PROVIDING SECURITY TO CLOUD IN SERVICES AND PRIVACY MODEL

Dhanam.M [1], Abitha.K[2], Arthi Rathna.R[3]

[1,2,3.] M.Tech Student, Department Of Computer Science And Engineering

Rajiv Gandhi College Of Engineering & Technology, Puducherry, (India)

ABSTRACT

Cloud computing is becoming increasingly a magical solution and a widely adopted technology for delivering services over the Internet thanks to its diverse benefits, including services on demand, reducing costs, sharing and configuring computing resources, and high services scalability and flexibility. However, with the emergence of this technology, the concept of security and privacy has become a major barrier to c10ud services adoption. lndeed, many research works have been done to identify c10ud security and privacy issues. It is in this context that in this paper, we will provide a new c10ud security and privacy model (CSPM) into layers which can be taken into account by cloud providers during all the stages of c10ud services building and monitoring. This model will permit to overcome this c10ud services barrier adoption and thus, to build confidence in c10ud services and also to provide secure services. Finally, we will present some security threats and attacks, and propose, according to CSPM, some countermeasures.

Keywords-Cloud Computing; Cloud Provider; Cloud Consumer; Cloud Service; Cloud Security And Privacy Model (CSPM); Security; Privacy.

I. INTRODUCTION

Thanl(s to the diverse advantages offered by cloud computing (including services on demand, reducing costs, sharing and configuring computing resources, and high services scalability and tlexibility), cloud computing has become a widely adopted technology for delivering services over the Internet.

Indeed, all this advantages have encouraged major of companies to outsource their IT infrastructure to cloud environment.

According to the National Institute of Standards and Technology (NIST), cloud computing is composed of three basic service models, namely: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), and four deployment models: public, community, private and hybrid cloud.

Furthermore, the NIST defined five essential characteristics that distinguish cloud from other technologies, namely: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

In the SaaS model, the cloud provider supplies the consumer with applications as a service running on a cloud infrastructure, accessible from various consumer devices through either a consumer interface (such as web browser and a program interface).

And is only responsible for managing and controlling the underlying cloud infrastructure including network, servers, operating systems and storage.

In the PaaS model, the consumer is not responsible for managing or controlling the underlying cloud infrastructure, but he has control over the deployed applications and possibly configuration settings for the application-hosting environment.

In the laaS model, the cloud provider is responsible for managing and controlling the underlying cloud infrastructure and the consumer has control over operating systems, networking components, storage, and deployed applications [1].

Indeed, the concerns about security and privacy have become a major barrier to cloud services adoption. As widely known, cloud environment is widely distributed and highly dynamic [2]; therefore, several threats and attacks at cloud infrastructure, network, access to cloud services, etc, can threaten both the availability and the security of cloud services. These threats and attacks can be outsider or insider to the cloud. Insider threats and attacks in the cloud are divided in two categories: first, a malicious insider working for cloud provider and second, an insider working for an organization which outsource its IT infrastructure into the cloud [3].

In case of attacks on cloud, it is easier to re-ensure the availability and the performance of cloud services than to re-ensure the availability of data with total integrity and confidentially. In general, the cloud providers are responsible for assuring the availability of cloud services. However, the responsibility of ensuring its security is shared between cloud providers and cloud consumers with different percentages depending on the types of cloud services. Indeed, in an insecure environment like in the cloud, sensitive data must be seeured. Therefore, cloud providers should adopt necessary security mechanisms and countermeasures to overcome these concerns and to strengthen confidence in c10ud services.

Newly, many research works have been done to identify and to c1assify cloud security and privacy issues. In [4], authors c1assified c10ud security issues into five categories: security standards, network, access control, cloud infrastructure and data. In [5], the Cloud Services Measurement Initiative Consortium (CSMIC) developed a standard measurement framework, called Service Measurement Index (SMI). SMI is hierarchical and divided into seven categories, one of these categories is Security and Privacy.

The Security and Privacy category of this framework includes attributes namely: Access Control and Privilege Management, Data Geographic/ Political, Data Integrity, Data Privacy and Data Loss, Physical and Environmental Security, Proactive Threat and Vulnerability Management, Retention/Disposition, and Security Management. In [6], we used these security and privacy c1assifications as a basis to propose a Cloud Security and Privacy Model (CSPM) into layer.

