Cloud Service Authentication Verification using 3D Graphic Signature

Abhishek Gopal
B.E Computer Science & Engg
KNS Institute of Technology
Bangalore
Email: abhishekgopal2008@gmail.com

Syed Aleemuddin Noor
B.E Computer Science & Engg
KNS Institute of Technology
Bangalore
Email: syedaleemuddinnoor@gmail.com

Chaithra M H
Lecturer, Dept of CSE
KNS Institute of Technology
Bangalore
Email: chaithra.mh14@gmail.com

Abstract: ***Cloud computing technologies are becoming popular because of the several benefits it offers. Many enterprises are adopting cloud computing technologies and its services to reduce the cost and complexity of their business infrastructure and maintenance. The technology is being accepted worldwide as a means to improve any kind of business performance. Our paper briefs the existing authentication methods for achieving security in the cloud. However to utilize these services by authorized customers, it is necessary to have strict authentication checks. At present authentication is done in several ways, such as textual, graphical, biometric 3D password and third party authentication. In this paper we are proposing the 3D graphic signature verification technique to ensure the authentication of users as an additional technique.***

Keyword: ***3D Graphics Signature Verification Techniques, Cloud Computing Technologies, Authentication.***

1. Introduction

Cloud computing technology is an open standard, service-based, Internet-centric, safe, convenient data storage and network computing services [1]. Cloud computing is an internet based model for enabling convenient, on demand network access to a shared pool of configurable computing resources [2]. It provides various services over internet such as software, hardware, data storage and infrastructure. Cloud computing providers deliver the applications via internet, which are accessed from web browsers, desktop and mobile applications. Cloud computing technologies are grouped into four sections: they are SaaS, DSaaS, IaaS and PaaS [7][8].

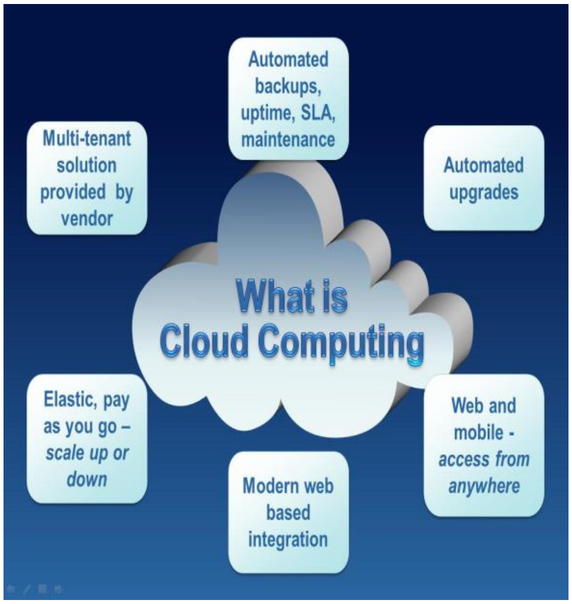

Automated backups, uptime, SLA, maintenance
Multi-tenant solution provided by vendor
Automated upgrades
What is Cloud Computing
Elastic, pay as you go – scale up or down
Web and mobile - access from anywhere
Modern web based integration

Figure 1: cloud computing technology

SaaS (Software as a Service) is an on-demand application service. It delivers software as a service over the Internet. It eliminates the need of installing and running the application on the customer's own computers [7][8]. **PaaS (Platform as a Service)** is an on-demand platform service to host customer application. Paas is delivery of computing platforms and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications. If facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers[7][8]. It improves the flexibility in having multiple platforms in business environment

