UNIVERSITI PUTRA MALAYSIA

IMPROVING THE SECURITY AND ENCRYPTION PERFORMANCE OF CLOUD STORAGE BY USING ELLIPTIC CURVE CRYPTOGRAPHY

NOORULDEEN QUTAIBA ISMAEEL

FSKTM 2016 29

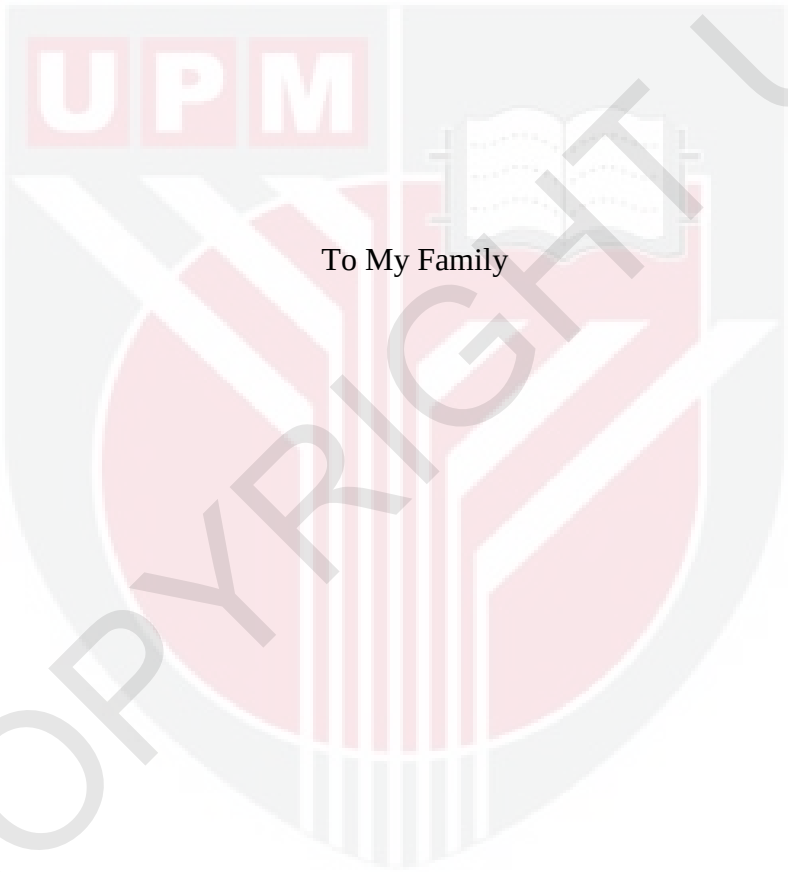
IMPROVING THE SECURITY AND ENCRYPTION PERFORMANCE OF CLOUD STORAGE BY USING ELLIPTIC CURVE CRYPTOGRAPHY

By

NOORULDEEN QUTAIBA ISMAEEL

Thesis Submitted to the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of
Master of Computer Science

January 2016



To My Family

ABSTRACT

Abstract of thesis presented to the Senate of Universit Putra Malaysia in fulfilment of the requirement for the degree of Master of Computer Science

IMPROVING THE SECURITY AND ENCRYPTION PERFORMANCE OF CLOUD STORAGE BY USING ELLIPTIC CURVE CRYPTOGRAPHY

By

NOORULDEEN QUTAIBA ISMAEEL

January, 2016

Supervisor: **Dr. Nor Asilah Wati Binti Abdul Hamid**

Faculty: **Computer Science and Information Technology**

Abstract. Cloud services have emerged as one of the most promising solutions for many real world issues. They can be used in a wide variety of applications ranging from cloud storage, cloud computing, and cloud applications. However, they are a double-edged sword from security and privacy standpoints, especially when storing sensitive data in cloud storage. Therefore, besides secure they require efficient security solutions to obtain the necessary security level. The current security solutions are designed to work mainly on either the client side or the server side, and this strategy may cause a reduction of either the performance of the system or the security of the data. In this thesis, we have proposed a security solution based on an ECC algorithm to improve the security and the performance of the data by dividing the file content and encrypting it on both the server and the client side. The proposed solution improves the performance of the standard ECC and outperforms the AES algorithm in terms of encryption speed and response time.

