A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments

Faraz Fatemi Moghaddam (*f.fatemi@ieee.org*)

Omidreza Karimi (*omid@medicatak.com.my*)

Dr. Ma'en T. Alrashdan (*dr.maen@apu.edu.my*)

November 2013

Introduction

Cloud Computing

- Storage
- Virtualization
- Connectivity
- Processing Power
- Sharing

Cloud Computing Models

- Infrastructure as a Service
- Platform as a Service
- Software as a Service

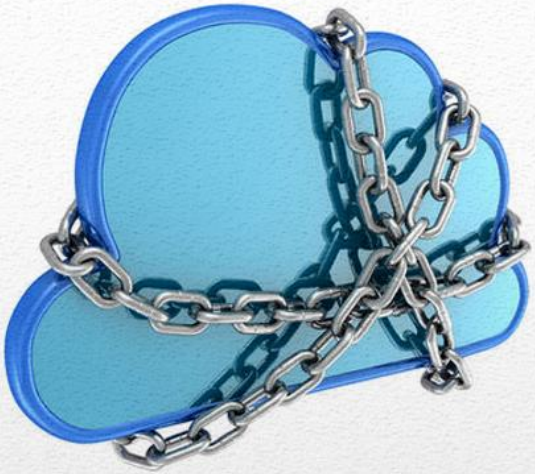
(Malathi, 2011)

- Unlimited storage.
- The most cost efficient method to use, maintain and upgrade resources.
- Easier back up and restore processes.
- Automatic software integration.
- Quick deployment.

(Viswanathan, 2010)

The Most Challenging Issue

- Ensuring the Security in Cloud Computing



Security Issues Types

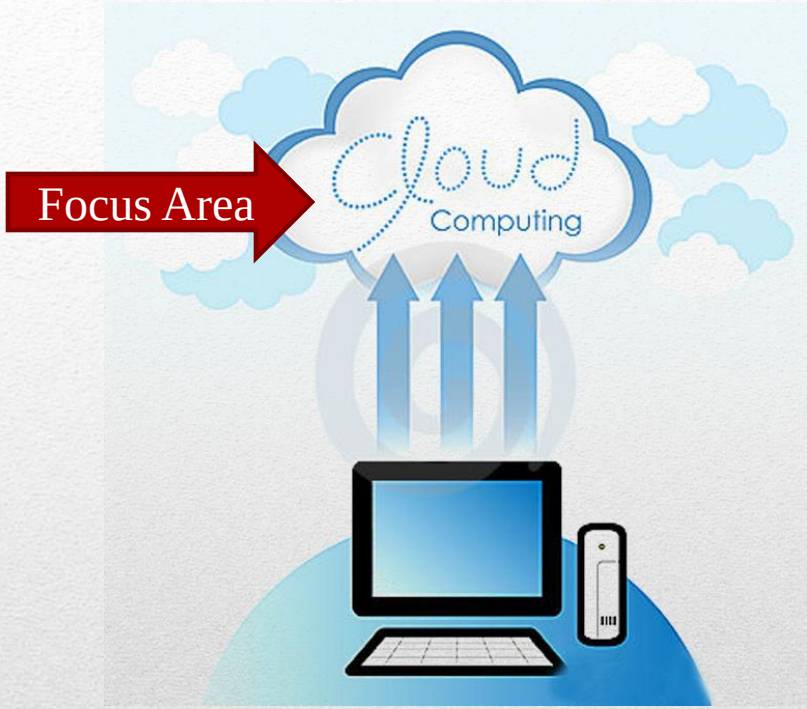
- Service Provider Security Issues
  - Identity and Access Management
  - Privacy
  - Securing Data in Transmission
  - User Identity
  - Audit and Compliance
- Infrastructure Security Issues
  - Securing Data-Storage
  - Network and Server
- End User Security Issues
  - Browser Security
  - Authentication
  - Loss of Governance
  - Data Protection

(Kulkarni, 2012)