CSPM is composed into five layers, which can be taken into account by c10ud providers during all the cloud services building and monitoring stages. This model can help also c10ud providers to make the difference between attacks whose threaten the availability and the security of c10ud services, and to adopt necessary countermeasures, in order to provide secure services to their c1ients.

The main goal of this work is to describe the layered model, to present some security threats and attacks, and to propose according to this model some countermeasures.

The remainder of this paper is organized as follows: after a presentation of some related works (Section 11), Section 111 will describe the layered c10ud security and privacy model, and present its advantages. Then, some c10ud security threats and attacks will be presented in Section IV. In Section V, we will propose according to CSPM, some countermeasures. And finally, in Section VI, we will present our conclusions and future worl.

II. RELATED WORK

Recently, many research works have been done to identify cloud computing security and privacy issues.

In reference [7], the authors provided a survey on cloud computing security issues and vulnerabilities connected with virtualization infrastructure, software platform, identity management and access control, data security, legal compliance, etc. They divided the cloud security issues into four main categories.

Firstly, cloud infrastructure, platform and hosted code. This category comprises concerns related to virtualization, storage and networking vulnerabilities. Secondly, the data category, which comprises concerns around data integrity, data lock, data confidentiality, etc. Then, the access category constituted by the concerns around authentication, authorization, and access control to cloud services. And finally, the compliance category which includes concerns about security audit, data location and operation traceability.

In [4], Issa M. khalil et al. based on work [7] and more other related works to provide a deep survey on cloud security and privacy concerns including, vulnerabilities, threats and attacks. They provided a c1assification of known cloud attacks and a comparative analysis of some Counter measures.

Also, they provided a c1assification of cloud security related issues of the five categories mentioned: security standards, network, access control, cloud infrastructure and data. In [5], the Cloud Services Measurement Initiative Consortium (CSMIC) developed a standard measurement framework, called Service Measurement Index (SMI). This framework is designed to become a standard method to help organizations to measure c1oud-based business services, based on their specific business and technology requirements.

The framework SMI is hierarchical and divided into seven categories including: Accountability, Agility, Assurance, Financial, Performance, Security and Privacy, and Usability, and each category is defined by three or more attributes. The Security and Privacy category of this framework, and particularly version 2.1 includes attributes namely: Acceess Control and Privilege Management, Data Geographlc/ Political, Data Integrity, Data Privacy and Data Loss, Physical and Environmental Security, Proactive Threat and Vulnerability Management, Retentionl Disposition, and Security Management.

According to reference [4], the security standards category includes service level agreements (SLA), auditing and other agreements between consumers, service provider and other stakeholders. However, CSMIC classified the principle of security standards category in accountability category of SMI framework.

Furthermore, in [4], the authors classified cloud applicable attacl(s into nine groups namely: theft of service, denial of service, cloud malware injection, cross VM side channels, targeted shared memory, phishing, botnets, audio steganography, and VM rollback attack. And they provided a comparative analysis of some famous security mitigation techniques. Indeed, these attacks can threaten both the availability and the performance of cloud services, and the security of data stored in the c1oud.

Regarding attacks on the availability and the performance of c1oud services, c10ud providers can easily re-ensure the availability and the performance of these services. However, regarding data attacks, it is difficult to ensure the re-availability of these data with complete integrity and confidentially. Therefore, cloud providers should be able to make the difference between attacks which threaten availability of services and those who threaten data security. This will permit to adopt countermeasures necessary to ensure both the availability of services and the security of data storage in c1oud environment and to build confidence in cloud services.

To solve this dilemma, in [6] we essentially take works provided in [4] and [5] as a basis to propose a c10ud security and privacy model (CSPM) into layer. This model will be divided into five layers. And can help c1oud providers to distinguish between attacks which threaten availability of cloud services and others which threaten security of c10ud services, and to adopt necessary countermeasures to provide secure services.

In the section 3, 4 and 5 respectively, we will describe this model and provide its advantages. We will present some security attacks and threats, and propose some countermeasures according to this model.

III. PROPOSAL MODEL FOR SECURITY AND PRIV ACY OF CLOUD COMPUTING

The cloud security and privacy model (CSPM) is a layered model, which is divided into five layers namely: Physical and Environmental Security, Cloud Infrastructure Security, Network Security, Data, and Access Control and Privilege Management. As shown in Figure 1 [6].

