# Risk based multi-factor authentication for cloud environments

Tjaart Bester[1], Moses Dlamini[1,2], Hein Venter[1]
[1] University of Pretoria, Pretoria, South Africa
[2]School of Computer Science, University of Kwa-Zulu Natal, Durban, South Africa
u14365848@cs.up.ac.za
{mdlamini, hventer}@cs.up.ac.za

**Abstract**: The increased availability of computing resources in conjunction with the success of the Internet has put the cloud computingparadigm at the cutting edge of a digital revolution. Cloud computing offers benefits such as high availability, on demand access fromanywhere, on any device at any time, cost saving, scalability,and etc. Cloud computing also offers a new business model that outsourcescomputing resources to a shared third party infrastructure. Cloud computing services can be classified into infrastructure as a service(IAAS), platform as a service (PAAS) and software as a service (SAAS). Delivering infrastructure, platforms or software as a servicerequires a high level of virtualization and implementation of virtual machines. Virtual machines are created, clustered together andoperated via a hyper-visor. A hyper-visor or virtual machine monitor creates a virtual platform for virtual machines and manages theexecution thereof. Cloud computing offers resources and services to users regardless of physical or geographical boundaries at anytime of day or night. However, the cloud as one of the most promising technology developments of this century is hampered by a stringof security challenges which has led to its low adoption rates, more especially for public cloud infrastructure. The low adoption rate of public clouds indicates that the business world is hesitant to make the necessary move to cloud computing due to perceived securitychallenges and vulnerabilities.

Hence, this research proposes a dynamic risk-based authentication mechanism. Securing IT-resources hosted on a public cloud, requires risk-based authentication. The proposed solution assigns a certain risk profile to each authentication attempt. The riskprofile determines the complexity of the challenge. A high risk profile requires a strong challenge and a low risk profile requires a username and password. This paper argues that authentication on the cloud can be improved by implementing a risk profile for eachauthentication attempt, as stipulated above. For example logging in from your work computer in business hours is a lower risk thanlogging in from an unknown mobile device in different country in the middle of the night. With a low risk authentication attempt, theproposed system would require a normal user to authenticate with a username and password only and this would suffice for just that particularscenario. However, as the risk increases so does the difficulty of the authentication challenge; for example, a one-time pin (OTP),supervisor authorization etc. would be required on top of the usual username and password. There is a need to improve authenticationsystems in order to assure prospective users that public cloud computing can give them competitive edge without exposing their confidentialdata to unnecessary risk of falling into the wrong hands of unauthorized third parties and threatening their business bottom line.

**Keywords:**Cloud computing,Authentication,Strong authentication, Risk-based multifactor authentication

## 1. Introduction

The increased availability of computing resources in conjunction with the success of the internet has put the cloud computing paradigm at the cutting edge of a digital revolution. Cloud computing offers benefits such as high availability, on demand access from anywhere on any device at any time, cost saving, scalability etc. (Zhang, Cheng, & Boutaba, 2010) Cloud computing also offers a new business model that outsources computing resources to a shared third party infrastructure.

Cloud computing resources may be clustered to offer public, private or hybrid networks. Private cloud: also known as internal or corporate cloud. A Private cloud is infrastructure created for a single entity but managed by a third party cloud service provider. Public cloud: is open to the general public over the internet on a pay-per-usage system. Placing systems and sensitive information into a public cloud in the middle of a hostile and open network (the internet) is seen as a risk that most companies are unwilling to take. Hybrid cloud: is a combination of at least one public and one private cloud (Onwubiko, 2010).

Cloud computing services can be classified into infrastructure as a service (IAAS), platform as a service (PAAS) and software as a service (SAAS). Delivering infrastructure, platforms or software as a service requires a high level of virtualization and implementation of virtual machines. Virtual machines are created, clustered together and operated via a hypervisor. A hypervisor or virtual machine monitor creates a virtual platform for virtual machines and manages their execution.

Cloud computing offers resources and services to users regardless of physical or geographical boundaries at any time of day or night. For example a pharmaceutical company may move their stock control and manufacturing scheduling systems to a public cloud. This will give their sales representatives across the world access to current stock levels and production schedules in real time. The move to cloud computing will allow greater monitoring and improvement to the company's logistical infrastructure. But the information contained within this system would also be very valuable to competitors trying to secure a competitive edge in the market. Securing such a system with in a public cloud requires more than single factor authentication. Risk-based authentication is non-static authentication system that assigns a certain risk profile to each authentication attempt. The risk profile determines the complexity of the challenge. A High risk profile requires a strong challenge and a low risk profile can require as little as user name and password.

