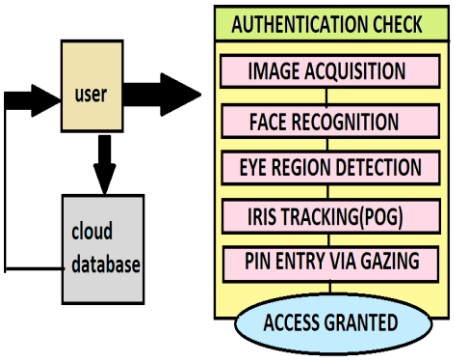

Fig 6: Eye gaze authentication process

1. The user establishes a security PIN (Personal Identification Number) for the first time, using a user-device application interface for authentication, and this PIN is used as master key for encrypting data.

2. The user requests for files (data) from the cloud service provider (CSP).The cloud service provider gets the requested encrypted files stored at cloud database.

3. To decrypt the files, the user goes through an eye gaze authentication check as follows:

An integrated camera on the device provides images to gaze estimation algorithm, the images are processed and goes through face detection and recognition phases. If it matches correctly the image is passed for eye detection, followed by iris (pupil) tracking for calculating the gaze point of the user

Fig 7: User Interface to enter PIN

After gaze point is established the user's gaze point projects over the device's screen, and user has to enter the PIN using eye gaze [13]. The device's screen displays a keypad which contains blocks of different colors corresponding to different symbols as per PIN specifications (as shown in fig 7). When the user gazes at a block for sufficient time (say 2 sec), an input is received by the device. After receiving an input, blocks get shuffled and are ready for next input. In this way, the PIN is entered. If the PIN is correctly entered, the user is granted access to the data, otherwise access is denied.

11. COMPARATIVE ANALYSIS OF AUTHENTICATION TECHNIQUES

There is a need of comparative analysis of authentication techniques used for security as shown in Table 1

.

Table 1: Comparison of different authentication techniques used for security

Paper Name	Technique used	Advantages	Limitations	Future scope
1. "Graphical passwords: a survey"by Xiaoyuan, S., Z. Ying,(2005) [14]	Graphical password techniques	• Stronger authentication than text-based passwords. • Easy to remember. • Cannot be easily cracked by simple brute force and dictionary attacks. • Easy to implement.	The graphical password schemes are vulnerable to major attacks due to static nature of passwords like: • Shoulder surfing • Replay attacks. • Screen capturing attacks.	Enhancement of computer vision system technology, easier image deformation and retrieval, stronger graphical password implementation.
2. " A Remote User Authentication Scheme Using Strong Graphical Passwords" by Wei-Chi, K. and T. Maw-Jinn,(2005) [15]	Draw A Secret (DAS) scheme(pure recall based technique)	• More secure than text-based passwords • Easy to implement	Vulnerable to graphical dictionary attacks and secret attacks.	Implementation of BDAS (Background Draw-a-Secret scheme) using background images as passwords on a large scale.
3. "Pure and cued recall-based graphical user authentication" by Masrom, M., F. Towhidi,(2009) [16]	Passdoodle system technique(pure recall based)	• More secure than DAS. • Easy to remember as compared to DAS and text based passwords	Vulnerable to attacks like shoulder surfing, key loggers, spyware and guessing	Password space can be improved; matching of passwords can be made more simple and accurate.
4. "PassPoints: Design and longitudinal evaluation of a graphical password system" by S.Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon,(2005) [17]	Passpoint system technique(pure recall based)	• High security due to increased password space • The image password is stored in hashed form. • More flexible due to small tolerance size. • High usability	Vulnerable to mouse click attacks, replay attacks, screen recording attacks.	Modelling the user's choice, prediction of chick point entropy. Texture information in image segmentation for better results.