ACKNOWLEDGEMENTS

First and above all, I praise God, the almighty for providing me this opportunity and granting me the capability to proceed successfully.

My deeply appreciation to my family; father and mother, brothers, sisters for their affectionate patience, support, and encouragement all time. Their prayers and good wishes always help me to be strong, especially in difficult times. I am very grateful and thankful to them.

I would like to express my sincere appreciation and deepest gratitude to my supervisor Dr. Nor Asilah Wati Binti Abdul Hamid for their encouragement, valuable advices, and guidance throughout this research.

Special thanks to my dearest friends who are always willing to help and to share ideas and knowledge at times when they are busy with their own project themselves. I will treasure their friendship.

APPROVAL SHEET

A thesis prepared by **Nooruldeen Qutaiba Ismaeel** with the title " **IMPROVING THE SECURITY AND ENCRYPTION PERFORMANCE OF CLOUD STORAGE BY USING ELLIPTIC CURVE CRYPTOGRAPHY** " submitted in partial to fulfilment of requirement of the master of Computer Science and Information Technology Universiti Putra Malaysia.

_____

Dr. Nor Asilah Wati Binti Abdul Hamid
Department of Communication Technology and Network
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Supervisor)

_____

Prof. Madya Dr. Zuriati Binti Ahmad Zukarnain
Department of Communication Technology and Network
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Assessor)

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

DECLARATION

I hereby declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institutions.

_____

Nooruldeen Qutaiba Ismaeel

Date: / 2 / 2016

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

Table **Page**

CHAPTER 1 - INTRODUCTION

1.1 Background

Cloud services have become a moderately new benefits of the business model in the computing reality such as task collaborating and universal accessibility. The National Institute of Standards and Technology (NIST) defines the cloud as a model that permits ubiquitous access to an imparted pool of configurable computing assets that can be quickly provisioned and discharged with administration or supplier cooperation (Zhang Q, Cheng L, and Boutaba R., 2010). This technique has been developed as an attractive modern model to use the massive inflation of computing requirements, data size, and demand for mobile access to important data (Chun-Ting Huang, Lei Huang, Zhongyuan Qin, Hang Yuan, Lan Zhou, Vijay Varadharajan and C.-C. Jay Kuo, 2014). Cloud service contains computing resources, storage, and networking services that are merged by cloud providers and offered to clients with a simple user interface and access (Armbrust M, Fox A, Griffith R et al., 2009, X. Yu and Q. Wen, 2010). Most recent studies have shown that 79% of companies are working on trying to use data outsourcing to mitigate the expenditures of maintenance and stockpiling of data (Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic, 2009).

The cloud can perform many services; however, there are two main services. First is high performance computing services that focus on performance and give users extra computing resources and the ability to perform high-complexity operations. Furthermore, it works quickly and securely, and it can handle as much data as we

need it to. Moreover, high performance computing services can be used to gain virtually unlimited computing power. With this service we only pay for what we use.

Second is cloud storage that gives users mobile accessibility to massive secure storage space (Grossman R., 2009). By using cloud storage, we can share data amongst specific clients who can be selected by the services' users. Common examples of uses of cloud storage today are Dropbox, Amazon's EC2 services, Microsoft SkyDrive, Google Cloud, Microsoft Cloud, and the CDN Cloud Flare.

Between the client and server side, when users upload their files into cloud storage, the control of file access is physically lost and goes to a cloud provider who is considered a third party and unreliable (Lifei Wei el. Al., 2014).

