ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

A Survey on Homomorphic Data Concealment and Reliability in Multi Cloud Computing

Swetha M.S[1], Chandana B N[2], Deepika M[3]

Assistant Professor, Department of ISE, BMS Institute of Technology, Avalahalli, Yelahanka, Bengaluru, India[1]

Students, Department of ISE, BMS Institute of Technology, Avalahalli, Yelahanka, Bengaluru, India[2, 3,]

ABSTRACT: Multi cloud computing has become the latest trend for the existing cloud computing these days. Multi cloud computing is considered secure and more efficient in maintaining the data regulation of the users. Cloud Computing can be described as mode for offering particular IT services that are hosted on the internet, like Platform as Service (PaaS), Infrastructure as a Service (IaaS) and Software as a service (SaaS). Cloud Computing is also marketed as an efficient and cheap solution that will be replacing the client-server paradigm. The paradigm shift results/involves in the loss of control over data as well as security and privacy issues. Because of this reason caution is advised during deployment and usage of Cloud Computing in enterprises. Homomorphic encryption can be defined as conversion of data into cipher text that can be analyzed and worked with as if it were still in its original form. Homomorphic encryptions also allows complex mathematical operations to be performed on the encrypted data without compromising with the encryption. The security of mobile multi cloud computing (MMC) and the given advantages for mobile user(s), beside that for the data security itself cover with homomorphic encryption which are predictable by man researchers as the optimum method for cloud computing environment. The implementation and evaluation of homomorphic encryption in mobile cloud computing are discussed under this topic.

KEYWORDS: cloud security scanner, security scanner, web application scanner.

I. INTRODUCTION

Cloud Computing is not a very new concept in IT, in fact Cloud Computing is a more advanced version of the Data Processing Service Bureaus that we had 40 years ago . Nevertheless, the best known companies in the IT field offer or will shortly offer Cloud Computing services to a range of customers from organizations of all sizes to individual. The paradigm of Cloud Computing can be described in simple terms as offering particular IT services that are hosted on the internet, the most common ones being Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a service (SaaS). Cloud Computing is often marketed as an efficient and cheap solution that will replace the client-server paradigm. The paradigm shift involves/results in the loss Computing is often marketed as an efficient and cheap solution that will replace the client-server paradigm. The paradigm shift involves/results in the loss of control over data as well as new security and privacy issues.

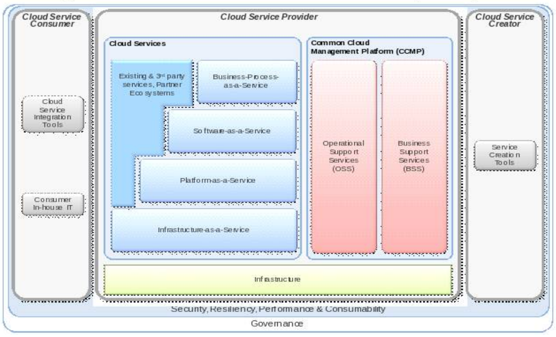
Cloud Service Consumer
Cloud Service Provider
Cloud Service Creator
Cloud Services
Common Cloud Management Platform (CCMP)
Existing & 3rd party services, Partner Eco systems
Business-Process-as-a-Service
Software-as-a-Service
Platform-as-a-Service
Infrastructure-as-a-Service
Operational Support Services (OSS)
Business Support Services (BSS)
Cloud Service Integration Tools
Consumer In-house IT
Service Creation Tools
Infrastructure
Security, Resiliency, Performance & Consumability
Governance

Fig 1.1 Structure of Cloud.

DOI: 10.15680/IJIRCCE.2017. 0502022

For this reason caution is advised when deploying and using Cloud .Computing in enterprises. After all, the first big issue in data protection in Europe arose at the end of the 1960's, when a Swedish company decided to have its data processing done by a service bureau in Germany and the data protection legislations in both countries were not alike. With Cloud Computing rapidly gaining popularity, it is important to highlight the resulting risks. As security and privacy issues are most important, they should be addressed before Cloud Computing establishes an important market share.

A. HOW CLOUD WORKS?

A cloud computing environment will also need to provide interfaces and tools for the service creators and users. This is the role of the Cloud Service Creator and Cloud Service Consumer component. Now, let's see how it works in reality. Generally, you log in to a portal (enterprise or public wise) and you order your services through the Cloud Service Consumer. This service has been created by the cloud service provider and can be a simple virtual machine (VM) based on an image, some network components, an application service such as an WebApp environment and a service such as MongoDB. It depends on the provider and type of resources and services.The cloud provider will validate, through the BSS, your request and if the validation is okay (credit card, contract), it will provision the request through the OSS.You will receive, in one way or another, the credentials to access your requested services and you will usually receive a monthly invoice for your consumption.

