SECURING CLOUD DATA SYSTEM (SCDS) FOR KEY EXPOSURE USING AES ALGORITHM

MOHAMMED SAMER HASAN THABET ALBATOL

A project report submitted in partial
fulfillment of the requirement for the award of the
Degree of Master of Electrical Engineering

Faculty of Electrical and Electronic Engineering (FKEE)

Universiti Tun Hussein Onn Malaysia

JULY 2021

DECLARATION

This thesis is dedicated to:

The sake of Allah, my Creator.

My great teacher, Mohammed (May Allah bless and grant him), who taught us the purpose of life;

My soul great parents, who lead me and support;

My beloved brothers and sisters and all family;

My friends who encourage and support me;

I dedicate this research.

ACKNOWLEDGEMENT

With the name of Allah, the most merciful, Alhamdulillah, with His blessing I am able to complete my Final Year Project 2 successfully as planned. Firstly, with full grateful, I would like to give a million of appreciation and thanks to my supervisor Dr. DANIAL BIN MD NOR for his guidance, encouragement, and advice throughout my project session. He has provided a good balance of freedom and interest and has been a constant source of ideas and suggestions and recommendations. Thank you very much. Here also, I would like to acknowledge in particular the continuous support of my parents. They have been consistent in encouraging and support me all last years of education at the university. Not forget, thanks to Prof. Madya Dr. Rosli Bin Omar who was helpful while doing my master course. I would like to thank a million thanks to Dr. Norfaiza Binti Fuad and Dr. Noran Azizan Bin Cholan, who have been helping me to complete my project. Thank you very much. Lastly, I want to thank all the teachers and staff of FKEE for the help and facilities thanks a million.

ABSTRACT

Nowadays the internet communication playing the imperative role that used to transfer large amount of cloud data in various fields and website applications. In the internet the cloud date and files for the websites transmitted through insecure channel from the sender to the receiver. In the transferring steps of data or files, the third party which called the attackers try to get an illegal access the data without any authorization. Different techniques and methods have been using by private and public sectors in order to protect sensitive cloud data from intruders because the security of electronic data is the crucial issue. Nowadays the recent problem in any website that the attacker tries to break the data confidentiality by acquiring cryptographic keys, means of coercion or backdoors in cryptographic software. The Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm that used for encryption and decryption data nowadays. The AES algorithm has its own structure to encrypt and decrypt sensitive data that make the attackers difficult to get the real data when encrypting by AES algorithm. In our research project we use to build a local website using the NetBeans Java averments and create our database management by using MySQL language. After that we use to build securing cloud data system (SCDS) for key exposure using the AES algorithm for encrypting and decrypting our website cloud data and files. The website tested by many users that use to register and upload them own data and files using them own e-mails and the unique key that generated after completing the registration. We used to insure for the users data and files in our website by checking the process of our generated system (SCDS) and we got match results for the same files in case of encryption and decryption process.