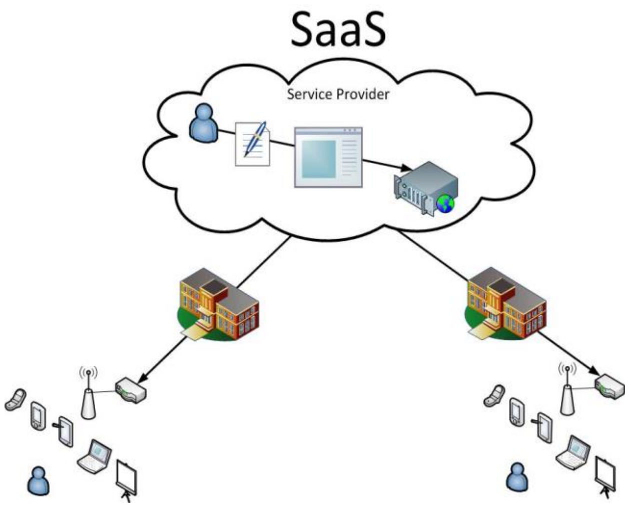


Figure 2: software as a service (SaaS)

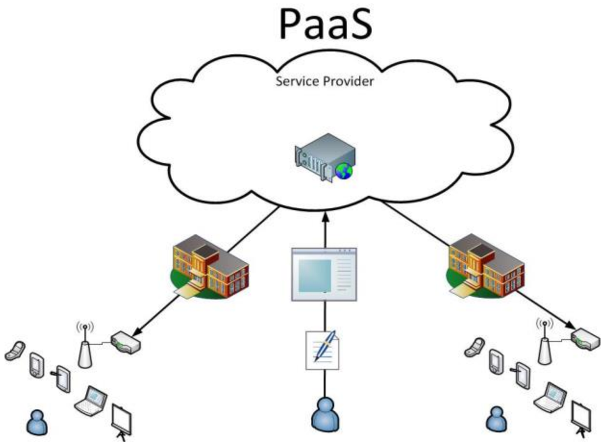


Figure 3: platform as a service (PaaS)

DSaaS (data storage as services) is an on-demand storage service. Cloud computing provides internet based on demand back up storage services to a customer. In this service, customers[8] can keep their data backup remotely over internet servers. These backup data maintenance is taken care by DSaaS service provider. Cloud DSaaS service providers are responsible for keeping the customer data confidential. Here customers need not worry on setting up the large discs array to keep their huge amount of data**.**

IaaS (Infrastructure as a Service) is an on-demand infrastructure service. It delivers the computer infrastructure typically a platform virtualization environment as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment, clients can buy those resources as a fully outsourced service [7][8].

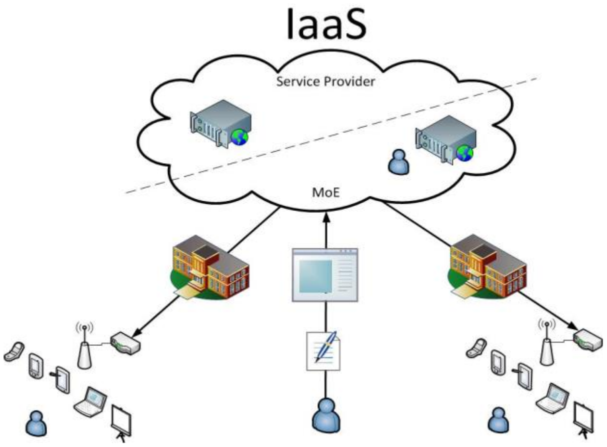
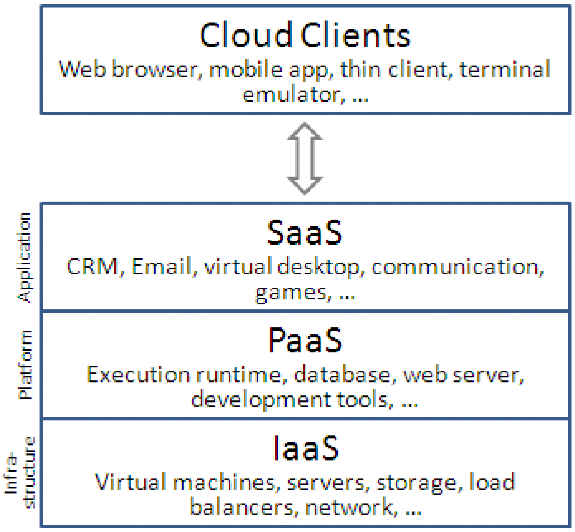


Figure 4: infrastructure as a service (IaaS)


Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...