Because the files have to be transmitted and stored in the cloud, they become vulnerable to unauthorized access. Therefore, the main issue in cloud storage services is the security of those files. In spite of the fact that the infrastructure of the cloud considers greatly robust and reliable than client's hardware but the data integrity, confidentiality, and availability are prone to attack from unauthorized accesses, which comes from inside and outside of the cloud (Xiao Zhifeng and Xiao Yang, 2013). Hence, the data must be secure from malicious users and unauthorized access not only inside the cloud but also when this data is being transmitted to the cloud destination. To handle this issue, the clients and cloud service providers use the data encryption technique to encrypt and secure the files.

Generally, there are two different types of encryption techniques based on the key generation and usage: symmetric-key cryptography (SKC), which is also called

secret key cryptography, and asymmetric key cryptography (AKC), which is also known as public key cryptography.

With the symmetric key cryptography (SKC) technique, one key, which is called the shared key, is used to encrypt and decrypt the data. Therefore, the key has to be exchanged between the system users through a secure communication channel prior to the start of data sharing. Although the algorithms of this technique are fast and secure, it suffers from limitations; first, even though the key size determines the strength of data security, the secret key must be shared and distributed before transmitting the data, and that requires providing a secure channel (Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman, 2014, Dharmendra S. Raghuwanshi, M. R. Rajagopalan, 2014). The second limitation is that the algorithm security depends on the key. Once the key is known by an attacker, the information can be simply decrypted, destructed, and modified (Rounak Sinha, Hemant Kumar Srivastava, and Sumita Gupta, 2013). The third limitation is that the algorithms of symmetric key cryptography have no digital signatures; therefore, the sender identity cannot be detected (Rounak Sinha, Hemant Kumar Srivastava, and Sumita Gupta, 2013, Atul Kahate). Finally, the message cannot be directed to a specific receiver when using SKC in a system of users. RC2, DES, 3DES, RC6, Blowfish, and AES algorithms are examples of using this technique.

On the other hand, in asymmetric key cryptography (AKC), which can be utilized to solve the limitations of SKC, two different keys, which are called the public and the private key, are used to encrypt and decrypt the data. With this technique, the data is encrypted by one key (known as the public key), but it cannot be decrypted by the same key. Hence, the sender encrypts the data by utilizing the public key. Then, on the receiver's part, the data will be decrypted by utilizing the private key (W.

Stallings, 2006, Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman, 2014). Nevertheless, data encryption/decryption speed performance is the main limitation of this technique and is less than SKC. The Rivest-Shamir-Adleman (RSA) algorithm and elliptic curve cryptography (ECC) algorithm are well-known examples of this technique.

1.2 Problem statement

Securing cloud storage data with encryption techniques brings many challenges because cloud services have many limitations and distinctive requirements. First, clients connect to their cloud storage from different locations; therefore, the encryption algorithm should be able to cope with that issue of key distributing and managing. Second, the cloud storage is not physically divided for the clients; therefore, the clients' files may be located on the same storage drive. This requires the encryption algorithm to keep the files secured for a specific client. For all of the above requirements and issues, researchers have proposed many solutions to modify and advance the standard encryption algorithms in order to be able to solve these issues. It is a fact that the previous solutions focus on improving the security of the communication channel, transmitted data, or the data in cloud storage. The solutions that proposed by researchers to secure the transmitted data and the data in cloud storage still have many problems to be investigated, which are; Firstly, the solutions encryption/decryption speed depend generally on the performance of the client device. Secondly, the solutions are not secure enough to protect the file in storage from the cloud service providers' access. Thirdly, the symmetric key cryptography (SKC)-based solutions still have the limitations of SKC techniques such as key

management and data signature issues, and finally the asymmetric key cryptography (AKC)-based solutions have not solved the low performance issue of the AKC technique.

Therefore, we propose a solution that is able to satisfy cloud services' security requirements and solve the issues that the current solutions have by using a distributed encryption solution. The solution is ECC-based; therefore, it is categorized under the AKC technique.

