THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATIONS
Vol. 24, No. 2, December, 2017

SECURITY AND ETHICAL ISSUES TO CLOUD DATABASE

A.A. Izang[1], A.O. Adebayo[2], O.J. Okoro[3] & O.O. Taiwo[4]

[1,2,3,4] Babcock University. Ilishan-Remo, Ogun State, Nigeria.

[1] aaronizang89@gmail.com, [2]wale_adebayo@yahoo.com [3]okoroo@babcock.edu,ng, [4]taiwobunmi02@gmail.com

ABSTRACT
Privacy and Security of data in cloud database is a vital issue as it enables the storage, management and sharing of complex data in a secure platform. Cloud database, a technology that clings onto Cloud Computing paradigm, has privacy and security challenges such as lack of awareness and hegemony of place of data stored, transaction log of data, malicious act, amongst others. Also, ethical issue in the cloud surrounds trust issues from tenants, as the tenants find it difficult outsourcing critical information to a cloud service provider without the interference of a third party. This and many more issues were considered in this paper. This paper, therefore, discussed security, privacy and ethical concerns associated with cloud database by reviewing variety of literatures that discussed about these issues. Furthermore, the paper proposed a conceptual framework for mitigating the security and privacy issues inherent in the cloud database as a way of improving the services of the cloud service providers when deployed.

Keywords: Cloud Computing, Cloud Database, Security, Privacy

1.0 INTRODUCTION

The inherent benefits of cloud computing technology from the time of its advancement cannot be over emphasized. It is seen that the wide spread availability of internet enabled services across the globe is what Cloud computing has plugged into as its advantage to revolutionize the world of Information Technology (IT). The National Institute of Standards and Technology [1] defined Cloud Computing as a "*model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) rapidly provisioned and released with minimal management effort or service provider*

intervention". It has several deployment models which are Public, Private, Community and Hybrid Clouds [1], [2], [3]. A public cloud is one in which the infrastructure in the cloud is made open and can be accessible to the public. A private cloud has its cloud infrastructure made opened and operated for an organization only for a private use. This cloud is being managed by a third-party company usually located within or outside the premise of the organization. It can also be managed by the organizations themselves. The community cloud infrastructure is being managed by multiple organization, the organization itself or a third party company. A hybrid cloud combines more than one cloud deployment models. It combines both private cloud and third-party, public cloud services, though planning between the two platforms used, by an organization for hosting their resources.

There are also service delivery models in Cloud Computing which are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [4]. In the SaaS model, users may gain access to applications running on the cloud only through various client interfaces, such as a web browser. Users do not access the management console of basic infrastructures such as network, servers, operating systems, storage, and other infrastructures. In the PaaS model, users do not have control of basic infrastructure, i.e. storage, operating systems, network, server, but have control over applications deployed or applications that has hosting configurations. The user has the ability to deploy any application on the infrastructure, which can be created using a programming language and the tool supported by the user. In the infrastructure as a service the basic functionality such as networks, storage and other essential computing resources are provided to the user. A random application can be run or deployed by users. In IaaS model, computing resources and applications such as operating system, storage platforms are under the control of users and there is little or no control of firewall and other basic networking components.

Cloud computing platform provided by Amazon, such as Amazon EC4, is responsible for running a cloud database. It is provided as a service. The idea behind the advancement of Cloud database was for the sole aim of managing data online through the use of distributed servers. Some advantages of cloud database include information sharing which is made simpler and convenient, and enables quick access to files and data. It is economically cheap to maintain, and granting opportunity for data manipulation wherever it exists. Figure 1 shows cloud computing system with all interrelated components.

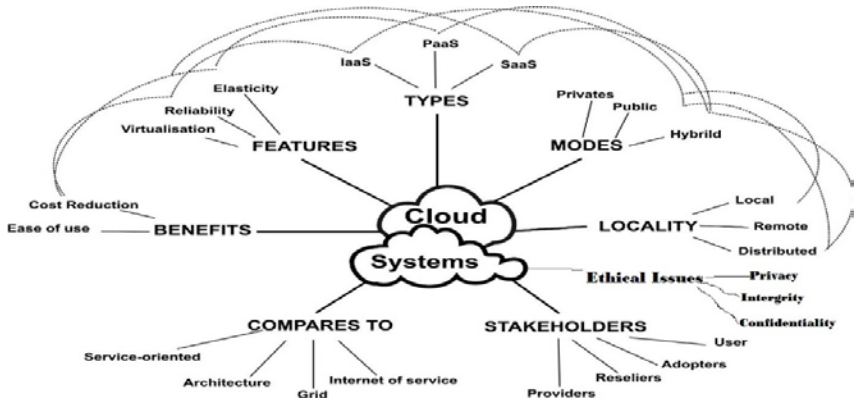

Figure 1: Diagram of Cloud System showing all interrelated components (Source: [5], modified)

