ISSN 2277-3061

HYBRID MODEL OF RSA, AES AND BLOWFISH TO ENHANCE CLOUD SECURITY

Jasleen Kaur [(1)], Sachin Bagga [(2)]
[(1)] Research Scholar, Department of Information Technology, LLRIET, Moga
jasleennanda123@gmail.com
[(2)] Assistant Professor, Department of Information Technology, LLRIET, Moga
sachin8510@gmail.com

ABSTRACT

Cloud is a term used as a metaphor for the wide area networks (like internet) or any such large networked environment. It came partly from the cloud-like symbol used to represent the complexities of the networks in the schematic diagrams. It represents all the complexities of the network which may include everything from cables, routers, servers, data centers and all such other devices. Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. We can do segregate data by creating virtual partitions of data for saving and allowing user to access data in his partition only. In our research work we have used the hybrid combination of RSA, AES and Blowfish for data encryption along with data fragmentation using Gateway.

Keywords

Cloud Computing, Cloud Security, Confidentiality, Security Issues, Gateway, AES, RSA, BlowFish, Distributor

ISSN 2277-3061

INTRODUCTION

Cloud Computing is the model for convenient on-demand network access, with minimum management efforts for easy and fast network access to resources that are ready to use. It is an upcoming paradigm that offers tremendous advantages in economic aspects, such as reduced time to market, flexible computing capabilities, and limitless computing power. Popularity of cloud computing is increasing day by day in distributed computing environment. There is a growing trend of using cloud environments for storage and data processing needs. To use the full potential of cloud computing, data is transferred, processed, retrieved and stored by external cloud providers. However, data owners are very skeptical to place their data outside their own control sphere. Their main concerns are the confidentiality, integrity, security and methods of mining the data from the cloud.The Greek myths tell of creatures plucked from the surface of the Earth and enshrined as constellations in the night sky. Something similar is happening today in the world of computing. Data and programs are being swept up from desktop PCs and corporate server rooms and installed in “the compute cloud”. In general, there is a shift in the geography of computation.Cloud computing is here. With its new way to deliver services while reducing ownership, improving responsiveness and agility, and especially by allowing the decision makers to focus their attention on the business rather than their IT infrastructure, there is no organisation that has not though about moving to the Cloud.

The move to the Cloud is a crucial step for any company, but has to be made with a lot of caution because it could turn against users. Organisations need to clearly understand the benefits and challenges, especially for the most critical applications. There are several concerns but, as shown in an IDC survey about the issues of the Cloud [GEN09], security is the main concern. The question is why security is such a complicated challenge in the decision of moving to the Cloud. The answer is easy: lack of control over their data.

Computing can be described as any activity of using and/or developing computer hardware and software. It includes everything that sits in the bottom layer, i.e. everything from raw compute power to storage capabilities. Cloud computing [1] ties together all these entities and delivers them as a single integrated entity under its own sophisticated management.

Figure 1. Cloud Computing Model

Types of Clouds

Clouds are divided into 4 categories:-

Public Cloud:- Public cloud [9] allows users toaccess the cloud publicly. It is access by interfaces using internet browsers. Users pay only for that time duration in which they use the service, i.e., pay-per-use.

Private Cloud:- A private clouds [10] operation is with in an organization’s internal enterprise data center. The main advantage here is that it is very easier to manage security in public cloud. Example of private cloud in our daily life is intranet.

Hybrid Cloud:- It is a combination of public cloud [11] and private cloud. .It provide more secure way to control all data and applications .It allows the party to accessinformation over the internet. It allows the organization to serve its needs in the private cloud and if some occasional need occurs it asks the public cloud for some computing resources.

Community Cloud:-When cloud infrastructure construct by many organizations jointly, such cloud model is called as a community cloud. The cloud infrastructure could be hosted by a third-party provider or within one of the organizations in the community.

SERVICS OF CLOUD MODEL

There are different types of services are provides by cloud models like: Software as a Service(SaaS)[2], Platform as a Service (PaaS) [3], and Infrastructure as a Service (IaaS) [6] which are deployed as public cloud, private cloud , community cloud and hybrid clouds.

1) Software as a Service (SaaS) [2]:- The capability provided to the consumer is to use the some applications which is running on a cloud infrastructure. The applications are accessible from many devices through an interface such as a web browser (e.g., web-based email). The consumer does not control the cloud infrastructure which includes network, and servers, all operating systems, and provides storages.