Focus Area

Service Providers Security Issues

- ✓ Security in Cloud Servers
- ✓ Security in SaaS Applications



Problem Background

Security of data in servers

↓

The most popular existing solution

↓

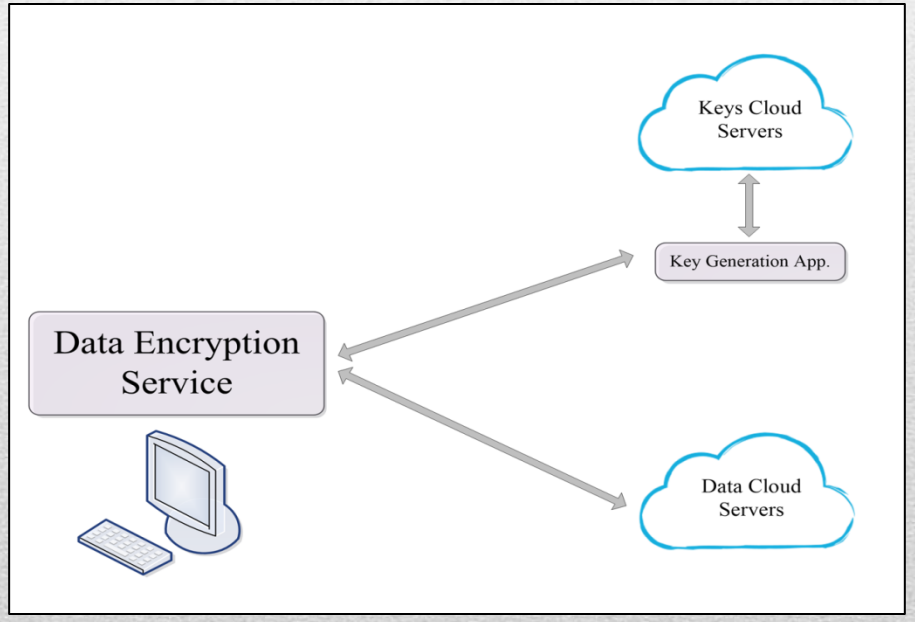
Cryptography in Server Side

↓

Asymmetric Keys or Symmetric Keys Cryptography?

DATA ENCRYPTION SERVICE

Data encryption service is a client-based service that is proposed for increasing reliability in cloud computing communications by applying real-time encryption in client side. In this model, data and keys are stored in different cloud storage and cryptography processes (*i.e.* encryption and decryption) are done in client side by requesting keys from Key Cloud Server (KCS) and data from Data Cloud Server (DCS). Moreover, the key generation process is done in KCS Software-as-a-Service (SaaS) application.



DATA ENCRYPTION SERVICE

According to the nature of this research that is based on sharing concepts, asymmetric key algorithms are more appropriate for data encryption service by using public and private keys. Symmetric key algorithms such as AES are faster than asymmetric algorithm but have considerable problems in sharing processes. Due to this reason and the importance of applying the most efficient encryption performance in client-side, six of the most popular asymmetric encryption models were reviewed and re-developed in the same situation for investigating the strengths and weaknesses of each model to choose the most secure and efficient model due to the nature of the data encryption service. The chosen models are: Original RSA, RSA Small-e, RSA Small-d, MREA, Efficient RSA, and EAMRSA.

General Overview of Cryptography Models

Original RSA

RSA Small-e

RSA Small-d

Modified RSA Encryption Algorithm (MREA)

Efficient RSA (E-RSA)

Encrypt Assistant Multi-Prime RSA (EAMRSA)

METHODOLOGY

According to the aim of this research, all of the described models were redeveloped by Microsoft .net Framework 4.0 in C# programming language for analyzing in the same situation. The simulation were done by using Dropbox co. cloud service provider as data cloud server, and two 2.40 GHz Intel® Core ™ i5 CPU PCs with 4.00 GB RAM as keys cloud server and client for implementing data encryption service

Key Generation Time

Effect of Changing the Key Sizes from 512 (bits) to 3072 (bits) on Key Generation Time (ms) in KGA according to RSA, RSA Small-e, RSA Small-d, MREA, EAMRSA, and E-RSA Algorithms

Key Size (bits)	RSA	RSA Small-e	RSA Small-d	MREA	E-RSA	EAMRSA
512	417	199	199	641	501	890
1024	612	316	316	916	694	1438
2048	890	714	714	1721	997	2864
3072	1943	1201	1201	2612	2281	3314

ENCRYPTION AND DECRYPTION

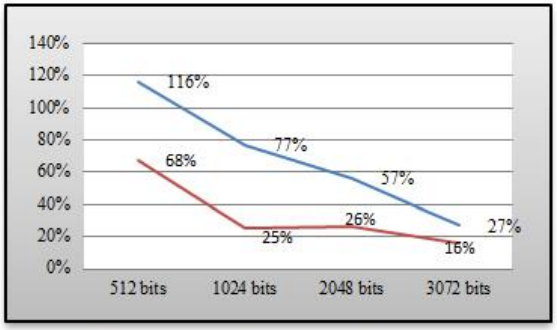


Fig. 2. Encryption and Decryption Time Increase by 10-fold Enhancement of Message Size in Original RSA

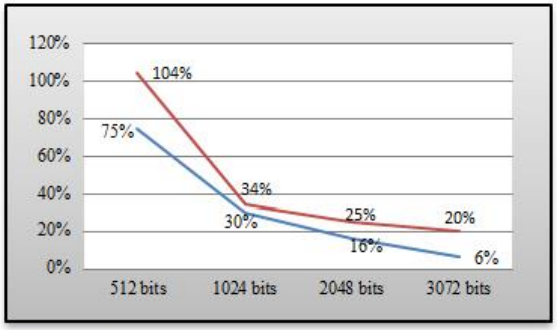


Fig. 3. Encryption and Decryption Time Increase by 10-fold Enhancement of Message Size in RSA Small-*e*