B. WHAT IS MOBILE CLOUD COMPUTING AND HOW IT WORKS?

Mobile Cloud Computing (MCC) is the combination of cloudcomputing, mobilecomputing and wireless networks to bring rich computational resources to mobile users, network operators, as well as cloud computing providers. The ultimate goal of MCC is to enable execution of rich mobile applications on a plethora of mobile devices, with a rich user experience.MCC provides business opportunities for mobile network operators as well as cloud providers. More comprehensively, MCC can be defined as "a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle."MCC uses computational augmentation approaches [by which resource-constraint mobile devices can utilize computational resources of varied cloud-based resources. In MCC, there are four types of cloud-based resources, namely distant immobile clouds, proximate immobile computing entities, proximate mobile computing entities, and hybrid (combination of the other three model). Giant clouds such as Amazon EC2 are in the distant immobile groups whereascloudlet or surrogates are member of proximate immobile computing entities. Smartphones, tablets, handheld devices, and wearable computing devices are part of the third group of cloud-based resources which is proximate mobile computing entities.

C. ENCRYPTION IN MULTICLOUD COMPUTING

Cloud encryption is the transformation of a cloud service customer's data into cipher text. Cloud encryption is almost identical to in-house encryption with one important difference -- the cloud customer must take time to learn about the provider's policies and procedures for encryption andencryption key management. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted. Because encryption consumes more processor overhead, many cloud providers will only offer basic encryption on a few database fields, such as passwords and account numbers. At this point in time, having the provider encrypt a customer's entire database can become so expensive that it may make more sense to store the data in-house or encrypt the data before sending it to the cloud. To keep costs low, some cloud providers have been offering alternatives to encryption that don't require as much processing power. These techniques include redacting or obfuscating data that needs to remain confidential or the use of proprietary encryption algorithms created by the vendor

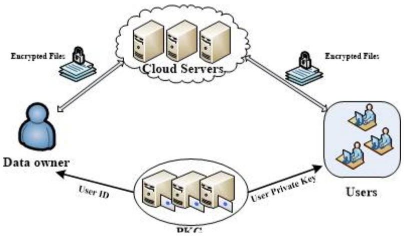

Fig 1.2 Encryption in Cloud

D. HOMOMORPHIC ENCRYPTION IN MCC:

Homomorphic encryption is the conversion of data into ciphertext that can be analysed and worked with as if it were still in original Form. The term is derived from the Greek words for "same structure."Because the datain a homomorphic encryption scheme retains the same structure, identical mathematical operation whether they are performed on encrypted or decrypted data will yield equivalent results. Homomorphic encryption is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services.

E. BENEFITS OF MOVING TO MOBILE CLOUD COMPUTING:

1) Data does not always flow across international boundaries .If IAAS provider
is in the US he may need a second service in another country where we want to operate.
2) If a small company wants to get big fast, will have to plan a major data center and staff it before it gets too big. Otherwise, develop successful service that is ready to take off and miss serving demand as it materializes.
3) If a small company that doesn't even want to run a big data center, but wants to be able to meet frequent spikes in demand will need a way to shift traffic to reserve capacity somewhere.
4) If we want the flexibility of presenting our service in either public cloud setting or private infrastructure operation, we need a way to quickly establish a private cloud without diverting all our engineering effort to do so.
5) If none of these seem to fit our case, avoid vendor lock in by always maintaining a relationship with two or more vendors.

F. PROBLEMS WITH THE CLOUD:

1. BREACH OF DATA:

Organizations must be most specifically concerned about breaches of data in their cloud system. The Cloud Security Alliance identified breaches of data as the biggest threat to the security of cloud computing last year. If you think hackers might be interested in stealing your most critical data, you should think carefully about your options before storing it in the cloud.

2. ABUSE OF CLOUD:

There are hackers and thieves out there who will take advantage of the vulnerabilities of cloud-based computing services. Encryption keys, for example, are sometimes easier to break than they would be if the data was simply stored on a computer or physical data center. Cloud providers may also be more vulnerable to things like malware attacks. When storing, sharing, accessing, working with and collaborating on content in the cloud, it's important to be aware of the threats that are out there.

