IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 2, Ver. I (Mar-Apr. 2016), PP 10-16
www.iosrjournals.org

A Novel Framework for Dependable Cloud Computing

Dr. Roy Joel Ureigho[1], Edje Abel[2], Felix Elugwu[3]
[1]*Department of Computer Science and Informatics, Federal University Otuoke, P.M.B. 126, Yenagoa. Bayelsa State, Nigeria.*
[2]*Department of Mathematics and Computer Science, Delta State University, Abraka. Delta State, Nigeria.*
[3]*Department of Computer Science, Delta State Polytechnic, Otefe-Oghara. Delta State, Nigeria.*

***Abstract*:** *The cloud computing is one technology that has taken the computing world by storm with potent opportunities that are so tempting to ignore. Yet many are skeptical about its adoption because of the many problems that came with internet usage. The belief is that since cloud computing is an offshoot of internet, there are possibilities of multifaceted problems possibly inherited from Internet. They opined that since data will be under the care of cloud service provider, there will be likelihood of compromising data integrity and other security risks. In this work, a framework for dependable cloud computing was designed in such a way that all stakeholders have one part or the other to play to ensure the security of data.An encryption system was designed to encrypt and decrypt data in transit between the client private cloud and the cloud service provider. This ensures that data is delivered to the service provider in encrypted form. Since the task of securing the data stored has the involvement of all stakeholders, it increases the trust level thereby making it dependable.*

***Keywords*:** *cloud computing, dependable cloud computing, internet, security*

I. Introduction

Cloud computing is a technology that is so equally transformational and feared by many. It is hard to find any other comparable technology both now and in the past which has the power to positively re-engineer the manner that technology supports organizational goals. But possibly by a combination of issues such as negative pundit messaging and well-founded suspicion of wide-scale technology and organizational readiness, cloud computing appears to be the most feared of the big technology innovations.

In a world that sees new technological trends bloom and fade out almost on daily basis, one new trend promises more longevity. This is because it extends the Internet capabilities. This trend is called cloud computing, and it will change the way we use computer and the Internet. Just as the benefits are obvious, however, so too are the security concerns.Cloud computing is based on open system architecture where costumers' data and program reside in cloud service provider premises. That's the reason why security is a major issue. Stakeholders always find themselves asking various question before they adopt cloud computing.

Cloud computing shares in common with other network-based application, storage and communication platforms certain vulnerabilities in several broad areas:

- Web application vulnerabilities.
- Accessibility vulnerabilities.
- Authentication of the respondent device or devices.
- Data Verification, tampering, loss and theft while on a local machine, or in transit, or at rest at the unknown third-party device, or devices, and during remote back-ups.
- Physical access issues, both the issue of an organization's staff not having physical access to the machines storing and processing a data, and the issue of unknown third parties having physical access to the machines.
- Privacy and control issues stemming from third parties having physical control of data.

Many prospective adopter of cloud computing are curious about what will happen to their data/information when it is hosted in the cloud. How would they be harmed if an employee of the cloud service provider or any other outsider accessed and manipulated their data/information? What will happen if as at the time they need the stored data, it is not available for that period? These are some of the basic questions that often arise in the mind of any prospective adopter of cloud computing.

The significance of this work is to contribute techniques to improve the vulnerability of cloud computing. In improving the techniques that prevent and detect security flaws, it is hoped that cloud services can justifiably be relied upon that is it can be considered dependable. The security model designed is also a significant advance in security of cloud computing.

II. Related Works

There are others who have carried out various studies successfully in cloud computing security. IBM developed a secured hypervisor called sHype to help solve the problem of separating private data between Virtual Machines, virtualization containment attacks and hypervisors attack against Virtual Machine (VM) [1].

[2]in their work proposed a trusted cloud computing platforms using Trusted Computing Group specifications.[3]presented the technical security issues in Cloud Computing; however, these issues are more related with the problems of web services and web browser and not of Cloud Computing.

[4]in his work titled "building trust into utility cloud computing" also proposed Private Virtual Infrastructure (PVI) and Locator Bot as a means of securing data processed by the VMs in the cloud. The various implementation strategies of securing cloud computing by these researchers form the basis for this study. They provided the needed platform for future work as their method of cloud security implementation serve as reference point.[5]discussed key challenges in achieving a trusted cloud through the use of detective controls, and presents the TrustCloud framework, which addresses accountability in cloud computing via technical and policy based approaches.

