ISSN No. 0976-5697

Volume 3, No. 1, Jan-Feb 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Security Design for Cloud Computing: An Implementation of an On Premises Authentication with Kerberos and IPSec within a Network

Mahmoud K.I Umar* and Xiaochun Cheng
Middlesex University
United Kingdom
mu117@live.mdx.ac.uk
x.cheng@mdx.ac.uk

Abstract: Cloud computing in the last few years has elevated to become a promising business concept to a lot of IT industries and even corporate industries too. It has raised IT to a higher level by offering environment data storage and a flexible computing processing power that is capable to help industries to be elastic to demand and supply, while reducing capital expenditure. However, the problem now is organizations are cautious about security; concerns always arise as soon as one begins to run applications that are far from within its own network. It has been shown that there exist a lot of security risk with cloud computing. This paper proposes a solution that can be adapted by large corporate networks. The existing authentication infrastructure will be used to enhance security of the cloud services.

Key words: Cloud computing, SSO, Kerberos, AD, IPSec.

I. INTRODUCTION

Over recent years, research shows that there is much bigger growth in cloud computing among companies with higher revenues. This is because they have seen the financial value –lover costs, economically scalable and easier to budget for in general. But with this comes security concerns of cloud computing. Whose responsibility is to provide the security to the cloud service and to what level? What will be the effect since cloud computing is more virtual than physical have on the companies' perspectives? So companies are left with huge holistic policies to accommodate both the physical and virtual infrastructure to avoid overwhelming their IT departments with specialized solutions.

Two decades ago, cloud computing was just a new concept being talked about by the computing world, the Internet then was referred to as the cloud and even illustrated in flow chats when explaining the Internet because was a form of decentralized architecture which took information in and will route it somewhere over invisibly to a final destination.

After decades, now cloud computing is more of a reality than it was before. But despite its growth and popularity, it still falls on significant concerns with security about them. Mariana Carroll, Alta van der Merwe and Paula Kotze (2011) have showed that information security in cloud computing is at a critical level of 91.7%, to show how adequate protection is needed [1]. So this kind of risks leads to corporate executives worrying about keeping data safe and available since it's a business place. They see that cloud service providers will not be well-educated to their companies specific regulatory needs. So we can say cloud computing presents a new cultural mind set for IT experts. The inability for the user to physically touch servers brings a lot of uncertainty.

So the biggest concern with cloud computing is security and privacy. The idea of handing over crucial data to a third party worries most people. Corporate organizations might hesitate to taking advantage of the technology. The purpose of this paper is to improve the authentication method of cloud computing infrastructure without compromising any of its security. Moreover, bring about new ways of designing an authentication in a cloud infrastructure using the available method available in a corporate network.

II. BACKGROUND

A. *Cloud Computing:*

Cloud computing has been compared to the early proliferation of electricity. People did not want to rely on their own source of power to run homes, businesses and towns. They began to connect to power grids, which is controlled and managed by power utilities. Together with this utility connection came time and cost saving, in addition to greater access to electricity, and more reliable availability.

So, the main goals of cloud computing is trying to develop a complete architecture to meet IT needs. Commercial companies will no longer have large IT departments, which try to cater for all the company's IT needs. The cloud provider will handle this entire task. Companies will no longer have to allocate large percentage of resources and time to building and maintaining complex IT infrastructures.

There are three main types of cloud computing services:

a. ***Software as a Service*:** End-users usually or use to acquire software and its license in order to install on their hard disk and use it. However, in the cloud users do not have to acquire the software rather they make payments based on pay-per-use model. It supports multi-tenant, which means the software can be share amongst more than one user but logically it's unique for each user [2].

b. ***Platform as a Service*:** This category allows users to develop applications with a development environment provided by the cloud provider. Developers will use

the provider's block of codes to create their own applications.

c. ***Infrastructure as a Service*:** from its name, infrastructure is provided as a service to a user where it is delivered in a form of technology, datacenters and IT services to the user.

B. Kerberos:

Kerberos was developed in the MIT labs in the 1980s to provide authentication and security facilities. It is based on the Needham and Schroeder symmetric key protocol [3]. The main goals when Kerberos was designed, was to be secure from any kind of eavesdropping, reliable especially for distributed server architecture, transparent to the users and to be scalable. It helps to avoid the normal security problems of replay by inserting time stamps with messages, thus ensuring that each message exchanged is fresh.