ABSTRAK

Pada masa kini komunikasi internet memainkan peranan penting yang digunakan untuk memindahkan sejumlah besar rangkaian data (cloud data) dalam pelbagaibidang dan aplikasi laman web. Di internet rangkaian data dan fail untuk laman web yang dihantar melalui saluran yang tidak selamat dari pengirim ke penerima. Dalam langkah-langkah memindahkan data atau fail, pihak ketiga yang memanggil penggodam berusaha mendapatkan akses data secara haram tanpa kebenaran. Teknik dan kaedah yang berbeza telah digunakan oleh sektor swasta dan awam untuk melindungi rangkaian data yang sensitif daripada penceroboh kerana keselamatan data elektronik adalah masalah penting. Pada masa ini masalah baru-baru ini di mana-mana laman web penggodam cuba memecahkan kerahsiaan data dengan memperoleh kunci kriptografi, cara paksaan atau jalan belakang dalam perisian kriptografi. Pada masa ini Algoritma Advanced Encryption Standard (AES) adalah algoritma cipher blok simetri yang paling biasa dan meluas yang digunakan untuk penyulitan dan penyahsulitan data. Algoritma AES mempunyai struktur tersendiri untuk menyulitkan dan menyahsulitkan data sensitif yang membuat penyerang sukar mendapatkan data sebenar ketika menyulitkan oleh algoritma AES. Dalam projek penyelidikan ini, kami membina laman web tempatan menggunakan Java NetBeans dan membuat pengurusan pangkalan data kami dengan menggunakan MySQL. Selepas itu kami membangun sistem rangkian data yang selamat (SCDS) untuk pendedahan kunci menggunakan algoritma AES untuk menyulitkan dan menyahsulitkan rangkaian data dan fail laman web kami. Laman web diuji oleh banyak pengguna yang menggunakan untuk mendaftar dan memuat naik data dan fail mereka sendiri menggunakan e-mel mereka sendiri dan kunci unik yang dihasilkan setelah menyelesaikan pendaftaran. Kami memastikan keselmatn data dan fail pengguna di laman web kami dengan memeriksa proses sistem yang dihasilkan kami (SCDS) dan kami mendapat hasil yang sesuai untuk fail yang sama sekiranya terjadi proses penyulitan dan penyahsulitan..

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

RSA	Rivest Shamir Adleman
KPG	Keypair Generator
MD5WithRSA	The MD5 full name Message-Digest Algorithm 5 is an irreversible encryption algorithm
SaaS	Software as a Service
SCDS	SECURING CLOUD DATA SYSTEM
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
VM	Virtual Machine
IEEE	Institute of Electrical and Electronics Engineers
AONT	All or Nothing Transformations
AES	Advanced Encryption Standard
DES	Data Encryption Standard
ECB	electronic codebook
UML	Unified Modelling Language
SLR	Systematic Literature Review
MSS	Multi Secret Sharing

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background of the study

A huge monitoring operation aiming at invading consumers' privacy was recently exposed throughout the world. The numerous security measures employed within the targeted services did not deter the perpetrators. For example, even though these services used encryption to ensure data confidentiality, the essential keying material was obtained through backdoors bribes or compulsion are both options. If the encryption key is broken, the only option to keep the cipher - text secret is to limit the opposition's access to it. by dispersing it across a large number of application components in the hopes that the enemy won't be able to poison them all at the same time. Even if the information is encrypted and dispersed across many domains, an attackers with the proper cryptographic keys can get into a domain's servers and decrypt the cipher - text blocks saved there. This study examines data privacy in the face of an attacker who has the encrypted message and access to a large number of ciphertext blocks. [1] . The Advanced Encryption Standard (AES) algorithms is a symmetric block cypher technology that is widely mostly used for encrypting and decrypting. The AES technique for encrypting and decrypting sensitive information has its own complex feature, making it more difficult for adversaries to decrypt the actual information. This is accomplished using the AES technique, which combines fundamental encryption algorithms with a fast linear transformation. Although an AONT is not a an encryption in itself, it may be used as a preprocessing step before securing information by using the block cypher. [2].

Cloud computing relates to a number of security problems. The problems are split into two groups. To begin, there is a level of security provided by cloud providers. Second, there are security concerns that their consumers have. They entrust the supplier with their data and put it in the cloud. That is why cloud computing data security is required. To decrease the danger, data security becomes a key problem in cloud computing. Open, shared upload, and distributed environments are typically connected with these dangers.

1.2 Problem Statement

Recent reporting has revealed a strong attacker that obtains cryptographic keys by coercion or backdoors in cryptographic software, compromising data secrecy. Once the encryption key has been revealed, the only method to protect data privacy is to restrict an attacker's exposure to ciphertext. [1]. The Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm that used for encryption and decryption data.

1.3 Objectives

The main objectives of this experiment are:

1. To build a website with a securing cloud data system (SCDS) for administering the encryption and decryption database for the website using AES algorithm.
2. To test the performance of the encryption and decryption in the securing cloud data system (SCDS) for the website database.