III. Risks And Security Concerns With Cloud Computing

Many of the risks frequently associated with cloud computing are not new, and can be found in enterprises today. Some examples of cloud computing risks for the enterprise that need to be properly managed include:

- Choice of trusted cloud service provider based on history and sustainability. Sustainability is of particular importance to ensure that services will be available and data can be tracked.
- The responsibility of information handling is transferred to the cloud provider, which is a critical part of the business. Failure to perform to agreed-upon service levels can impact not only confidentiality but also availability, severely affecting business operations.
- The dynamic nature of cloud computing may result in confusion as to where information actually resides. When information retrieval is required, this may create delays.
- High risk of compromise to confidential information since sensitive information is kept under the control of a third-party. This can pose a significant threat to ensuring the protection of intellectual property (IP) and trade secrets.
- Technical risks such as data leakage, distributed denial of service attacks, loss of encryption keys, and conflicts between customer hardening procedures and cloud platforms.
- Legal risks such as data protection and software licensing risks. Risks not specific to the cloud such as network problems, unauthorized access to data centers, and natural disasters [6].

IV. Dependable Cloud Computing

While there is no universally accepted definition of dependable cloud computing, it is important to clarify its components and meaning. In dictionaries, *dependable* is synonymous with *reliable.* Therefore, we can view dependable cloud computing as *cloud computing which everybody (mainly consumers or information owners) can relied on to do what they want or need with all the security concerns adequately taken care of and data integrity is not compromised.* Security concerns of cloud computing has been one of the drawbacks affecting the full adoption of cloud computing by many organisations [7]. As long as internet has been accepted by all, cloud computing will soon become the order of the day! This is due to the cost savings that is associated with cloud computing. Users of cloud computing have low technical cost of ownership (TCO) as compared with those using conventional computing.

Dependable cloud computing can be achieved with the following components:

- Security: there must exist mechanisms (e.g. encryption) which make it extremely difficult or uneconomical for an unauthorised person to access some information
- Privacy: protection against the exposure or leakage of personal or confidential data (e.g. personal identifiable information (PII)).
- Accountability: the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed upon expectations. This goes beyond responsibility by obligating an organisation to be answerable for actions.
- Auditability: It allows an action to be reviewed against a pre-determined policy to decide if the action was compliant, and if it was not, to hold accountable the person or organisation responsible for the action [5].

V. The Design Of Encryption System

An encryption system was designed to test the dependability of the data stored and/or transferred from cloud. The programming language suitable for designing encryption system must have security API for accessing and developing cryptographic functionality. Java programming language on NetBeans IDE was used

for the design. This is because Java has security API built around the java.security package (and its subpackages) and it also has Java Cryptography Extension (JCE) which extends the Java Cryptography Architecture (JCA) API to include APIs for encryption, key exchange, and Message Authentication Code (MAC).

The Object Oriented Methodology (OOM) was used for this system development. The underlying idea of OOM was to create the logical design from a physical design based on observing the properties of the "real world".

OOM is a new system development approach encouraging and facilitating re-use of software components. With this methodology, a computer system can be developed on a component basis which enables the effective re-use of existing components and facilitates the sharing of its components by other systems. Through the adoption of OOM, higher productivity, lower maintenance cost and better quality can be achieved. This methodology employs international standard Unified Modeling Language (UML) from the Object Management Group (OMG).

The system analysis stage involves two distinct stages:

1. The preliminary study of the system
2. The detailed analysis of the system

Preliminary Study of the System: This involves the problem identification and definition, specifying objectives, establishing technical feasibility and making preliminary cost. It also includes benefit estimates and estimating schedules.

Detailed Analysis of the System: This is the second stage of the analysis of the system. Here, the user requirements were identified, and the methods and procedures of the new system were established. The process involves collection of facts and analysing the facts collected.