Kerberos issues clients credentials that allow them to get access to services in the network. The credentials are made up of a ticket and a session key. The tickets identify a client to a particular service. Each ticket contains the clients ID and network address, the end of time value, and a session key. The validity of a ticket is usually set to 10 hours but can be change to the validity time needed. In Kerberos architecture, there is the Key Distribution Centre (KDC) that issues tickets for accessing the TGS and the Ticket Granting Server (TGS), which issues the service tickets. An Authenticator is added to the tickets which contains the client ID, timestamp, and a checksum. Here is a view of the authentication process:

a. Alice: the client requesting service
b. Bob: a file share Alice would like to access
c. Key Distribution Centre (KDC): the Kerberos server that issues TGTs
d. Ticket Granting Server (TGS): the Kerberos server that issues Service Tickets

C. IPSec:

IPSec was designed to add encryption to the Internet protocol (IP) over the network [4]. IPSec [5] is an IP layer protocol that enables cryptographic protection of any kind (TCP, UDP etc.) without modifying them when sending or receiving. IPSec provides to distinctive kinds of cryptographic services. Either it can provide confidentiality or authentication with integrity or it can provide authentication only [6]:

a. AH (Authentication Header)
b. ESP (Encapsulated Security Payload)

AH adds a header (Authentication Header) to the message when it's applied. The main contents in the authentication header are the security parameter index (SPI) and authentication data. The SPI provides the security association (SA) that was used over the packet for the destination address to know which SA to apply to the packet. There is also the Integrity Check Value that helps to show that a packet kept its integrity [4]. AH adds a new IP header to the packet and protects the original, this will help stop IP spoofing.

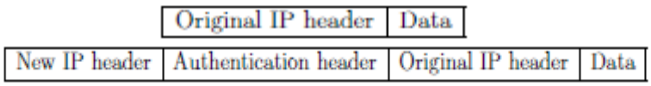

Figure 1: AH encapsulation of a packet

ESP is the most complex amongst the two methods. It introduces three headers into the packet: ESP header, ESP trailer, and ESP auth. The SPI and sequence number are found in the ESP header. The ESP trailer has the padding information and next header field that shows the ESP data filed, ant ESP auth for authentication data. It protects the payload in transport mode for protection and the inner datagram in tunnel mode. However, it does not protect the sequence number by encryption.

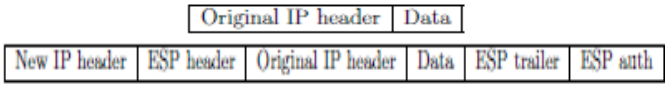

Figure 2: ESP encapsulation of a packet

The figure illustrations where adapted from M. Jarvinen's thesis paper [4]. IPsec can be uses two modes. There is the transport mode and tunnel mode [5]. Transport mode is used between two hosts. It is used to protect layers above the IP layer in the OSI. Tunnel mode is used between two gateways to protect IP layer and the layers above it. The following sub chapters below will show the differences between the two modes.

III. RELATED WORK

A search of literature shows that not much of a coordinated effort has been made to this kind of authentication design. This might be due to organizations preferred to use grid computing since they are well in a good financial situation so the design might have not been looked into more. Nevertheless, some cloud providers do offer it with their services [7] [8]. And a paper by the Citrix Labs also had some work, which was a blueprint that can be used with their technology [9].

Providers that offer authentication methods similar to the design proposed is Safenet, which is a cloud provider for SaaS. It offers a multi-factor authentication which helps organizations leverage a unified authentication method for their infrastructure for both cloud based services and on premises services with a centralized, comprehensive way to manage all access methods and policies. Multi-factor authentication uses one-time passwords (OTP) tokens or certificates to authenticate. Identification of users between the on premises and cloud based solution uses SAML protocol. This is possible by allowing their users to access enterprise cloud services that are available such as Salesforce or Google apps. With multi-factor authentication for SaaS services, it makes it much easier for organizations to maximize their authentication security.

