Using AES, RSA, SHA1 for Securing Cloud

Conference Paper · March 2014

2 authors:

Anas Amro
Palestine Polytechnic University
8 PUBLICATIONS **11** CITATIONS
SEE PROFILE

Mohammed Abutaha
Palestine Polytechnic University
29 PUBLICATIONS **108** CITATIONS
SEE PROFILE

Using AES, RSA, SHA1 for Securing Cloud

Mohammad S. Abutaha, Anas A. Amro

***Abstract*—** In cloud computing, everything you can do is now web based instead of being desktop based. You can follow up all your programs and documents from any computer that's connected to the Internet. Cloud computing infrastructure gives the users the chance for sharing software ,information ,data ,services ,storage over the WWW .security of the cloud is a big issue .In this paper, we propose a new method for saving data in the cloud system. We use AES and RSA algorithms for securing data and connection based on different keys in encryption and decryption also we use a SHA1 algorithm to secure the hash table of data. Our model deals with the whole cloud system security to protect data .A key management center has used as a third party to distribute keys in all stages.

***Keywords*—** SHA1, RSA, AES.

I. Introduction

Cloud computing is an umbrella term used to refer to internet based development and services. The cloud is a metaphor for the internet. A number of characteristics define cloud data, applications services and infrastructure [2]:

- Remotely hosted: Services or data are hosted on someone else's infrastructure.
- Ubiquitous: Services or data are available from anywhere.
- Commodified: The result is a utility computing model similar to traditional that of traditional utilities, like gas and electricity. You pay for what you would d).

II. CLOUD COMPUTING SERVICES

A. *Software as a Service (SaaS)*

Application is hosted as a service provided to customers across the Internet. SaaS is generally used to refer to business software rather than consumer software, which falls under Web 2.0. By removing the need to install and run an application on a user's own computer it is seen as a way for businesses to get the same benefits as commercial software with smaller cost outlay. Saas also alleviates the burden of software maintenance and support but users relinquish control over software versions and requirements [3].

B. *Infrastructure as a Service (IaaS)*

Infrastructure-as-a-Service (IaaS) like Amazon Web Service provides virtual servers with unique IP addresses and blocks of storage on demand. Customers benefit from an API from which they can control their servers. Because customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing [3].

III. Cloud Storage

Several large Web companies (such as Amazon and Google) are now exploiting the fact that they have data storage capacity which can be hired out to others. This approach, known as 'cloud storage' allows data stored remotely to be temporarily cached on desktop computers, mobile phones or other Internet-linked devices. Amazon's Elastic Compute Cloud (EC2) and Simple Storage Solution (S3) are well known examples [2].

IV. CLOUD DATA

Cloud Services can also be used to hold structured data. There has been some discussion of this being a potentially useful notion possibly aligned with the Semantic Web, though concerns, such as this resulting in data becomes undifferentiated, have been raised [4].

V. Opportunities and Challenge

The use of the cloud provides a number of opportunities:

- It enables services to be used without any understanding of their infrastructure.
- Cloud computing works using economies of scale. It lowers the outlay expense for start-up companies, as they would no longer need to buy their own software or servers. Cost would be by on-demand pricing. Vendors and Service providers claim costs by establishing an on-going revenue stream [6][7].
- Data and services are stored remotely but accessible from 'anywhere'.

In parallel there has been backlash against cloud computing:

- Use of cloud computing means dependence on others and that could possibly limit flexibility and

Mohammad S. Abutaha, Palestine Polytechnic University, Palestine, Hebron, (Phone: 0097-599-555770, e-mail:m_abutaha@ppu.edu)

Anas A. Amro, Palestine Polytechnic University, Palestine, Hebron, (Phone: 00972-599-079484, e-mail:anasamro@ppu.edu).

innovation. The ‘others’ are likely become the bigger Internet companies like Google and IBM who may monopolies the market. Some argue that this use of supercomputers is a return to the time of mainframe computing that the PC was a reaction against.

- Security could prove to be a big issue. It is still unclear how safe outsourced data is and when using these services ownership of data is not always clear.
- There are also issues relating to policy and access. If your data is stored abroad whose FOI policy do you adhere to? What happens if the remote server goes down? How will you then access files? There have been cases of users being locked out of accounts and losing access to data [8].

