ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Efficient Multi Algorithm Based Security for Cloud with Claim

Shalini Shrivastava[1], Nagendra Kumar[2]

M.Tech Student, Dept. of CSE, SRIST, Jabalpur, M.P, India[1]

Asst. Professor, SRIST, Jabalpur, M.P, India[2]

ABSTRACT: When people are moving from web applications to cloud computing platform, the main concern is to raise privacy of their sensitive data in cloud environment. The user authentication with login which is causing new security risks such as virtualization attack, account/password sniffing, or phishing attack. Even though existing researches have addressed various security algorithms, it is still insufficient. This work provides a security mechanism applied using claim-based identity management system. The proposal has a model to extend the claim-based identity management scheme for cloud applications and provide a more secure way to access the cloud services. A new implementation has been done to create the experiments for the proposed work. This work proposes to use proactive application migration on Microsoft Azure. For simulation a database has been created to track the records of the various migrations applied. User has been provided with the facility of adding Virtual Machines and Applications. User can also select if the application being added is to be hosted on which particular virtual machine. As per the proposed flow, application migrations are done. After executing the simulation several times records in the database has been filtered / grouped to generate the results.

KEYWORDS: Cloud Computing, Claim, Security Token Service, Identity Providers, Federation Provider

I. INTRODUCTION

Cloud computing [1] [2] provides a cloud infrastructure that is used to provide cloud services to their cloud users. During the access time, consumers provide sensitive data such as name, SSN number, credit card information for accessing the online services of a cloud service provider. Privacy of the information totally depends on the cloud service security as well as value of the information. Consumers do not know that a provider of a service follow which privacy laws and how they protects their digital information. So as a consumer, consumer decides what type of information they could provide. For instance, all information of Twitter stored on Google Apps [3]. First the hacker hijacks the company data stored on Google Apps. Then, he takes the advantage of poor password practices. All information about Hotmail's stored on the web to pinch hundreds of Twitter documents. As the result, a username/password security token is used by the most service provider to authenticate [4], which may result in the phishing/password guessing attacks to consumer.

There is a need for a solution to address the above problem in form of an identity management (IDM) solution. For a developer, working with identity management traditionally hasn't been much fun. First a developer decides which identity technology is used in which application, that is accessed in an organization or across an organization via the internet. Each application uses different identity technology to find and keep track of identity of users in different applications. The application gets some information from those users and might get other access from the directory services or some other identity provider. So, our concern is to create a single interoperable platform for identity management. That is much better approach in every situation, both in enterprise application as well as in cloud application. Rather than using multiple identities, using this single approach user access to the cloud services gives the better result.

When a user access the windows application, windows does not know much about its user, because application is accessed by the users within a single organization. This application trusts on Integrated Windows Authentication (IWA) [5], which uses Kerberos tickets for authentication that is implemented as a part of Active Directory Domain Services (AD DS) [5]. Again it uses a claim-based approach to handles identity in which user supply a single identity (username, password).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Problem in the research can be resolved by the different factors such as login information, proper authorization techniques, and other techniques which are not being applied or applied partially by the researchers. The problem can be better solved by applying composite methods in which combination of the two or more techniques will provide an exact solution for the problem.

Claim-based identity management system is used to address the above problem. This approach provides a single identity that is used to access the cloud services within an organization or outside an organization in the form of digital identity via the internet. Claim-based identity management systems store user's information in the form of digital identity that is used to authenticate and get the role of the user in an application. This paper describes existing claim-based architecture and how to improve this approach to authenticate user. Additionally, it also describes how to manage user's digital information. Finally, our work is to extend the existing claim-based identity management with some little modifications.

II. LITERATURE SURVEY

Researchers are being extensively done in the area of security of Cloud. Authors have applied different mechanisms for solving the problem.

In the last few years, many organizations/users have adopted cloud storage systems. These storage systems provide a large virtual storage. When people move from web applications to cloud computing platform, their main concern point is how-to raise privacy of user's sensitive data in cloud infrastructure. The traditional form of accessing cloud services is to use a username and password as a security token. During login/access time, new security risk may arise like virtualization attack, account/password sniffing, or phishing attack. Hence, cloud service provider (CSP) does not provide a complete security. Even though existing authentication scheme have addressed various security properties, there is still need of a secure authentication mechanism. This paper describes the need of claim-based identity management system, the basic terminology that is used in claim based approach and what is the advantage to use this approach.