Citrix labs also proposed a blueprint of an authentication method that allows a user from a cloud provider get access to data on his corporate network (work place). The main aim of their project was to allow Amazon EC2 to get access to a corporate data without affecting performance, security communication, support between the technologies and having a bi-directional connection. But the problem was that allowing accesses to the corporate network no auditing and logging of user activity is done which can be hazardous to an organizations data security.

There are a lot of articles and journal reports on cloud computing security, but as stated earlier, there was no much-related work that was done on the specific kind of design. So

I reviewed authentication methods that are immensely used by corporate organizations when authentication users in cloud computing and protecting their data and credentials. These methods will be explained through the paper.

D. Trusted Computing:

Cloud computing provides ways that enable large-scale data sharing and interoperations among resources that may be located on different networks [10]. Therefore, security becomes a major importance in cloud infrastructure; to ensure only the right authorized people get access to it. Therefore, cloud-computing environments should have trust amongst their selves because cloud users change dynamically. Trusted computing was designed or brought about to tackle these security worries, since hackers develop new approaches to getting into systems [11]. Trusted computing brings about the integration of security into core operations, not only being an add-on to the application. To achieve this, researchers proposed using TCP to provide that security mechanism and incorporating it in as a service.

TSS components is the part of TCP that can be enabled in cloud computing. It acts as a bridge between the application and the hardware [10]. Whenever called, it provides some basic security functions modules. The problem with this method for security is even though it provides security; there might still be features that can be abused. If configured to stop a particular kind of system breach, it may not stop another. Again, a trusted computer can be untrusted due to the tree it falls on to that system. Lastly, the attestation model for TCG's design can equally effectively prevent the software on a computer from being changed deliberately by the computer owner or administrator of the network.

E. Identity and Access Management:

Identity and Access Management (IAM) is a method of cloud security that is used to provide an adequate level of protection to resources and data by the use of rules and policies that are enforced on users either by enforcing log on passwords, given or assigning privileges to users and by providing of user accounts. IAM helps in providing authentication, authorization and auditing for users accessing the cloud. There are certain protocols and standards that are used for managing identity with IAM [2]. The once that we will consider are Security Assertion markup Language (SAML) and Open Authentication (OAuth) protocol.

a. SAML:

SAML is based on XML standards [12] used as a means of getting authorization and authentication of a user. In the case of cloud services, that is exchange between an Identity provider (IDP) and cloud service provider (CSP). The main idea or goal of SAML is to achieve SSO support using the Internet. It supports digital signatures and encryption. The figure below [13], show the authentication exchange.

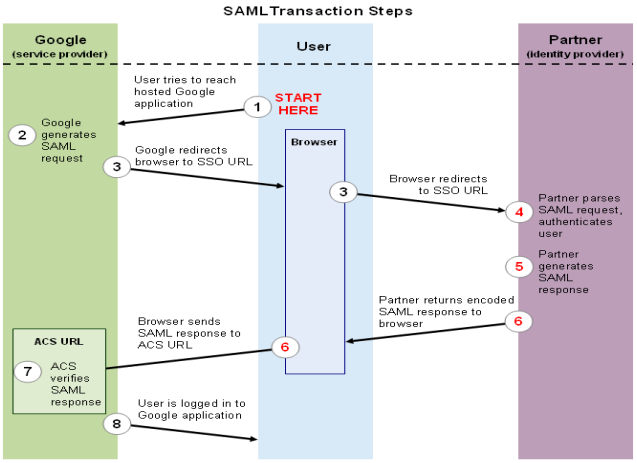

Figure 3: SAML Authentication

b. Open Authentication (OAuth) Protocol:

OAuth is an interactive protocol that allows users to share their resources that are located on one CSP with another CSP without exposing the personal identity info of the user [2]. The main objective of the protocol is to authorize access to a secure application that is based on open source implementations. From a CSP point of view, it provides a service that users can use to access applications that are hosted on different service providers without disclosing their personal credentials.

In the figure below, it illustrates the communication process between the user and the service provider and its steps [13].