5. "IPAS: Implicit Password Authentication System" by Sadiq Almuairfi, Parakash Veeraraghavan and Naveen Chilamkurti ,(2011).[18]	• Implicit Password Authentication scheme (DAS, Passpoint, Passdoodle are its typical cases).	• The data is represented in explicit form to the user. • It is protected from shoulder surfing and screen-dump attacks.	During the process of registration, the system asks the user an alphanumeric question and the user is asked to input the answer using a graphical keyboard.	Development of dynamic IPAS with more features for obtaining better balance of security and usability.
6. " Foiling the Cracker: A Survey of, and Improvements To Password Security" by D.V. Klein,(1990) [19]	2 factor authentication • Password • Smart card	• High usability • High scalability • More secure than single factor password based authentication • Cost effective	• Vulnerable to dictionary and brute force attacks. • Less secure. • Password can be easily cracked using key loggers and other means.	Development of strong passwords by improving password space.
7. "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems" by Xinyi Huang, Yang Xiang, Ashley Chonka, Jianying Zhou, and Robert H. Deng ,(2011)[20]	3 factor authentication • Password • Smart card • biometrics	• High security • High scalability • Less vulnerable to attacks • Improved system assurance. • Provides source of high entropy information.	• The biometric characteristics of the model cannot be easily changed • Cost of implementation is very high.	Development of protocols with better performance and fully identify threats in 3 factor authentication
8. "The SSL Protocol, Version 3.0" by Freier, A.O., Karlton, P., Kocher,(1996)[21]	SSL Authentication Protocol(SAP)	Data on cloud is secured.	• It is complicated • Certificate based • Less efficient • More authentication time • High computation cost	SSL terminations will be able to handle more data transactions at faster rate. Efficient for web security and encryption lengths and cipher suites used.
9. "An Identity-based Non-interactive Authentication Framework for Computational Grids" by Mao,(2004)[22]	ID-based non-interaction framework	• High scalability • Certificate- free framework	• It has private key distribution issues • There are Private Key Generator(PKG)	Can be implemented in bootstrapping security of Wireless Sensor Networks (WSN) using pairing-based cryptography(PBC)
10. "A dynamic key infrastructure for GRID" by Lim, H.W., Robshaw ,(2005)[23]	Hybrid approach that combine IBC(identity based cryptography)	This approach solves the private key distribution issues.	• It is not certificate-free • Non-interactive quality is lost in this approach.	Enhancements can be made to overall security and efficiency of the scheme. Elimination of public key distribution load by combining user identity with public key.
11. " Identity-Based Authentication	IBHMCC (Identity Based Hierarchical	• The authentication protocol is efficient and lightweight on user side.	• It is vulnerable to identity –based intrusion attacks	Development of hierarchical identity-based key management

for Cloud Computing" by Hongwei Li, Yuanshun Dai, Ling Tian, and Haomiao Yang,(2009)[24]	Model For Cloud Computing.	• High scalability • Certificate-free framework		systems with better performance and faster key reconstruction.
12. "Painless migration from password to two factor authentication" by Mao Z., Florencio, D., and Herley C,(2011) [25]	Possession based multifactor system	• Ease of integration • High security • Low implementation cost.	• Integration is given higher priority than usability • Vulnerable to attacks like shoulder surfing • Security is compromised by relying on possession of trusted device.	Improvement in password space and cost effective implementation.

12. CONCLUSION

Cloud computing is an emerging technology which is used by enterprises and companies for making their business more collaborative. Also it faces major challenges on its way. The data security is a serious matter of concern since the data has to be entrusted upon a third party. There is a need for strong authentications on the data put on cloud, to prevent intrusions, leakage or loss of critical information. The gaze-based authentication model discussed in the paper provides an efficient, feasible, cost effective procedure which has high scalability, usability and security.

13. FUTURE SCOPE

The advancement of cloud technology and overcoming the challenges faced by it, ranging from user interaction up to security issues will be topics of great research in the upcoming years to provide more secured and efficient clouding. The gaze-based authentication can be made more flexible by developing efficient tracking methods which can reduce the complexity of biometric models. Gaze technology can be used for securing any critical data, and can be a reliable choice for authentication.

14. ACKNOWLEDGEMENTS

This work is supported by the computer science department of IMS engineering college and the ACM Student chapter of IMSEC.

15. REFERENCES

[1] D. Catteddu and G. Hogben. Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA, 2009.

[2] H. Takabi, J.B.D. Joshi, and G.-J. Ahn. SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments. Proc. 1st IEEE Int'l Workshop Emerging Applications for Cloud Computing, IEEE CS Press, 2010, pp. 393–398.

[3] Bonneau, J., Herley, C., van Oorschot, P., and Stajano, F.,The quest to replace passwords: A framework for comparative evaluation of web authentication schemes, IEEE Symposium on Security and Privacy (SP), 2012, pages 553-567.