[2] To meet ever-changing business needs, organizations are required to invest time and budget to scale up IT infrastructure such as hardware, software and services. However with own premises and investment in IT infrastructure scaling process can be slow and costly. Moreover, even if organizations scale up their IT infrastructure, these are hardly able to achieve the optimal utilization of the same. This has been a major hurdle in organizations decision to invest huge capital and resources for scaling up its operations. All this has forced companies to continuously look for innovative solutions in the form of new technological solutions that are easy as well as cost effective. One such technology that has come as a boon today is cloud computing. "Cloud computing" is a paradigm shift to provide computing over the internet. It implements Service Oriented Architecture (SOA) resulting in less investment on IT infrastructure, rapid elasticity and finally reduced total cost of ownership. However, implementing Cloud Computing is not so easy and there are lot of issues that may need to be taken care of before it can deliver intended benefits. Unfortunately, there is not enough of research available which has researched various implementations issues in a structured way.

[3] The cloud computing paradigm has been advocated in recent video conferencing system design, which exploits the rich on-demand resources spanning multiple geographic regions of a distributed cloud, for better conferencing experience. A typical architectural design in cloud environment is to create video conferencing agents, i.e., Virtual machines, in each cloud site, assign users to the agents, and enable inter-user communication through the agents. Given the diversity of devices and network connectivity's of the users, the agents may also trans-code the conferencing streams to the best formats and bitrates. In this architecture, two key issues exist on how to effectively assign users to agents and how to identify the best agent to perform a Transco ding task, which are nontrivial due to the following: (1) the existing proximity-based assignment may not be optimal in terms of inter-user delay, which fails to consider the whereabouts of the other users in a conferencing session, (2) the agents may have heterogeneous bandwidth and processing availability, such that the best Transco ding agents should be carefully identified, for cost minimization while best serving all the users requiring the trans-coded streams.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

III. CLAIMS-BASED ARCHITECTURE

Claim-Based Architecture provides a better solution. By using a single UserID and Password to get access to many applications those reside in the clouds or across the clouds.

In this architecture, common assumption is that every participating entity has an identity, which is stored in some other central active directory and every entity follows a consistent identity-management technology.

This section describes some basic definitions, WS standards and claim-Based Architecture.

A. Basic Definitions

1) Claim: Claim is referred to some attributes about an entity, sometime called subject, stated by another entity called Identity Provider [9]. Classic examples of claims are Bob is older than 21, Bob is in the group etc.

2) Trust: An entity A is a trust to an entity B if a claim coming from entity B to entity A and entity A considers coming claim is true and valid issued by B.

3) Security Tokens: Security token is digital information across the network, collection of bytes, construct by XML and signed by an authority containing one or more claims and possibly credentials information.

4) Security Token Services: Security Token Services refers to a Web service that issues security tokens to applications as described by WS-Trust.

5) Identity Metasystem (IdM): The Identity Metasystem refers to a model that provides a technology agnostic abstraction layer for obtaining claims. The IdM has three roles [10]:

Subject: Subject refers to the entities those are involved in the transaction and mentioned in the claim definition.

Relying party (RP): RP refers to a resource that is accessed by client. Before being accessed, resource requires an authentication. Examples of RPs are Website or Web services.

Identity provider (IP): IP is defined in the claim definition. It possesses knowledge about the subject and transforms it in the form of claims. It will be able to provide authentication and authorization on subjects in the form of security tokens.

6) Federation Providers: In the claim-based management, each user gets her identity from a trusted STS that is owned by an identity provider. But, suppose that the application does not trust this STS then federation provider provide a solution in which it offers another STS that is configured by an administrator.

7) Identity library: In the identity library, with the token, a reusable set of codes work and run some protocols that convey them. Here it processes the token, verifies the token signature.

It also knows which token is used by which provider and then checks whether this STS is in the trusted list or not.

8) Security Assertion Markup Language (SAML): It is nothing but a language, which exchanges security information expressed in term of assertions about subjects (person, computer).

The assertions in the token contain information about authentication status, details of the subject, and define role for the subject. SAML-P protocol is used to transmit SAML [11] tokens in different domains.

9) Simple Web Token (SWT): It refers to a compact namevalue pair security token included in an HTTP header. HTTP web resources and responses help in the process of transferring the tokens between different domains.

B. WS-Standards WS-Extensions define a suite of security standards which help in making Web service requests. The WS-Standards include the following extensions [5]:

1) WS-Security: WS-Security [12] supports various security token formats, trust domains, signature formats and encryption technologies. This specification provides the ability to send end to end security token as a part of message. It also provides message integrity and confidentiality.

