International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.341-352
http://dx.doi.org/10.14257/ijsia.2016.10.2.30

User Privacy and Security in Cloud Computing

AL-Museelem Waleed[1, a], Li Chunlin[2,b]

[1, 2]*School of Computer Science, Wuhan University of Technology, Wuhan, CHINA*
[a]*waleed_aboanas@hotmail.com*, [b]*waleedalmuseelem@gmail.com*

Abstract

Many clients worry about their susceptibility to attack if their businesses' crucial IT resources and information are outside the firewall. The extremely scalable nature of Cloud Computing allows its users to access huge amounts of data and use distributed computational resources via different interfaces. Cloud entities such as cloud service providers, users and business associates share the offered resources at diverse levels of technological operations. This research paper focuses on the user privacy and security in cloud computing and the solutions to improve privacy and security of cloud computing. The study employs UEC (Ubuntu Enterprise Cloud) Eucalyptus for simulation, which is the accepted open source cloud computing software as a solution. The paper assesses how security and privacy issues transpire in the context of cloud computing and examines ways in which they might be addressed. This paper aims to solve privacy and security issues in cloud computing using UEC (Ubuntu Enterprise Cloud). The methodology used involves encrypting and decrypting data to ensure privacy and security in the cloud.

Keywords*: Cloud computing, Ubuntu Enterprise Cloud, Data Encryption, Data Decryption.*

1. Introduction

Despite Cloud computing potential to present low cost security; organizations may enhance risks by storing vulnerable data in the cloud. Currently many organizations, particularly medium and small business (MSB) enterprises, are gradually realizing the importance by putting their data and applications into the cloud [13]. Cloud computing is defined as both the applications distributed as services over the Internet and the systems software and hardware in the data centers that offer those services [13]. There are four essential cloud delivery models depending on who supplies the cloud services. Among the delivery models are Private cloud where cloud services are provided exclusively for an organization and are controlled by a third party or the organization.

This paper aims to demonstrate an innovation for user privacy and security in cloud computing open source software. It is accomplished by use of UEC (Ubuntu Enterprise Cloud) Eucalyptus popular open source cloud computing software. In this paper, simulation of some of the potential attacks to users' metadata and data stored in Eucalyptus database files is used in order to supply the necessary information on the consequences of abuse of cloud users' information privacy and how to improve the situations.

1.1. Problem Statement

This paper focuses on using Ubuntu Enterprise Cloud (UEC) model to enhance user's privacy and security in Cloud computing by protecting data at rest, preventing other users in the cloud infrastructure who may have access to the same

ISSN: 1738-9976 IJSIA

storage from reading the information stored in the cloud, and preventing system administrators running cloud computing service from reading the data.

1.2. Disadvantages of Cloud Computing

The main disadvantage of cloud computing is that the user has no control over the performance of his/her applications or over his/her data that he/she may require, or the aptitude to change or audit the policies and processes under which the individual must work [13]. The other disadvantage is that the cloud clients may risk losing data by locking them into proprietary formats hence losing control over their data since the apparatus for monitoring the person using them or the person viewing them are not always given to the clients [11]. Data loss is, thus, a probable risk in several specific deployments.

2 Privacy Issues for Cloud Computing

Current cloud services cause an intrinsic challenge to data privacy [12]. This is because they normally result in data being accessible in unencrypted form on a machine operated and owned by dissimilar organization from the data owner. The different aspects of illustrating privacy issues include potential unauthorised secondary usage, lack of user control, complexity of regulatory compliance and lack of training and expertise.

2.1. Potential Unauthorised Secondary Usage

There is a risk that data processed or stored in the cloud may be set to unauthorised users. It is branch of standard business technique of cloud computing that the service supplier may gain proceeds from authorised secondary utilizes of users' information most frequently the targeting of advertisements [11]. Nevertheless, secondary data users such as resale of detailed sales to their competitors would be unsolicited to the data owner. Thus, it will be essential for CSPs and consumers to make officially binding agreement of how information provided to CSPS can be used.

2.2 Lack of User Control

User-centric control appears incompatible with the cloud: since a SaaS environment was used, the service supplier becomes responsible for data storage, in a way which control and visibility is limited [11]. Consumers cannot maintain control over their data when it is processed and stored in the cloud since it is prohibited requirement. The key aspect of lack of user control is the control over and ownership of the infrastructure: In cloud computing, clients' data is processed in the machine they do not control or own (the cloud), furthermore, there is unauthorised resale or misuse and a threat of theft. In addition, there can be lack of transparency about where the data is stored, who possesses it, and what is being done to it.

2.3. Complexity of Regulatory Compliance

Because of the worldwide nature of cloud computing and the several legislations in place around the world, it can be difficult to guarantee compliance with all the legislation that may be relevant in a particular place [13]. Placing data in the cloud may affect obligations, status and privacy rights, for instance, it may make it unfeasible to conform with some laws such as Canadian health Laws or Privacy Act. Trade privacy may be impacted and legal security can be reduced. Location matters

from authorized point of view since different laws can affect depending on place where the information exists, however, in cloud computing the data may sometimes be in manifold places simultaneously.

2.4. Lack of Training and Expertise

Running and deploying cloud services may require many jobs involving high skills [11]. In particular lack of trained persons can be a problem from the security approach. Furthermore, more employees activate privacy consequences rather than protecting information on a server to which extremely few individuals' can access. In relative to cloud computing, it is quite easy and quick to go to the portal to call for a service that is immediately provided, therefore unless appropriate management procedures are prepared, there is a risk that employees could change to using cloud computing services without sufficiently considering the risk and consequences for that specific situation.

3. Security Issues for Cloud Computing

3.1. Backup Vulnerabilities

Cloud service providers create multiple copies of information and store them in diverse locations to present a high level of performance and reliability [13]. This serves as a form of backup, though it can cause threats from attackers and can lead to further liability. Furthermore, there is a probability for data to be lost, specifically with storage as a service.

3.2. Gap in Security

Security controls for the cloud are similar to those utilized in IT environments. However, as the client relinquishes control to the cloud supplier, there is a related danger that the CSP will not sufficiently address the protection that they should be managing [13]. The risk will rely on the deployment model employed [13]. The inferior down the stack the cloud provider, the extra security the clients is accountable for: therefore, the clients of Infrastructure as a Service (IaaS) needs to incorporate security as they are mainly responsible for it, while in Software as a Service (SaaS) environments defence controls and their capacity are negotiated into the agreements for service [11].

3.3. Unwanted Access

There needs to be a proper intensity of access control in the cloud environment to defend the security of the assets [11]. Cloud computing may really increase the danger of access to confidential data [13].This may include foreign countries; there can be amplified risk because of government surveillance over information stored in the cloud, because the information may be stored in countries where formerly it was not.

3.4. Inadequate Data Deletion

Ensuring that the client has control over the lifecycle of their data and particularly deletion, in the logic of how to be certain that data that ought to be deleted actually are deleted and are not recuperate-able by CSP is a major issue for cloud [13]. Currently, there are no approaches to prove this as it depends on trust. Furthermore, the risk of data exposure varies according to service model employed such models include IaaS and platform as a service (PaaS) [13].

4. Ubuntu Enterprise Cloud (UEC)

UEC is an open source Linux based architecture which is included with Ubuntu server edition [12]. It provides virtualization capability; flexibility and applications to assist in deploying a cloud within an organization [11]. UEC will aim to solve the above privacy and security issues by ensuring that there is a reasonable balance between unrestricted cloud administrators' competence of fulfilling their duties and disclosure of only the precisely identified information based on administrators [13]. Furthermore, UEC should be able to limit the system level modifications requisite in order to make the use of privacy preservation technique trouble free and swift. In addition, UEC should not sustain any data loss on users' private information stored in the cloud database [12].

4.1. Case Study: Amazon's EC2 Infrastructure

In the case of Amazon's EC2 infrastructure, it portrayed that there had been multiple virtual machines (VMs) of various organizations having virtual boundaries separating each virtual machine can run within one physical server. Furthermore, their VMs have IP (internet protocol) address visible to cloud users. VMs situated in the same physical server appear to have close IP addresses since they were allocated at the same time [4]. An attacker can figure out the machine sharing the same resources as the intended target by looking at Ip addresses and setting up a lot of his own virtual machines [11]. It is possible to observe how access to the resources varies once the malicious virtual machine is placed on the server as its target hence potentially gather sensitive data about the victim [13]. In addition, the data in Amazon's EC2 virtual machine and S3 storage products were stored in readable form on cloud computing service.