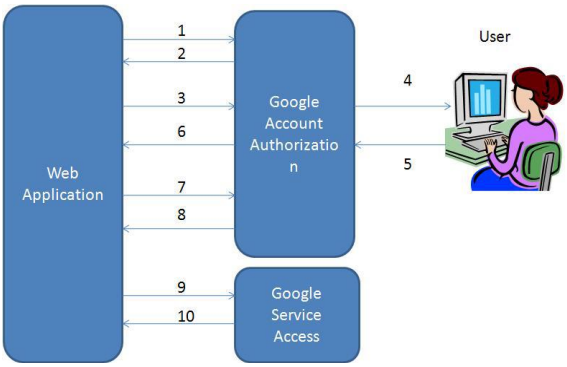

Figure 4: OAuth Authentication.

i. The application asks the Google Authorization for an OAuth token.
ii. An unauthorized token is sent back.
iii. The application will then direct the user to the Google Authorization for an authorized token.
iv. User will get access to Google Authorization to verify their identity and then to allow or deny the application to get access to their data.
v. If denied by the user, the user will be directed back to the Google page not the application.
vi. If granted access, the user will be directed to the application with the authorized token.
vii. This token will be exchanged between the application and Google Authorization.
viii. Google will verify and return an Access token.
ix. The application will then request for the user data from Google.

x. The request is verified by Google Authorization and if the access token is valid for the data asked, it will be provided.

IV. IMPLEMENTATION

The method I am proposing is a hybrid model of authenticating a user within a corporate network when accessing cloud services over the Internet, which is provided to the network. This is a method that is put in place and enforced within the corporate network (Note: its note for public access just for the employees within an organization). It acts as the gateway to accessing any cloud service provided to the particular organization. This will limit the amount of credentials passed over the Internet for authenticating a single user. It will help to audit the people getting access to which service.

I will use a Kerberos authentication for users to get access to a home portal that is located within the corporate network. The home portal acts as the gateway to the cloud service provided to the corporate network, users would be able to choose a cloud provider that is affiliated with the organization and choose a service. When accessing the services, I would use the SSO function that is a part of Kerberos to get access to the services without any log in request by the cloud provider. To provide a secure channel for communication between the corporate network and the outside network, an IPsec tunnel will be created. In addition, when there is a packet returning to the network, the tunnel will be down to the client computer. Therefore, we will be using both Main mode and Transport mode in our IPsec implementation. To have a control over who gets access to a cloud service, there will be a form of access control on the network that won't allow the user to get Tickets for accessing the cloud service.

The main idea to my work is to reduce the risk of any attack or security hazards to an organizations data and communication to a cloud provider over the Internet. So an on premises method of authentication is introduced to the scenario that will enable a SSO to the cloud services over the Internet to reduce any user credentials and organizational identity given away in the cloud (Internet) and maintain a secretive way (encryption) of data exchange throughout the course of communication.

A. Implementation:

The environment for this cloud computing model of authentication is based on the Ethernet. We construct a basic client-server connection of corporate network, and then connect an outside server. The server located outside acts as the gateway of the cloud provider. The will be a node within the cloud provider's network. The client and servers are connected through switches and routers. The server within the corporate network will act as a portal for the clients in the network and will have an Active directory (AD) database.

a. Implementation Flow:

When a user wants to get access to a cloud service, it needs to login to the home portal of the corporate network.

When connecting the user enters a username and password, this will enable the user to get a ticket from the KDC, if the user is registered in the AD of the network and the credentials entered are correct. The LDAP is use as a bridge to allow the application to get access to users from the AD [15] [14]. Microsoft's AD stores the Kerberos database in its LDAP store. Once logged on, the user will be able to view the home portal where access to the cloud service provided to the corporate network is available. This process is shown in the figure below.

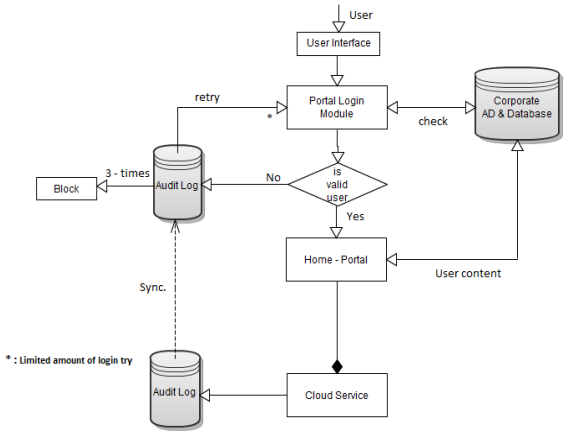

Figure 5: Flow chart of the design model.