2) Platform as a Service (PaaS):- PaaS [5] provides all the resources that are required for implementation of applications and all services completely from the Internet. In this no downloading or installing is required of any software. The capability provided to the consumer is to deploy onto the cloud infrastructure [4] .Consumer uses all the applications by using different programming languages and tools which are provide by the provider. Any consumer has not any control on cloud infrastructure including all networks, servers and operating systems, but has control over the applications which they deployed.

3) Infrastructure as a Service (IaaS) [6]:- The capability provided to the consumer isto access all the processing, storage, networks and other many fundamental computing resources [8]. Consumer is able to deploy arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems , storage ,deployed application ,and possibly limited control of select networking components[4].

RESEARCH MOTIVATION

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through the adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model differ widely from those of traditional architecture[6] as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. We can do segregate data by creating virtual partitions of data for saving and allowing user to access data in his partition only. Malicious activity monitoring is a tough task in cloud system as logging data might be spread over multiple hosts and data centres. Restricting user to his own virtual partition only will not allow logs to be dispersed allowing access to logs for monitoring easily.

User access is another major concern in restricting user access is a major challenge in cloud based storage system. Use of virtual partition and enhanced user access control in cloud system will allow us to improve data security.

Enhanced Cloud system will be compared with existing secure cloud systems. We will compare enhanced system against security, performance & ease of use.

Three cloud service models (SaaS, PaaS and IaaS) not only provide different types of services to end users but also disclose information security issues and risks of cloud computing systems [9].

• The hackers might abuse the forceful computing capability provided by clouds by conducting illegal activities. IaaS is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud.

• Data loss is an important security risk of cloud models. In SaaS cloud models, companies use applications to process business data and store customer's data in the data centers.

• Traditional network attack strategies can be applied to harass three layers of cloud systems. For example, web browser attacks are used to exploit the authentication, authorization, and accounting vulnerabilities of cloud systems.

RELATED WORK

In the research work titled "Controlling various network based ADOS Attacks in cloud computing environment :By Using Port Hopping Technique". E.S.Phalguna Krishna has proposed the concept that cloud computing security is sub domain of computer security ,network security ,and information security. It refers to a broad set of security policies ,technologies and flow controls deployed to protect data, applications, and associated infrastructure resources of cloud computing .

In the research work titled "Packet Monitoring Approach to Prevent DDoS Attack in Cloud Computing" in March 2012.Sateesh kumar peddoju has presented an approach in cloud Environment to prevent DDoS attacks. This new approach of Hop Count Filtering provides a network independent and readily available solution to prevent DoS attack in cloud environment .Also this method decreases the unavailability of cloud services to legitimate clients ,reduces number of updates and saves computation time .The presented approach is simulated in cloudSim toolkit environment and corresponding result are then produced.

In the research work titled "Data security model for cloud computing" in March 2014.Eman M.Mohamed has proposed the concept of data security for cloud computing. This paper is on the basis of data security in cloud computing,which has always been an important aspect of quality of service,cloud computing focuses oa new challenging security threats. Therefore, a data security model must solve the most challenges of cloud computing security.The proposed data security model provides a single gateway as a platform.

In the research work titled “On Modeling Confidentiality Archetype and Data Mining in Cloud Computing “in March 2013 [11]“ Alawode A. olaide” has proposed the concept of data mining in the cloud. This paper discus effort directed to which degree this skepticism is justified, by proposing to model Cloud Computing Confidentiality Archetype and Data Mining 3CADM. The 3CADM [10] is a step-by-step framework that creates mapping from data sensitivity onto the most suitable cloud computing architecture and process very large datasets over commodity clusters with the use of right programming model.

In the research work titled“An Approach to protect the privacy of the cloud data from data mining based attacks [12]” in April 2013 “Himeldev, Tanmoysen” has proposed the concept of privacy of the cloud data from data mining and attacks on the cloud data. We first identify the data mining based privacy risks on cloud data and propose a distributed architecture to eliminate the risks. Cloud data distributor is an entity that receives data from single client, where data is partitioned into multiple parts. These parts are distributed among several cloud providing companies cloud providers. In a nutshell our approach consists of categorization, fragmentation and distribution of data.

In the research work titled“Information Retrieval through Multi -Agent System with Data Mining in Cloud Computing [13]” in February 2012 “Vishal Jain and Mahesh Kumar” has proposed the concept of retrieving the useful information through Multi-Agent system. The aim of this research paper is to develop a practically implemented research model for the information retrieval using Multi-Agent System with Data Mining technique in a Cloud Computing environment.