**Motivation:**Authentication on the cloud can be improved by implementing a risk profile for each authentication attempt. For example logging in from your work computer in business hours is a lower risk than logging in from an unknown mobile device in different country in the middle of the night. With a low risk authentication attempt, a normal user name and password will suffice but as the risk increases so does the difficulty of the challenge for example a one-time-pin, supervisor authorization etc.(Dlamini, Venter, Eloff, & Mitha, 2012)

The low adoption rate of public clouds indicates that the business world is hesitant to make the move to cloud computing due to perceived security challenges and vulnerabilities. There is a need for cloud computing authentication to be improved and to assure prospective user that cloud computing can give them the competitive edge without unnecessary risk to their business.

**Problem:**The usage of mobile devices within the cloud computing is set to rise, even within corporate environments with the adoption of BYOD (bring you own device). Combined with the increase of different cloud services supplied by a myriad of service providers, has highlighted the need for a federated identity management with single sign-on service.How to construct a multifactor risk based authentication method with federated identity management to be used to secure cloud computing? The next section discusses related work.

## 2. Related Work

This section discusses existing authentication mechanisms for public cloud solutions. This is to demonstrate that this work is grounded on existing work and does not exist in isolation. A number of authors have already made some attempts to address the issue of weak authentication on public cloud infrastructures.

For instance, J Archer et al. (Archer & Boehm, 2009) presents some credentials (for example username and password) which are checked against registered information for said user. If the credentials match the systems values, then the user is then deemed authenticated. However, should the data store containing usernames and passwords be modified or leaked the entire system is compromised.

A. Cecil Donald et al. (Donald, Jenis, & Arockiam, 2014) proposes a novel authentication mechanism to enhance security in the cloud environment. From this work a trusted authority creates digital signatures to compare with the users created digital signatures when services are requested from a cloud service provider. This approach uses the digital signature contained in the Portuguese identity smart card. However, the challenge with this approach is that a breach or loss of confidentiality (if pin becomes public knowledge) would require the re-issuing of an ID card. This has the potential to render IT resources unavailable or inaccessible at least for the time it takes to issue a new ID card. If not done timeously could result in lost productivity.

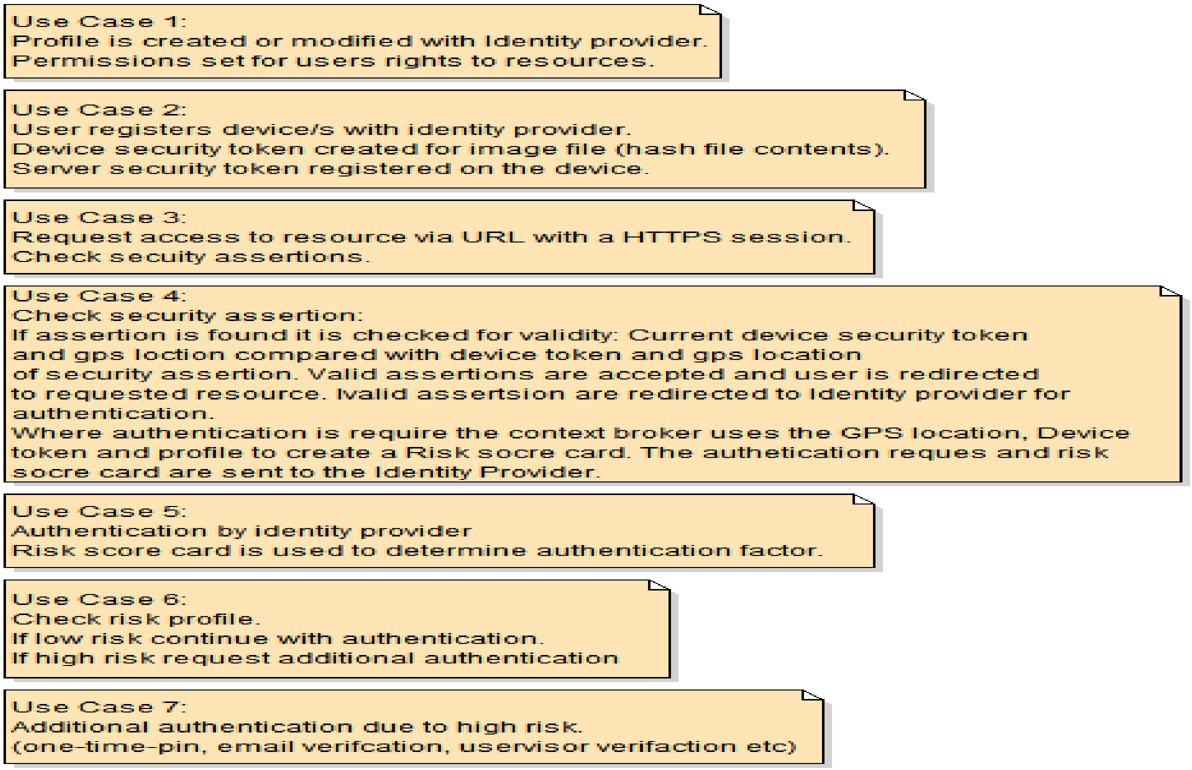
Richard Chow et al. (Chow, Jakobsson, & Masuoka, 2010) extends the knowledge base and proposes a novel authentication framework for mobile devices to cloud services. The recent history and activity is used to determine the appropriate level of authentication required. A Major issue with the high emphasis on the user's mobile device is the risk of make the device an even bigger target for theft and spoofing (as seen with internet banking theft/fraud). The use of SMS history and other information form mobile devices for authentication could be seen as an invasion of the user's privacy, possible exposing other unforeseen mobile security issues.