For a user to get logged on to the network, the user has to identify itself being a credible user and the server also has to show it's the right server being accessed. This is why tickets are used which implementations are found in Kerberos. The Kerberos will authenticate with the AD, and in order to do so a user will authenticate to the AD. The user supplies a valid LDAP path. This path can be represented as follows within the web.config file of the code:

<connectionStrings>
<add name="ADConnectionString" connectionString="LDAP://cloudusers.project.com/OU=Users,DC=cloud users,DC=project,DC=com" />
</connectionStrings>

The argument above lets the application when running go to the specific location in the AD to get the user and the group it belongs to in the network. Communication between the two entities (I.e., user and the server) will lead to series of exchange of messages, which are encrypted both ways by the client user and the server to authenticate each other.

But the important aspect of the project is how the SSO occurs to get access to the cloud service. In the figure 8 shows the procedures that take place for a user to get access to the services. When a user initially logs on to the workstation to get access to the home portal, Windows authentication is applied which uses Kerberos (Step 1). It verifies a user against their Windows credentials in the AD (Step 2). The AD checks the users group and policies that it's under. If the user is valid access is granted to the home portal. Once authenticated, the user's identity is retrieved from the database (Step 3) and retrieves the list of applications the user is allowed to get access to from the available cloud services. From the initial log in and authentication, it triggers a creation of tokens that will be used to get access to the services over the Internet with SSO (Step 4). When the user tries to get access to a particular service, it checks the users token if it valid and allows access if it's valid. The form authentication is formed also at the cloud provider end which if a user is not from the corporate

network has to log on a username and password to get access to the service provided.

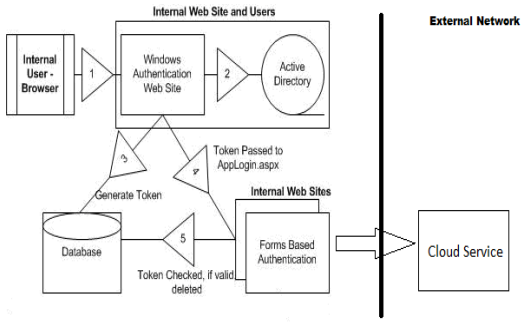

Figure 6: Modes of Authentication

To establish a connection to the cloud services over the network and allow the SSO to work, the cloud provider should have a realm trust with the corporate network. But the trust should be established one-way outgoing trust from the corporate network. This will only allow users from the corporate network to get in but no one from the cloud providers can get access to the corporate network.

After the entire authentication, traffic going through and from the network has to be protected. Therefore, we create a VPN with IPsec for traffic going out of the network to the cloud provider's network and back to the corporate network. Decided to go with IPsec because its transparent to the user and the application unlike SSL, which is a part of my project scope. All users workstations have to be IPsec enabled to have an SA that will allow a transport mode connection to the home portal webserver. Within my SA, ESP will be used to provide both confidentiality and integrity for packets going out. But when returning as an incoming AH should be applied. The servers also have to be IPsec enabled to be able to deal with any IPsec traffic. Between the gateway servers, the SA to be agreed on is tunnel mode. Here both ESP and AH will be applied. ESP will be applied first to the packets, then AH to protect the destination IP address. Before this would be a problem if it comes across any firewall that is NAT enabled. To solve address problems there is a NAT Traversal (NAT-T). It works by sensing that a NAT connection will be to translate and subsequently to encapsulate the entire IPsec packet into a UDP packet with a normal UDP header. It handles UPD flawlessly. NAT-T works well but requires that both ends of IPsec connections understand the protocol so as to properly pull out the IPsec packets out of the UDP encapsulation.

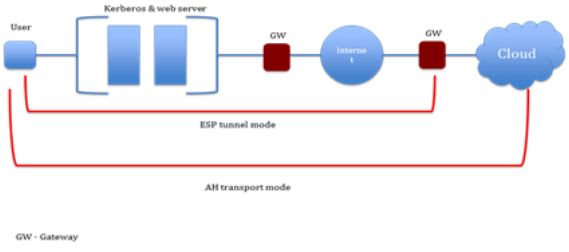

Figure 7: Network Architecture with IPsec.