The concept of Security and privacy of information in the cloud is a critical issue. This may be due to the fact that in the Clouds there is no borders and the data stored in the cloud can be located physically anywhere across the world or at any data center across the network geographically distributed, as stipulated by the Cloud Security Group [6]. In other words, Cloud databases, raises serious security issues such as availability, privacy, confidentiality, data integrity and information integrity, amongst others, which are of outmost importance. Solutions should, therefore, be proffered to resolve all these issues, particularly confidentiality and integrity of data on the Cloud database, for storing, accessing, manipulation and interaction with and amongst users.

The vibrant nature of the Cloud database has made it to be highly vulnerable to several security attacks, privacy and ethical issues. Most ethical issues associated with the cloud deals with the issues of trust and mistrust between the Cloud service providers and the Cloud subscribers. This study therefore examines the security, privacy and ethical issues associated with cloud database in a cloud computing environment by reviewing several literatures that discussed this issues. The study also recommend strategies or ways by which such issues can be mitigated by proposing a security and privacy framework.

2.0 LITERATURE REVIEW

Businesses are engaged in heavy transactions on daily bases and data is constantly been generated. The management of this large chunk of business data generated has become a tremendous challenge among business organizations. This challenge has necessitated the creation of database platforms which has been the traditional solution to these challenges. Cloud computing technology, has enabled providers to initiate ways in which databases can be hosted in the cloud such as the public cloud so that users will not make use of their own dedicated hardware. It provides the ability to scale the databases into large capacities. The International Data Cooperation (IDC) in 2016 predicted that big data annual growing rate for structured and unstructured data is at 60% [7], [8]. In other words, the cloud has now become the storage point for big data and for business organization to move forward in the management of business data. Despite these improvements, there remain a security issues in the cloud databases or databases as a services as regards to sensitive data and information stored in the cloud. However, the cloud database services still remains an emerging market and tools which seems to be evolving fast.

There are two models that can be deployed to enable users run or host a database on the cloud. This is either by the use of a virtual machine image or either by obtaining a database service which is maintained and provided by a second or third party in the cloud. In the context of the Virtual machine image model, Users are allowed to purchase virtual machines for a limited number of time in which database can be run and managed within that stipulated time on the virtual machine. In the same instance, users can decide to upload their machine image with an already installed databases or decide to use a ready-made machine image embedded with some optimized databases. Examples according to [9] includes Oracle databases 11g enterprises edition which is provided by oracle on an Amazon EC2 Platform. Microsoft Azure is another example according to [10]. In the DBaaS model, the installation and maintenance of databases is the responsibility of the databases provider not the user. In other words, for maintaining the databases, the owners of the application charge according to the usage of service.

According to [11] Amazon Web Services (AWS) provides three DBaaS offerings as part of its cloud portfolio: SimpleDB, a NoSQL

key-value store; Amazon RDS, a relational database service that includes support for MySQL, Oracle, and more; and DynamoDB. Microsoft offers its SQL Database service. Cloud computing platforms are also provided by mLab which is MongoDB. This enables users and customers alike to host databases on google, Azure or AWS cloud platform amongst other providers such as oracle that has launched its own databases as service enabling customers to have access to the databases.

Previous research on security issues in cloud database attempted to suggest solutions to the inherent issues. However, they did not look at the privacy aspect of data in concert with the cloud and the users. This research will however combine both security and privacy issues to cloud database and will also come up with a conceptual framework for the mitigation of these issues in the cloud database.

A. Data Model of Cloud Database

The design and development of database systems use data management including relational databases as key building blocks. The queries expressed in SQL that are advanced, work well with stringent relationships that are provided by relational databases technology. Relational database technology designed initially for use on a distributed system. [12] States that, this issue has been addressed with the addition of clustering enhancements to the relational databases. Adding that some basic tasks require complex and expensive protocols, such as data synchronization. [13] Mentioned that modern relational databases have shown poor performance on data-intensive systems, hence the idea of NoSQL has been utilized within database management systems for cloud-based systems. There are no requirements within the NoSQL implementations storage, fixed table schemas and joint operation is avoided according to [14] Therefore, it provides efficient, good performance, scalable cloud applications.