L. B. Jivanadham et al. (Jivanadham, Islam, Katayama, Komaki, & Baharun, 2013) proposes an integrated authentication mechanism called cloud cognitive authenticator (CCA). CCA is an application program interface (API) integrating bio-signals, one round Zero Knowledge Protocol (ZKP) for authentication and Rijndael algorithm in Advance Encryption Standard (AES). The novelty of this approach is in the two levels of authentication. The interoperability of the CCA and AES algorithm compatibility was questioned by A. Cecil Donald (Donald et al., 2014).

Liliana F.B. Soares et al. (Soares, Fernandes, Freire, & Inácio, 2013) suggests a model where a proxy VM is placed between inbound connections and cloud management interfaces. This novel approach of compartmentalizing VM's to limit the spread of security breaches. This proposed model strengthens security against inter VMattacks.The model can be extended to include multifactor authentication to improve VM access control.

## 3. Proposed solution

The following use case diagram demonstrates the proposed solution and illustrates how authentication could beapproached in order to prevent unauthorised access on the cloud.



Use Case 1:
Profile is created or modified with Identity provider.
Permissions set for users rights to resources.

Use Case 2:
User registers device/s with identity provider.
Device security token created for image file (hash file contents).
Server security token registered on the device.

Use Case 3:
Request access to resource via URL with a HTTPS session.
Check secuity assertions.

Use Case 4:
Check security assertion:
If assertion is found it is checked for validity: Current device security token
and gps loction compared with device token and gps location
of security assertion. Valid assertions are accepted and user is redirected
to requested resource. Ivalid assertsion are redirected to Identity provider for
authentication.
Where authentication is require the context broker uses the GPS location, Device
token and profile to create a Risk socre card. The authetication reques and risk
socre card are sent to the Identity Provider.

Use Case 5:
Authentication by identity provider
Risk score card is used to determine authentication factor.

Use Case 6:
Check risk profile.
If low risk continue with authentication.
If high risk request additional authentication

Use Case 7:
Additional authentication due to high risk.
(one-time-pin, email verifcation, uservisor verifaction etc)