The two gateways (GW) each are all located in the vicinity of each network so that the GW will be able to sync data when need to for auditing. IPsec configurations are done to my own specifications and needs. The SA's may vary depending on how a network administrator wants to configure his own network or even how traffic is treated on that particular network they control. In general this design model will have to adapt to the initial organizational network structure to reduce or minimize any complexity to the entire design.

V. DISCUSSION

After implementing the hybrid Model authentication proposed, certain limitations and development problems occur. First of all, the database implementation keeps having problems when accessing the other database from the cloud provider side. So I changed that and implemented group policy that was available on windows servers [15]. So when a user is not being allowed to get access to the service from the group policy put in place will let the user know if access is granted or not. But with a better understanding of the operating system, the use of database will be possible.

Now to address how well our design can solve common threats for cloud computing, we will compare with used authentication methods used for cloud services. It will help evaluate the model designed and implemented with current available authentications methods. This is will be based on research done on the authentication methods. Will use a grade mark for each authentication method on the threats mentioned in the CSA paper [16].

Table 1: Threat Analysis Table

	Cloud Threat							
	Threat 1	Threat 2	Threat 3	Threat 4	Threat 5	Threat 6	Threat 7	AV.
Kerberos & IPSec	3	2	1	2	2	2	3	2
IAM	1	1	2	1	1	1	2	1.3
Trusted Computing	2	2	1	1	2	1	2	1.8

0 – Poor, 1 – Fair, 2 – Good, 3 – Satisfactory.

a. Threat #1: Abuse and Nefarious Use of Cloud Computing: Our implementation helps to reduce the amount of service misuse because of the access control added to the system. That is why it gets a relatively high point that the other authentication methods.

b. Threat #2: Insecure Interface and APIs: While most providers try to ensure security is well integrated into their services, it is also critical for the consumers to understand the security implications associated with the usage of the cloud service. With our Kerberos and IPsec implementation, we able to limit this by enforcing strong authentication and access control in implementing. However, we won't understand much of the dependency chain of the associated with the API since is being provided to the consumer.

c. Threat #3: Malicious Insider: For our kind of implementation this is a strong weakness, because the impact malicious insiders can have on an organization is considerable. Once you can get access an authenticated within the network, you can have access to the cloud services. This brings in the human factor, which will bring a big limitation of this system.

d. Threat #4: Shared Technology Issues: Our implementation will have to share the same authentication technology to work, so this makes it

strong from any issues concerning technology interoperability. Kerberos we used is well implemented to support different Operating systems, and IPsec works with the used technologies available as long as they are installed on the systems.

e. Threat #5: Data Loss or Leakage: This problem exist in most systems not only cloud services. Data loss can have a devastating impact on a business. That is why back up is initiated in a lot of big business now. Our implementation helps to reduce this by providing encrypting and protecting integrity of data while in transit. With the on premises KDC, we have strong keys that are generated, stored and managed. But with cloud Service other than IaaS that can provide a private cloud, other categories will fall to threats such as data lost and leakage.

f. Threat #6: Account or Service Hijacking: This remains one of the top threats. With stolen credentials, an attacker can access critical areas of deployed cloud services. In the Kerberos and IPsec implementation, security policies have been incorporated to detect and limit the threat. Audit logs for service accessing are kept for user usage information.

g. Threat #7: Unknown Risk Profile: Usually when cloud services are advertised, features and functionalities are talked about, but what about details or compliance of internal security procedures and so forth. This Kerberos and IPsec implementation will help the consumer have a safer addition to security since from the network not relying on the cloud provider totally for security.

After analyzing the authentication protocols with the new design of ours with the threats mentioned, it shows significant resistant to most of the threats mentioned. The figure below (figure 8) shows that in average it is resistant to most threats mentioned in the paper [16]. The figure shows as in table 1 how each authentication method is ranked with the grades provided earlier (0 – Poor, 1 – Fair, 2 – Good, 3 – Satisfactory). From all the methods, IAM was the least immune to the threats because authentication methods like the OAuth is still a new protocol and its design has lapses that will be very hazardous to a consumer.