Application
SaaS
CRM, Email, virtual desktop, communication, games, ...

Platform
PaaS
Execution runtime, database, web server, development tools, ...

Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Figure 5: cloud computing service layers

To access these cloud services securely, cloud authentication systems are using different methods like**: i) simple text password ii) Third party authentication iii) Graphical password iv) Biometric and v) 3D password object**.

The weakness of textual password authentication system is that it is easy to break and vulnerable to dictionary or brute force attacks.

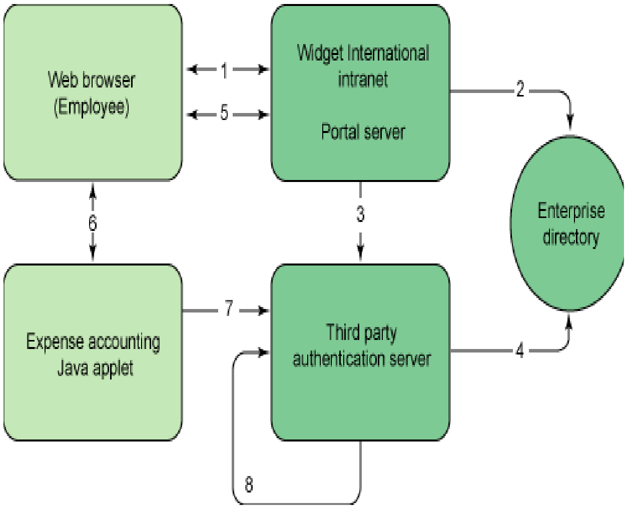


Figure 6: third party authentication

Third party authentication [3] is not preferred for smaller cloud deployment [2]. Graphical passwords have memory space that is less than or equal to the textual password space.

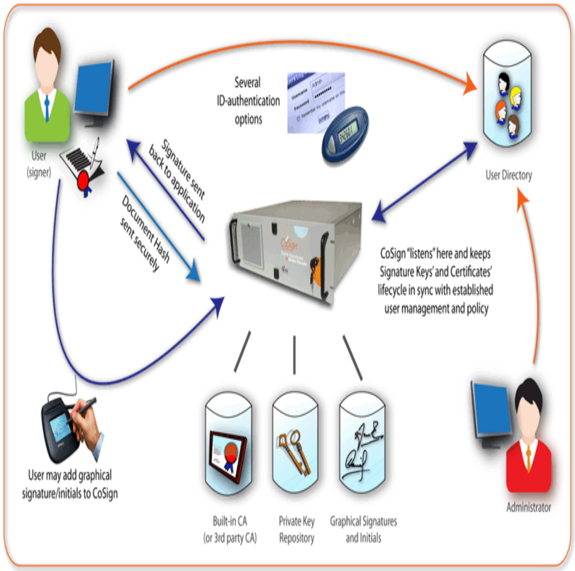


Figure 7: graphical password/signature

Graphical passwords are based on the idea that users can recall and recognize pictures better than words. However, some of the graphical password schemes require a long time to be performed [4][5]. Bio-metric authentications such as, fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition, have been proposed in literature. Each bio-metric recognition scheme has its own advantages and disadvantages based on many factors such as consistency, uniqueness, and acceptability. One of the main drawbacks of applying bio-metrics is its intrusiveness upon a user's personal characteristics. 3d password does not support the multiple levels of authentication.

Figure 8: biometric in authentication

2. Cloud Service authentication

Authentication is bigger than just user authentication in the cloud. Ultimately, all "objects" need to "wake up" and orient, which is another way of saying they need to "authenticate" their environment. Of all that has been written about cloud computing, precious little attention has been paid to authentication in the cloud. Before we get to that, let's review how authentication works on a private network [6]. When we log on to our machine and then try to access a resource, say a file server or a database, something needs to assure that your username and password are valid. If you're logging onto a windows machine, this authentication is performed by a component called the "Local security Authority Subsystem Service". If you run windows Task manager and list the running processes for all users. You will see a program called "Isass.exe" [9]. If you run likewise on a Linux/UNIX/Mac machine you'll see it is called "Isassd". Either one can authenticate a user in one of the two ways: using local credentials or using Active Directory credentials. If your machine is "joined" to

Active directory, you will typically log on with your AD account (including the appropriate domain name). If your machine is not joined to AD it is in work group mode and you log on using local credentials [2]. With the latter, your username and password are validated against account information stored on your own machine. In the AD case, however, something more significant happens: LSASS authenticates your credentials using the Kerberos protocol to talk to an AD domain controller.