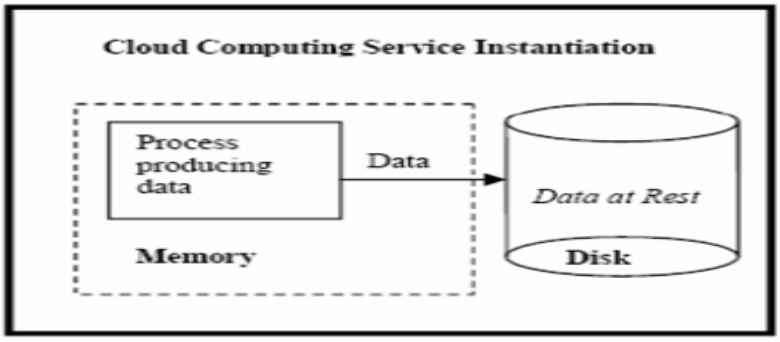


Figure.1 Amazon's EC2 Data Storage

5. Innovation Using Ubuntu Enterprises Cloud for Simulation

5.1. Methodology

DI string is the identity node from the root node to present node. The identity of entity M is ID_M = DI_0 || DI_M || DI_

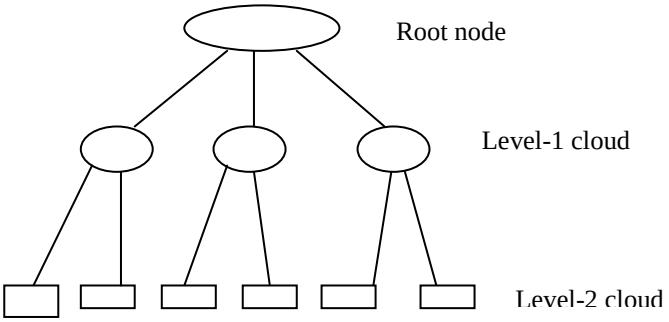


Figure 2. Hierarchical Model of Cloud

A. Root setup

Generate group A_1, A_2 of some prime order c and admissible pairing of â: A1*A2→A2;

Select an arbitrary generator Q ϵA_1;
Select cryptography hash functions B_1 :{ 0, 1}*→A_1, B_2:A_2→ {0, 1} ^{n}for some m;
Choose a random$\beta \epsilon Z^*_q$ and set R_o=α Q, Q_o=B_1(DI_o),H_o=α Q_o
The root master key is H_o and system parameters are < A_1, A2, ê, R_o, Q, Q_oB_1, B_2>

B. Lower level Setup

Assuming that there are z nodes in level 1, for every node, the root act as follows (let P be an arbitrary node in the z nodes).
The public key of node P:Q_x=B_1 (ID_p), where ID_p=D I_o||DI_p is computed;
The secret point node for P.$\rho_p$is $\rho_p \epsilon Z^*_c$
Set secret key node P: H_p=H_o+ ρ_p Q_p

5.2. Implementation and Results

Encrypted data is collected and decrypted with the collection users' private key which stays on the host. In this case, the client is the owner of the private key which cloud service provider has no control or view. The data is encrypted by computing Q_1=B(D I_o|| DI_1)
Q_2= B_1 (DI_o||DI_1||DI_2), random value such as s ϵZ^*_c is selected and output the cipher text by T=<sQ, sQ_1, rQ_2, B_2(g^s)+|- z>

During decryption, the entity receives the cipher text such as T= <V_o, V_1, V_2, U>then it decrypt using its secret key by k=ê (V_o, H_{E2})/$\prod^2_{i=1}$ê (R_{IDE2}I1, V_i) where E2 is the entity receiving the text and R_{IDE2}=ρ_1Q, R_{IDE2}I2= ρ_2Q. The output message will be z= B_2(k)+/- U

After this, the level one node acquires and securely keeps secret keys and points, R value and public key is then publicized.