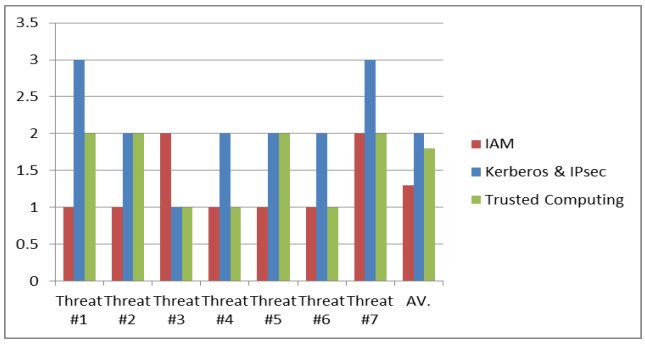

Figure 8: Threat analysis chart for authentication methods.

In general, this design has not hindered the performance of the entire system. Scalability of users and infrastructure is not limited. To evaluate the contribution made in general, we can see it has a potential of pass a lot of given security threat to a cloud service over the Internet. These threats are just a few but from contrast; it will pass on well to other threats as long as the entire system design is considerate to the possible attacks that are known to security experts and network administrators.

VI. CONCLUSION

Cloud computing is still a new and interesting part of IT, which will continue to evolve to human demand. This paper has been able to show how cloud authentication can be integrated with corporate networks on premises authentication for cloud authentication. This has helped reduce the dependence of security provision by cloud provider. The only limitation to this thesis is cloud providers might not support the kind of authentication used, so there will be an interoperability problem unless an agreement is met, before implementation.

This paper would outline an authentication model that provides an end to end security for organizations and cloud providers. The model involves a lot of components, so can act as a blueprint. Because it will need additional software development and network design for the pilot system to provide a complete and cascade authentication method.

VII. REFERENCES

[1] M. Carroll, A. van der Marwe, and P. Kotze. Secure Cloud Computing Benefits, Risk and Controls (2011). IEEE Conference.

[2] T. Mather, S. Kumarasuwamy, and S. Latif, "Cloud Security and Privacy", O'Rielly, ISBN: 978-0-4596-802769, 2009.

[3] C. Kaufman, R. Perlman, and M. Speciner, "Network Security: Private Communication in a Public World" Prentice Hall PTR, ISBN: 0-13-046019-2, 2002.

[4] M. Jarvinen, "PKI Requirements for IPSEC" Thesis University of Helsinki, May 2003, [Online], Available: http://www.tml.tkk.fi/Publications/Thesis/jarvinen.pdf

[5] S. Kent and R. Atkinson, Security Architecture for the Internet protocol, Nov. 1998, RFC 2401. [Online], Available: ftp://ftp.isi.edu/in-notes/rfc2401.txt

[6] A. Alshamsi and T. Saito, A Technical Comparison of IPsec and SSL, IEEE Conferences 2005.

[7] Safenet Cloud providers [Online]. Available: http://www2.safenet-inc.com/trusted_cloud_fabric/saas.html

[8] L. M. Kaufman, "Data Security in the World of Cloud Computing", IEEE Security & Privacy, vol. 7, no. 4, 2009.

[9] Citrix Labs (C3 Lab Blueprint). [Online]. Available: http://community.citrix.com/download/attachments/87458064/Bridging+to+a+Corporate+Network+from+Amazon+EC2.pdf

[10] Z. Shen, L. Li, F. Yan, and X. Wu, Cloud Computing System Based on Trusted Computing Platform, (ICICTA) IEEE Conferences, 942 - 945 (2010).

[11] Z. Shen and Q. Tong, The Security of Cloud Computing System based on Trusted Computing Technology, (ICSPS) IEEE Conferences, V2-11 – V2-15 (2010).

[12] J. W. Rittinghouse, J. F. Ransome, "Cloud Computing: Implementation Management and Security" CRC Press, ISBN: 978-1-4398-0680-7, 2009.

[13] S. A. Almulla, C.Y. Yeun, Cloud Computing Security Management, (ICESMA) 2010. IEEE Conferences.

[14] J. M. Johansson, "Windows Server 2008 Security". Microsoft Press, 2008.

[15] D. Holme, N. Ruest, and D. Ruest, "Configuring Windows Server 2008 Active Directory". Microsoft Press, 2008.

[16] Cloud Security Alliance (CSA), "Top Threats to Cloud Computing V 1.0", March 2010. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf