



3D Security Cloud Computing using Graphical Password

Ms. Sneha Vasant Thakare¹, Ms. Deipali V. Gore²

ME student (CSE), Computer, P.E.S. Modern College of Engineering, Pune, India¹

Professor, Computer, P.E.S. Modern College of Engineering, Pune, India²

ABSTRACT: Cloud computing is an emerging, on-demand and internet- based technology. It provides variety of services over internet such as, software, hardware, data storage and infrastructure. To utilize these services by authorized customer and to secure a data on the cloud, it is necessary to have strict security checking system. The 3D security checking system by using the multi-level authentication technique generates the password in multiple levels to access the cloud services. This system is able for thwarting Shoulder attack, Tempest attack, and Brute-force attack, dictionary attacks and many more which are present at client side, with the use of strong techniques in the Graphical password.

Keywords: 3D security, Cloud Computing Authentication, Graphical password, multi-level authentication

I. INTRODUCTION

Cloud computing is internet based technology which provides variety of services over internet such as software, hardware, data storage and infrastructure. Within the cloud computing systems environment, the virtual environment lets user's access computing power that exceeds that contained within their own physical worlds. Fundamentally, abundant security issues arises as it comprises many technologies including networks, virtualization [6], operating systems, resource scheduling, transaction management(when user query about some secure data), load balancing(preventing the cloud from crashing when the user demand increases),concurrency control(many users simultaneously requesting or accessing the same data on the cloud) and memory management. Data security doesn't only engross encrypting the data but also comprises on implementing and enforcing the appropriate policies for data sharing and as well as authenticating the user who required to access the data on cloud. It also encompasses scheduling data backup and safe storage of the backup media. Security is implicit within these capabilities, but moreover elementary concerns exists that need attention. To beat these concerns, a security model must be developed which ensures CIA (confidentiality, integrity, and availability). With the competence provided by the cloud systems, as

the number of users enhances, the probability of cybercrime increases. Cloud computing is becoming a tempting target for cybercrime. If not all cloud providers supply adequate security measures, then these clouds will become high-priority targets for cybercriminals. As cloud systems are inherited architecture so a single cyber attack offers opportunity to the attacker to influence a large number of sites through a single malicious activity.

There are many security issues are arises for accessing these services in cloud. To remove these issues the 3D security system is provided with powerful and more secure authentication techniques. This system is responsible to categories the files or confidential data on cloud. Categorization is depends on 3 important factors: Confidentiality, Integrity and Availability.

II. SECURITY ISSUES IN CLOUD

The cloud security and privacy is a big concern now a day. Security, privacy and secure storage of data [9] are two barriers which are preventing the organizations and users from adopting the cloud computing. Emphasis must be given on security, privacy and stability on the cloud based technologies and computing to make them admirable among the corporate multitenant environment. Malicious and Abusive attacks are proliferating cloud security. The data leakage and security attacks can be caused by insufficient authentication, authorization, and audit (AAA) controls [6], inconsistent use of encryption



and software keys, operational failures, persistence and reminisce challenges: disposal challenges, risk of association, jurisdiction and political issues, data center reliability, and disaster recovery. Some of the risks in cloud computing are well known in traditional computing models [6].

		CLOUD ARCHITECTURE (SERVICE BASED)			
		SAAS	PAAS	IAAS	DAAS
SECURITY CONCERNS	Abuse and Nefarious Use of Cloud Computing	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Insecure interfaces and API	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Malicious Insider	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Shared Technology Issue	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Data Loss or Leakage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Unknown Risk Profile	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 1. Security concerns in Various Clouds Architecture

These risks include, for example, malicious insiders, insecure user authentication (such as usage of weak passwords), malicious code running on the cloud, vulnerabilities of the shared resources leading to information leakage, or account hijacking by phishing methods, unknown risk profile[12], data loss(no stability in data storage on cloud). Many of these risks can be handled using conventional security practices.

III. 3D SECURITY TECHNIQUE

The 3D security system is provided with powerful and more secure authentication techniques. This system is responsible to categories the files or confidential data. It is a multi-level authentication system. The system makes the confidential data secure using highly secure graphical passwords. It removes the time complexity issue.

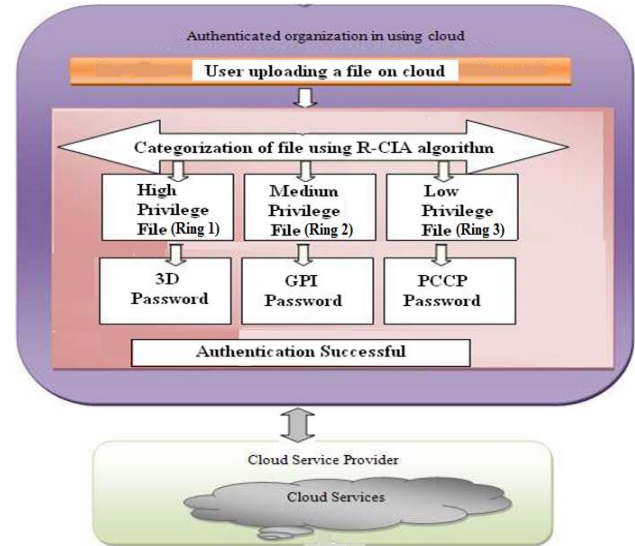


Figure 2. Architecture of 3D security system

Architecture of 3D security system is shown in fig 1.2 In 3D security system, User accesses the cloud services. User is going to upload a file on the cloud. There are 3 protection rings. The inner most ring is most secure. The file categorization is done using Revised- CIA algorithm. The R-CIA divides the files into ring 1, ring 2 and ring 3. 3D password is used for ring1. GPI (Graphical password with icons) password is used for ring2. PCCP (Persuasive clued click point) password is used for ring3. At the time of downloading, this password should be match. If it is matched, then the authentication is successful. The user can access the cloud services.