1.4 Scope of Study

The Scope of the research will cover the following topics:

1. The build website created using the HTML and Java Script with CSS tags.
2. The implementation of the securing cloud data system (SCDS) was achieved by using JAVA NETBEANS software.

3. The AES algorithm was used for encrypting and decrypting the website database.
4. The database created using MYSQL to manage the website database.

1.5 Research contribution

This project aimed to study and understood the AES algorithm for the encryption and decryption of the files. This project has proven with three members type on the system they are the admin, the owners, and the users. this system builds to fix the problem of weak security and the powers of the new attackers by do encryption and decryption of the files inside the system. the system can decrease risk of the attacks and increase the security.

1.6 Outline of the report

This research presents the work for secure cloud data system for key exposure using AES algorithm.

Chapter 1 shows the Introduction, problem statement of the research, research objective, the scope of the study, and the research organization.

Chapter 2 describe literature review and the related work to achieve the research gap.

Chapter 3 provide the description for the research methodology and research framework with its parameters set up.

Chapter 4 shows the output of the system.

Chapter 5 arrange the research by discussing the findings, limitations, and its recommendations.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this chapter, first introduce the cloud computing and how it works and its security, then discuss encryption for AONT (All or Nothing Transform) and how the AONT works for securing the data. Then it discusses the main method in data securing concept that refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Then next will discuss the different ways of encrypting and data securing.

2.2 Cloud Computing

Cloud computing is quickly expanding in tandem with the fast growth of massive amounts of data. By providing storage and calculating power, the cloud makes massive data preparation possible. Since a result, massive data drives distributed computing ahead, as a rising number of customers may wish to use the cloud to store and analyse their data. Open mists, private mists, and half-and-half mists are the three types of mists that can usually be distinguished. An open cloud is an outside or openly available cloud environment that may be used by any client on a pay-per-use basis. as shown in Figure 2.1.

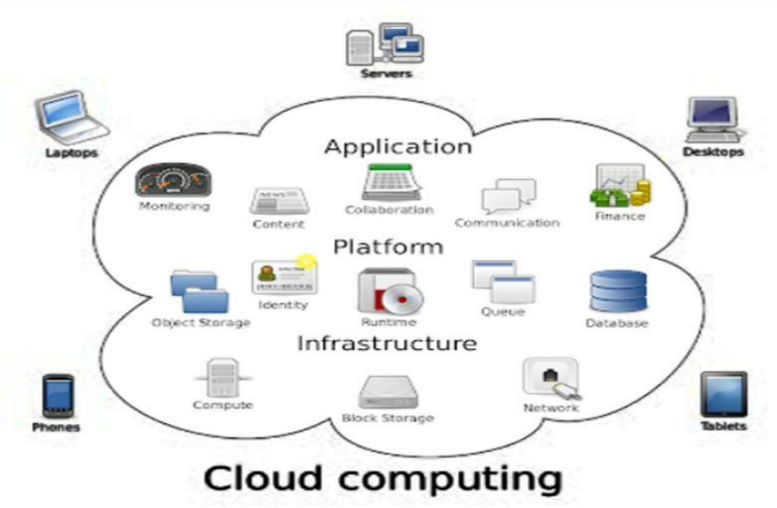

Figure 2.1:Structure of cloud computing [3]

2.3 Cloud properties and models

Cloud computing is a paradigm for providing ubiquitous convenient on demand access to the network to a pool of configurable computing resources that can be rapidly provisioned and published with minimal management effort or interaction fromservice providers. This computing model is made up of five key features, three servicetypes, and four deployment options. [4].

2.3.1 Software as a Service (SaaS)

It is a cloud service that allows users to access software applications housed on a cloud infrastructure over the internet. SaaS eliminates the need for an upfront setup charge and continuous equipment maintenance, as well as automating any updates. SaaS provides the least level of security control because the infrastructure as well as the executing platform are out of the user's reach. [5].