2) WS-Trust: WS-Security protocol helps in building this specification, which defines additional extension to help in exchanging the security tokens in different trust domains [13].

3) WS-Secure Conversation: It helps in defining extensions that support the creation and sharing of security context for exchanging multiple messages, which leads in increasing overall performance and security.

4) WS-Federation: WS-Security and WS-Trust protocols help in building this specification [14], which provides a way for the relying party to select the right access control decisions.

It also defines mechanisms to allow different security techniques, which enhances the overall security of the system.

5) WS-Federation: Passive Requester Profile: This specification defines how the cross trust realm identity, authentication, and authorization federation mechanisms are defined in

WS-Federation and used by a passive requester [15], such as a Web browsers to provide identity services.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

IV. COMPARISON OF THE VARIOUS LITERATURES

Identifying issues in implementing and deployment of cloud computing in real environment. Identified problem like license management, load balancing, automated service management, security of data, data lock in and API design. They have not proposed any solution for the identified key issues.

Provides a secure authentication mechanism using Claim based identity management scheme for cloud application. Claim based identity solution is required their application for cloud service provider. It uses SAML which is a textual communication and can be easily hacked.

On Cloud providers collaboration for a higher service level in cloud computing. They have addressed lac of cross leverages of available resources across cloud, global efficient cooperation between clouds. Field programmable gate arrays(FPGA) within the cloud and K means clustering. The results illustrated are of great advantage of using hardware acceleration while processing massive amounts of data. Their next step is to finish the various system components and test its complete functionality and then compare its performance to a standard Hadoop platform. The implementation is not feasible without the availability of high and lab as in the base paper. Hardware accelerator are not readily available and are very costly. Lots of communication is happening before actual data transmission for authentication of client which makes it very slow.

A new technique of data integrity for analysis of cloud computing. Security in terms of integrity and availability of client data Cooperative provable data possession scheme The details of the owner shall be stored on the server which will be used to verify the client using public and private key in two steps of security key generation n very tag generation. They investigated the problem of data security in cloud data storage which is essentially a distributed storage system.

V. PROBLEM STATEMENT

Claim based security is applied for the users of the cloud but in general claim based authentication is one way that is once a user logs in on the identity server then he need not provide any further authentication to the identity server. This leads to sever problem that is if somebody hacks the authentication details then all of the service accesses are hacked.

Present system requires user to register on cloud for every service separately which is a security lacuna for the users and the user has to carry additional burden.

VI. PROPOSED WORK

The proposed work is to create centralize identity server which is trust server which can be chosen by the user and cloud service provider in cooperation. The identity server provides following facilities:

- Registration
- Selection of cloud service
- Implementation of cloud mechanism

In this proposal work user will be providing all its details to the identity server only and cloud will receive the authentic session id from the identity server.

For any usage of any service user must be logged in and must have got a authenticated session-id to be presented to the cloud.

If a user is using two different services then he will only require to login once and provide service claim id to get the authenticated session id from the identity server.

The proposed system shall be providing performance details and smooth working that is accuracy of the system.

The flow of data in the cloud and proposed system has been depicted in the above figure 1. The cloud user will first try to fetch data from the cloud, which will be redirected to identity servers. The identity server will accept the login and password of the user and provide a key and authentication session id to the user. The user will be redirected to cloud for fetching data where cloud will directly confirm the key and session id from the identity server. The identity server will verify the user's session id to the cloud and cloud will provide data to the users. All communication will be based on encryption and authorisation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