Figure 1: Use case commentary

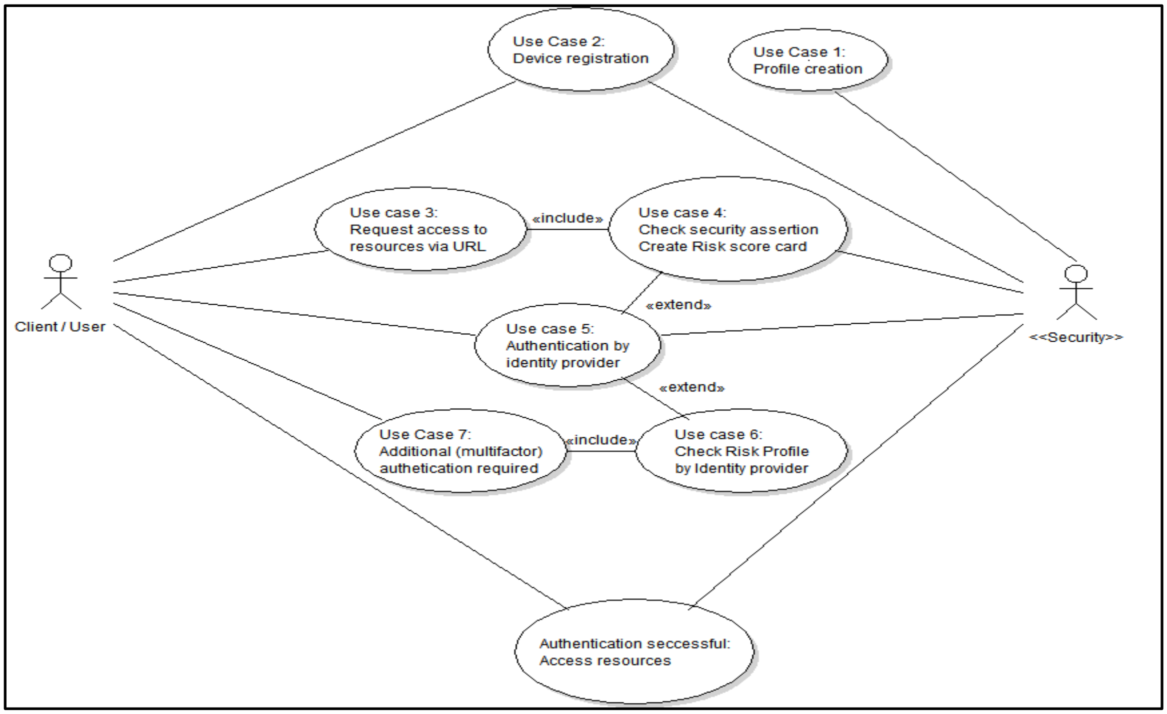


Figure 2: Use case diagram of a risk-based multi-factor authentication for cloud environments

### 3.1 User profile registration:

A user profile is created on the identity provider by the cloud service provider security team with the applicable user rights to the cloud resources. This profile is also registered on the context broker to be used when creating a risk score card for an authentication request. The profile credentials, username and temporary password is sent to the user via encrypted email. From the email the user is redirected to the identity provider for changing of their password and device registration.

### 3.2 Changing the user password:

After initial authentication the user is prompted for a new password. The new password must comply with the password strength requirements of the identity provider.

### 3.3 Device registration:

After authentication is completed with the identity provider the user is requested to select an image or any file should an applicable image file not be available. The selected file's contents are hashed to create a token that is registered on the device and with the identity provider. The device is allocated a unique device number which will be used in conjunction with the device security token as authentication for the device. The security token for the server is also registered on the device at this time.

### 3.4 User requests for access to a resource on the cloud:

The resource is requested via a URL and is checked for a security assertion. The URL points to the cloud proxy server, should the security assertion be valid the proxy server will load the request resource from the cloud, ensure the user has a smooth single sign on experience. If the security assertion is not found or is invalid the proxy server will prompt the user for authentication details (username, password) the GPS location and device security token will also be collected. The context broker creates a risk score card based on the user profile (username), GPS location, unique device number and encrypted device security token which is sent with the authentication request to the identity provider for authentication.

### 3.5 Encryption and evaluation of the device security token:

A random value like a date time stamp is added to the device security token and hashed again. When the identity provider checks the device security token the same random value is added to the token registered with the identity provider for the specific unique device number and hashed, the result is checked against the encrypted token value of the request. This will ensure that device security token is not visible when sent for authentication.