3.LOSS OF DATA:

You don't only have to worry about hackers stealing or altering your data; you also have to worry about data being destroyed and lost altogether, without a trace in the world. There are many reputable cloud service providers that offer top-notch protection from data loss, but there are still all sorts of errors that can occur. The most common causes for loss of data are simple matters of human error. This makes a good case for backing up all data on a physical device before working on it in the cloud.

4. LACK OF DELIGENCE:
This disadvantage is often avoidable, but the fact is that far too many companies fall into the trap of under-preparedness when they switch over to the cloud because they simply don't know what to expect and what they're getting into. It's important to know what the risks are, what the potential benefits are and what all the different options are within the spectrum of cloud services. You wouldn't want to switch your data to a cloud-based platform only to find out it goes against your contractual obligations or conflicts with your operational functions; yet, many companies do just that when they fail to do their due diligence before getting into the cloud.

5. SPITEFUL ACTIVITY:
One of the most unfortunate disadvantages of cloud computing is the potential for spiteful people to do harm, which would be much more difficult to do with a physical server. There may be former employees, disgruntled employees, unhappy contractors, displeased business partners or even industry insiders working for the competition interested in doing harm to your data, network or system. It may sound like fiction or fantasy, but this kind of malicious activity goes on far more often than most people imagine.

G.SECURITY ISSUES IN MOBILE CLOUD COMPUTING:

DATA OWNERSHIP
Mobile Multi-Cloud Computing provides the facility to store personal data and other data (purchases) beside that user need to be aware of different rights on purchases of their own data in the cloud.

PRIVACY
Until today, Privacy is one of the biggest challenges. Some apps store user's data remotely, which may be sold to others (agencies, etc.) without thepermissions of user. (Like updates about location)

DATA SECURITY

- Mobiles are famous for malicious code, gives possibilityof loss.
- Data loss from lost/stolen devices.
- Info stealing by malicious malware.
- Data leakage due to poorly written third party app.
- Not assured network access, unreliable APs.
- Insecure Market Places.
- Near Field Communication and Proximity based hacking.

DATA SEGREGATION
Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. The cloud provider should provide evidence that encryption schemes were designed and testedby experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability".

II. LITERATURE SURVEY

1) WHY WE TWITTER: UNDERSTANDING MICROBLOGGING USAGE AND COMMUNITIES
Microblogging is a new form of communication in which users can describe their current status in short posts distributed by instant messages, mobile phones, email or the Web. Twitter, a popular microblogging tool has seen a lot of growth since it launched in October, 2006. In this paper, they presented microblogging phenomena by studying the topological and geographical properties of Twitter's social network. People use microblogging to talk about their daily

activities and to seek or share information. Finally, they analysed the user intentions associated at a community level and showed how users with similar intentions connect with each other.

2) SOCIAL NETWORKS THAT MATTER: TWITTER UNDER THE MICROSCOPE

Scholars, advertisers and political activists see massive online social networks as a representation of social interactions that can be used to study the propagation of ideas, social bond dynamics and viral marketing, among others. But the linked structures of social networks do not reveal actual interactions among people. Scarcity of attention and the daily rhythms of life and work make people default to interacting with those few that matter and that reciprocate their attention. A study of social interactions within Twitter reveals that the driver of usage is a sparse and hidden network of connections underlying the “declared” set of friends and followers.

3) TWEET, TWEET, RETWEET: CONVERSATIONAL ASPECTS OF RETWEETING ON TWITTER

Twitter - a microblogging service that enables users to post messages ("tweets") of up to 140 characters - supports a variety of communicative practices; participants use Twitter to converse with individuals, groups, and the public at large, so when conversations emerge, they are often experienced by broader audiences than just the interlocutors. This paper examines the practice of retweeting as a way by which participants can be "in a conversation." While retweeting has become a convention inside Twitter, participants retweet using different styles and for diverse reasons. In this paper they showed how authorship, attribution, and communicative fidelity are negotiated in diverse ways. Using a series of case studies and empirical data, this paper maps out retweeting as a conversational practice.

4) PREDICTING ELECTIONS WITH TWITTER: WHAT 140CHARACTERS REVEAL ABOUT POLITICAL SENTIMENT

Twitter is a micro-blogging website where users read and write millions of short message s on a variety of topics every day. This study uses the context of the German federal election to investigate whether Twitter is used as a forum for political deliberation and whether online messages on Twitter validly mirror offline political sentiment. Using LIWC text analysis software, conducted a content analysis of over 100,000 messages containing a reference to either a political party or a politician. The results show that Twitter is indeed used extensively for political deliberation. The mere number of messages mentioning a party reflects the election result. Moreover,joint mentions of two parties are in line with real world political ties and coalitions. An analysis of the tweets’ political sentiment demonstrates close correspondence to the parties' and politicians’ political positions indicating that the content of Twitter messages plausibly reflects the offline political landscape. They discussed the use of micro-blogging message content as a valid indicator of political sentiment and derive suggestions for further research.