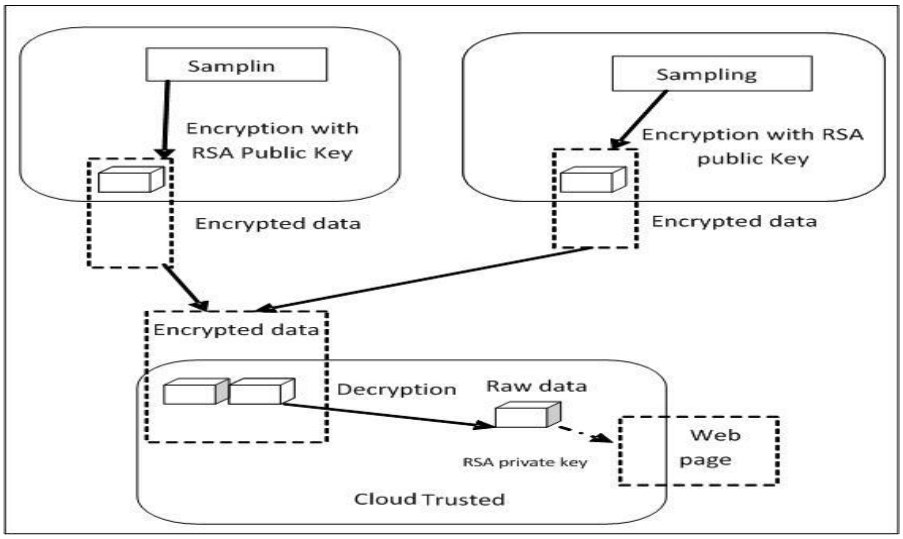


Figure .3. Advancing the User's Privacy and Security through Encryption of Data

UEC stresses the point whereby the management of cloud infrastructure by cloud administrator should not unconsciously lead to the abuse of cloud users' data privacy. The use of web interface for controlling user accounts, related administrative tasks (Eucalyptus) and data classification phase of UEC guarantees that the cloud database schema does not expose superfluous user related data to the cloud administrators. Furthermore it requisite cloud infrastructure associated configuration and authentication information to improve on data confidentiality of the cloud. UEC will ensure that there is no information loss incurred by protecting the private attributes using encryption instead of perturbation or generalization. Furthermore, UEC uses transitional tables to ensure integrity of private attributes. In the case of modification of data UEC ensures that no additional security parameters are required to obtain by cloud users and also user authentication processes are maintained unchanged. After the innovation of UEC in cloud computing, the administrators will not be able to view the users' data and furthermore they will not be able to modify data without the permission of the user. Encrypting the information available in the cloud increases the privacy and security of the cloud user. In addition it boosts the trust and confidentiality of the individuals who uses the cloud.

6. Enhanced Algorithms

The major issues faced on security for cloud computing are: integrity, availability and confidentiality of data [11]. Availability is assurance that data is available to user irrespective of their locations through mechanism like network security, authentication and fault tolerance. Integrity is assurance that message sent is similar to the message received with no alterations in between. This is ensured through the use of intrusion detection and firewalls. Confidentiality is prevention of exposition of user's data through unauthorized access [13]. This is ensured through use of data encryption, authentication methodologies and use of security protocols.

It is purely a demanding task for the cloud provider to provide data security and as such, they need to employ data encryption mechanisms as well as prevent data theft. Ubuntu Enterprise Cloud (UEC) has proved to have cloud security issues although they have provided numerous data security mechanisms. As users accesses

large volumes of data from cloud, complex cryptographic algorithms needs to be used to ensure speedy and efficient access to the secured data.

6.1. RSA-Public-Key Algorithm

This rides on the model that user data is encrypted before storing it to the cloud. User is required to place a request to the cloud provider, gets authenticated and data rendered. RSA as a block cipher maps every message to an integer. The cloud provider encrypts the data using the public key while the cloud user decrypts the data using the private key. RSA algorithm involves three steps key generation, encryption and decryption

6.1.1. Key Generation: This process is carried out before data is encrypted between the cloud provider and cloud user.
Steps:

1: Two distinct prime numbers are chosen a and b, due to security, the integers a and b should be selected at random and should be of same bit length.
2: Calculate n = a * b.
3: Calculate Euler's totient function, Ø(n) = (a-1) * (b-1).
4: Pick an integer e, such that 1 < e < Ø(n) and greatest common divisor of e, Ø (n) is 1. At this stage e is the Public-Key exponent.
5: At this stage d is determined as follows: d = e-1(mod Ø(n)) such that d is multiplicate inverse of e mod Ø(n).
6: d is regarded as Private-Key component, therefore, d * e = 1 mod Ø(n).
7: The Public-Key contain modulus n and the public exponent e for example, (e, n).
8: The Private-Key contains modulus n and the private exponent d, which are kept secret such as (d, n).

6.1.2. Encryption: Encryption is a method of converting original plain data into cipher data.
Steps:

1: Cloud service provider should transmit the Public- Key (n, e) to the user who wants to store the data.
2: User information is now mapped to an integer through the use of agreed upon reversible protocol, referred to as padding scheme.
3: Data is encrypted and the resulting cipher data C is C = me (mod n).
4: This cipher data or encrypted data is presently stored with the Cloud service provider.