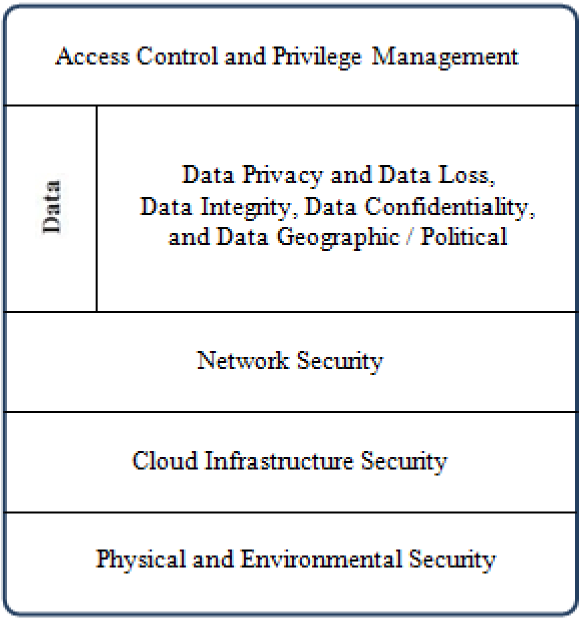

Access Control and Privilege Management
Data
Data Privacy and Data Loss, Data Integrity, Data Confidentiality, and Data Geographic / Political
Network Security
Cloud Infrastructure Security
Physical and Environmental Security

Figure I. Cloud Security and Privacy Model

Physieal and Environmental Seeurity Layer (PESL):

Processes and policies adopted by the c10ud providers to protect their facilities against unauthorized physical access, damage, etc [5],[6].

Cloud Infrastrueture Seeurity Layer (CISL): Includessecurity issues specific to cloud inrrastructure (IaaS, PaaS andSaaS) and is particularly related with virtualization environment. Security issues of this layer includes: msecure interface of API, sharing technical tlaws, security misconfiguration, multi-tenancy, etc. [4],[6].

Network Seeurity Layer (NSL):

Refers to the medium through which the users connect to cloud services, including browsers, network connections, etc [4],[6].

Data Layer (DL):

This layer is composed of Data Geographic I Political, Data confidentiality, Data Integrity, and Data Privacy and Data Loss.

Data Geographie / Politieal:

Constraints of the consumer on the location of services, based on geographical or political risk [5], [6].

Data Conjidentiality:

Ensures that data remains confidential and invisible even to the cloud provider, and even if the provider data centre have been attacked, customer data can neither be stolen nor reused [6],[8].

Data Integrity:

Keeping data in its correct form. It means that the system must prevent undue modification of information (i.e. a modification by unauthorized consumers or incorrect modification by authorized consumers) [5],[6], [8].

Data Privacy and Data Loss:

The c1oud providers enforce the restrictions on consumers to use and share data. Any failures of these protections are rapidly detected and reported to the consumer service [5],[6].

Aeeess Control and Privilege Management Layer

(ACPML):

Policies and processus used by c10ud providers to ensure that only the consumers granted appropriate privileges can use or modify data. It includes identification,

authentification and authorization issues [4], [5], [6].

Advantages of CSPM and the interest of structuring it into layers can be summarized into:

- Can help cloud providers and researchers to identify and
- classify different cloud security and privacy issues.
- Can help c10ud providers to identify and make the
- difference between different sources of cloud threats.
- Can help c10ud providers to adopt counter measures (intrusion detection system or/and intrusion prevention system) necessary for each CSPM layer, in order to ensure both the availability and the security of cloudservices.
- Can facilitate the security monitoring of c10ud services.

IV. CLOUD SECURITY THREATS AND ATTACKS

Currently, there are many threats and attacl(s in the ITworld. Indeed, c1oud environment is widely distributed andcan provide the services to consumers who have maliciouspurposes; therefore, c10ud environment is more minatory ofthreats and attacks than other environments. These threats and attacl(s are numerous including denial of service, c1oud malware injection, etc [4]. Indeed, these threats and attacks can be outsider or insider of the c1oud, and can affect the availability and the security of cloud services. In this section we will focus on threats and attacks which threaten the security of c10ud services. This type of threats and attacks are also numerous; thus, we will present some of them wellknown.