2.3.2 Platform as a Service (PaaS)

PaaS (Platform as a Service) is a cloud computing platform which allows the creation, deployment, and administration of programs. It is the web-based distribution of a

computer platform. The CSP has control over the underlying cloud infrastructure, such as the network, servers, operating systems, and storage, whilst customers have some control and over installed apps and perhaps the framework environment's configuration options. The PaaS paradigm gives more flexibility and system security to customers than SaaS, but still less than IaaS. [4].

2.3.3 Hybrid Cloud

The clouding infrastructure is made up of two or more separate cloud infrastructures (private, communal, or public) that operate independently but are linked by standardised or exclusive technology which enables data and application mobility. Hybrid cloud provides the affordability and scalability of public clouds while simultaneously providing the access and safety of private clouds. Data security and integrity problems arise when data goes from a public to a private clouding environment or vice versa, because privacy restrictions in the public clouding environment differ considerably from those in the private clouding environment [6].

2.3.4 The Infrastructure as a Service (IaaS)

IaaS stands for "infrastructure as a service" which refers to the virtual supply of computer resources such as hardware, network, and memory. Customer control in this approach extends to the operating system, installed services, and chosen network segments. The CSP is solely responsible for the infrastructure. In comparison to earlier models, IaaS gives a greater set of security control in the customer's court.

2.3.5 The public Clouding

Clouding services are offered to individuals or large businesses, and the Cloud is hosted by the supplier. While the public cloud provides scalability and dependability, it also presents several challenges that are detrimental to clients. Customers have no idea what sort of storage the CSP uses, where their data is kept geographically, or who

the entity is that stores their data. As a result, while moving to the public cloud, companies must compromise on some security features. [5].

2.3.6 The Private Clouding

The Cloud services are supplied solely for a single organisation, and the Cloud is either controlled by the business or a third-party, and it can be on or off premises. While Private Cloud addresses the security concerns of Public Cloud, it also adds overheads such as storage management, capacity monitoring, and provision.

2.3.7 The Community Clouding

Cloud services are solely offered for a community of organisations with a shared interest (e.g., purpose, security needs, policy, or compliance concerns), and the Clouding is owned by the organisations or a third party and is situated on or off premises. The disadvantage of this approach is that there are still a number of unsolved problems about service failures, contractual and security consequences, such as issues with data being dispersed across many companies and domains.

2.4 Risks and data security in cloud computing

Cloud computing and its data relate to several hazards and security issues. However, this research will focus on virtualization, public clouding storage, and multitenancy, all of which are linked to data security in cloud computing. In cloud computing, the data security entails more than just data encryption. The three of service models of SaaS, PaaS, and IaaS have different data safety requirements. [7].

2.4.1 Virtualization

Virtualization is a method of capturing a fully working operating system image in another operating system so that the real operating system's resource may be fully

utilised. To execute a guest operating system as a virtual machine in a host operating system, a specific feature called hypervisor is required.

Virtualization is a fundamental component of cloud computing that aids in the delivery of cloud computing's key principles. Virtualization, on the other hand, offers certain data security issues in cloud computing. Compromise of the hypervisor itself is one such concern. If a hypervisor is susceptible, it might become a major target. If a hypervisor is hacked, the entire system, and hence the data, is at risk.

Another risk connected with virtualization is allocation of resources and de-allocation. If Virtual machine operation data is loaded to memory and not deleted before memory is reallocated to the next Virtual machine, data exposure to another Virtual machine may occur, which may be undesired.

2.4.2 The Storage in Public Clouding

Another security risk in cloud computing is storing data on a public cloud. Normally, clouds use centralised storage, which makes them a tempting target for attackers. Storages resources are complex systems that include hardware and software implementations, and a little breach in the public clouding might result in data disclosure. [8].