6.1.3. Decryption: Decryption is the process of converting the encrypted data to the original data.
Steps:

1. In this process the cloud user requisite the Cloud service provider for the data.
2. Cloud service provider confirms the authenticity of the user and provides the encrypted data C.
3. The Cloud user decrypts the data by calculating, m = Cd (mod n).
4. Once m is achieved, the user can retrieve the original data by reversing the padding scheme.

7. Results of the Experiment

Sample data is taken and implementing RSA algorithm over it. During the implementation, different bits are used and the time taken to generate a key depends on the amount of bits used for the value of n.

Table 1. RSA Key Generation

Number of Bits	Computational time
512	0
600	0
800	0
1024	10
1700	15
2048	20
2300	65
3223	60
4200	75

7.1. Key Generation

1. Two distinct prime numbers a=61 and b=53.
2. n=a*b, therefore n=61*53 = 3233.
3. Euler's totient function, Ø (n)=(a-1)*(b-1), therefore Ø(n)=(61-1)*(53-1) = 60*52 = 3120.
4. Integer e =17, such that 1 < e < 3120 that is co-prime to 3120.
5. To compute d, d = e-1(mod Ø(n)), therefore d=17-1(mod 3120) = 2753.
6. As a result the Public-Key is (e, n) = (17, 3233) and the Private- Key is (d, n) = (2753, 3233). This Private-Key is reserved secret and it is identified only to the user.

7.2. Encryption

1. The Public-Key (17, 3233) is given by the Cloud service provider to the user who wishes to store the data.
2. If the user mapped the data to an integer m=65.
3. Data is encrypted by the Cloud service provider through the use of corresponding Public-Key which is shared by both the Cloud service provider and the user. C = 6517(mod 3233) = 2790.
4. This encrypted data is stored by the Cloud service provider.

7.3. Decryption

1. Provided that the user is valid, Cloud service provider will authenticate the user and delivers the encrypted data when user requests for the data.
2. The cloud user then decrypts the data by computing, m = Cd (mod n) = 27902753(mod 3233) = 65.
3. Once the m value is obtained, user will get back the original data.

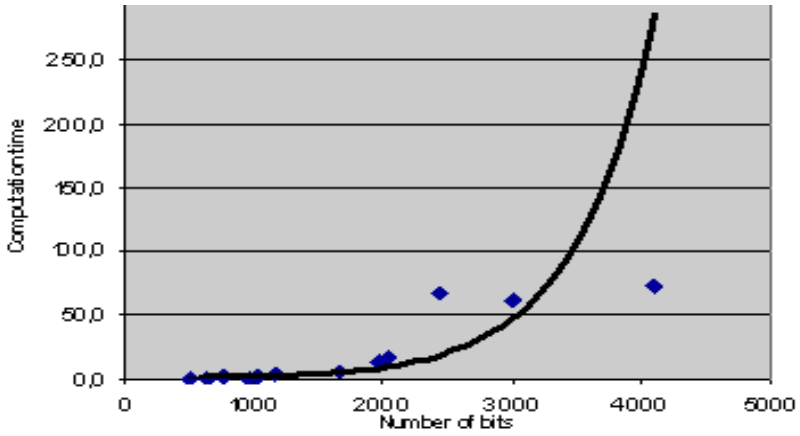


Figure 3. A Graph of Computation Time Verses Number of Bits

Based on the research, RSA is secure if *n* is adequately large. Even though the Keys of 512 bits are easy to be generated, it has a disadvantage that it is not much secure compared to 3223 bits. Once the number of bits is beyond 3223 bits, it takes a long time to factor until it reaches appoint that the hardware cannot factor it out.

8. Conclusion

This research paper emphasizes on the security deficiencies and the subsequent repercussions regarding the commonly ignored area of private cloud users' information privacy. UEC can prove to be a valuable point of cloud database designers, researchers and the cloud platform vendors seeking to progress the existing cloud solutions in order to argument the cloud users' assurance in using cloud based devices. UEC ensures privacy and security in cloud computing by making sure that there is a reasonable balance between unrestricted cloud administrators' competence of fulfilling their duties and disclosure of only the precisely identified information based on administrators. UEC guarantees that the cloud database schema does not expose superfluous user related data to the cloud administrators, hence increasing the privacy of cloud computing. The innovations of UEC in cloud computing increases privacy and security of the information since all the data in the cloud are encrypted and each cloud user keep their private key secretly.