In the research work titled “Data mining for high performance data cloud using association rule mining [14]” in January 2012 “ T.V Mahendra , N. Deepika and N.Keasava Rao ” has proposed the concept of mining the data for high performance data cloud using sector/sphere framework with association rules. In this paper we have discussed an algorithm to mine the data from the cloud using sector/sphere framework with association rules. Mining association rules is one of the most important aspects in data mining. Association rules are dependency rules which predict occurrence of an item based on occurrences of other items.

In the research work titled“Data mining in the cloud computing [15]” in April 2012 “Bhagyashree Ambulkar and Vaishali Borkar” has proposed the concept of mining of the data from the cloud. This paper deals with the study of how data mining is used in cloud computing. Data Mining is a process of extracting potentially useful information from raw data. How SaaS [6] is very useful in cloud computing. The integration of data mining techniques into normal day-to-day activities has become common place. We are confronted daily with targeted advertising, and businesses have become more efficient through the use of data mining activities to reduce costs.

In the research work titled“Cloud Computing: An overview [16]” in September 2013 “Eng. Anwar J. Alzaid and Eng. Jassim M. Albazzaz” has proposed the concept of cloud computing in detail. Cloud computing is a relatively new term, it refers to a new way of processing and storing information this new style of processing promises to offer a huge amount of computing power to its users without requiring them to invest in expensive hardware. This paper is a brief survey based on readings on cloud computing, it will provide an overview of the basic concepts, definitions, and outlines of the general architecture of this technology.

In the research work titled“Mitigating Data Mining Attack in Cloud [17]” in April 2014 “A. Raja Rajeswari and R.Sakkaravarthi” has proposed the concept of data mining based privacy attacks in the cloud. As an alternative of maintaining personal data on the own hard drive or updating important applications for user needs, user can use a service over the network, to a different location, to store user information and / or use its applications.

RESEARCH OBJECTIVES

Various data analysis techniques are available now a day that are successfully extract valuable information from a large volume of data. These analysis techniques are being used by cloud service providers. Attackers can use these techniques to extract valuable information from the cloud.

By distributing data on different clouds it introduces performance overhead when client needs to access all data frequently, e.g. client needs to perform a global data analysis on all data. The analysis may have to access data from multiple locations, with a degraded performance.

By simply using in single cloud provider can having the following main issues: Less Security. Loss of data; No privacy; Cost of maintenance is high. Uploading data on distributed cloud providers: - Although this scenario will protect the client’s data as the data will be distributed to the different cloud providers. But it will increase the cost to the client as purchasing different cloud will increase the cost. But using only single cloud also has the issues. So by using single cloud and then dividing the single cloud into multiple zones overcomes the problem of cost and privacy.

Here; user will create his/her own account at the cloud Provider. Cloud Provider will assign the different privileges to the user depending upon the role of the user. Different access policies for different zones will be implemented over here. If the user has been assigned a role as a Read, then he/she can only read the data from the server. If the policy allows writing the data, then only user can write the data into the server. The file sent by the user is stored into the multiple zones available at the server. If the company tries to perform the mining at the user’s data, then proper results will not be available.

We will be implementing cloud security aspects for data mining by implementing cloud system. After implementing cloud infrastructure for data mining for cloud system we shall be evaluating security measure for data mining in cloud. We will be fixing threats in data mining to Personal/private data in cloud systems.

METHODOLOGY

This thesis aims to provide an understanding of the different attack vectors created by multi-tenancy and virtualization in a public IaaS cloud. The vectors will be explored, focusing on the threats arisen from different tenants coexisting in the same physical host. A critical analysis of the different vectors will be provided along with guidance on how to approach them. This analysis will be performed using previous works from different entities and authors, along with personal knowledge obtained from experience. As part of the aim of this research, a strong foundation will be provided on the terms of cloud computing, multi-tenancy and virtualization. All these areas will be explored giving a strong definition.

The different security issues will be also explored in order to provide an introduction to the main focus of the research.

Client will upload the file that has to be sent to the cloud provider

RSA encryption will be performed at the client side before sending the file to the cloud provider and hence preventing the system from the man-in-the-middle attack.

This encrypted data is further sent to the gateway.

Gateway will receive the file sent by the client and will perform the AES (Advanced Encryption Standard) on it.