1.3 Objectives

The objectives of our work are:

I. To improve the security of files in cloud storage by using the ECC encryption algorithm.

II. To improve the encryption speed of the ECC algorithm and response time on the client side.

1.4 Project Scope

- Our solution in this research is to advance the security of files in cloud storage and improve the encryption speed of the elliptic curve cryptography algorithm (ECC).

- The solution is proposed to secure document files that consist of text-based documents, spread sheet files, and database records files.

1.5 Structure of the thesis

Chapter 2, Literature *Review*, has sections that are divided as follows: Section 2.1 briefly explains what cloud computing is, including its benefits, characteristics, service models, and deployment models. Section 2.2 shows the authentications in cloud, and Section 2.3 illustrates the importance of security in cloud computing. Section 2.4 explains cryptography and its types, and Section 2.5 shows the use of public key cryptosystems. Section 2.6 discusses about mathematical problems for public-key cryptosystems, and 2.7 answers "Why elliptic curve cryptography?" And Section 2.8 illustrates elliptic curve arithmetic. Section 2.9, *Data Security* in *the* Cloud, it discusses what authors of previous works have done and the related work.

Chapter 3, Methodology, shows the architecture and processing of our proposed solution, experiment tools, platforms, and the data size that has been used.

Chapter 4, Result and Discussion, all the results that have been acquired will be shown and discussed.

Chapter 5, Conclusion, shows the conclusion of our work and future work.

REFERENCES

Armbrust M, Fox A, Griffith R et al (2009) Above the clouds: a Berkeley view of cloud computing. Technical Report No UCB/EECS-2009-28, University of California at Berkeley.

Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16,108-114. doi:10.1016/j.istr.2011.08.006.

Andreas Enge, 1999, Elliptic Curves and Their Applications to Cryptography, ISBN: 978-1-4613-7372-8, 978-1-4615-5207-9, SPRINGER SCIENCE+BUSINESS MEDIA, LLC. http://ezproxy.upm.edu.my:2078/book/10.1007/978-1-4615-5207-9

Atul Kahate, "Cryptography and Network Security", TMH

B. P Rimal 2009, Eunmi Choi, and I. Lumb. A taxonomy and survey of cloud computing systems. In Fifth International Joint Conference on INC, IMS and IDC, 2009. NCM '09, pages 44{51. IEEE, August 2009

Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45.doi:10.5121/ijnsa.2011.3103.

(Bruce1996) Schneier, Bruce; "Applied Cryptography", John Wiley & Sons, Inc 1996.

Chun-Ting Huang, Lei Huang, Zhongyuan Qin, Hang Yuan, Lan Zhou, Vijay Varadharajan and C.-C. Jay Kuo :" Survey on securing data storage in the cloud" APSIPA Transactions on Signal and Information Processing / Volume

3 / 2014 / e7 DOI: 10.1017/ATSIP.2014.6, Published online: 23 May 2014. http://journals.cambridge.org/SIP

Clavister 2014- (n.d.) White Paper, *Security in the cloud*, retrieved march 5, 2015. https://www.clavister.com/globalassets/documents/resources/white-papers/clavister-whp-cloud-security-en.pdf

Cloud Computing. International Journal of Soft Computing and Engineering, 3(2), 110-113.

Diaa Salama, Hatem Abdual Kader and Mohiy Hadhoud "Studying the Effects of Most Common Encryption Algorithms" International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011. http://www.researchgate.net/directory/publications

Dou, W., Chen, Q. and Chen, J. (2013). A confidence-based filtering method for DDoS attack defense in cloud environment. Future Generation Computer Systems, 29, 1838–1850, 2012.12.01.

Dr. Prerna Mahajan and Abhishek Sachdeva, "A study of Encryption Algorithms AES, DES, and RSA for Security," Global J. of Computer Science and Technology Network, Web & Security, Vol. 13, Issue 15, Version 1.0, 2013.

Dharmendra S. Raghuwanshi, M.R.Rajagopalan, "MS2: Practical Data Privacy and Security Framework for Data at Rest in Cloud," ISBN: 978-1-4799-3351-8/14 IEEE, 2014.