Figure 1: Collaboration diagram of the proposed system

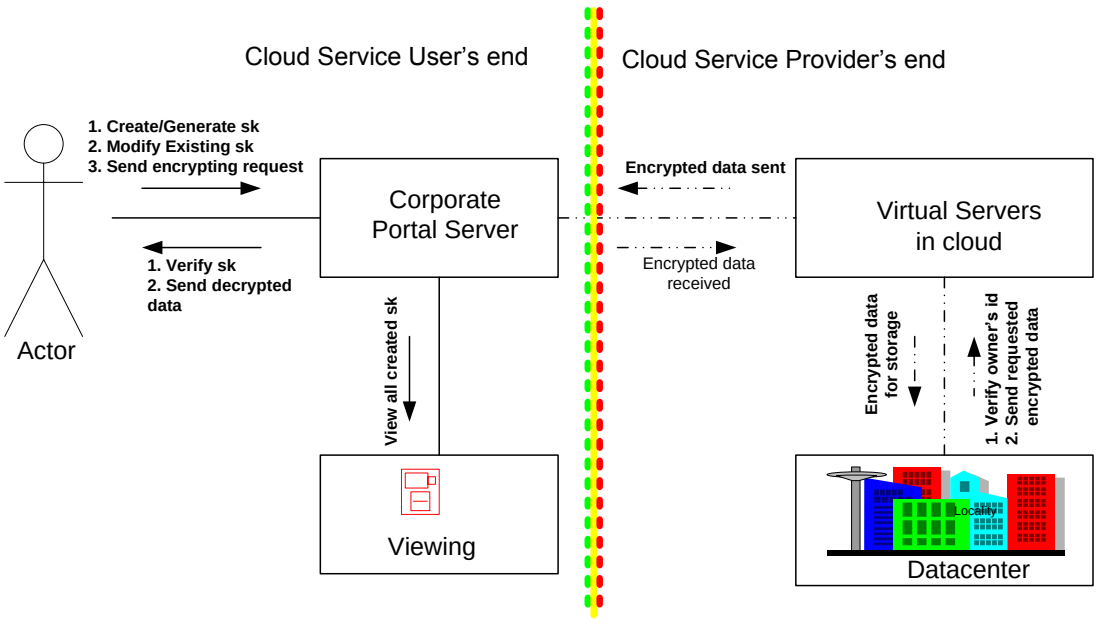

Figure 1: Collaboration diagram of the proposed system

VI. Development Of System Requirement

At this stage, the requirements for the system were developed. These include input and output requirements.

Input Requirements Analysis: In order to produce the required output, the input necessary for the output was specified and designed. The input screens are all user-friendly to make usage easy for all kinds of users. The inputs for the encryption system are in two forms; unencrypted format and the encrypted format. Input from the client end into the datacenter in the cloud are unencrypted and the data are of text , files in the form of audio, video, graphics, databases and any other format that the user may want to store in the cloud. When a client requests for stored data from the cloud, they are delivered in the form of cipher text and needs to be decrypted

for the client to understand them. In this case, the input to the system is the encrypted file been sent from the cloud. The system then decrypts this file before they are sent to the client. See Fig. 1.

Output Requirements Analysis: The logical place to begin a detailed study of the system requirements and the design of the entire system is the output. The output display is designed in such a way that is user-friendly and suitable for use by both expert and novice users. The output of the encryption system to the cloud server is in encrypted form. The output to the client whenever a request is made to the cloud is unencrypted file which is decrypted by the proposed encryption system as shown in Fig. 2.

The system designed is only intended to serve various encryption operations at the cloud users' end and not in the service provider's cloud. It is expected that users of cloud services should ensure that the data being uploaded into the cloud (i.e. data in transit) are reasonable secured. This system is built into the customer's internal private cloud (a kind of LAN). It is depicted as 'Security Policy Cust-X' in Fig. 3.

It must be noted that Cust-A's security policy may not be the same for Cust-B. The kind of security policy employed by each customer is a function of the sensitivity of data in question and the business rule of such customer