Gateway will further distribute the file into multiple fragments and store the name of the files in the distribution table. Afterwards Gateway will transfer all the splitted files to the cloud provider for storage.

Cloud Provider will receive the file and will apply the BlowFish algorithm on all the fragmented files received from the gateway.

So, Using this approach, we have achieved two purposes.

- If anyone tries to hack the data while transferring from client to the gateway, he/she will get only encrypted data.
- If anyone tries to perform the mining on the files stored at the cloud provider, no results will be retrieved.

During Downloading the file from cloud end, the client will follow the following steps:

1. Client will ask the gateway to download his/her stored file.
2. Gateway will forward the request to the cloud provider and cloud provider will apply the BlowFish decryption on all the fragmented files and will send all the stored splitted files of that client to the gateway.
3. Gateway will receive all the files and will try to combine them into a single file.
4. After linking of all the files, gateway will apply the AES decryption on the single linked file. After applying the decryption, gateway will send this file to the client.
5. Client will further perform the RSA decryption to fetch the stored data inside the file.

EXPERIMENTAL SET UP

This section gives the details of the experiments that we have conducted during the research period. Many different files of different sizes have been uploaded to the cloud provider using this approach. Different sizes that we have taken are 4KB , 10KB ,25.6KB, 40.3KB, 105KB, 245KB, 560KB, 786KB, 1.3MB etc. Like this 40 files are tested. These experiments are conducted on a machine with the following configuration: IntelCore 2 CPU, 980 MHz, 1.99 GB RAM, Microsoft windows 7. We have the Java version 8 with the Netbeans IDE version 8. The working system calculates the processing time, cost , number of files splitting, encryption time and decryption time.

Table 1. Encryption and Decryption Time

S.NO	Size of file (in KB)	Start time	Finish time	Transfer time	Encryption time	No. of files splitted	Cost	Decryption time
1	4.96	0.1	1.96	1.86	30105	64	18.56	25694
2	5.79	0.1	1.9	1.8	9421	51	18.4	8564
3	8.11	0.1	1.98	1.88	11899	71	18.84	11256
4	8.16	0.1	1.91	1.81	8778	52	18.08	9564
5	11.7	0.1	2.1	2.0	11920	89	19.1	12214

ISSN 2277-3061

Evaluation of the System

After implementing the proposed methodology, we have reached up to a solution that the cloud security can be enhanced by applying the hybrib model of RSA, AES and BlowFish as well as data distribution on the client's data. The data sent/received by the client is of utmost importance and it needs to be handled carefully. We have been able to reduce the processing time, encryption time, processing cost which increases the overall efficiency of the system.

Accuracy of the System

Accuracy of the System can is enhance by measuring Processing time ,Cost and Data distribution as shown in the graphs below, which increases the overall efficiency of the system.

- **Processing Time**

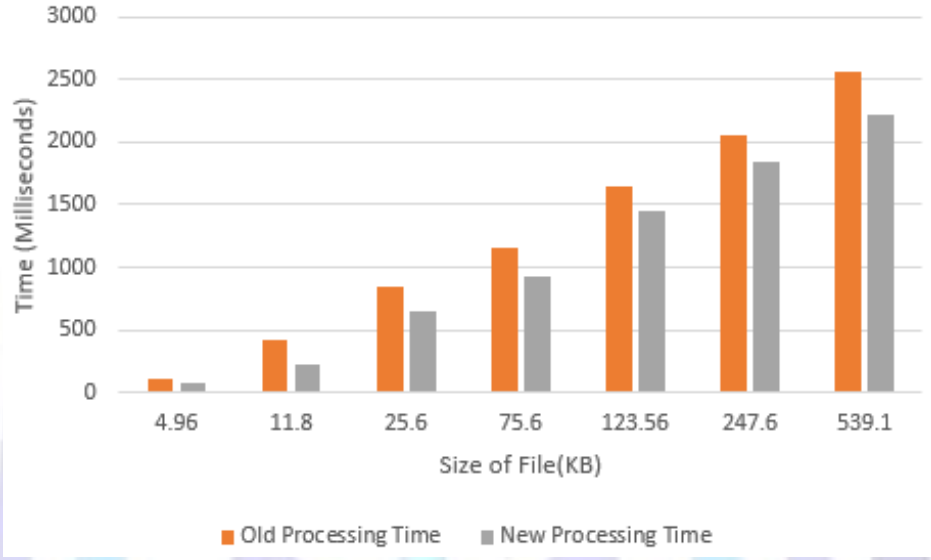

Figure 2. Processing time

From the above bar chart, it is clear that the processing time has been reduced. The processing time depending upon the size of the file. As the size of the file increases, the processing time will also increase. But we have been able to reduce the processing time of the proposed work as it will finally increase the overall efficiency of the system.