D. Mahto, D. K. Yadav, 2015, Enhancing Security of One-Time Password using Elliptic Curve Cryptography with Biometrics for E-Commerce Applications, ISBN:978-1-4799-4446-0, IEEE.

Emam, A.H.M. (2013). Additional Authentication and Authorization using Registered Email-ID for Han, J., Susilo, W. and Mu, Y. (2013). Identity-based data storage in cloud computing. Future Generation Computer Systems, 29, 673–681, 2012.07.010.

Federal Information Processing Standard 46-3. Data Encryption Standard (DES), FIPS PUB (46-3), Oct. 25, 1999.

FIPS PUB 197, Nov. 26, 2001, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards publication 197. Federal Information Processing Standards Publication 197.

Grossman R., The case for cloud computing. IEEEXplore, IT Professional, 11(2), (2009) 23–27.

G. H. Nobari (2010) , Omar Boucelma, and Stephane Bressan. Privacy and anonymization as a service: PASS. In Hiroyuki Kitagawa, Yoshiharu Ishikawa, Qing Li, and Chiemi Watanabe, editors, Database Systems for Advanced Applications, volume 5982, pages 392{395. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Naslund, M. and Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing, 1(11), 1-18.

G. Lin 2008, G. Dasmalchi, and J. Zhu. Cloud computing and IT as a service: opportunities and challenges. In Web Services, 2008. ICWS'08. IEEE International Conference on, pages 5{5, 2008.

GuPaWaEbSh, 2004, N. Gura, A. Patel, A. Wander, H. Eberle, S.C. Shantz, *Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs*, Sun Microsystems Laboratories, Proc. CHES '04, 2004.

Hutton A 1996. Meisel A. Windel A. Mohammed A. Licciardi A. Seccombe, A. Security guidance for critical areas of focus in cloud computing, v2.1. CloudSecurityAlliance, page 25, 2009. cited By (since 1996).

H. Chan, A. Perrig and D. Song, 2003, "Random Key Pre-distribution Schemes for Sensor Networks", Proceedings of the IEEE Symposium on Security and Privacy- SP '03, California, USA, 11-14 May, 2003, pp. 197-213.

H. Chien 2004, "Efficient Time-Bound Hierarchical Key Assignment Scheme", IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 10, pp. 1301-1304, 2004.

Hardjono, "Security In Wireless LANS And MANS," Artech House Publishers 2005.

HankMenVan, 2004, Darrel Hankerson, Alfred Menezes, Scott Vanstone, *Guide to Elliptic Curve Cryptography*, Springer ISBN 0-387-95273-X, 2004

Ismail, N. (2011).cCursing the Cloud (or) Controlling the Cloud? Computer Law & Security Review, 27, 250 – 257. doi:10.1016/j.clsr.2011.03.005

John 2009 Rittinghouse and James Ransome. Cloud Computing: Implementa- tion, Management, and Security. CRC Press, 1 edition, August 2009.

J. H. Loxton, D. S. P. Khoo, G. J. Bird and J. Seberry: A Cubic RSA Code Equivalent to Factorization, Journal of Cryptology, 5, 2, pp.139-150, 1992-Springer.

J. Stern, Advances in Cryptology — EUROCRYPT '99, Lecture Notes in Computer Science, (1999), vol-1592, pp. 223-238, Springer-Verlag.

Joint, A. and Baker, E. (2011). Knowing the past to understand the present 1 e issues in the contracting for cloud based services. Computer Law & Security Review, 27, 407 - 415. doi:10.1016/j.clsr.2011.05.002

Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman. An Introduction to Mathematical Cryptography. Springer-Verlag, 2st edition, 2014. Page 37- 47.

Kim, J. and Hong, S. (2012). A Consolidated Authentication Model in Cloud Computing Environments. International Journal of Multimedia and Ubiquitous Engineering, 7(3), 151-160.

Kumar, A. (2012). World of Cloud Computing & Security. International Journal of Cloud Computingand Services Science, 1(2), 53-58.