B. Types of Cloud Databases

There exist several Cloud databases available for business organizations to adopt for their daily business transactions. The management of business data are easier in a public cloud as business constantly engage in business transactions, data are generated daily. According to [5] there are ten useful types of cloud databases. Examples in clouds SQL, relational databases, NoSQL databases, while others are open source databases. Table 1 shows the cloud database classified under the type of deployment and data model they belong (SQL or NoSQL Vs Virtual Machine or DBaaS)

Table 3.1: Cloud database vendors by deployment and data model (Source: [15])

	Database as a Service (DBaaS)	Virtual Machine Deployment
NoSQL Data Model	Amazon Simple DB, Enterprise DB, Postgres Plus Cloud Database, Azure Document DB, MongoDB Database as a Service (several options), Google App Engine Data store, Amazon Dynamo DB, Cloudant Data Layer (Couch DB)	Microsoft Azure, or Rackspace Neo4J on Amazon EC2 or Microsoft Azure, Cluster point Database, Couch DB on Amazon EC2, EDB Postgres Advanced Server, MarkLogic on Amazon EC2, MongoDB on Amazon EC2, Apache Cassandra on Amazon EC2, Hadoop on Amazon EC2 or Rackspace
SQL Data Model	Clustrix Database as a Service, Xeround Cloud Database, Enterprise DB, Postgres Plus Cloud Database, Amazon Relational Database Service, Heroku PostgreSQL as a Service (shared and dedicated database options), Microsoft Azure SQL Database (MS SQL)	IBM DB2, PostgreSQL Ingres (database), Nuo DB, MySQL, Oracle Database, Maria DB, SAP HANA, EDB Postgres, Advanced Server

3.0 SECURITY AND ETHICAL ISSUES OF CLOUD DATABASES

Many researchers have studied the security issues ravaging cloud computing and Cloud databases. Some key aspects of security issues in cloud database includes Middleware muddles issue, authentication and regulatory compliance issues [16]. Middleware muddle deals with the technology that enables the integration of components in a distributed system. As a software it allows elements of applications to interoperate across network links. Despite the differences in underlying system architectures, communications protocols and other application services. Middleware enables the development of architectural patterns that represent innovative design solutions for specific system design problems. It has been observed and attested by some managers in an organization that unauthorized access to database causes security gaps. To avoid this challenges,

The authorization and un-authorization of middleware in granting access to a databases component is the responsibility of database security administrators. To establish connections and communications between middleware and the database, standardized authentication mechanisms must be maintained. Authentication is seen as the process of confirming the identity of a computer user. The process of authentication verification requires user to supply his user name and password which the databases will verify by requesting for the password of the user. The system will then verify that the user has provided a proof that is acceptable by checking the password provided against centralized server or a local password database

The benefits of cloud computing are enormous yet there seems to be a poor commercial acceptance of cloud computing and utilization of cloud databases especially in this divide. Its growth has been somewhat slower than expected. A factor that may be behind this apparent reluctance to embrace cloud computing is regulatory and compliance problems directed governing the activities in the cloud. There are challenges and uncertainty as to the exact regulatory requirements for the services provided in the cloud. In the same instance cloud computing providers may not adherer to the regulations undersigned in a contract, which may involve data protection provision although location is key in the cloud environment from a legal point of view. This act becomes a serious concern because an organization may not provide sensitive data to be managed by a cloud provider without a stringent laws, rules and regulation to protect the data and adhering to those rules. These is where the ethical issues come to play because its goal is to protect the integrity, confidentiality, availability, and authenticity of vital information stored in the cloud database.

A. Ethical Issues in Cloud Computing and Cloud Databases

In the context of law and ethics as regards cloud computing usage, a major concern is associated with entrusting sensitive, confidential organizational data to a third party to protect. With the advent of Cloud computing, essential ethical principles with respect to the management of analogy data remains unchanged. When it comes to the services provided in the cloud, there are three relevant ethical issues in Cloud Computing which are: (1) privacy issues, (2) integrity of data and; (3) confidentiality. Privacy has to do with the protection of sensitive data belonging to a consumer or a user of the cloud services as provided by the third party. This is because there is a shift of control from the users to the third party who provides the service and technological functionality in the cloud. A violation of any written contract from the third party will affect the privacy of cloud subscribers.