9. Future Research

Cloud computing is an evolving area that handles part of an entire company's data. It therefore becomes a prime responsibility to the cloud provider to offer data security and thus a need to rely on cryptography and trusted computing techniques. Thus, by implementing RSA algorithm on cloud computing, data security is achieved. In the proposed works, cloud resources should only be available to the authorized user. Other enhanced ways of encrypting the data in transit should be researched, thus, if any unauthorized user gets access to the data, the data should only be rendered in unreadable format. Future research should investigate the hardware that can factor RSA bits with shorter time, hence, increasing cloud security due to the use of larger bits.

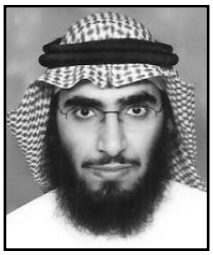
Acknowledgements

The work was supported by the National Natural Science Foundation (NSF) under Grants (Nos. 61472294, 61171075), Key Natural Science Foundation of Hubei Province (No. 2014CFA050), Applied Basic Research Project of Wuhan (No. 2015010101010021), National Key Basic Research Program of China (973 Program) under Grant No. 2011CB302601, Program for the High-end Talents of Hubei Province.

References

[1] AL-Museelem Waleed & Li Chunlin , Data Security and Data Privacy in Cloud Computing, Advanced Materials Research Vol. 905 (2014) pp 687-692.
[2] He, Debiao & Khan, Muhammad Khurram & Wu, Shuhua , On the security of a RSA-based certificateless signature scheme. International Journal of Network Security, v 16, n 1, p 78-80, January 2014; ISSN: 1816353X, E-ISSN: 18163548.
[3] Mehdi Hussain & Ainuddin Wahid Abdul Wahab& Ishrat Batool&Muhammad Arif ,Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography, International Journal of Security and Its Applications Vol.9, No.2 (2015), pp.179-188.
[4] B. Halpert, Auditing cloud computing: A security and privacy guide. Hoboken, N.J: John Wiley & Sons, 2011.
[5] J.W. Rittinghouse & J.F. Ransome, Cloud computing: Implementation, management, and security. Boca Raton: CRC Press, 2010.
[6] Y. George & P. Siani, Privacy and Security for Cloud Computing. Springer: London, 2012.
[7] International Conference on Knowledge Management in Organizations: Service andCloud Computing, & L. Uden, 7th International Conference on Knowledge Management in Organizations: Service and Cloud Computing. Berlin: Springer, 2013.
[8] A.C. Simmons, Once more unto the breach: Managing information security in an uncertain world. Ely, Cambridgeshire, U.K: IT Governance Pub, 2012.
[9] M.H. Wittow & D.J. Buller, Cloud Computing: Emerging Legal Issues for Access to Data, Anywhere, Anytime.Journal of Internet Law, 14(1), 2010, pp. 1-10.
[10] Metropolia & E. Guchu, Implementation of cloud infrastructure using open source software. Metropolia Ammattikorkeakoulu, 2012.
[11] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, & J. Molina, Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In Proceedings of the ACM Workshop on Cloud Computing Security (CCSW'09), Chicago, Illinois, USA, pp 85-90, ACM Press, New York, USA. 2010.
[12] B.R. Chang, Z.Y. Lin, C.M. Chen, F. Huang, C.-H.F. Tsai, International Conference on Machine Learning and Cybernetics, ICMLC 2012.(2012). Intelligent VVoIP implementation in UEC cloud computing. Proceedings - International Conference on Machine Learning and Cybernetics, 2, 2012, pp. 519-524.
[13] Turun & A.O. Ayoola, On-premise cloud computing: deploying a private cloud infrastructure with Ubuntu Server 10.04 Enterprise Cloud (UEC). Turunammattikorkeakoulu, 2013.

Authors



AL-Museelem Waleed, I'm from Kingdom of Saudi Arabia birth in 5th January 1981 at Capital City Riyadh. Currently I'm a PhD student in College of Computer Science and Technology at Wuhan University of Technology. I received M.S in Computer Science and Technology from Wuhan University of Technology, China, in 2012. My research interests are cloud computing security and data privacy.

Li Chunlin, she is a Professor of Computer Science in Wuhan University of Technology. She received the M.S in Computer Science from Wuhan Transportation University in 2000, and PhD in Computer Software and Theory from Huazhong University of Science and Technology in 2003. Her research interests include cloud computing and distributed computing.