- **Cost**

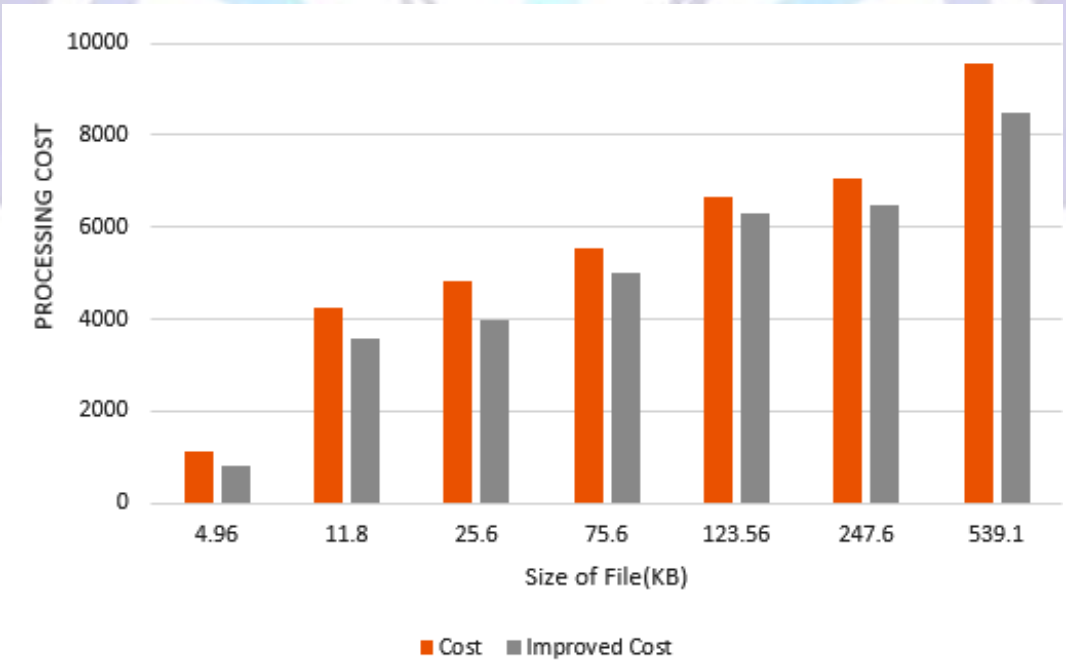

Figure 3. File Size v/s Cost

From the above bar chart, it is clear that the cost has been reduced. Usually Cloud Computing providers have detailed costing models which are used to bill users on *pay per use basis* The Cost depends upon the size of the file. As the size of the file increases, the Cost will also increase. But we have been able to reduce the Cost of the proposed work as it will finally increase the overall efficiency of the system.

