University POLITEHNICA of Bucharest

Faculty of Automatic Control and Computers

Department of Computer Science and Engineering

No. Senate Decision 000 in 00.00.2019

Doctoral Thesis

Privacy of cloud computing

Name of the thesis in Romanian,

Author: **Anwer Chitheer Jasim Al Bazooni**

Scientific Supervisor: **Prof. Dr. Eng. Nicolae Ţăpuş**

DOCTORAL COMMITTEE

Chairman	Prof. Dr. Eng.	from	University of
Scientific Supervisor	Prof. Dr. Eng. Nicolae Ţăpuş	from	University Politehnica of Bucharest
Reviewer	Prof. Dr.	from	University of
Reviewer	Prof. Dr.	from	University of
Reviewer	Prof. Dr.	from	University of

Bucharest 2018-2019

Rezumat

In informatica, una dintre tehnologiile cu creștere rapidă este cloud computing, care are cateva beneficii, precum și unele dezavantaje.

Cloud computing implică un set de servere care sunt utilizate împreună pentru a furniza conturi și servicii diferite. În general, cloud computing include două laturi, primul este front-end utilizat de utilizatori și clienți, iar al doilea este mediul din spatele locației furnizorilor. Interfața aplicației variază în funcție de utilizatori și depinde de serviciile cloud furnizate clienților. În ciuda diversității aplicațiilor, acestea sunt adesea unite în cerințele privind confidențialitatea. Beneficiile utilizării cloud computing în companii sunt reducerea costurilor și economisirea de timp. De asemenea, utilizarea cloud-ului comun este mai ușor decât construirea și dezvoltarea infrastructurii proprii. Furnizorii de cloud computing se concentrează pe furnizarea de servicii flexibile, infrastructuri IT eficiente din punct de vedere al costurilor și medii sigure pentru companii și organizații.

Aceasta lucrare de cercetare pornește de la concepte generale ale subiectelor care au legătură cu munca noastră. În capitolul I, prezentăm pe scurt fundalul subiectelor legate de teza noastră. De asemenea, explicarea tuturor problemelor legate de confidențialitatea cloud-ului și de confidențialitatea clienților. Apoi, spre a realiza acest obiectiv, în capitolul al doilea, începe cu o revizuire sistematică a literaturii pentru a examina rezultatele generale ale operelor conexe pentru a asigura confidențialitatea cloud-ului.

In capitolul III, descoperim intimitatea datelor în subiecte de cloud computing sau probleme de date mari, una dintre cele mai importante probleme. Metodele de confidențialitate studiate în capitolul II au arătat că încălcarea confidențialității pentru cloud computing sau date mari, sa produs din cauza riscurilor multiple (atacatori externi sau interni). Un risc important de luat în considerare atunci când vorbim despre confidențialitatea tranzacțiilor stocate este reprezentat de informațiile despre tranzacții, care nu sunt sub controlul proprietarului. Un astfel de caz este reprezentat de serverele cloud, care sunt administrate de către furnizorii, care nu pot fi de încredere în întregime de către utilizatorii cu date sensibile, cum ar fi planuri de afaceri sau

informații private. O metodă simplă pentru protejarea confidențialității datelor este prin aplicarea anumitor tehnici de confidențialitate asupra datelor tranzacțiilor, urmată de încărcarea datelor modificate în cloud. Propunem un studiu de caz care să se bazeze pe niveluri care să conțină trei modele: Furnizori de Cloud, manager de tranzacții și clienți. În plus, considerăm că studiul nostru de caz se bazează pe premisa de încredere zero între cele trei modele, prin urmare toate tranzacțiile au loc cu terțe părți, iar mișcările de date se realizează prin diferite niveluri de securitate.

In capitolul IV, am examinat datele clienților securizați în cloud, din perspectiva integrității și autenticității datelor. Acestea sunt probleme asociate cu partajarea datelor în cloud. Primul aspect de analizat este mecanismul de acces, ceea ce ridică probleme de securitate dacă nu este suficient de securizat pentru datele sensibile. Datele stocate în cloud (date mari) sunt adesea accesate de terți, ceea ce sporește expunerea la atacuri. În consecință, riscurile de violare a confidențialității devin mai mari. În mod obișnuit, datele stocate sunt prelucrate sau utilizate de terți. Proprietarii de date (clienții) trebuie să asigure confidențialitatea informațiilor despre datele stocate sau prelucrate. Soluția propusă în această lucrare pentru gestionarea și clasificarea datelor în cloud este o schemă organizată pe mai multe niveluri și bazată pe reguli, pentru a crește fiabilitatea cloud computing-ului în ceea ce privește confidențialitatea datelor sensibile. Lucrarea din capitolul al patrulea se bazează pe o structură solidă de politică(reguli) de securitate care respectă specificațiile și abilitățile. Algoritmul prezentat în lucrarea noastra noastră asigură în mod eficient acuratețea și validitatea datelor cu angajarea și gestionarea regulilor prezentate, respectând specificațiile clienților din cloud și posibilitățile furnizorilor de cloud.