Integrity of data deals with the protection of the original data stored in multiple physical

location in servers owned and managed by different organizations world over. Therefore, it becomes a serious ethical concern if organization cannot guarantee the security of their data stored in this servers around the world. This assumption is buttressed by [17] in stating that the interconnection of multiple services across the cloud, at different levels of functionality provisioned by different providers connected to provide a specific service for their customers, affects the confidentiality of cloud subscriber's information [18]. These are some of the ethical issues affecting the usage of cloud computing in terms of its administration by the cloud service providers.

B. *Legal and Regulatory Issue and Third-Party Involvement*

Different security threats to cloud databases can occur. Most of the threats that occur in cloud database are due to legal and regulatory issue, and third-party involvement. It has been noted that location matters and are important in a cloud computing environment. In advance nations of the where cloud computing is high accepted and utilized laws are been proposed, enacted to guide the practices and relationship between the cloud subscriber and the third party. In countries like the United State and Canada, cloud computing providers are subject to written regulatory requirements. This requirements involves control objectives for these related technology and safe harbor. These laws lay emphasis to where the data is stored, transferred and how it is being protected. Violation of this laws may amount to serious legal implication in which the organization may be subject to fines [19].

It is important to emphasis that any cloud computing subscriber that users that infrastructures sources from the cloud provided by a third party should impose rules and regulations that applies to their organization on the service provider as well. This is because of rising security concern in the cloud. It is seen that even with the storage of encrypted data, cloud service providers may have means of accessing this data without permission. It becomes a more security concern when there are more than one originations subscribed to. More risky is the contractors who may be working with the cloud providers who may add up to the challenges and porousness of the cloud.

4.0 SECURITY AND PRIVACY ISSUES TO CLOUD DATABASE AND MITIGATION APPROACHES

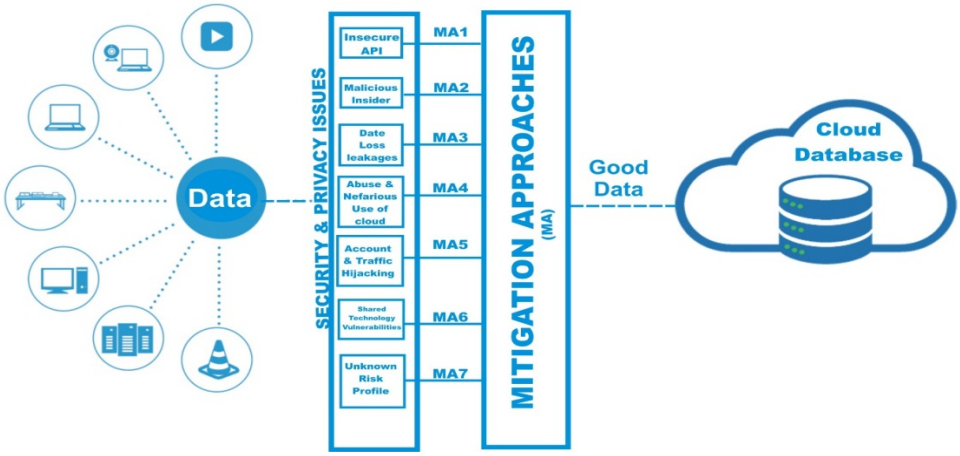

Figure 2: Conceptual Framework for Mitigating Security and Privacy Issues in Cloud Database

The figure 2 above shows the conceptual framework for mitigating security and privacy issues inherent in a cloud database. As IT organization subscribe to the cloud for storing their key resources, various security and privacy issues attack users data. These issues can be mitigated before storing them in the cloud as can be seen in the figure above, where the issues are mitigated and data free of threat can finally be stored in the cloud database.

[20] Highlighted seven security issues/threats inherent in the cloud environment as shown in the conceptual framework. This section discussed these issues and their mitigation approaches in details.

A. Insecure Application Programming Interfaces (API): Cloud computing providers expose a set of software interfaces or Applications Programming Interface (APIs) that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers.

How to Mitigate this Issue

This issue can be mitigated by ensuring strong authentication interfaces, analyzing the security models provided by the cloud provider, ensuring access control and authentication are implemented in line with encrypted transmission.