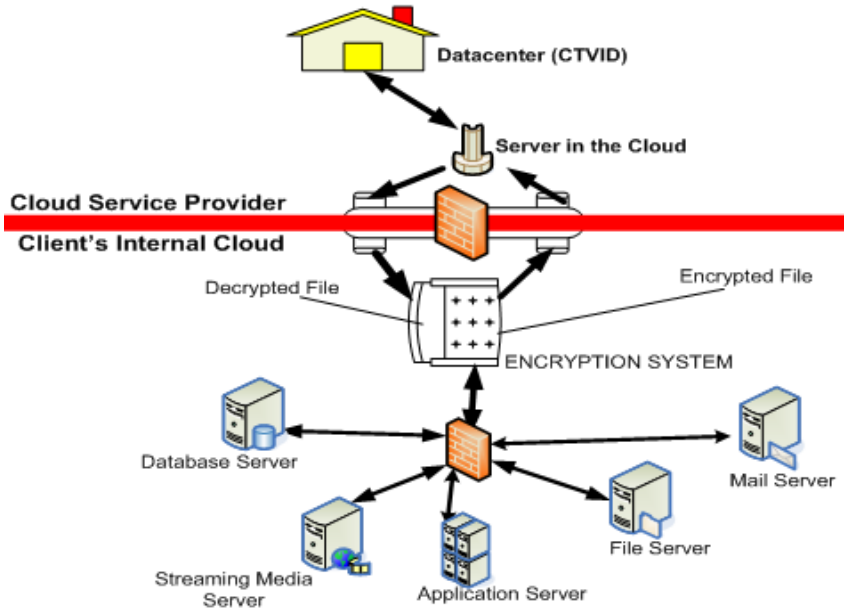

Figure 2: Block diagram of the proposed system

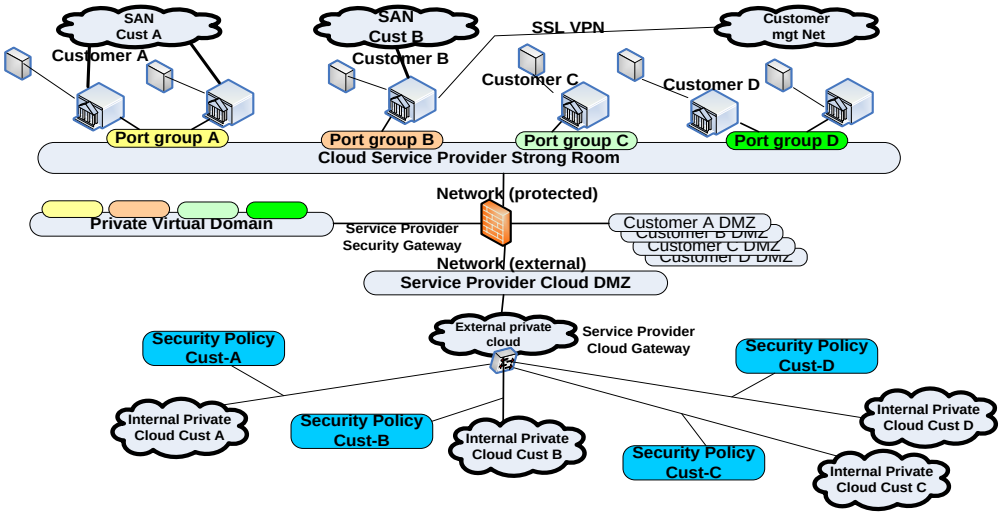

Figure 3: Dependable cloud computing physical model

VII. The Algorithm

In this algorithm, the client is depicted with CT and server in cloud as SIC.

1. CT □ {sk, pk}

The client takes as input a security parameters *secret key sk* and *public key pk.* The public key pk is sent to SIC while it stores the secret key sk

2. CT: {sk, pk, F, info, M} □ SIC: {E(F), E(info), E(M)}

The client prepares part of its file F for storage in SIC which is not trusted. As input, it takes a secret key and public key, part of the file F with the definition info of the update to be performed and the previous metadata M. The output sent to SIC is encrypted version of F, info and M as a request for update.

3. SIC: {pk, F_{i-1}, M_{i-1}, E(F), E(info), E(M) □ CT: {F, M, M'c, $P_{M'c}$}

The server in response to update request by client sends the new version of F and M together with the metadata M'_c and its proof $P_{M'c}$. The input in SIC are the public key pk, the previous version of F and M which are F_{i-1}, M_{i-1} and the client provided values E(F), E(info) and E(M).

4. CT: {sk, pk, F, info, M_c, M'c, $P_{M'c}$} □ SIC:{accept, reject}
CT: {sk, pk, M_c}□ SIC: {c}

The client verifies the server's behaviour during update. The CT has all the previously sent input from SIC in (3) above, it then sends acceptance or rejection signal to the server. Then, there is a probabilistic procedure run by CT to create a challenge for SIC by sending

5. SIC: { pk, F_i, M_i, c} □ CT: {P}

Upon the receipt of a challenge c, SIC sends proof P to client.