A. Insider Attacks

Indeed, both the c1oud providers and the c10ud consumers (entreprises, ...) should adopt the hardest policies and processes to ensure that only the authorized consumers (simple consumers, system administrators, ...) can have access to their data centers.

An authorized system administrator who wishes to access to data centers of his organization needs to go physically on-site or remotely through VPN, sign in, and use specific access credentials (such as: smart card, RFID system,...) [3]. These credentials have to valid the access to each organization system.

Even if the techniques which ensure that only the authorized consumers can have access to cloud services are adopted, a malicious system administrator working for the c10ud providers or for the c10ud consumers can exploit appropriate privileges to disclose, to use or to illegaIly alter the sensitive data of her organization's c1ients. This attack can target the physical and the environmental security, the cloud infrastructure security layers, and also threaten on safety of both systems and data. Detecting such an attack can be a difficult task due to the circumvention of malicious (in order to hide from the detection of intrusion) on organization's security mechanisms.

B. Cloud Malware Injection Attacks

In case of cloud malware injection attack, the attackers upload a manipulated copy of the c10ud victim's service instance into cloud environment. This will allow them to
process some service requests of the victim's service in their
malicious instance. This type of attack targets c1oud infrastructure layer, and can give to attackers unauthorized access to c10ud resources, to c10ud consumers private data, etc.[4][9].

C. Cryptographic Attacks

The concerns around data confidentiality as weIl as its integrity have become a major barrier to cloud services adoption. Indeed, cloud computing security which is based on cryptographic techniques appears to be an effective way to overcome these concerns and to strengthen confidence into cloud services.

The cryptographic techniques can ensure both confidentiality and integrity of data when transmitted and when stored. However, these techniques when adopted to secure data in cloud environment are somewhat different to the traditional use. In the cloud case only the c1oud consumer can have the private key. Thus, the private data remain confidential and incomprehensible even to the c1oud provider. In effect, cryptographic techniques can ensure a high level of both data confidentiality and data integrity. However, various attack techniques on ciphers are being serious threats on safety of private data. Among these attacks: linear, differential, algebraic and error regulation-based cryptanalysis[10], and each one has particular features according to the design of cryptosystems. As weIl, side channels attacks can target the hardware implementation of a cryptographic cryptosystem [11].

The main goal of aIl these attacl(s are to reveal or/and to alter the originals data. Indeed, cloud environment is widely distributed and provides aIl the services over the Internet. Therefore, this type of environment is more threatened by attacks than other environments. These attacks can threaten three levels: the cloud consumers, the data transmitted over Internet and the data stored in c1oudenvironment (as described in the figure 2).

Cloud Consumer: Although only the c10ud consumer can have the decryption key, the attackers use some attacks techniques that target the consumer's device so that they can steal the consumer private key. Norrnally, the encryptionl decryption software is provided by c10ud provider; therefore, a malicious system administrator working for the cloud provider can inject software by some malware into other to steal the private key of c10ud consumer.

Data over the Internet :

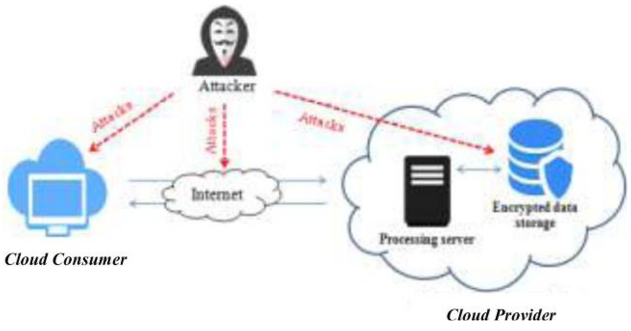
As widely known, c1oud computing provides aIl the services over the Internet; therefore, many attacks can threaten the transmitted data between the c1oud service provider and the c1oud consumer. The attackers can intercept the ciphers and try to re cover the decryption key or the plaintext. Also, they can change these transmitted data in order to effect on data integrity.