### 3.6 Creation of the risk score card:

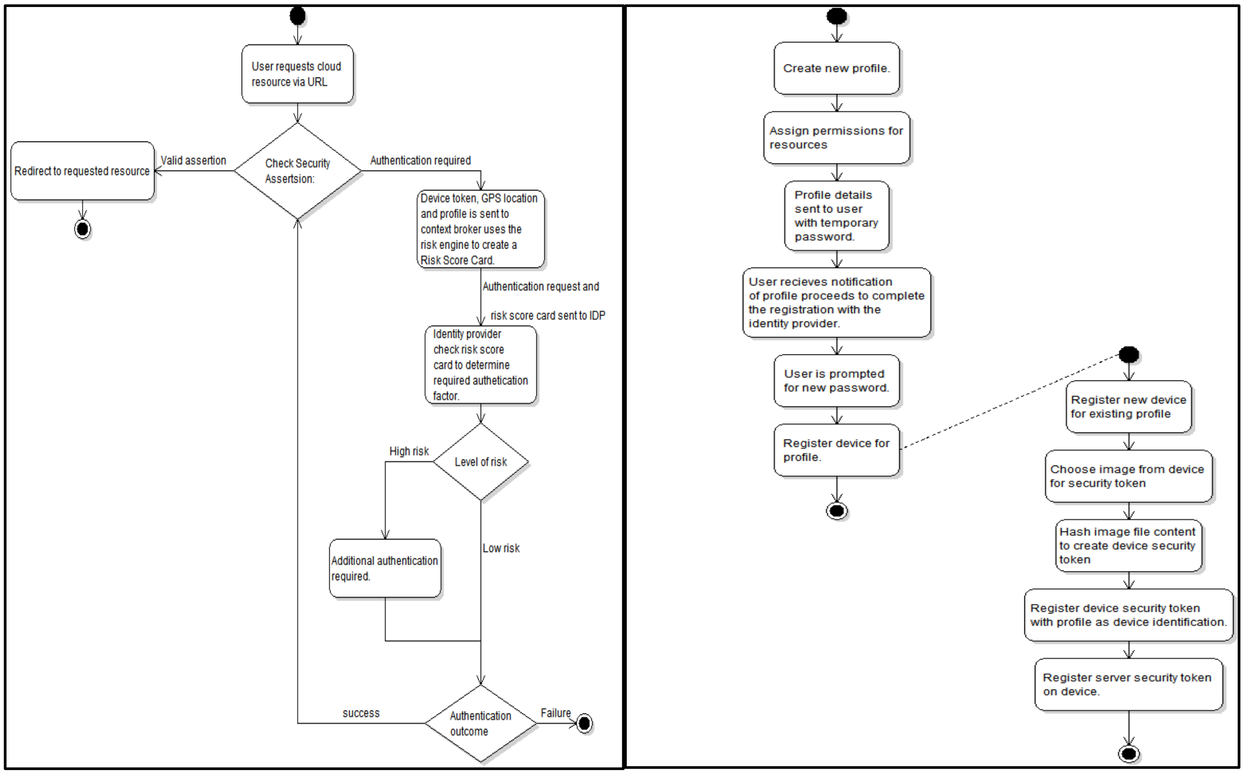
The context broker supplies the risk engine with the profile, GPS location (of the requesting device), unique device number and encrypted device token. The risk engine uses the unique device number to retrieve the stored device security token from the profile. The same random value is added to the registered device security token in this case the date time stamp of the authentication request and hashed in the same way then the results compared. If the result of the comparison shows a difference the risk on the score card is increased. Should the GPS location fall outside of thresholds the risk is also increased on the score card.

### 3.7 Risk score card used by identity provider:

On receiving an authentication request by the identity provider, the risk score card is checked for level of risk. In the event of a low risk score card the authentication is completed with the username and password. Should the risk score card show high risk the applicable additional authentication factor is requested from the user (i.e. one-time-pin etc.).

### 3.8 Additional authentication factor:

Should the risk score card indicate high risk, a system generated one-time-pin will be logged at the identity provider and sent to the users email via an encrypted email. Once the one-time-pin has been logged a notification and an input field will be shown on the user's browser. Should the user fail to enter the one-time-pin before the time-to-live expires the authentication request is failed and discarded.


User requests cloud resource via URL
Check Security Assertsion:
Valid assertion
Redirect to requested resource
Authentication required
Device token, GPS location and profile is sent to context broker uses the risk engine to create a Risk Score Card.
Authentication request and
risk score card sent to IDP
Identity provider check risk score card to determine required authetication factor.
High risk
Level of risk
Low risk
Additional authentication required.
success
Authentication outcome
Failure
Create new profile.
Assign permissions for resources
Profile details sent to user with temporary password.
User recieves notification of profile proceeds to complete the registration with the identity provider.
User is prompted for new password.
Register device for profile.
Register new device for existing profile
Choose image from device for security token
Hash image file content to create device security token
Register device security token with profile as device identification.
Register server security token on device.