B. Malicious Insiders: Business organizations are familiar with malicious insider. This security threat becomes more visible within the cloud environment. Due to the fusion of customers and services providers into one management domain coupled with poor transparency in the provision of

process and procedures it becomes imperative that this convergence will result to Security gap. A service provided may not direct inform the subscribe his operational capabilities or highlight explicitly how access is granted to cloud employees to physical and virtual assets of the organization including how monitoring takes place also procedures and process of handling reports and policy compliance on complicated matters. These anomalies, create opportunities for corporate espionage, hobbyist hackers, organized crimes, even sponsored intrusions to take place.

The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection [15].

How to Mitigate this Issue
This issue can be mitigated by: conducting an assessment on supply chain management and enforcing stringent rules on supply chain management. Human resource requirements must be specified as part of contracts backed up by law requiring transparency in the general information security and management practices of the organization. Standard reporting of compliance and notification process on security breaches must be determined.

C. **Data Loss/Leakage:** Data loos and leakages may stem from deletion or alteration of records without a backup. Poor linking of documents from the larger records when lost or altered renders it unrecoverable. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment [15],[21].

How to Mitigate this Issue
The implementation of a strong API access control, encrypting as well as protecting integrity of data will help to resolve these issues. Also, the practice of efficient data storage, management and destruction process including an analysis of data protection at design and run time and contractual specification of backup and retention procedures will be helpful.

D. **Abuse and Nefarious Use of Cloud Computing:** The abuse and nefarious use of cloud computing steam form the activities of cloud infrastructures as a service provides. They tend to offer customer with services that are not real such as unlimited computing and network storage capacity coupled with free, easy and fast registration process where an individual or an organization can immediately state using the cloud services without frictions. Therefore, spammers, malicious code authors and other criminals utilizes this opportunities to the detriment of the subscribers. It is seen in some scholarly writings that hackers have begun to target IaaS vendors as PaaS providers have suffered from this the most.

How to Mitigate this Issue
The placement of stricter registration and validation processes will help mitigate this treat. Also, credit card fraud monitoring mechanisms must be

put in place including an introspection of traffics in a customer's network also monitoring of public blacklist for one's own network blocks.

E. Account, Service and Traffic Hijacking: This treat involves Attack methods such as phishing, fraud and exploitation of software. Credentials and passwords are often reused, which amplifies the impact of such attacks. If an attacker gains access to certain credentials, they can eavesdrop on activities and transactions, manipulate data, return falsified information, and redirect legitimate clients to illegitimate sites. Someone's account or service instances may become a new base for the attacker who may leverage the power of the person's reputation to launch subsequent attacks.

How to Mitigate this Issue

In other to mitigate this treat, the limitation of account sharing between a client and the services provides is a must. Leveraging on strong two-way authentication techniques and employing proactive monitoring measures to detect unauthorized activity is crucial.

F. Shared Technology Vulnerabilities: IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (e.g. Central processing unit (CPU) caches, graphic processing unit (GPU), et cetera.) Were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc. [22].

How to Mitigate this Issue

These issues can be mitigated by deploying best practices for installation and configurations. The cloud environment should be monitored for unauthorized changes and activity. There should also be an emphasis on promoting strong authentication and access control for administrative operations. The enforcement of service level agreements for patching and vulnerability remediation, and conducting vulnerability scanning and configuration audits is important.

G. Unknown Risk Profile: Cloud computing enables the reduction in the ownership of hardware and software including the maintenance. This is to allow organizations to pay more attention to the core business objectives. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concerns complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security ramifications. Versions of software, code updates, security practices,

vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating particular company's security posture. Information about who is sharing infrastructure with the company may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs. Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required of highly controlled or regulated operational areas.

How to Mitigate this Issue

Application logs and data should be disclosed, partial/full disclosure of infrastructure details (e.g. patch levels, firewalls, et cetera.) including monitoring alerting on information that are necessary as it relates to the organization.

5.0 CONCLUSION

The adoption and usage of cloud computing technologies is gradually gaining prominence and appreciated by business organizations around the World with a handful in the developing nations. However, there are security, privacy and ethical issues that affect the optimum use of cloud services. Due to the numerous threats that becloud the usage of cloud infrastructure it becomes a thing of concern as the protection of sensitive business data emanates. Customers may stand to benefit from the cloud infrastructure if there is an improved threat and data protection mechanism and the confidentiality of the subscribers determined. Therefore, in other to maintain the progress made in cloud computing especially in the area of cloud database, this research proposed a conceptual framework for mitigating the security and privacy issues, which helps to continually improve on strategies for maintaining security of data in the cloud, in other to have a solid relationship between the subscriber and the cloud provider for efficient service delivery.