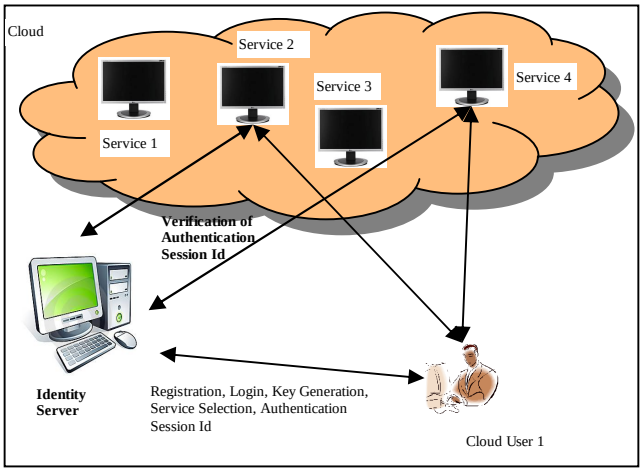
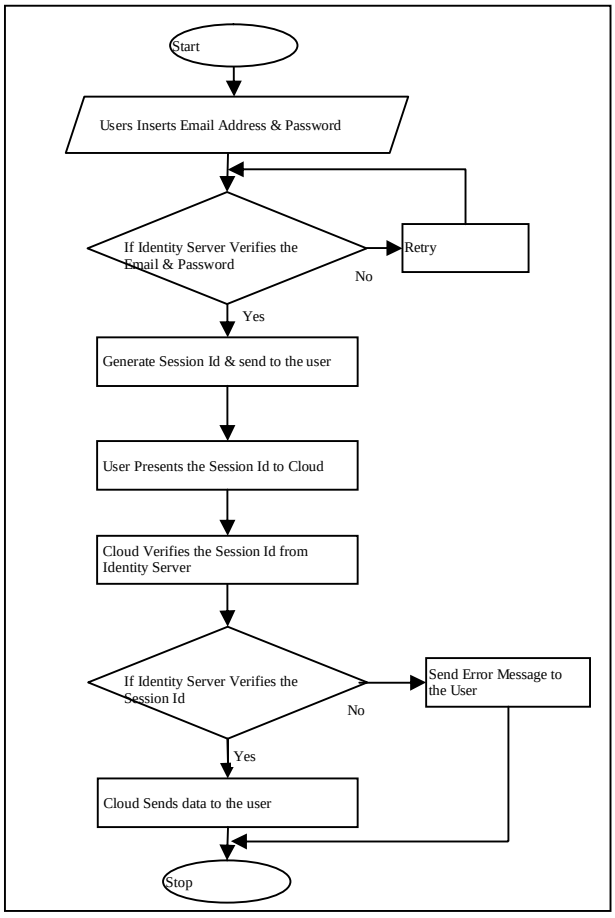


Figure 1: Flow of transfer of data

Flow chart of the Algorithm



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Double Authentication Process

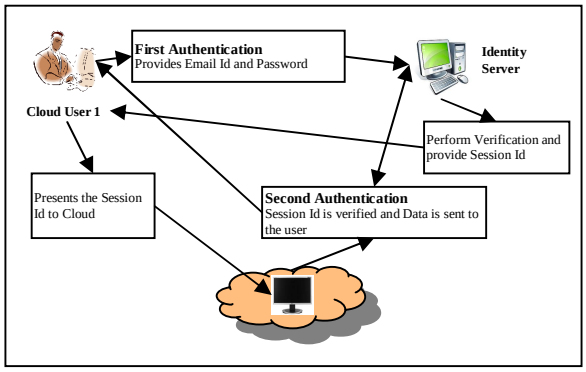


Figure 2: Double authentication process

The double authentication process is being applied in the proposed system. The first authentication is explicit where user provides the login details to the identity server. After verification by the identity server, user accesses the cloud with key and session id provided by identity server. These key and session ids are again verified by the cloud from identity server in second authentication process. The second authentication is hidden from the users.

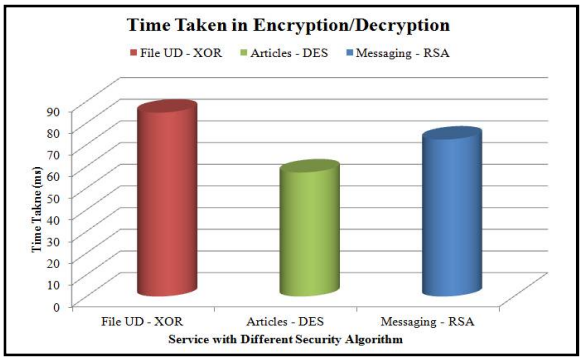
VII. RESULTS & DISCUSSION

Readings obtained from execution of the various services:

Table 4.1: Readings obtained from different services

SNO	File Upload/Download – XOR Time Taken (ms)	Article Submission - DES Time Taken (ms)	Messaging - RSA Time Taken (ms)
1	72	28	77
2	61	91	85
3	88	53	112
4	125	31	25
5	78	83	63
Average	84.8	57.2	72.4

The graph is drawn from the readings obtained as in above table. The graph shows the time taken in encryption/decryption in the different applications. The time taken is found to be min in article processing whereas max in file uploading/downloading. Encryption technique used is the major cause of the delays.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