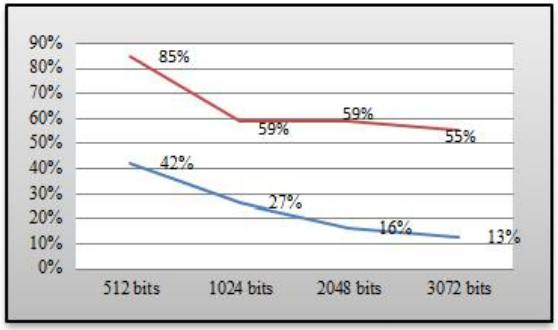


Fig. 4. Encryption and Decryption Time Increase by 10-fold Enhancement of Message Size in RSA Small-*d*

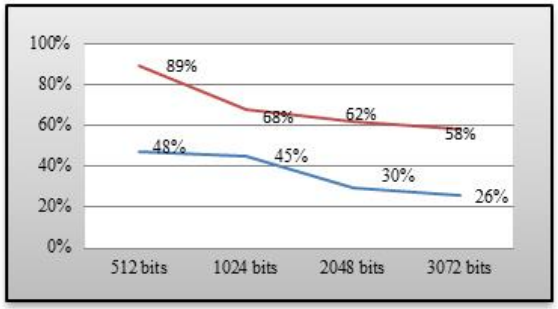


Fig. 5. Encryption and Decryption Time Increase by 10-fold Enhancement of Message Size in MREA

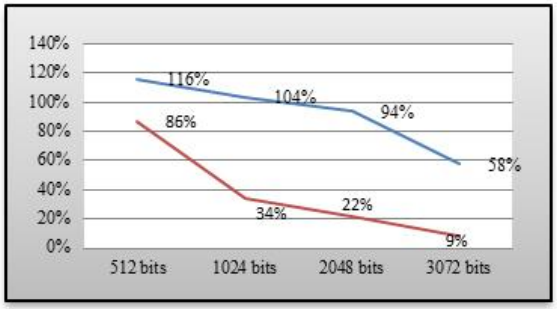


Fig. 6. Encryption and Decryption Time Increase by 10-fold Enhancement of Message Size in E-RSA

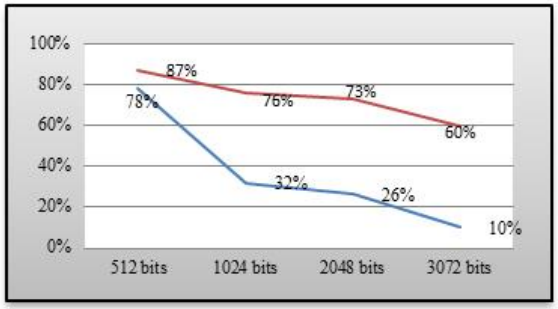


Fig. 7. Encryption and Decryption Time Increase by 10-fold Enhancement of Message Size in EAMRSA

Encryption Time Increase Percentage *Decryption Time Increase Percentage*

SECURITY ANALYSIS

Brute Force Attack

Mathematical Attack

Timing Attack

Conclusion

According to the nature of client-based data encryption service, E-RSA is suggested to be used in proposed model because it is more secure and has more acceleration, accuracy in comparison with other algorithms. Furthermore, the compatibility of E-RSA is more specified than other algorithms in limited power devices.

.

References

I. Bojanova, and A. Samba, “Analysis of Cloud Computing Delivery Architecture Models,” in Proc. *IEEE International Conf. on Advanced Information Networking and Applications (WAINA)*, Biopolis, Singapore, 2011, pp. 453-458.

M. Armbrust, 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,” *ACM Trans. On Communications*, vol. 53, no. 4, pp. 50-58, April 2010.

F.B. Shaikh, and S. Haider, “Security Threats in Cloud Computing,” in *Proc. International Conf. for Internet Technology and Secured Transactions (ICITST)*, 2011, pp. 214-219.

T. Mather, S. Kumaraswamy, S. Latif, “Data Security and Storage,” in *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, M. Loukides, Sebastopol, CA, O’Reilly Media, 2009, ch.4, pp. 61-71.

M. Ahmed, Y. Xiang, S. Ali, “Above the Trust and Security in Cloud Computing: A Notion towards Innovation,” in *Proc. IEEE/IFIP 8th International Conf. on Embedded and Ubiquitous Computing (EUC)*, Hong Kong, 2010, pp. 723-730.

S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” in *Proc. IEEE INFOCOM*, San Diego, USA, 2010, pp. 1-9.

J. Daemen, and V. Rijmen, “The block cipher Rijndael,” *Smart Card Research and Applications Trans. in Cmoputer Science*, Springer-Verlag, vol. *1820,* pp. 277-284, Jan 2000

R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *ACM Trans. On Communications*, vol. 21, no. 2, pp. 120-126, Feb 1978.

H. M. Sun, M. E. Wu, W. C. Ting, and M. J. Hinek, “Dual RSA and Its Security Analysis,” *IEEE Trans. on Information Theory*, vol. 53, no. 8, pp. 2922-2933, Aug 2007.

Thank you