[4] Phiri, J., Zhao, T.-J., and Agbinya, J., Biometrics, device metrics and pseudo metrics in a multifactor authentication with artificial intelligence, 6th International Conference on Broadband and Biomedical Communications (IB2Com), 2011, pages 157-162

[5] Maeder, A. J. and Fookes, C. B., A visual attention approach to personal identification. In Faculty of Built Environment and Engineering; School of Engineering Systems, 2003, pages 1-7.

[6] Yang, C., Sun, J., Liu, J., Yang, X., Wang, D., and Liu, W, A gray difference-based pre-processing for gaze tracking, IEEE 10th International Conference on Signal Processing (ICSP), 2010, pages 1293-1296.

[7] Liang, Z., Tan, F., and Chi, Z., Video-based biometric identification using eye tracking technique, IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC), 2012, pages 728-733.

[8] Corcoran, P., Nanu, F., Petrescu, S., and Bigioi, P., Real-time eye gaze tracking for gaming design and consumer electronics systems. IEEE Transactions on Consumer Electronics, 2012, pages 347-355.

[9] Mei, Z., Liu, J., Li, Z., and Yang, L.Study of the eye-tracking methods based on video, Third International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), 2011, pages 1-5.

[10] Viola, P. and Jones, M., Rapid object detection using a boosted cascade of simple features. In Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001, volume 1, pages I-511-I-518 vol.1.

[11] Viola, P. and Jones, M., Robust real-time face detection. In Eighth IEEE International Conference on Computer Vision, 2001. ICCV 2001. Proceedings, volume 2, pages 747-747.

[12] Majumder, A., Behera, L., and Subramanian, V. Automatic and robust detection of facial features in frontal face images. In UkSim 13th International Conference on Computer Modelling and Simulation (UKSim),2011, pages 331-336.

[13] De Luca, A., Weiss, R., and Drewes, H. , Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. In Proceedings of the 19th Australasian conference on Computer-Human Interaction: Entertaining User Interfaces, 2007, page 199202, New York, NY, USA. ACM.

[14] Xiaoyuan, S., Z. Ying, et al.,Graphical passwords: a survey. Computer Security Applications Conference, 21st Annual,2005.

[15] Wei-Chi, K. and T. Maw-Jinn,A Remote User Authentication Scheme Using Strong Graphical Passwords. Local Computer Networks, 2005. 30th Anniversary.

[16] Masrom, M., F. Towhidi, et al., Pure and cued recall-based graphical user authentication. Application of Information and Communication Technologies, 2009. AICT 2009. International Conference.

[17] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon. PassPoints: Design and longitudinal evaluation of a graphical password system. International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), 63 (2005) 102-127.

[18] Almuairfi, S., Veeraraghavan, P., and Chilamkurti, N. , IPAS: implicit password authentication system. In IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA), 2011, pages 430-435.

[19] D.V. Klein. Foiling the Cracker: A Survey of, and Improvements to, Password Security. Proc. Second USENIX Workshop Security, 1990.

[20] Huang, X., Xiang, Y., Chonka, A., Zhou, J., and Deng, R.-H., A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. IEEE Transactions on Parallel and Distributed Systems, 2011,pages 1390-1397.

[21] Freier, A.O., Karlton, P., Kocher, P.C. The SSL Protocol, Version 3.0.INTERNETDRAFT (November 1996)

[22] Mao, W.B.: An Identity-based Non- interactive Authentication Framework for Computational Grids, May 29 (2004)

[23] Lim, H.W., Robshaw, M.: A dynamic key infrastructure for GRID. In: Sloot, P.M.A., Hoekstra, A.G., Priol, T., Reinefeld, A., Bubak, M. (eds.) EGC , LNCS, vol. 3470, pp. 255–264. Springer, Heidelberg (2005)

[24] Hongwei Li, Yuanshun Dai, Ling Tian, Haomiao Yang.Identity-Based Authentication for Cloud Computing, M.G. Jaatun, G. Zhao, and C. Rong (Eds.): CloudCom , LNCS 5931, pp. 157–166, 2009.© Springer-Verlag Berlin Heidelberg.

[25] Mao, Z., Florencio, D., and Herley, C. , Painless migration from passwords to two factor authentication. In IEEE International Workshop on Information Forensics and Security (WIFS),2011, pages 1-6.