Data stored in cloud : The consumers (companies, ...)chose to outsource their data in encrypted form to the cloud. In this case the data must be encrypted before sending it to the cloud environment. Indeed, the safety of the encrypted data is based on the robustness of both the cryptosystem and its encryption/decryption keys. Normally, the encrypted data and the public keys (in the case of using asymmetric-key cryptosystems to encrypt the data), will remain stored for a long time by the same encryption keys in c1oud environment.

Therefore, the attackers (insiders or outsiders) that can accede to cloud data center, can exploit this long duration to recover originals data or private keys from ciphers or from public keys. These attackers can also have an effect on data integrity. Among cryptographic attacks, the brute force attack [10] that consist in trying all the possible keys to decrypt ciphers.

In the normal case of using cryptographic cryptosystem, a feasible attack which can allow to find the correspondent decryption key in a reasonable time.

But, in the c1oud case the brute force attack can be feasible even with the hard keys, due to the long duration of encrypted data storage in c1oud servers.



D. Account and Service Hijacking Attacks

Account and service hajacking attack is not new, but still achieves results and remains a top threat on IT services delivered over the Internet. Frequently, the attackers exploit the software vulnerabilies and use many deceptions like sending the links to users through emails or instant messages which lead to illegitimate sites so that they can obtain users sensitive informations such as credentials, passwords and credit card information. If an attacker gains access to consumer service credentials, he can eavesdrop on his activities and transations.

And can leverage the power of consumer's services reputation to launch other attacks. In c1oud case this attack can be executed by illegitimate use of c1oud services or through tradition al social engineering techniques [4][12].

V. COUNTERMEASURES

In this section, we will propose some countermeasures of cloud security attacks. Particularly, we will focus on security methods and techniques that can be adopted at level of Data, and Access Control and Privilege Management layers of CSPM.

A. Data layer

Indeed, the fear of seeing private data be processed in raw is a major obstacle to cloud services adoption. Thus, researchers stressed the useful techniques in this type of environment: cryptographic techniques.

The cryptographic cryptosystems are divided into two main types [10]: symmetric-key and asymmetric-key cryptosystems. These techniques can ensure a high level of the confidentiality of data storage or/and data treatment. Originally, asymmetric-key cryptosystems are created to ensure the confidentiality of exchange secret keys of symmetric-key cryptosystems. The performance (in terms of response time) of this cryptosystems type is very slower than other type. Regarding the confidentiality storage service, data can be encrypted before sending them to cloud environment, using some symmetric-key cryptosystems. But, regarding the confidentiality of data storage and data treatment, the homomorphic encryption technique appears to be an effective way to ensure this type of service.

1)Symmetrie Key eryptosystems:

Can encrypt the data and convert them into incomprehensible format. These cryptosystems are numerous (such as: AES, Blowfish, RC4,...), which use same key to encrypt and decrypt data and divided into block ciphers and stream ciphers [10]. The philosophy of symmetric key cryptosystems when used in cloud environment is somewhat different to other use cases. Normally, these types of cryptosystems were created to ensure confidentiality of communication between a sender and a recipient over the Internet. In cloud case, these cryptosystems are used to ensure data confidentiality when transferred and stored in cloud servers and only the consumer can have the private key [6].

2) Homomorphie eneryption teehnique :

Homomorphic encryption [13] is a form of encryption which allows a third party the ability to perform the operations on encrypted data without knowing the private key. The cryptosystems of this technique are asymmetric key. These operations are depending on the properties of the cryptosystem, and generate an encrypted result. The result obtained is the same as working directly on raw data. Thus, the data and the result of any operation remains confidential and unreadable even to the cloud provider [6].

B. Access Control and Privilege Management layer

The access control and privilege management are policies and processes used by cloud providers to ensure that only the consumers granted appropriate privileges can accede, use or modify data. Lately, the researchers have proposed many models (such as: Attribute Based Encryption (ABE), Key Policy Attribute ßased Encryption, Cipher Text Policy

Attribute Based Encryption, etc[see 2]) that are useful to provider security and access control. The majority of these proposed models are the modified form of classical model of AßE. Attribute Based Encryption (ABE) is introduced by Sahai and Waters in 2005 so as to provide security and access control. ABE is a public-key based one to many encryptions which allows users to encrypt and decrypt data based on user attributes. The secret key of user and the ciphers are dependent upon user attributes (such as user geographicai ...). A cipher text decryption is possible only if the set of attributes of the user key matches the cipher text attributes [2].