VI. Cloud Computing Security

Cloud computing security is a huge trend because the data is open and shared for the entire world and everywhere the internet is available. We must protect the connections in uploading in the cloud and downloading from it, also the data in the storage must be protected [5].

In this paper we proposed a new model to make a cloud more secure. this paper is divided as the following: first section we talked about introduction, second section we described the related work ,section three we proposed our model ,section four we described an experiment .

VII. Related Work

Many research on security in cloud computing has been proposed in recent times.

A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture by KawserWazedNafi and others worked on the security of the cloud using more than encryption function to secure the connection and data.

Many researcher work on the cloud computing security, the outsider and insider attack still the big concern to transferring form traditional way to cloud computing technique[12], works on security on cloud not include the secure of whole system which another problem. [9,10].

Although these models ensures secured communication between users and servers, but they do not encrypt the loaded information. For best security ensuring process [13, 11], the uploaded information needs to be encrypted so that none can know about the information and its location [11, 12]. Recently some other secured models for cloud computing environment are also being researched [19, 20]. But, these models also fail to ensure all criteria of cloud computing Security issues [21].

VIII. Proposed Model

Our new model depends on using three famous functions that combined with each other to make whole system protections. First we use the AES function to encrypt the data that uploaded from users to the system and the RSA to encrypt the data that stored on the database file. Then we use the SHA1 algorithm to hash a user key [10].

First the user login the system using a password that hashed using SHA1 and saved, the user being connected to the system and he can uploaded his file that is being encrypted using the key that is distributed from the server with 192 bit then hashed using SHA1.Then the data is transferred from the system to the database file that hashed with SHA1. When the user request the data its encrypted using RSA algorithm using system public key then user decrypt the file using his private key, and shown in Figure 1.

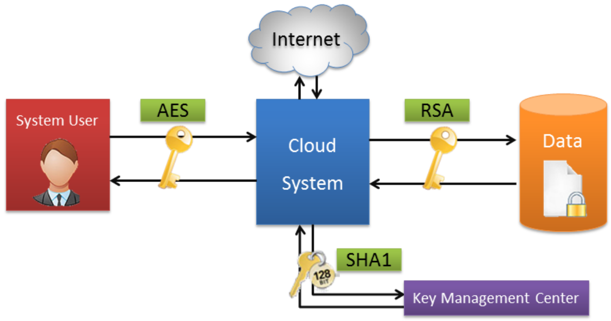

Fig. 1 Proposed Model

IX. Experimental Results

In the lab, we have worked with about 50 users, as well as with their own files to study and prove the efficiency of the proposed model. We tried to find out the results of the various implementations that have helped us to prove our model with a better result. The conditions were observed and different situations at work and the time of implementation of this proposed model.

A. *Lab Setup*

- Platform: Visual Studio 2012 (ASP.NET)
- Processor: Core i5 (2.30 GHz),
- RAM: 4 GB
- HD: 320 GB
- Internet 1024 kbps

In this environment, a complete sample average of 5 seconds to execute all the steps. Hardware configuration takes up 2 seconds to encrypt a file 10 KB. This model is fast enough and can be applied to the current cloud computing environments.

B. *Case studies*

Working with the sample in the laboratory at different times and with different user and individual files, which differ from each other in size and content, guidance, etc. take different times to implement the comprehensive model.

Depending on the size of the file, the program execution time varies from person to person. Among the users as a result of the 50, 10 of who appear in table (I) and table (III).

TABLE I
EXECUTION TIME FOR UPLOADING FILE OF 10 PEOPLE

User No	File Size	Time Required for file Upload (Full Process)	User No	File Size	Time Required for file Upload (Full Process)
1	1 KB	3 sec	6	17 KB	11 sec
2	5 KB	5 sec	7	14 KB	10 sec
3	16 KB	10 sec	8	4 KB	5 sec
4	9 KB	9 sec	9	3 KB	3 sec
5	7 KB	6 sec	10	8 KB	8 sec