Khorshed, T.M., Ali, A.B.M.S. and Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems, 28, 833–851. doi:10.1016/j.future.2012.01.006

K. Popovic 2010 and Zeljko Hocenski. Cloud computing security issues and challenges. In MIPRO, 2010 Proceedings of the 33rd International Convention, pages 344{349, 2010.

King, N.J. and Raja, V.T. (2012).Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Reviews, 28, 308-319.

Kakkar and P. K. Bansal, "Reliable Encryption Algorithm used for Communication", M. E. Thesis, Thapar University, 2004.

Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong,Weiwei Jia, Yunlu Chen, and Athanasios V. Vasilakos, Security and privacy for storage and computation in cloud computing, ScienceDirect, Elsevier, Volume 258, 10 February 2014, Pages 371–386.

L. Wang 2010, G. Von Laszewski, A. Younge, X. He, M. Kunze, J. Tao, and C. Fu. Cloud computing: a perspective study. New Generation Computing, 28(2):137{146, 2010.

L.M. Kaufman 2010. Can a trusted environment provide security? Security & Privacy, IEEE, 8(1):50{52, 2010.

Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Application, 6(4), 25-32.

M. Habib, T. Mehmood, F. Ullah, M. Ibrahim, Performance of wimax security algorithm (the comparative study of rsa encryption algorithm with ecc encryption algorithm), International Conference on Computer Technology and Development, ICCTD'09., volume 2, IEEE, 2009, pp. 108–112.

Malik, M. Y., "Efficient implementation of elliptic curve cryptography using low-power digital signal processor," In Advanced Communication Technology (ICACT), 2010, The 12th International Conference on Vol. 2, pp. 1464-1468. IEEE, 2010.

M. Sudha , Dr.Bandaru R. K. Rao , M. Monica "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment," in International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, Dec. 2010.

M. Savari, M. Montazerolzohour, and Y. Eng Thiam, “Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application”, 2012 International Conference on, pp.49-53. IEEE, 2012.

Mitali, Vijay Kumar and Arvind Sharma “A Survey on Various Cryptography Techniques,” International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 3, Issue 4, ISSN 2278-6856, July-August 2014.

NIST (2011) Peter Mell. 'The NIST Definition of Cloud ', *Reports on Computer Systems Technology*, sept., p. 7.

NIST Special Publication 800-67,2012, Recommendation forthe Triple Data Encryption Algorithm (TDEA) Block Cipher Revised January 2012, Information Security, William C. Barker, Elaine Barker.

Nadeem and Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

Nasrin Khanezaei, Zurina M. Hanapi “A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services” ISBN: 978-1-4799-6105-4, IEEE, 2014.

Ogigau-Neamtiu, F. (2012). Cloud Computing Security Issues. Journal of Defense Resource Management, 3(2), 141-148.

O'Melia and J. Elbirt, "Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions", IEEE Transactions on Very Large Scale Integration (VLSI) Syst., vol. 18, no. 11, pp. 1505-1518, Nov. 2010.

O. D. Alowolodu, B.K. Alese, A.O. Adetunmbi, O.S. Adewale, O.S. Ogundele, Elliptic curve cryptography for securing cloud computing applications, Int. J. Comput. Appl. 66 (2013).

Prof. Dr.-Ing. Christof Paar, Dr.-Ing. Jan Pelzl, Understanding Cryptography, Springer Heidelberg Dordrecht London, New York, 2010, pp 149-171.

Pratap Chnadra Mandal: Superiority of Blowfish. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, pp. 196-201, September 2012.

Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems 25, 6 (2009), 599–616.

Ryan, P. and Falvey, S. (2012). Trust in the clouds. Computer Law and Security Reviews, 28, 513-521. http://dx.doi.org/10.1016/j.clsr.2012.07.002

Rounak Sinha, Hemant Kumar Srivastava, Sumita Gupta, "Performance Based Comparison Study of RSA and Elliptic Curve Cryptography", International Journal of Scientific & Engineering Research, Vol. 4, Issue 5, May-2013 ISSN 2229-5518.