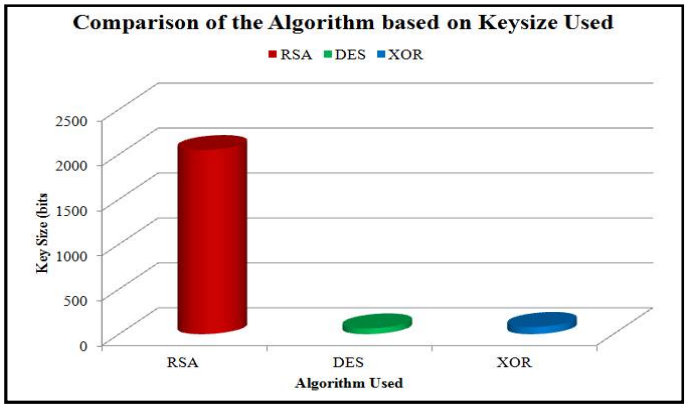
Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Table 4.2: Algorithms Used and their Key Sizes

ALGORITHM	KEY SIZE
RSA	2048
DES	64
XOR	80

The graph is drawn from the readings obtained as in above table. The graph shows the key size of bits in different encryption/decryption techniques used in the different applications. The key size is highest in RSA whereas other technique uses size of the keys to be very less. This causes the security weakness in different algorithms.



VIII. COMPARISON WITH EXISTING SYSTEM

The Oakley Key Determination Protocol is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie–Hellman key exchange algorithm. There following weaknesses of the Oakley Key Determination Algorithm:

- The first is the addition of a weak address validation mechanism (e.g. "cookies") to help avoid denial of service attacks.
- This work proposed to use a new key generated randomly and hashed using one way hash function MD5, which is stored on the cloud. Even the key is not generated by the cloud itself, but is got from the identity server which is trust server.
- The second is to allow the two parties to select mutually agreeable supporting algorithms for the protocol: the encryption method, the key derivation method, and the authentication method.
- This work makes the key and hash transparently from the communicating parties and hence is having higher security and hacker may not have any idea about its application. Since cloud is a web technology hence users over the cloud cannot be expected to participate in any such decisions and cloud service provider can also compromise on security of the users data hence the key provided to the user is generated at the Identity server, which will be further used in encryption and decryption of the data.
- Thirdly, the authentication does not depend on encryption using the Diffie-Hellman exponentials; instead, the authentication validates the binding of the exponentials to the identities of the parties.
- MD5 is a one way hash function and therefore the key cannot by decrypted by the hackers. Validation process is also normal and users will not be burdened to provide or remember any extra authentication mechanisms.
- The protocol does not require the two parties compute the shared exponentials prior to authentication.
- In this proposed system user will never be required to compute the shared keys and its application system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

- This protocol adds additional security to the derivation of keys meant for use with encryption (as opposed to authentication) by including a dependence on an additional algorithm. The derivation of keys for encryption is made to depend not only on the Diffie-Hellman algorithm, but also on the cryptographic method used to securely authenticate the communicating parties to each other.
- Proposed work applies three additional security mechanism using symmetric key algorithms.
- This protocol explicitly defines how the two parties can select the mathematical structures (group representation and operation) for performing the Diffie-Hellman algorithm; they can use standard groups or define their own. User-defined groups provide an additional degree of long-term security.

This work uses different algorithms for different services and key determination, therefore has higher security then the Oakley Algorithm. Also, there is no manual decision to be made by the communication parties hence the algorithm works transparently from them and hence the security is higher and implicit.

Table 4.3: Comparison of Security Algorithms Used:

FACTORS	XOR	DES	RSA
Key Size	Variable	56 bits	>1024 bits
Block Size	Depends on Key	64 bits Minimum	512 bits
Ciphering & deciphering key	Same	Same	Different
Scalability	Scalable	It is scalable algorithm due to varying the key size and Block size.	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Secured	Not Secure Enough	Least Secure
Deposit of keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	1	16	1
Stimulation Speed	Faster	Faster	Faster
Trojan Horse	Not proved	No	No
Hardware & Software Implementation	Faster	Better in hardware than in software	Not Efficient
Ciphering & Deciphering Algorithm	Same	Different	Same

IX. CONCLUSION

This work has provided a claim based security using double authentication process. The identity server has been introduced for managing the user details to make them transparent from the cloud. The identity server is authenticating the user and provides a session key encrypted using one way hash mechanism MD5. For any usage of any service user

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

must be logged in and must have got an authenticated session-id to be presented to the cloud. The services are applied with different encryption and decryption algorithms for second authentication, which uses the session key provided by the identity server as the key. The work has been implemented successfully and provides the necessary security and performance as claimed. The results and discussion in above chapter causes to reach to the conclusion that double authentication makes the system to be highly secured and does not affect to the performance of the system.