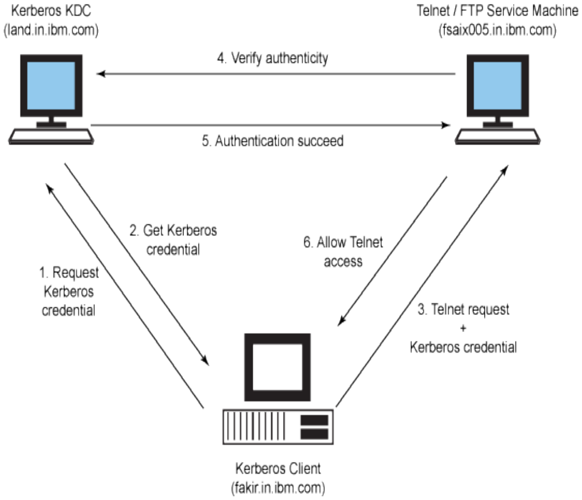

Kerberos KDC
(land.in.ibm.com)
Telnet / FTP Service Machine
(fsaix005.in.ibm.com)
4. Verify authenticity
5. Authentication succeed
2. Get Kerberos credential
1. Request Kerberos credential
6. Allow Telnet access
3. Telnet request + Kerberos credential
Kerberos Client
(fakir.in.ibm.com)

Figure 9: Kerberos authentication (protocol)

Kerberos is a wonderful thing[12]. It can authenticate credentials without ever transmitting a password in either clear or hashed form. This is important because it makes it impossible to perform offline password cracking(i.e. trying millions of passwords until the cracking code matches your hashed password) Kerberos is also great because it supports single sign-on. Once you are logged on to your machine, you have a special "ticket" that can be used to acquire additional tickets for other services.

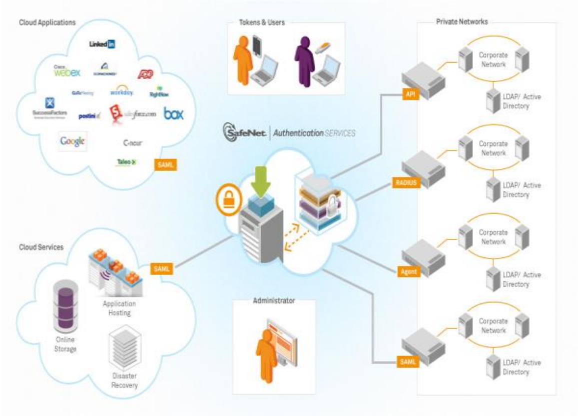


Figure 10: SafeNet Authentication service

Some of the existing authentication services are **Safe Net Authentication service, Protiva strong Authentication service** and many more. The main two factors or strong authentication is easy to implement and manage. These provide

- They provide wide range of tokens and token less authentication methods allowing each user to choose the right token type for their individual needs.
- Strong authentication can be provided anywhere a password is used today through support of industry standards such as RADIUS and SAML and the availability of API's and agents for other applications.

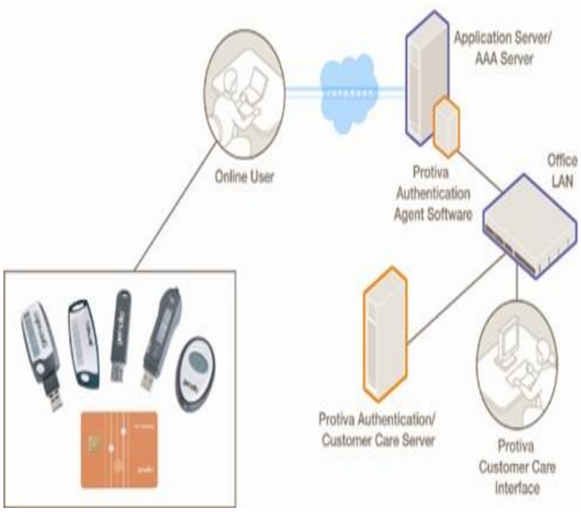


Figure 11: Protiva Authentication

- The comprehensive degree of automation in the solution drastically reduces the cost of management and administration
- The tokens do not expire and they can be reused or re-issued to new users reducing the cost of ownership and administrative burden.
- They provide comprehensive self-service portal allowing users to carry out many functions which would have traditionally been resolved.
- They support 3rd party tokens ensuring that existing investment in tokens is not lost when users migrate to our solution

3. Problems and challenges of authentication in the cloud

Now consider the cloud, or, rather clouds because we'll find several offering that fit under the cloud umbrella. Things get messy with pure public cloud options. Public cloud is generally defined as being external to the companies that use it. It is where software–as-a-service [7][8] (SaaS) type applications (typically Web based) run.

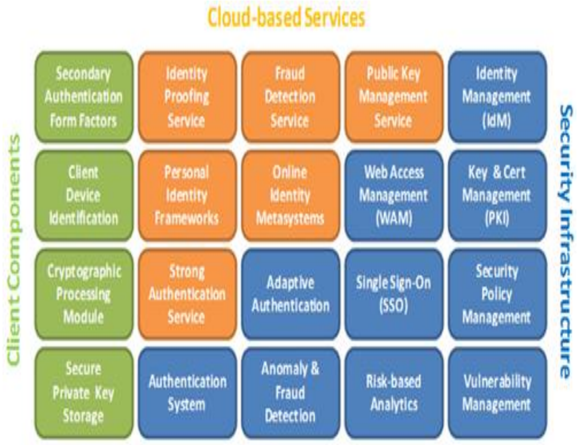

Cloud-based Services
Client Components
Security Infrastructure
Secondary Authentication Form Factors
Identity Proofing Service
Fraud Detection Service
Public Key Management Service
Identity Management (IdM)
Client Device Identification
Personal Identity Frameworks
Online Identity Metasystems
Web Access Management (WAM)
Key & Cert Management (PKI)
Cryptographic Processing Module
Strong Authentication Service
Adaptive Authentication
Single Sign-On (SSO)
Security Policy Management
Secure Private Key Storage
Authentication System
Anomaly & Fraud Detection
Risk-based Analytics
Vulnerability Management

Figure 12: cloud based services

How does authentication work in this context? When you log on to a Web application, how are your credentials validated? The answer is, unfortunately, "all kinds of ways" LDAP, database lookups, file lookups even Kerberos sometimes.

Figure 13: problems in cloud

The problem with this lack of cohesion is it makes it difficult to affect things that we take for granted in the private cloud[5][4][3]. When somebody leaves the company, how do we disable His/her user accounts on outside SaaS applications? How do users keep track of passwords for all their various applications since they don't support single sign-on? How can we enforce password policies when no two systems use the same authentication mechanism? Ultimately, we need to remove the distinction between corporate and web authentication—all authentication should be based on Internet-routable protocols and the nature of identity federation should become simpler (there should be no need for internal/external identity federation servers). This will take long time. When we do figure this out, however we should make sure that we do not lose the many benefits of our current mechanisms. Currently the various issues can be broadly classified into four issues [11]

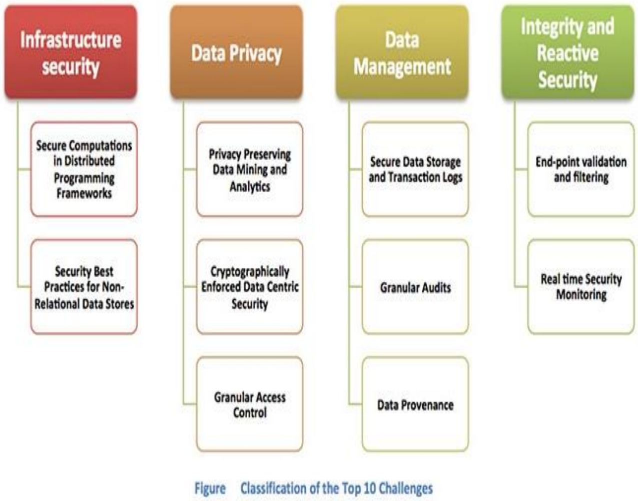

Infrastructure security
Secure Computations in Distributed Programming Frameworks
Security Best Practices for Non-Relational Data Stores
Data Privacy
Privacy Preserving Data Mining and Analytics
Cryptographically Enforced Data Centric Security
Granular Access Control
Data Management
Secure Data Storage and Transaction Logs
Granular Audits
Data Provenance
Integrity and Reactive Security
End-point validation and filtering
Real time Security Monitoring
Figure Classification of the Top 10 Challenges

Figure 14: Top 10 challenges in cloud

- Cloud service providers request customers to store their account information in the cloud, cloud service providers have the access to these information. This presents a privacy issue to the customers information

- Various cloud service providers guarantee the privacy of information; however it is difficult for the customer to check if those rules are enforced.
- If a customer uses multiple cloud services, it means that multiple copies of the user information will be online.

- Multiple accounts will lead to multiple authentication process, as each service provider will have a different authentication process.

4. Existing Schemes

In[10] **Three Dimensional Authentication Mechanisms for Secured Transfer of Data**, the authors (R.MirunaDevi,Dr.A.Marimuthu,Fawaz A Alsulaiman ,Abdulmotaleb El Saddik and Dinesha H.A) have suggested a 3 level scheme where the user first uses his finger prints(biometric) for registration, through which a secret key is generated, then the login process in initiated, it generates a graphical key, through which data can be later on encrypted and decrypted to be sent over a network, we will be using the logic for authentication for 3D signatures[13].

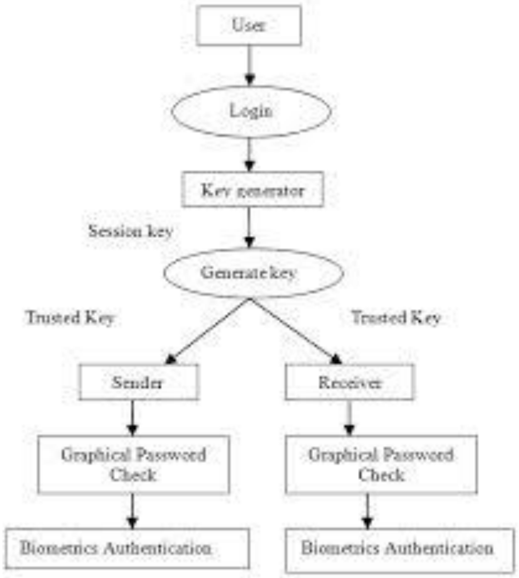


Figure 15: 3D authentication for secured data transfer

Similarly, in[a] **A Novel 3D Graphical password Schema**, the author Dinesha H.A suggests a 3D virtual environment in which the user interacts with the environment to login to any services needed by the user. The actions of the users in virtual environment are matched with patterns placed on the authentication mechanism, which will authenticate the user to avail the service [8].

Finally in [10] **3D security Cloud Computing using graphical password**, in this paper the authors suggest a 3D architecture for 3D security system where, the Ring-1 uses the scheme deployed in [10], then in ring 2, Graphical Password with Icons, where a user click on icons as their password instead of the conventional methods and the Ring 3, the Persuasive Clue Click Point, the password consist of five click points, one on each of five images.

5. Proposed scheme

A 3D graphic signature can be easily created using either Blender, which is an open source free program used to create various graphics for movies and images or using the popular paid software Adobe Creative suit, Photoshop exactly. Both the tools are relatively easy and do not require very high level of understanding of the software to create a 3D graphic signature and there are always online tutorials which give a detailed explanation on how to create a 3D graphic signature, where one can simply look up on the internet to create any kind of 3D graphic signature.

Since the signature exists in three dimensions, the size can be SxSxS. Each point in the three dimensional environment space can be represented by the coordinates (x,y,z) ∈ [1..S] x [1..S] x [1..S]. A copy of the signature along with the coordinates will be saved onto the cloud, which can be used for authentication.

During the login or authentication, two 3D graphic signatures are equal to each other when they match visually and also, the coordinates map or match similarly. Even in the case of forgery, it will be hard enough to match the signature visually, even if this is accomplished, the coordinates of the forged 3D graphic signature and the coordinates of the authentic signature match will be next to impossible.

The information content of a password space defined in [12][13] as "the entropy of the probability distribution over that space given by the relative frequency of the passwords that users actually choose". It is a measure that determines how hard the attack us, thus the selection of the design, complexity, types, etc. of the 3D graphic signature are very critical. The said factors affect the strength, usability and performance of the 3D graphic signature.

6. Comparision with other schemes.

None of the schemes in section existing schemes or proposed scheme have been actually implemented in the real world, and it is quite difficult to assess how much of an impact any scheme may have on enhancing the authentication of cloud users and boosting security and integrity of cloud services, while [10] uses a generic and secure three factor authentication , where the process starts with registration though finger print scan, many users will be quite skeptical to give away their finger prints, where there is no guarantee that it will not be misused, after which a secret key is generated, then the user needs to specify the username, password and the secret key, through which another key- the graphical key is generated and then finally the finger prints are scanned before any data exchange, the said process done not only take too much time but will require a large memory space and multiple combination of keys to be generated, it might work fine for small operations, but for large scale system, it requires large memory have an inexhaustible secret and graphical key, but it has been stated by the authors in section 3 that, most of them will require a large over head, epically in [10] and in [11], like wise in [a] it is specifically mentioned that "by increasing the number of objects in the three dimensional virtual environment, the 3D password space would increase exponentially", the same can be said on [11] as the first layer employs the same mechanism used in [8][9], this will cause a very large overhead and performance issues at both server and client side, as the memory and/or computationally need for a very large password space and virtual environment needed at the authentication stage may slow down the services, thus problem will only grow when a large number of user traffic in frequently accessing the cloud.

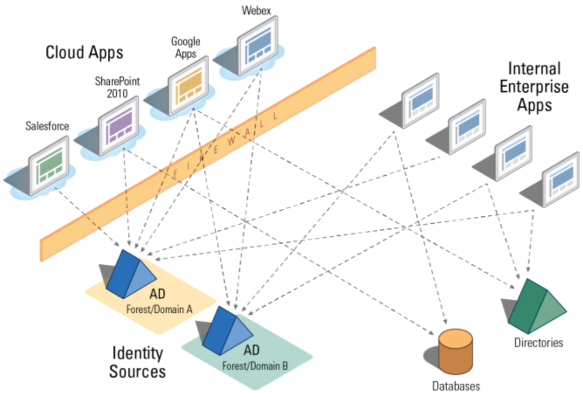


Figure 16: Other scheme

Our proposed scheme does not require a large over head in terms of space, memory or computation, as stated before two 3D graphic signatures are authentic or equal when they match visually and also their respective coordinates match or pair up similarly/equally.

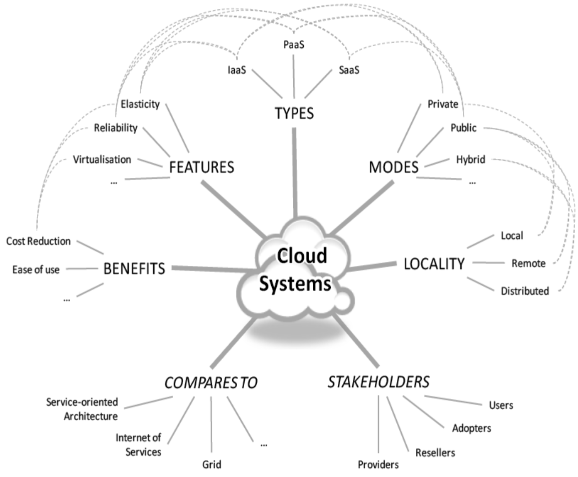


Figure 17: How it works in other scheme.

Since the coordinates will only be matched, these can be easily stored in a data structure on the server side, and whenever the user logins though his/her 3D signature it can be matched visually by any image authentication technique followed by extracting the coordinates of the given signature and match then with the coordinates already present on the server side, this will reduce time and complexity of authentication currently required, thus supporting large scale access even when the user traffic is very high. But for any scheme, a very large study on the number of people using the scheme must be carried out to truly understand how the proposed scheme will affect the authentication and security in the cloud.

7. Conclusion and future scope.

Simple text password, Biometric and token-based passwords are the most widely used authentication schemes. There have been multilevel authentication mechanisms, 3D virtual reality environment schemes being used for authentication. The motivation of this signature is to have a scheme that has a very large password space. A 3D password gives the user the choice of modeling their own signature. They won't have to provide their fingerprints or part with personal information. They can model the password on their preferences. The signature's space can be reflected by the design of the 3D graphic signature. For example, teachers can use a signature which may have pen/paper/etc embedded in the design of the signature or anything they are familiar with. The 3D signature is in its nascent stage, we can still design different 3D objects and

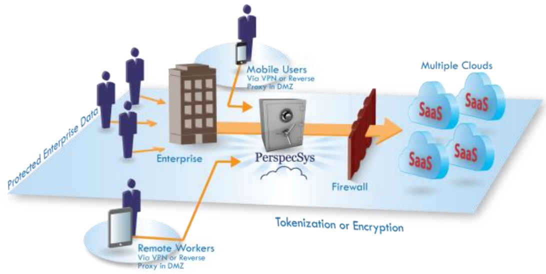

Mobile Users
Via VPN or Reverse Proxy in DMZ
Multiple Clouds
SaaS
SaaS
SaaS
SaaS
Protected Enterprise Data
Enterprise
PerspecSys
Firewall
Tokenization or Encryption
Remote Workers
Via VPN or Reverse Proxy in DMZ

Figure 18: Encryption and Decryption

Signatures with various authentication schemes.

The main application domains of 3D signatures are critical systems and resources, though it can also be applied to protect other systems, but may cause a bigger overhead for authentication.

References

[1]. IEEE – The Application of cloud computing in education informatization, madern educational tech...Center Bo Wang, HongYu Xing.

[2].NISTdefinition http://www.au.af.mil/au/awc/awcgate/nist/cloud-def-v15.doc

[3]. CA technologies cloud authentication system http://www.ca.com/us/authentication-system.aspx

[4]. X.sou,Y.zhu, G.S Owen, "Graphical passwords: A survey, "in proc. 21st Annual computer security application Conf. Dec.5-9,2005,pp 463-472.

[5] S.Wiendenbeck,J. waters, J.C. Birget, A.Brodskiy,
"Basic results using graphical password"

[6] cloud computing services and coparisons http://www.thbs.com/pdfs/comparison%20of%20cloud%20computing%20services.pdf

[7] a user identity management protocol for cloud Computing paradigm safiriyu eludioral, Olatunda abiona2, ayodeji oluwatope1, adeniran

Oluwaranti 1,client onime3,lawerence kehinde.2011,4,152-163

[8] A Novel 3D Graphical Password Schem" http://www.123seminarsonly.com/Seminar-Reports/016/51840778-04016678.pdf

[9] "THREE DIMENSIONAL AUTHENTICATION MECHANISMS FOR SECURED TRANSFER OF DATA IN NETWORKS " http://www.ijcsmr.org/vol1issue5/paper155.pdf

[10] 3D graphics for everyday communication http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1491703&queryText%3D3d+graphics+for+everyday+use

[11] Title -Multi-level authentication technique for accessingcloudserviceshttp://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6179130&queryText%3D3d+passwords

[12] Title -Three Diamentional Object Used for Data Securityhttp://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5702003&queryText%3D3d+passwords

[13] "3D Security Cloud Computing using Graphical Password” http://www.ijarcce.com/upload/january/12-%203D%20Security%20Cloud.pdf