2.4.3 The Multitenancy

One of the main hazards to data in cloud computing is shared access, commonly known as multitenancy. Because numerous users share the same shared computing resources such as CPU, storage, and memory, it poses a hazard to not just one but many users. There is always the possibility of private data being unintentionally leakedto other users in such situations. Multitenancy vulnerabilities are particularly dangerous since a single flaw in the system might provide another user or attacker access to whole other data. [9].

2.4.4 Data at Rest

Data on the cloud, or any data that can be accessed over the Internet, is referred to as data at rest. This covers both backup and live data. As previously said, companies who do not maintain a private cloud may find it challenging to safeguard data at rest since they do not have physical control over the data. This problem may be overcome, though, by keeping a private cloud with tightly limited access.

2.4.5 Data in Transit

In most cases, data in transit applies to data that is travelling in and out of the cloud. This data can be in the form of a cloud-based file or database that can be retrieved for usage at a different location. When data is stored in the cloud, it is referred to as data in transit at the moment of upload. Data in transit, such as passwords and usernames, might be highly sensitive and secured at times. Unencrypted data, on the other hand, is data in transit as in the Figure 2.4 [10].

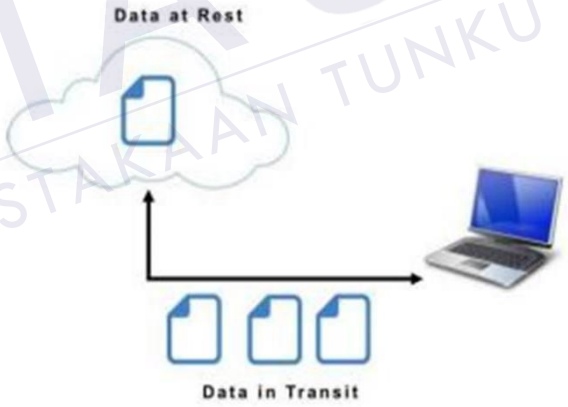

Figure 2.2: Data at rest and data in Transit

2.5 Protecting Data Using Encryption

Data encryption methods for data in transit and data at rest might differ. Encryption keys for data in transit, for example, might be short-lived, but keys for data at rest can be kept for extended periods of time refer to Figure 2.2

REFERENCES

[1] A. Hussain, "Securing Cloud Data under Key Exposure," *Int. Innov. Res. J. Eng. Technol.*, vol. 3, no. 4, pp. 17–19, 2018, doi: 10.32595/iirjet.org/v3i4.2018.65.

[2] G. Amrulla, M. Mourya, R. R. Sanikommu, and A. A. Afroz, "A survey of: Securing cloud data under key exposure," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 7, no. 3, pp. 30–33, 2018, doi: 10.30534/ijatcse/2018/01732018.

[3] P. K. Thakur and A. Verma, "Review on various techniques of energy saving in mobile cloud computing," *Int. Conf. Adv. Comput. Commun. Technol. ACCT*, vol. 2015-April, pp. 530–533, 2015, doi: 10.1109/ACCT.2015.104.

[4] S. Basu *et al.*, "Cloud computing security challenges & solutions-A survey," *2018 IEEE 8th Annu. Comput. Commun. Work. Conf. CCWC 2018*, vol. 2018-Janua, pp. 347–356, 2018, doi: 10.1109/CCWC.2018.8301700.

[5] R. Barona and E. A. M. Anita, "A survey on data breach challenges in cloud computing security: Issues and threats," *Proc. IEEE Int. Conf. Circuit, Power Comput. Technol. ICCPCT 2017*, 2017, doi: 10.1109/ICCPCT.2017.8074287.

[6] A. Gordon, "The Hybrid Cloud Security Professional," *IEEE Cloud Comput.*, vol. 3, no. 1, pp. 82–86, 2016, doi: 10.1109/MCC.2016.21.