5) MICROBLOGGING FOR LANGUAGE LEARNING: USING TWITTER TO TRAIN COMMUNICATIVE AND CULTURAL COMPETENCE

Our work analyses the usefulness of micro-blogging in second language learning using the example of the social network Twitter. Most learners of English do not require even more passive input in form of texts, lectures or videos, etc. This input is readily available in numerous forms on the Internet. What learners of English need is the chance to actively produce language and the chance to use English as tool of communication. This calls for instructional methods and tools promoting `active' learning that present opportunities for students to express themselves and interact in the target language. In this paper they describe how they used Twitter with students of English at the Distant College of Shanghai Jiao Tong University. Theyanalyse the students' messages and show how the usage of Twitter trained communicative and cultural competence.

III. PROBLEM STATEMENT

Twitter is categorized as a microblogging service. Microblogging is a form of blogging that enables users to send brief text updates or micro media such as photographs or audio clips. Microblogging services other than Twitter include Tumblr, Plurk, Jaiku, identi.ca, and others. Users can know how other users are doing and often what they are thinking about now, users repeatedly return to the site and check to see what other people are doing.

DOI: 10.15680/IJIRCCE.2017. 0502022

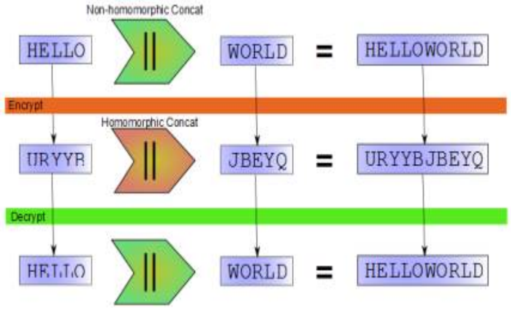

Fig 3.1 Homomorphic vs Non Homomorphic Encryption

A. DISADVANTAGES OF EXISTING SYSTEM:

1. Each Twitter user is regarded as a sensor and each tweet as sensory information. These virtual sensors, which we designate as social sensors, are of a huge variety and have various characteristics: some sensors are very active and others are not.
2. A sensor might be inoperable or malfunctioning sometimes, as when a user is sleeping, or busy doing something else.
3. Social sensors are very noisy compared to ordinary physical sensors. Regarding each Twitter user as a sensor, the event-detection problem can be reduced to one of object detection and location estimation in a ubiquitous/ pervasive computing environment in which has numerous location sensors: a user has a mobile device or an active badge in an environment where sensors are placed

IV. METHODOLOGY

Homomorphic encryption is the conversion of data into ciphertext that can be analysed and worked with as if it were still in its original form.Fully homomorphic encryption is a term which was coined when were first found encryption schemes which preserved two algebraic operations in a ringstructure: namely, given E(a) and E(b), you can compute E(a+b) and E(ab). It turns out that with those two operations, you can compute just about everything. This is where the "cloud" gets into the picture: the cloud ispowerful, but not trustworthy; hence, you could encrypt your data, send it to the cloud which performs the computation you want to do, and then decrypt the result.

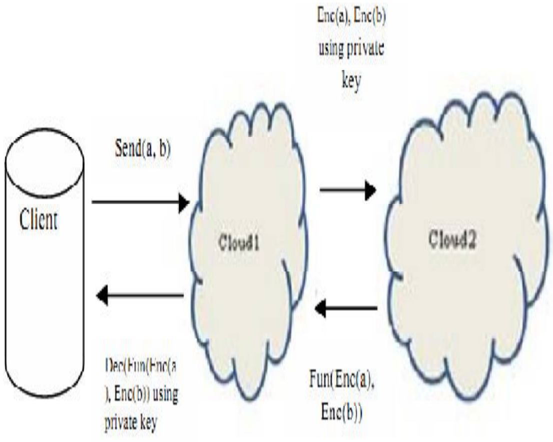
Enc(a), Enc(b) using private key
Send(a, b)
Client
Cloud1
Cloud2
Dec(Fun(Enc(a), Enc(b)) using private key
Fun(Enc(a), Enc(b))

Fig 4.1 System Model

Homomorphic Property:
Encrypt (m) x encrypt (n) = encrypt (m x n)

RSA allows only multiplication: other operations onciphertext (e.g. +) break decryption.Other scheme allow different operations (e.g. + and -)Algebra homomorphism allows x and +: much morepowerful but need to select appropriate homomorphicencryption scheme for application.