6. CT: {sk, pk, M_c, c, P} □ SIC: {accept, reject}

Once the proof P is received by CT, it then send accept or reject signal. If accept, then the off-loading commences, it is otherwise if reject signal is sent. The data is then migrated to CTVID (cloud trusted virtual infrastructure datacentre) where dependable virtual infrastructures are based

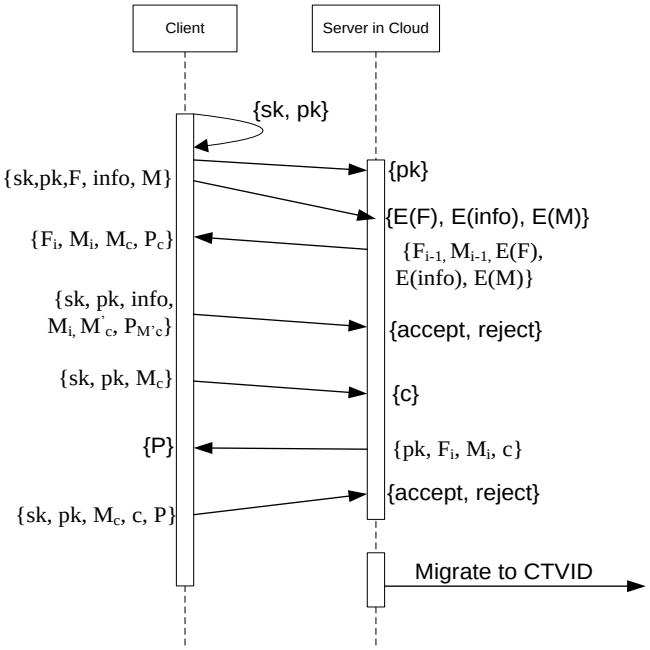

Figure 4: Sequence diagram of client off-loading files to server in cloud for further migration to CTVID

As the data owner or client initiates a request for file retrieval from server in the cloud (SIC), the following adding processes take place in order to transfer the file from the destination platform (DP) which has a direct connection with the SIC (server in cloud) to the CT (client) :

1. CT: {sk, pk, M_c, info} □ SIC: {E(info), c}

The client requests part of the file from SIC along with associated proof. It takes the sk, pk and the latest clients metadata M_c and the information about what to request as input and output the encrypted information and an associated challenge c that is then sent to the server.

2. SIC: {pk, F_i, M_i, E(info), c} CT: {$F'_{E(info)}$, P}
Once the retrieval request is received from CT by the SIC, it takes as input the pk, the latest version of the file and metadata, the information about request and the challenge c and then out the requested file along with the proof P to the client CT.
3. CT: {sk, pk, M_c, info, c, $F'_{E(info)}$, P} SIC: {F}
After the client has received the part of the file and its associated proof P from the server, it takes as input the sk, pk, the client metadata M_c, the request information info, the challenge c, the part of the file $F'_{E(info)}$ and the proof P sent by SIC. CT then checks if the proof corresponds to the part of file that is received and output the decrypted file otherwise the client output null.

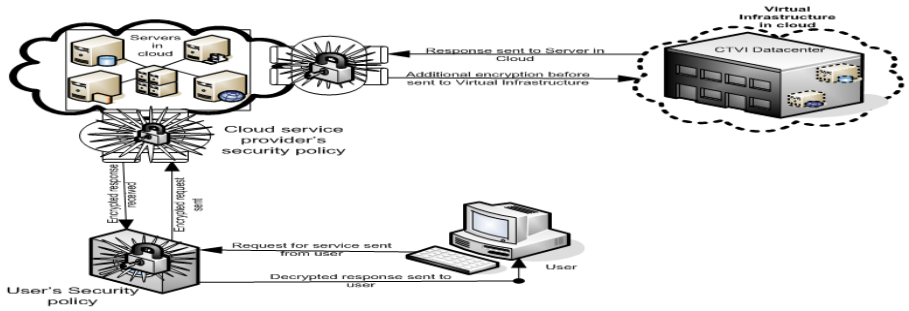

Figure 5: The architecture of dependable cloud computing

The user connects the cloud service provider's server via its own security policy and server tier firewall rules that are defined within a vApp. This security policy includes server security patch levels, anti-virus status and file-level access restrictions. The dependable cloud computing model in Fig. 5provides a method to communicate the policies and server tier firewall rules.