[7] M. Bellaiche, A. Abusitta, and T. Halabi, "A cooperative game for online cloud federation formation based on security risk assessment," *Proc. - 5th IEEE Int. Conf. Cyber Secur. Cloud Comput. 4th IEEE Int. Conf. Edge Comput. Scalable Cloud, CSCloud/EdgeCom 2018*, pp. 83–88, 2018, doi: 10.1109/CSCloud/EdgeCom.2018.00023.

[8] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," *Security*, no. February, pp. 1–14, 2013, [Online]. Available: http://www.cloudsecurityalliance.org.

[9] L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan, and F. Desprez, "Building safe PaaS clouds: A survey on security in multitenant software

platforms," *Comput. Secur.*, vol. 31, no. 1, pp. 96–108, 2012, doi: 10.1016/j.cose.2011.10.006.

[10] F. Yahya, V. Chang, R. J. Walters, and G. B. Wills, "Security challenges in cloud storages," *Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom*, vol. 2015-Febru, no. February, pp. 1051–1056, 2015, doi: 10.1109/CloudCom.2014.171.

[11] H. Qian, J. He, Y. Zhou, and Z. Li, "Cryptanalysis and improvement of a block cipher based on multiple chaotic systems," *Math. Probl. Eng.*, vol. 2010, pp. 7–9, 2010, doi: 10.1155/2010/590590.

[12] L.-D. Radu, "Disruptive Technologies in Smart Cities: A Survey on Current Trends and Challenges," *Smart Cities*, vol. 3, no. 3, pp. 1022–1038, 2020, doi: 10.3390/smartcities3030051.

[13] N. A. Moldovyan, A. A. M. Nashwan, D. T. Nguyen, N. H. Nguyen, and H. M. Nguyen, *Deniability of symmetric encryption based on computational indistinguishability from probabilistic ciphering*, vol. 672. Springer Singapore, 2018.

[14] N. Moldovyan, A. Berezin, A. Kornienko, and A. Moldovyan, "Deniable encryption protocols based on probabilistic public-key encryption," *Conf. Open Innov. Assoc. Fruct*, vol. 2017-April, pp. 284–289, 2017, doi: 10.23919/FRUCT.2017.8071324.

[15] M. Klonowski, P. Kubiak, and M. Kutyłowski, "Practical deniable encryption," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4910 LNCS, pp. 599–609, 2008, doi: 10.1007/978-3-540-77566-9_52.

[16] M. Baldi, L. Senigagliesi, and F. Chiaraluce, "The Security of All-or-Nothing Encryption: Protecting against Exhaustive Key Search," pp. 964–969, 2016.

[17] H. Qiu, K. Kapusta, Z. Lu, M. Qiu, and G. Memmi, "All-Or-Nothing data protection for ubiquitous communication: Challenges and perspectives," *Inf. Sci. (Ny).*, vol. 502, pp. 434–445, 2019, doi: 10.1016/j.ins.2019.06.031.

[18] B. Lee, E. K. Dewi, and M. F. Wajdi, "Data Security in Cloud Computing Using AES Under HEROKU Cloud Bih-Hwang," pp. 4–8, 2018.

[19] G. O. Karame, C. Soriente, K. Lichota, and S. Capkun, "Securing Cloud Data Under Key Exposure," *IEEE Trans. Cloud Comput.*, vol. 7, no. 3, pp. 838–849, 2017, doi: 10.1109/tcc.2017.2670559.

[20] I. A. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, "Secure Framework Enhancing AES Algorithm in Cloud Computing," *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8863345.

[21] T. Hidayat and R. Mahardiko, "A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing," *Int. J. Artif. Intell. Res.*, vol. 4, no. 1, pp. 49–57, 2020, doi: 10.29099/ijair.v4i1.154.

[22] P. V. Bankar and Y. Sisodiya, "A Survey on Confidential Cloud Data under Secure Key Exposure," *Int. J. Res. Eng.*, vol. 5, no. 4, pp. 355–359, 2018, doi: 10.21276/ijre.2018.5.4.3.