S. P. Singh and R. Maini, "Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication, Vol. 2, No. 1, pp. 125-127, Jan-June 2011.

Singh, S. and Jangwal, T. (2012). Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues. International Journal of Computer Science & Information Technology, 4(2), 17-31.

Sharma, S. And Mittal, U. (2013). Comparative Analysis of Various Authentication Techniques in Cloud Computing. International Journal of Innovative Research in Science, Engineering and Technology, 2(4), 994-998.

SANS Institute InfoSec Reading Room, "PGP: A Hybrid Solution" by Jessica J. Benz. https://www.sans.org/reading-room/whitepapers/vpns/pgp-hybrid-solution-717

S. Chandra, S. Paira, S.S. Alam, and G. Sanyal. A comparative survey of symmetric and asymmetric key cryptography. International Conference on Electronics, Communication and Computational Engineering (ICECCE), Nov. 2014 IEEE.

Sunil Mankotia and Manu Sood "A Critical Analysis of Some Symmetric Key Block Cipher Algorithms" (IJCSIT) International Journal of Computer Science and Information Technologies, ISSN: 0975-9646, Vol. 6 (1) , 2015, 495-499.

T. Jaeger (2010) and J. Schiman. Outlook: Cloudy with a chance of security challenges and improvements. Security & Privacy, IEEE, 8(1):77{80, 2010.

T. Dillon 2010, Chen Wu, and E. Chang. Cloud computing: Issues and challenges. In 2010 24th IEEE International Conference on Advanced Informa- tion Networking and Applications (AINA), pages 27 {33, April 2010.

Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. Information Security Technical Report, 16, 102-107. doi:10.1016/j.istr.2011.08.005

Wood K, Pereira E. (Nov.2010) 'An Investigation into CLoud Configuration and Security', 2010 International Conference for Internet Technology and Secured Transactions, 1-6.

W. Stallings, Cryptography and Network Security: Principles and Practices, 5rd. Upper Saddle River, NY 07458, Inc., publishing as Prentice Hall, ISBN 10: 0-13-609704-9, ISBN 13: 978-0-13-609704-4, 2006 Pearson Education, pp. 269–270.

X. Yu and Q. Wen, "A view about cloud data security from data life cycle," Computational Intelligence and Software Engineering (CiSE), 10-12 Dec. (2010) 1 - 4.

Xiao Zhifeng and Xiao Yang. 2013. Security and Privacy in Cloud Computing. IEEE Communications Surveys & Tutorials 15, 2 (2013), 843–859..

Yassin, A.A., Jin, H., Ibrahim, A., Qiang, W. and Zou, D. (2012). Efficient Password-based Two Factors Authentication in Cloud Computing. International Journal of Security and Its Applications, 6(2), 143-148.

Y. Zhang, W. Liu, W. Lou and Y. Fang, 2006 "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE

Transactions Selected Areas in Communications, Vol. 24, No. 2, pp. 1-14, 2006.

Y. Zhang, W. Liu, W. Lou and Y. Fang, 2006 “Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks”, IEEE Transactions Selected Areas in Communications, Vol. 24, No. 2, pp. 1-14, 2006.

Zhang Q, Cheng L, Boutaba R (2010) Cloud Computing: state-of-the-art and research challenges.

J. of Internet Services Applications (2010) 7–18.

BIODATA OF STUDENT

Nooruldeen Qutaiba Ismaeel was born in Iraq/Baghdad on 19th September 1988. He obtained Degree in Computer Hardware and Software Engineering from Al-Mustansiriya University on 2010. He peruses his Master of Computer Science and Information Technology majoring in Distributed Network Department at Universiti Putra Malaysia by focusing on cloud storage security. His research interests include investigating new approach to improve the performance and security of data in cloud storage by using elliptic curve cryptography as he did his Master project in the same area. Recently, he did some publications in these areas.