The majority of these access control techniques use the concept of keys to allow cloud consumers accede to services delivered over Internet. Indeed, many well-known attacks such as: Account and service hajacking attacks, that can allow attackers to obtain the private keys of cloud consumers; therefore, these techniques must be irnproved or changed to work effectively with the cloud nature in order to ensure a high level of access security to cloud services

VI. CONCLUSION AND FUTURE WORKS

In this paper, we have proposed a new cloud security and privacy model into layers that can help cloud providers to identity and class different cloud security and privacy issues, to make the difference between different sources of cloud threats, and to adopt necessary countermeasures in order to build confidence in cloud services and also to provide secure services. Also we have presented in this work some security threats and attacks and proposed some countermeasures.

These countermeasures can be used to ensure the security and the privacy of "Data", and "Access Control and Privilege Management" layers of CSPM.There are many traditional countermeasures to mitigate security and privacy issues. Indeed cloud environment is widely distributed, highly dynamic and more threatened by attacks.

Therefore, these countermeasures must be improved or changed to work effectively in this type of environment.

In our future worles we will focus on countermeasures that can ensure the security and the privacy of both "Data layer" and "Access Control and Privilege Management" layer. We will study the feasibility of existing techniques and we will try to improve and adapt them in cloud environment.

REFERENCES

[1]. P. Mell, T. Grance, "The NIST Definition of Cloud Computing,"National Institute of Standards and Technology, U. S. Department of Commerce, September 2011.

[2]. RajaniKanth, M. Lakshmi, "A Survey on Access Control Models in Cloud Computing," Emerging ICT for Bridging the Future. Advances in Intelligent Systems and Computing, Vol. 337. Springer International Publishing, Switzerland, pp. 653-664, 2015.

[3]. M. Kandias, N. Virvilis, D. Gritzalis, 'The Insider Threat in Cloud Computing," Critical Information Infrastructure Security. Lecture Notes in Computer Science, Vol. 6983. Springer-Verlag, Berlin Heidelberg,pp. 93-103,2013.

[4]. Issa M. Khalil, A. Khreishah, M. Azeem, "Cloud Computing Security:A Survey," Computers, Vol, 3, pp. 1-35,2014. The Cloud Services Measurement Initiative Consortium (CSMIC):Service Measurement Index Framework Version 2.1. Carnegie Mellon University Silicon Valley Moflett Field, CA USA, July 2014.

[5]. K. EL MAKKAOUI, A. EZZATI, A. BENI-HSSANE, C. MOTAMED,"Data confidentiality in the word of c1oud," Journal of Theoretical and Applied Information Technology, Vo1.84. No.3, 2016.

[6]. S. Sengupta, V. Kaulgud, V.S. Sharma, "Cloud computing security -Trends and research directions," In Proceedings of the 2011 IEEE World Congress on Services, Washington, DC, USA, pp.524-531, 2011.

[7]. S. Kamara, K. Lauter, "Cryptographic Cloud Storage," Financial Cryptography and Data Security. Lecture Notes in Computer Science, Vol. 6054. Springer-Verlag, Berlin Heidelberg, pp. 136-149,2010.

[8]. N. Gruschka, M. Jensen, "Attack surfaces: A taxonomy for attacks on c10ud services," In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, pp. 276-279, 2010.

[9]. O. Cangea, G. Moise, "A New Approach of the Cryptographic Attacks," Digital Information and Communication Technology and Its Applications. Communications in Computer and Information Science,Vol. 166. Springer-Verlag, GmbH Berlin Heidelberg, pp.521-534, 2011.

[10] K. HyunHo, B. Ndibanje, L. Hoon-Jae, C. YongJe, C. Dooho, "Side Channel Attacks on Cryptographic Module: EM and PA Attacks Accuracy Analysis," Information Science and Applications. Lecture Notes in Electrical Engineering, Vol. 339. Springer-Verlag, Berlin Heidelberg, pp. 509-516,2015.

[11]. CLOUD SECURITY ALLIANCE: The Notorious Nine: Cloud Computing Top Threats m 2013. https://c1oudsecurityalliance.org/group/top-threats/M.

[12]. Ogburn, C. Turner, P. Dahal, "Homomorphic Encryption," Procedia Computer Science 20, Elsevier, pp. 502 - 509, 2013