SECURE CLOUD STORAGE MODEL TO PRESERVE CONFIDENTIALITY AND INTEGRITY

SARFRAZ NAWAZ BROHI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Software Engineering

Advanced Informatics School
Universiti Teknologi Malaysia

JANUARY 2015

To

my supportive parents,

and

beloved siblings

ACKNOWLEDGEMENT

First of All, I thank ALLAH (SWT), the God Almighty, for granting me the health, knowledge, strength, ability, and patience to accomplish this research, and for blessing me with sympathetic and supportive supervisors as well as family members.

I am glad to express tremendous gratitude to my supervisor Dr Suriayati Chuprat for her compassionate character, knowledge sharing, ideas and continuous support from the first until the last day of this study. Her sincere behaviour and constructive feedback enabled me to achieve significant research milestones within the required time-frame.

I would also like to thank my external supervisor Dr Jamalul-lail Ab Manan for enriching me with innovative ideas and skills by sharing his expertise and knowledge in the field of cloud computing security. Due to his unlimited support for reviewing, improving and evaluating my research, I was able to publish several high quality research papers.

At various stages during this study, I faced several undesirable challenges which overburdened me with mental and physical stress. However, this never stopped me from progressing further due to encouraging, moral as well as financial support from my father Dr Muhammad Nawaz Brohi. I am extremely thankful to him for his understanding, kindness, believe, and trust on me.

I also wish to express deepest appreciation to my mother for her prayers regarding my success during this entire study. I will always remember my *late* grandmother in prayers. This research would have never been possible without her wishes for my success.

ABSTRACT

Cloud Service Providers (CSPs) offer remotely located cloud storage services to business organizations which include cost-effective advantages. From an industrial perspective, Amazon Simple Storage Service (S3) and Google Cloud Storage (GCS) are the leading cloud storage services. These storages are secured using the latest data security approaches such as cryptography algorithms, data auditing processes, and strict access control policies. However, organizations where confidentiality of information is a significant act, they are not assertive to adopt these services due to emerging data confidentiality and integrity concerns. Malicious attackers have violated the cloud storages to steal, view, manipulate, and tamper clients' data. The researchers have attempted to overcome these shortcomings by designing and developing various security models. These solutions incorporate limitations and require enhancements as well as improvements before they can be widely accepted by CSPs to guarantee secure cloud storage services. In order to solve the stated problem, this research developed an improved security solution namely Secure Cloud Storage Model (SCSM) which consists of Multi-factor authentication and authorization process using Role-Based Access Control (RBAC) with Complex Random Security Code Generator (CRSCG), Partial homomorphic cryptography using Rivest, Shamir and Adleman (RSA) algorithm, Trusted Third Party (TTP) services including Key Management (KM) approach and data auditing process, Implementation of 256-bit Secure Socket Layer (SSL), and Service Level Agreement (SLA). SCSM was implemented using Java Enterprise Edition with glassfish server and deployed on a cloud computing infrastructure. The model was evaluated using extended euclidean algorithm, system security analysis, key management recommendations, web-based testing tool, security scanner, and survey. The survey results presented that 83.33% of the respondents agreed for SCSM to be widely accepted by CSPs to offer secured cloud storage services. The aggregate evaluation results proved that SCSM is successful in preserving data confidentiality and integrity at remotely located cloud storages.

ABSTRAK

Penyedia perkhidmatan awan (CSP) menawarkan servis storan awan secara jauh yang memberi kelebihan kos yang efektif. Mengikut perspektif industri, *Amazon Simple Storage Service* (S3) dan *Google Cloud Storage* (GCS) merupakan peneraju utama servis storan awan. Storan ini adalah selamat kerana mereka menggunakan pendekatan keselamatan data yang terkini seperti algoritma kriptografi, proses pengauditan data serta polisi kawalan capaian yang ketat. Walau bagaimanapun, bagi organisasi yang mengutamakan kerahsiaan maklumat, mereka tidak tertarik untuk menggunakan servis tersebut kerana bimbang akan kerahsiaan dan integriti data. Penyerang yang berniat jahat telah mencabuli storan awan dengan mencuri, melihat, memanipulasi dan mengganggu data pelanggan. Para penyelidik telah mencuba menangani masalah-masalah ini dengan mereka bentuk dan membangunkan pelbagai model keselamatan. Penyelesaian yang telah dibangunkan ini masih mempunyai had tertentu dan memerlukan penambahbaikan sebelum ianya diterima secara meluas oleh CSP demi menjamin keselamatan servis tersebut. Untuk menyelesaikan masalah yang dinyatakan, penyelidikan ini telah membangunkan penyelesaian keselamatan yang telah ditambahbaik dan ianya dinamakan *Secure Cloud Storage Model* (SCSM). Model ini terdiri daripada pengesahan pelbagai-faktor, proses kebenaran menggunakan *Role-Based Access Control* (RBAC) dengan *Complex Random Security Code Generator* (CRSCG), kriptografi *homomorphic* separa menggunakan algoritma *Rivest, Shamir and Adleman* (RSA), servis-servis *Trusted Third Party* (TTP) iaitu pendekatan pengurusan kunci (KM) dan proses pengauditan data, perlaksanaan *Secure Socket Layer* (SSL) 256-bit, dan *Service Level Agreement* (SLA). SCSM dibangunkan menggunakan *Java Enterprise Edition* dengan pelayan *Glassfish* dan dilaksanakan pada infrastruktur pengkomputeran awan. Model ini kemudiannya dinilai menggunakan algoritma *Extended Euclidean*, analisis keselamatan sistem, cadangan-cadangan pengurusan kunci, alatan ujian berasaskan sesawang, pengimbas keselamatan serta kajian. Hasil kajian menunjukkan 83.33% responden bersetuju SCSM boleh diterima secara meluas oleh CSP yang menawarkan servis storan awan yang selamat. Keputusan penilaian membuktikan SCSM berjaya dalam memelihara kerahsiaan data dan integriti pada storan awan jarak jauh.