The cloud service provider needs to validate the patch level and security level prior to bringing user's data into the server in the cloud. Data from the user's DMZ area are validated in order to mitigate any security violations according to each user's security profile.The cloud service provider also separates and isolates the resources each customer virtual machine uses from other customers' virtual machine resources to prevent DDoS attacks. These attacks are usually caused by log files not having limits or CPU or memory utilization increasing on a single virtual machine through memory leaks or poorly behaving applications.

In order to ensure data security, the cloud service provider provides access paths to only the physical servers that must have access to maintain the desired functionality by using zoning system via SAN N-Port ID virtualization (NPIV). The SAN (storage area network) is within the user's network.This architecture also provides a method to communicate the access controls and authentication needs to the cloud service provider. The dependable cloud computing model in Fig. 5 shows how the user access is controlled in the cloud environments require. Cloud provider defines a virtual machine identity that ties each virtual machine to an asset identity within the provider's virtual infrastructure. Based on this identity, cloud service providers are able to assign user, role and privilege access within the extended infrastructure to provide role-based access controls. Service providers can prevent cloning and copying of virtual machines using a combination of virtual machine identity and server configuration management policies.

VIII. Conclusion

This work represents a new paradigm of information protection and security in cloud computing. We examined and defined a new model for dependable cloud computing and addressed the core security challenge of cloud computing with multi-tenancy. We have shown that using dependable computing technologies where clients and service providers ensure conformity to security rules in the cloud computing environment can benefit all. Making cloud computing dependable cannot be left in the hands of service providers alone, consumers have to play their own role so that data integrity is maintained uncompromisingly while enjoying the benefits that cloud has provided.

Therefore, as a rule, security concerns should not be a block to the adoption of Cloud Computing. While the Cloud has unique challenges, those challenges do not mean it is inherently insecure. The cloud computing has come to stay; making it dependable and trustworthy is a task that can be done.

References

[1]. R. Sailer,E. Valdez, T. Jaeger, et al., sHype: Secure hypervisor approach to trusted virtualized systems,RC23511, IBM, Yorktown Heights, NY 2005. (On-line:http://www.research.ibm.com/secure_systems_department/projects/hypervisor.)

[2]. N. Santos, K.Gummand, and R. Rodrigues, Towards trusted cloud computing,In: Workshop on hot topics in cloud computing, San Diego, CA, 2009.

[3]. M. Jensen, J. Schwenk, N. Gruschka. and L. Iacono, On technical security issues in cloud computing,In: IEEE International Conference on Cloud Computing (CLOUD-II 2009), Bangalore, India, September 2009, 109-116.

[4]. F.J. Krautheim, Building trust into utility cloud computing, doctoral diss., University of Maryland, Baltimore County, Baltimore, MD, 2010.

[5]. R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, B. S. Lee, TrustCloud: A framework for accountability and trust in cloud computing. HP Laboratories HPL-2011-38, 2011.

[6]. D. Catteddu and G. Hogben Cloud computing: Benefits, risks and recommendations for information security. Technical Report, European Network and Information Security Agency, 2009.

[7]. R.J. Ureigho, Modeling a security framework for dependable cloud computing, doctoral diss., Ebonyi State University, Abakaliki, Nigeria, 2012.

[8]. D. Challener, K. Yoder and R. Catherman, A practical guide to trusted computing (Upper Saddle River, NJ: IBM Press, 2008)

[9]. T. Velte, J. Velte and R. Elsenpeter, Cloud computing: A practical approach(McGraw-Hill Osborne Media, 2009).

[10]. M.A. Vouk, Cloud computing - issues, research and implementations. Journal of Computing and Information Technology 16(4), 2008, 235-246.

[11]. S. Pearson,Trusted computing platforms: TCPA technology in context (Upper Saddle River, NJ: Prentice Hall, 2003).

[12]. A. Stamo, A. Becherer, and N. Wilcox,Cloud computing models and vulnerabilities: Raining on the trendy new parade. In: BlackHatUSA, LasVegas, NV, 2009, 245-310

[13]. J. Viega, J. Cloud computing and the common man. Science applications International Cooperation Computer42(8),2009, 106-108.