## 3.9 Authentication overview:

The user tries to access a resource on the cloud (in this example a hosted VNC connection to a VM hosted with the cloud) using a URL from his/her registered device. The URL points to the cloud proxy server that hosts the VNC connections via Guacamole: clientless remote desktop gateway.

The gateway is single sign on enabled via SAML2.0 security assertions. The user doesn't have a valid assertion and is prompted for a username and password, unbeknownst to the user the browser is queried for GPS location, device unique number and encrypted device security token. The SAML 2 authentication request is constructed and the context broker is used to generate a risk score card. The risk on the score card is set to high because the GPS location falls outside of the threshold for the specific profile.

Using the risk score card the identity provider determines what authentication factor is requires, in this case a one-time-pin is emailed to the address registered on the user's profile. The user has a fixed amount of time to supply the correct one-time-pin to the identity provider. The user supplies the required one-time-pin within the time limit and access to the VNC connection via the gateway is granted.

**Conclusion:**

Given the delivery of on demand resources to the exact needs of the business world at any time, cloud computing is set to change the fundamentals of provisioning IT resource in the near future. Although an exciting prospect, it also presents unique challenges towards securing the cloud-hosted resources over a hostile environment (the Internet). This paper has made attempts to enhance the understanding of the challenges and implications thereof, particularly that of failing authentication systems. The authors deduced that determining the risk profile of any authentication request to the cloud computing resources is a fundamental step towards a robust security implementation. Hence, this work proposed a risk-based multifactor authentication for the cloud environment to help prevent unauthorized access to cloud hosted resources.

**References:**

Archer, J., & Boehm, A. (2009). Security guidance for critical areas of focus in cloud computing. *Cloud Security Alliance*, 0–176. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:SECURITY+GUIDANCE+FOR+CRITICAL+AREAS+OF+FOCUS+IN+CLOUD#1

Choudhury, A. J., Kumar, P., Sain, M., Lim, H., & Jae-Lee, H. (2011). A Strong User Authentication Framework for Cloud Computing. *2011 IEEE Asia-Pacific Services Computing Conference*, 110–115. doi:10.1109/APSCC.2011.14

Chow, R., Jakobsson, M., & Masuoka, R. (2010). Authentication in the clouds: a framework and its application to mobile users. *… Workshop on Cloud …*. Retrieved from http://dl.acm.org/citation.cfm?id=1866837

Dlamini, M., Venter, H., Eloff, J., & Eloff, M. (n.d.). Security of Cloud Computing: Seeing Through the Fog. *Computing*. Retrieved from http://www.satnac.org.za/proceedings/2011/papers/Internet_Services_and_Applications/178.pdf

Dlamini, M., Venter, H., Eloff, J., & Mitha, Y. (2012). Authentication in the Cloud: A Risk-based Approach. *University of Pretoria*. Retrieved from http://www.satnac.org.za/proceedings/2012/papers/8.Data_Centre_Cloud/108.pdf

Donald, A., Jenis, A., & Arockiam, L. (2014). An Authentication Mechanism to Enhance Security in the Cloud Environment, *4*(5), 3278–3281. Retrieved from http://inpressco.com/wp-content/uploads/2014/09/Paper353278-3281.pdf

Ghazizadeh, E., & Manan, J. A. (2012). 2012 IEEE 4th International Conference on Cloud Computing Technology and Science A Survey on Security Issues of Federated Identity in the Cloud Computing, 562–565.

Jivanadham, L. B., Islam, a. K. M. M., Katayama, Y., Komaki, S., & Baharun, S. (2013). Cloud Cognitive Authenticator (CCA): A public cloud computing authentication mechanism. *2013 International Conference on Informatics, Electronics and Vision (ICIEV)*, 1–6. doi:10.1109/ICIEV.2013.6572626

Kantarcioglu, M., Bensoussan, A., & (Celine) Hoe, S. R. (2011). Impact of security risks on cloud computing adoption. *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 670–674. doi:10.1109/Allerton.2011.6120232

Soares, L., Fernandes, D., Freire, M., & Inácio, P. (2013). Secure User Authentication in Cloud Computing Management Interfaces. *Di.ubi.pt*, 6–7. Retrieved from http://www.di.ubi.pt/~mario/files/2013-IPCCC.pdf

Yang, J. (2013). A user authentication scheme on multi-server environments for cloud computing. *2013 9th International Conference on Information, Communications & Signal Processing*, 1–4. doi:10.1109/ICICS.2013.6782791

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7–18. doi:10.1007/s13174-010-0007-6