- 1) Ring-1: The 3-D password is a multifactor authentication scheme. For the authentication, it is require to presents a 3-D virtual environment where the user navigates and interacts with various objects. [3] The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment.[5] The design of the 3-D virtual environment and the type of objects selected determine the 3- D password key space.



FIGURE 3. 3D PASSWORD

2) Ring-2: GPI (Graphical Password with Icons) is the first graphical password scheme we propose in this paper. In GPI, to mitigate the hot spot problem users may click on a subset of displayed icons as their passwords instead of selecting specific locations on a background image. Experimental results show that the use of icons in GPI makes possible to evenly distribute possible click-points to a certain extent.



Figure 4. GPI interface

3) Ring-3: To address the issue of hotspots, Persuasive Clue Click Point (PCCP) was proposed. As with Clue Click Point, a password consists of five click points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in Fig 1.5 Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process.



Figure 5. Persuasive Clue Click Point

TABLE I
COMPARATIVE STUDY OF SECURITY SYSTEMS

System	Comparison of security System	
	3D security system	Multilevel authentication technique
Time complexity	Less than multilevel authentication system	Time complexity is more than 3D security
Performance	High	Low
Flexibility	good	Less than 3D security
Algorithm used	Revised- CIA	CIA

IV. CONCLUSION



To provide Cloud services to the intended customer, it is a better option to use 3D Security system rather than multi-level authentication technique. This technique helps in generating the password in many levels of organization so that the strict authentication and authorization is possible. The security level of cloud environment is much stronger by using multi-level security system. Depending on rings, levels of multi-level security system increases for secure access of cloud services. This system is able for thwarting Shoulder attack, Tempest attack, and Brute-force attack, dictionary attacks and many more which are present at client side, with the use of strong techniques in the Graphical password.

Acknowledgment

Acknowledgement is not a mere formality as, it is the general notation. It is the only way through which express our deep and profound gratitude to the people who directly or indirectly contribute to our work.

It's not until you undertake a Project like this one that you realize how much you must rely upon others help.

I highly obliged and respond to express my admiration to the best conscious to convey respect towards **Prof. (Ms.) D. V. Gore** for valuable contribution towards completion of our seminar.

I thank all the Staff members & lab Assistants of Computer Department who have helped me directly or indirectly in making this work a success.

REFERENCES

- [1] Surabhi Anand, Priya Jain, Nitin and Ravi Rastogi, "Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication" the 14th IEEE International Conference on Modeling and Simulation, Oregon, USA, 2012
- [2] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and Paul C. van Oorschot, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism", IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2 March/April 2012
- [3] Chippy.T and R.Nagendran, "Defenses against large scale online password guessing attacks by using persuasive click points", International Journal of Communications and Engineering Volume 03- No.3, Issue: 01 March 2012

[4] Fawaz A Alsulaiman and Abdulmotaleb El Saddik, "A Novel 3D Graphical Password Schema", VECIMS 2006-IEEE International Conference on Virtual Environment, Human-Computer Interfaces and Measurement Systems. La-Coruna-Spain 10-12 July 2006

[5] Prof. Sonkar S. K. and Dr. Ghungard S. B., "Minimum space and huge security in 3D Password Scheme." International Journal of Computer Application (0975-8887) Volume-29 No. 4, September 2011

[6] Kuyoro S. O., Ibikunle F. and Awodele O. "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3):Issue (5):2011.

[7] Kemal Bicakci, Nart Bedin Atalay, Mustafa Yuceel, Hakan Gurbaslar and Burak Erdeniz TOBB University of Economics and Technology, Ankara, TURKEY, "Towards Usable Solutions to Graphical Password Hotspot Problem", 33rd Annual IEEE International Computer Software and Applications Conference. 2009.

[8] F. A. Alsulaiman and A. El Saddik, "A novel 3D graphical password schema," in *Proc. IEEE Int. Conf. Virtual Environ., Human-Comput. Interfaces, Meas. Syst.*, Jul. 2006, pp. 125-128.

[9] 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)

[10] Parikshit Prasad, Badrinath Ojha, Rajeev Ranjan shahi, Ratan Lal, "3 Dimensional Security in Cloud Computing", Computer Research and Development (ICCRD), 3rd International Conference on Volume: 3 2011.

[11] Dinesha H A Agrawal V K, "Multi-level Authentication Technique for Accessing Cloud Services", Computing, Communication and Applications (ICCCA), 2012 International Conference on Feb 2012.

BIOGRAPHY



Ms. Sneha V. Thakare is an Lecturer in the Marathwada Mitra Madals college of engineering, loahgao, Pune. Her main research interests are in usable security: the intersection between human-computer interaction (HCI) and computer security. Current projects are on user authentication, usable security for web applications and crucial areas for teaching about computer security.



Prof. Ms. D. V. Gore is an assistant professor in the *P.E.S. Modern College of Engineering*, Pune. Her main research interests are in artificial intelligence and software design: Her current research projects are on usable security, especially authentication and security decision making, and on large-scale multi touch devices, especially environments for collaborative design and visualization.