TABLE II
EXECUTION TIME FOR DOWNLOADING FILE OF 10 PEOPLE

User No	File Size	Time Required for file Upload (Full Process)	User No	File Size	Time Required for file Upload (Full Process)
1	1 KB	3.5 sec	6	17 KB	12 sec
2	5 KB	5.5 sec	7	14 KB	11 sec
3	16 KB	11 sec	8	4 KB	5.5 sec
4	9 KB	10 sec	9	3 KB	3.5 sec
5	7 KB	7 sec	10	8 KB	9 sec

TABLE III
ADVANTAGES OF THE PROPOSED MODEL

Points for discussion	Identification Based Model	File encryption based Model	Secured channel using model	User Authentication & File encryption model	Proposed Model
Information leakage probability	Medium	Medium	Medium	Low	Low
Complexity	Low	Medium	Low	Medium	Medium
Cost of establishing and maintaining	Low	Medium	High	Medium	Medium
Ensuring User Authentication	Main theme	If key is chosen by user, then slightly authenticate users	Probably not maintained	One time password system is used for user authentication	Login (username, password)
Execution time	Small	Medium	Small	Medium	Greater than others
Security Breaking probability	Medium	Medium	Medium	Probably Low than others	Low

From table (I) and table (II) we can see that the proposed model takes the same time to implement like other existing models. But ensure higher security. The information is stored in the main server databases are kept encrypted files. Thus, only database encryption in the main server is enough to be leaking any information.

This makes cost effective model and less time required for the implementation of the entire process. Secured information exchange between users and the system gives protection to hide information from unauthorized users and intruders. Shows the comparative analysis of the model proposed in table (III).

From the previous analysis, we can see that the proposed model works smoothly as others and ensure higher security than other current models run in a cloud computing environment.

X. CONCLUSION

In this work we made a new model for cloud computing security but using a key management center.

We made a good authentication way by using AES function to system user in login case and RSA function to encrypt data on storage.

The SHA1 function which is a secure hash algorithm to hash the key function on the system, SHA1 has rather more powerful and security rather another technique. But we have a greater time and size because of SHA1 space and speed. But the new model ensures security for whole cloud computing structure.

ACKNOWLEDGMENT

We wish to thank warmly the people who through their help and their work. We must thank most especially to our friends for their help us.

REFERENCES

[1] Joan Daemen, Vincent Rijmen, "Announcing the *ADVANCED ENCRYPTION STANDARD (AES)*", Federal Information Processing Standards Publication 197, November 26, 2001

[2] R.L. Rivest, A. Shamir, and L. Adleman, "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*", Laboratory for Computer Science, Massachusetts Institute of Technology, Cam-bridge, November, 1977

[3] Burt Kaliski, *The Mathematics of the RSA Public-Key Cryptosystem,* RSA Laboratories

[4] Joan Daemen, Vincent Rijmen, "*AES Proposal: Rijndael*", 1999

[5] "*Securing Data at Rest: Developing a Database Encryption Strategy*"- A White Paper for Developers, e-Business Managers and IT

[6] Mladen A. Vouk, "*Cloud Computing – Issues, Research and Implementations*", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[7] Ngongang Guy Mollet, "*CLOUD COMPUTING SECURITY*" , Thesis Paper, April 11, 2011

[8] Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy, "*Token - Based Cloud Computing Secure Outsourcing of Data and Arbitrary Computations with Lower Latency*", TRUST 2010, LNCS6101, pp . 417–429, 2010.

[9] Nafi Kawser, Kar Tonny, Hoque Sayed, Hashem M, "*A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture*", IJACSA, 2012.

[10] Hongwei Li, Yuanshun Dai, Ling Tian and Haomiao Yang, "*Identity-Based Authentication for Cloud Computing*", CloudCom 2009, LNCS 5931, pp. 157–166, 2009

[11] Sven Bugiel, Stefan Nurnberger, Ahmad-Reza Sadeghi, Thomas Schneider, "*Twin Clouds: Secure Cloud Computing with Low Latency*", CASED, Germany, 2011

[12] Luis M. Vaquero, Luis Rodero-Merino, Daniel Morán, "Locking the sky: a survey on IaaS cloud security", Computing (2011) 91:93–118

[13] Yang Tang, Patrick P. C. Lee, John C. S. Lui, and Radia Perlman, "*FADE: Secure Overlay Cloud Storage with File Assured Deletion*", 2010.