REFERENCES

[1] Mell, P., & Grance, T. (2011, september). The NIST Defination of Cloud Computing. Gaithersburg, MD, United States. Retrieved September 2016, from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Dhar, S. (2012). From Outsourcing to Cloud Computing: Evolution of it Services. *Management Research Review, 35*(8), 664-675.

3] Ogu, E. C., Alao, O., Omotunde, A., gbonna, A., & Izang, A. (2014). Partitioning of Resource Provisions for Cloud Computing Infrastructure against DoS and DDoS Attacks. *International Journal of Advanced Research in Computer Science, V*(7), 67-71. doi:10.13140/2.1.2259.7129

[4] Strommen-Bakhtiar, A., & Razavi, A. R. (2011). Cloud Computing Business Models. *Springer Computer Communications and Networks*, 43-60.

[5] Brandon, B. (2014, June 4). *10 Of The Most Useful Cloud Databases.* Retrieved from Network World blog: http://www.networkworld.com/article/2162274/cloud-storage/cloud-computing-10-of-the-most-useful-cloud-databases.html

[6] CSO, (. S. (2012). Data Security in the Cloud. *Vormetric Data Security Simplified*, 1-6.

[7] Awodele, O., Izang, A. A., Kuyoro, S., & Osisanwo, F. (2016). Big Data and Cloud Computing Issues. *International*

Journal of Computer Applications, 133(12), 0975-8887.

[8] IDC. (2016). *International Data Cooperation Big Data Prediction.* Retrieved from International Data Cooperation: http://www.idc.com

[9] Anjomshoaa, a. A. (2011). How the cloud computing paradigm could shape the future of enterprise information processing. *",Proceedings of the 13th International Conference on Information Integration and Web-based Applications and Services, II*, pp. 7-15. Retrieved December 4, 2016

[10] Cass, S. (2009, June 9). *Designing for the Cloud.* Retrieved October 4, 2016, from MIT Technology Review: https://www.technologyreview.com/s/414090/designing-for-the-cloud/.

[11] J'NoSQL. (2009, June 11). *J'NoSQL writeup on cloud database.* Retrieved from Oracle International Incooperation: http://oracleinc.com

[12] Dave, R. (2011). *Are databases in the cloud really all that different.* Retrieved November 22, 2016, from CNET: http//

[13] Ken, N. (2011). *SQL, NoSQL or SomeSQL?* Retrieved from oracle incooperation: http://www.oracle.com

[14] AWS. (2011, 11 9). *Amazon Machine Images - Oracle Database 11g Release 2 (11.2.0.1) Enterprise Edition - 64 Bit.* Retrieved January 29, 2017, from Amazon Web Services: http://www.amazonwebservice.com

[15] Te-Shun, C. (2013, June 30). Security Threats on Cloud Computing Vulnerabilities, . *International Journal of Computer Science & Information Technology (IJCSIT), V*(3), 12-21.

[16] Leena, M. A., & Kakoli, R. (2012). Centralized Database Security in Cloud . *International Journal of Advanced Research in Computer and Communication Engineering, I*(8), 50-68. Retrieved from www.ijarcce

[17] Izang, A. .., Mensah, Y. A., Omotosho, O. J., & Obioma, C. P. (2016, April 30). Overview of Cloud Computing and Recent Addendum. *journal of Communications Technology, Electronics and Computer Science, V*(5), 54 63.

[18] Muhammad, K., & Shao, Y. Z. (2015). A survey on top security threats in cloud computing,. *International Journal of Advanced Computer Science and Applications (IJACSA), VI*(3), 109-113.

[19] Ken, N. (2012). *Bar Rules of Professors' 1 Conduct Communication.* Retrieved from Bar Rules of Professors' 1 Conduct Communication. pp. 6,.

[20] Glen, B., & Rich, M. (2010, March 10). *Cloud Security Alliance (CSA) Top Threats to Cloud Computing.* Retrieved November 23, 2016, from The Cloud Security Alliance: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[21] Ganesh, C. D. (2015). Cloud Database Security Issues and Challenges. *IGI Global Publishing*, 153-157. doi:10.4018/978-1-4666-6559-0.ch00

[22] Yunchuan, S., Junsheng, Z., Yongping, X., & Guangyu, Z. (2014). Data Security and Privacy in Cloud Computing. *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, II*(4), 1-9. doi:10.1155/2014/190903