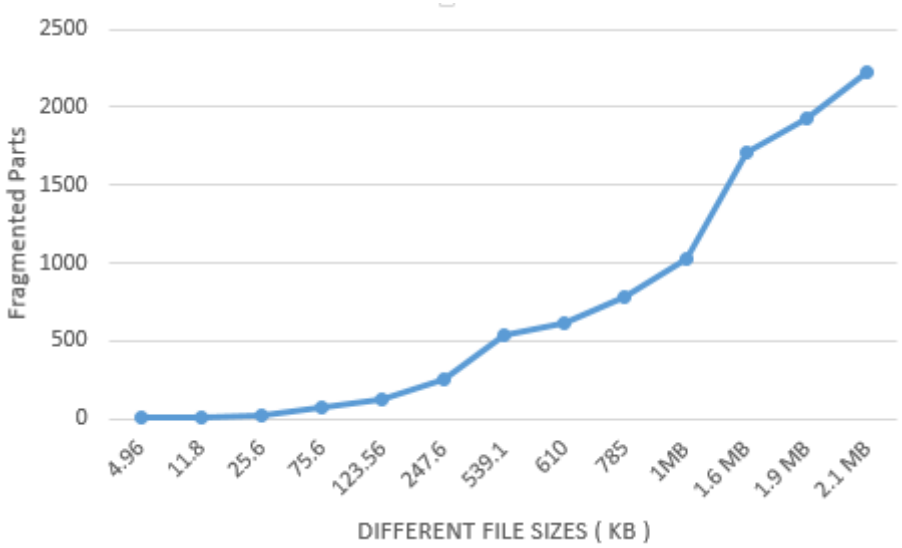

Figure 4. File Size v/s Parts

From the above bar chart, it is clear that as the file size increases number of partitions of the file also goes on increasing which helps to secure data at the cloud end. As data is not present in one file so it cant be hacked by the third party easily which hence ensuring the data security.

CONCLUSION

The primary conclusion of our research is that adoption of user-centric security models and shifting certain parts of communication and computation to the client side allows us to provide the cloud consumers with more visibility and control over their resources. Therefore, using this approach not only the security and privacy concerns of cloud consumers can be addressed more effectively, but also the burden of managing end-users' identities and access control will be reduced from cloud service providers.

This study collectively describes cloud computing security challenges in general and describes the mitigation practices that have been proposed to handle the identified challenges. We have successfully implemented the above proposed system and has reached to a solution that by splitting the files into multiple fragments we can achieve the better security in cloud computing. However, most important future work identifies here is that there are concrete standards for cloud computing security still missing. There are some open cloud manifesto standards and few efforts made by the cloud security alliance to standardize the process in the cloud. The cloud vendors and users do not encourage the usage of these standards as they are restrictive. In addition to this the cloud computing with such great offering such as storage, infrastructure and application designing capabilities on the go to the IT industry still fail to have proper standards for interoperability with other cloud service providers. This failure to provide concrete security standards, common underlying framework for data migration and global standards for cloud interoperability, make the leading technology the cloud computing" still a vulnerable option for aspiring users.

REFERENCES

[1] Bhagyashree Ambulkar and Vaishali Borkar,“Data Mining in Cloud Computing”, MPGI National Multi Conference 2012 (MPGINMC-2012), 7-8 April 2012.

[2] Peter Mell, and Timothy Grance,“The NIST Definition of Cloud Computing”, the National Institute of Standards and Technology, USA, 2011.

[3] ORACLE, “Oracle Data Mining Mining Techniques and Algorithms”

[4] M.Kantardzic, “Data Mining: Concepts, Models, Methods and Algorithms”, John Wiley & Sons Inc., 2002.

[5] “Introduction to Cloud Computing Architecture”, Sun Microsystems, 2009.

[6] “Top 10 Algorithms in Data Mining”, Springer-Verlag London Ltd., 2007.

[7] Jianzong Wang,Zhuo Liu, Peng Wang,”Data Mining of Mass Storage Based on Cloud Computing”.

[8] M. Bramer. Principles of Data Mining. Springer, 2007.

[9] M. Brantner, D. Florescu, D. A. Graf, D. Kossmann, and T. Kraska. Building a database on s3. In J. T.-L. Wang, editor, ACM, pages 251–264, 2008.

[10] S. H. Brown. Multiple linear regression analysis: A matrix approach with matlab. Alabama Journal of Mathematics, 2009.

[11] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control Pages 85–90, 2009.

[12] C. Clifton and D. Marks. Security and privacy implications of data mining. In ACM SIGMOD Workshop, pages 15–19, 1996.

[13] Gentry, C.: Fully Homomorphic Encryption Using Ideal Lattices. In: 41st ACM Symposium on Theory of Computing, May 31-June 2, 2009, Bethesda, Maryland, USA, pages 169–178 (2009) Boneh, D., Goh,

[14] E-J., Nissim, K.: Evaluating 2-DNF formulas on ciphertexts. In: Proceedings of TCC 2005, volume 3378 of LNCS, pages 325-341. Springer-Verlag (2005)

[15] Lindell, Y., Pinkas, B.: Privacy Preserving Data Mining. J. Cryptology 15(3), 151—222 (2002) .Liu, K.: Privacy Preserving Data Mining Bibliography.

[16] C. Gong, J. Liu, Q. Zhang, H. Chen and Z. Gong, The Characteristics of Cloud Computing, Proceedings of the 39th International Conference on Parallel Processing Workshops, pp. 275-279, 2010.

[17] http://searchcloudcomputing.techtarget.com

[18] http://www.techsmith.com/morae/whitepaper/ux20.asp