Apoi, în capitolul al 5-lea, prezentăm combinația de metode pe care am sugerat-o în capitolele 3 și 4 pentru a furniza confidențialitate pentru serviciile bazate pe cloud Locations. Am examinat metoda de partajare a locațiilor securizate în capitolul al doilea și venim cu faptul că acest subiect necesită mai multe atenții. Aceste probleme asociate cu partajarea datelor în locații bazate pe cloud. Informațiile despre locație reprezintă o informație secundară care poate oferi informații personale despre viața cuiva. De exemplu, un spital este un spațiu public, iar locația reală a spitalului nu conține informații sensibile. Cu toate acestea, poate deveni sensibil dacă se analizează specialitatea spitalului. În acest capitol am propus că designul prezintă o combinație de metode pentru protejarea confidențialității datelor pentru serviciile bazate pe locație (LBS) cu utilizarea serviciilor cloud. Lucrarea construită în zero încredere și începem să gestionăm accesul la sistem prin diferite nivele.

Abstract

In computing, one of the rapidly growing technologies is cloud computing, which comes with great benefits, as well as with some drawbacks.

Cloud computing implies a set of servers that are used together to provide different accounts and services. In general, cloud computing includes two sides, the first one is the front end used by users and clients and the second one is the environment behind the providers' location. The application interface varies for users and it depends on the cloud services provided to the clients. Despite the diversity of applications, they are often united in privacy requirements. The benefits of using cloud computing in companies are cost reduction and time saving. Also, using shared cloud services is easier than building and developing own infrastructure. The providers of cloud computing focus on providing flexible services, cost-effective IT infrastructure and secure environments for companies and organizations.

The research work here starts from journey through general concepts of subjects which related of our work. In 1st chapter, we present in brief the background of the subjects related of our thesis. Also, explanation the whole of issues in cloud privacy and privacy of clients. then, towards achieving this aim, in 2nd chapter, starts with a systematic review of the literature to examining the general results of related works to provide privacy of cloud.

In 3rd chapter, we discover privacy of data in subjects of cloud computing or big data is one of the most principal issues. The privacy methods studied in 2nd chapter showed that privacy infringement for cloud computing or big data happened because multi risks on data by external or internal attackers. An important risk to take into consideration when speaking of the privacy of the stored transactions is represented by the transactions' information which is not in the owner's control. Such a case is represented by the cloud servers that are administered by cloud providers which cannot be wholly trusted by the users with sensitive, private data such as business plans or private information. A simple method for protecting data privacy is by applying certain privacy techniques onto transactions' data, followed by the upload of the modified data into the cloud. We are proposing a case study that is built on levels containing three models: Cloud Functions Providers, transaction's manager and clients. Moreover, we consider that our case study is based

on the premise of zero trust among the three models, therefore all the transactions take place with third-parties and the data movements are realized going through various levels of security.

In 4th chapter, we examined the secure clients' data in cloud, from the perspective of data integrity and authenticity. These are issues associated with sharing of data in clouds. The first aspect to analyze is the access mechanism, which raises security issues if it is not secured enough for sensitive data. Data stored in cloud (big data) is often accessed by third party, which increases the exposure to attacks. The privacy violation risks thus become higher. Cloud-stored data usually is processed or used by third party. Data owners (clients) must ensure information privacy of the stored or processed data. The solution proposed in this work for cloud data management and classification is a schema organized on multiple levels and based on policy in order to increase reliability of cloud computing in terms of confidentiality of sensitive data. The work in 4th chapter is based on a solid security policy structure which follow the specifications and abilities. The algorithm presented in our work efficiently provides data accuracy and validity with the employment and management of the outlined policies, complying to cloud customers' specifications and cloud providers' possibilities.

Then in 5th chapter, we present the combine of methods that we suggested in 3rd and 4th chapters to provide privacy for cloud Locations based-services. We had examined the secure clients' location sharing method in 2nd chapter and we come-out with fact is this subject need more attentions. These issues associated with sharing of data in cloud-based locations. Location information is a secondary information that can provide personal insight about one's life. For example, a hospital is a public space and the actual location of the hospital does not carry any sensitive information. However, it may become sensitive if the specialty of the hospital is analyzed. In this chapter we proposed design presents a combination of methods for providing data privacy protection for location-based services (LBSs) with the use of cloud service. The work built in zero trust and we start to manage the access to the system through different levels.