X. FUTURE WORK

The work uses three different algorithms for services; other security algorithms can be applied and tested for better performance of the proposed system. Even the MD5 hash can be substituted with SHA or other one way hash functions to test the performance and the security of the proposed system. The system can be applied in real time environment to test the security and performance.

REFERENCES

1. Singh, A.; Chatterjee, K., "Identity Management in Cloud Computing through Claim-Based Solution," Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on , vol., no., pp.524,529, 21-22 Feb. 2015 doi: 10.1109/ACCT.2015.89
2. Rastogi, G.; Sushil, R., "Cloud computing implementation: Key issues and solutions," Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on , vol., no., pp.320,324, 11-13 March 2015
3. Hajiesmaili, Mohammad H.; Mak, Lok To; Wang, Zhi; Wu, Chuan; Chen, Minghua; Khonsari, Ahmad, "Cost-Effective Low-Delay Cloud Video Conferencing," Distributed Computing Systems (ICDCS), 2015 IEEE 35th International Conference on , vol., no., pp.103,112, June 29 2015-July 2 2015 doi: 10.1109/ICDCS.2015.19
4. Peter Mell and Tim Grace,"The NIST definition of cloud computing", NIST Special Publication 800-145 (SP800-145), National Institute of Standards and Technology, Gaithersburg, January 2011, pp. 1-52.
5. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing", Communication of the ACM, vol.7, No.4, Apr. 2010, pp. 50-58.
6. Google App Engine, http://appengine.google.com/
7. Amazon.com, "Amazon Web Services (AWS), Online at http://aws.amazon.com, 2008.
8. Dominick Baier, Vittorio Bertocci, Keith Brown, Scott Densmore, Eugenio Pace, Matias Woloski, "A GUIDE TO CLAIMS-BASED IDENTITY AND ACCESS CONTROL" Authentication and Authorization for Services and the Web, 2nd ed http://msdn.microsoft.com/enin/library/ff423674.aspx.
9. OpenID Explained, http://openidexplained.com/
10. Bharat bhargava, Noopur Singh, Asher Sinclair "Privacy in Cloud Computing Through Identity Management", pages 1-6.
11. Pashalidis, A., Mitchell, C., "A taxonomy of single sign-on systems", Proceedings, volume 2727 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, July 2003, pp.249-264.
12. "Claims types: http:// blogs.msdn.com /vbertocci /archive /2008 /05 /05/ claimtypes - a-coarse-taxonomy.aspx
13. Claims and Identity: On-Premise and Cloud Solutions by Vittorio Bertocci, http://msdn.microsoft.com/en-us/library/cc836390.aspx
14. Security Assertion Markup Language, A Brief Introduction to SAML, Tom Scavo, NCSA.
15. (2011) Understanding WS-Security http://msdn.microsoft.com
16. WS-Trust: http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust- 1.3-os.pdf
17. (2011) Understanding WS-Federation http://msdn.microsoft.com
18. http://en.wikipedia.org/wiki/WS-Federation Passive Requestor Profile
19. Claims-Based Identity For Windows http://download.microsoft.com/
20. msdn.microsoft.com/en-us/library/hh446535.aspx
21. Bharat bhargava, Noopur Singh, Asher Sinclair "Privacy in Cloud Computing Through Identity Management", pages 1-6.
22. Pashalidis, A., Mitchell, C., "A taxonomy of single sign-on systems", Proceedings, volume 2727 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, July 2003, pp.249-264.
23. "Claims types: http://blogs.msdn.com/vbertocci/archive/2008/05/05/claimtypes- a-coarse-taxonomy.aspx
24. Claims and Identity: On-Premise and Cloud Solutions by Vittorio Bertocci, http://msdn.microsoft.com/en-us/library/cc836390.aspx
25. (2011) Understanding WS-Security http://msdn.microsoft.com
26. WS-Trust: http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf
27. (2011) Understanding WS-Federation http://msdn.microsoft.com
28. http://en.wikipedia.org/wiki/WS-Federation Passive Requestor Profile
29. Claims-Based Identity For Windows http://download.microsoft.com/
30. msdn.microsoft.com/en-us/library/hh446535.aspx