File size(Mb)	Encryption time(ms)	Decryption time(ms)
20	5	4
50	12	10
100	20	17
200	35	30
500	90	75
1000	196	180
2000	420	400

V. RESULTS AND ANALYSIS

Mechanism:

1. Client sends an encrypted data to cloud.
E.g.: let two encrypted number be a and b
2. Client sends request to Cloud for calculating function i.e. f (a,b)
3. Client and Cloud communicate through a cryptosystem based on fully Homomorphic encryption.
4. Cloud stores encrypted data.
5. Cloud calculates the result of request sent by the client without knowingactual number i.e. f(a,b) is calculated .
6. Cloud then compute f (Enc(a),Enc(b)) without knowing a and b
7. Client decrypts f (Enc(a),Enc(b)) using its private key.

BGV is an asymmetric encryption scheme which can be used for the encryption of the bits. Dealing with integer vectors (whose security is dependent on the hardness of decisional LWE (Learning with Errors) anddealing with the integer polynomials (whose security is dependent on the hardness of the decisional R-LWE (Ring LWE). The security of the AHEE is IND-C PA which is the highest level of the security of AHEE. Additivehomomorphism of this algorithm refers the same k for encryption but uses the random number of k in E1 which makes AHEE able to resist plaintext attack.

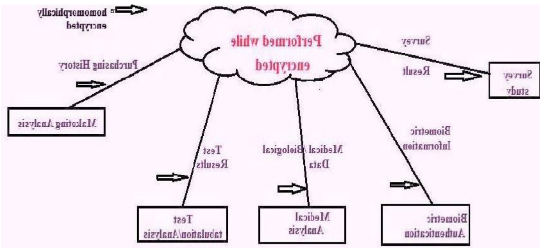

Fig 5.1 Homomorphic Encryption in Applications.

VI. CONCLUSION

Multi-clouds is one of optimal solution for data security and efficiency and effectively than single cloud. The technology is changing over the time; mobile cloud is becoming a trend among the user. This seminar gives a research in mobile multicloud computing (MMC) and the data security from user side through homomorphic encryption. Homomorphic encryption claimed by many research as an optimal encryption for cloud computing environment. This will prove the result performance in homomorphic encryption suitable for mobile multi-cloud computing. Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption.Because the data in a homomorphic encryption scheme retains the same structure, identical mathematical operations whether they are performed on encrypted or decrypted data will yield equivalent results. Homomorphic encryption is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services. Future works for the researcher is improving the performance security aspects in mobile multi cloud computing and improve the encryption itself and research for the space or memory consumption for mobile environment.

VII. FUTURE ENHANCEMENT

A hybrid technique is proposed for data confidentiality and integrity, which uses both key sharing and authentication techniques. The connectivity between the user and the cloud service provider can be made more secure by utilizing powerful key sharing and authentication processes. RSA public key algorithm can be used for secure distribution of the keys between the user and cloud service providers.

A three-layered data security technique is proposed the first layer is used for authenticity of the cloud user either by one factor or by two factor authentications; the second layer encrypts the user's data for ensuring protection and privacy; and the third layer does fast recovery of data through a speedy decryption process.

In-Memory Database encryption technique is proposed for the privacy and security of sensitive data in untrusted cloud environment . A synchronizer exists between the owner and the client for seeking access to the data.

REFERENCES

[1] Maya Louk, Hyotaek Lim" Homomorphic Encryption In Multi Cloud Computing"Proceedings of the Information Networking(ICOIN) International Conference, page(s) 493-497,2015.

[2].Jian Li, Member IEEE/ACM, Ruhui Ma, Haibing Guan, Member IEEE/ACM "TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud".

[3] John Bethencourt, Amit Sahai and Brent Waters, "Ciphertext-policy attribute-based encryption", *Proceedings of the 2007 IEEE Symposium on Security and Privacy (S&P'07). IEEE Computer Society*, pp. 321-334

[4] K. Rege, N. Goenka, P. Bhutada and S. Mane, "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA", *International Journal of Computer Applications (0975–8887)*, vol. 71, no. 22, 2013.

[5] Junbeom Hur and Dong Kun Noh, "Attribute-based access control with efficient revocation in data outsourcing systems", *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214-1221, 2011.

[6] Ximeng Liu, Jianfeng Ma and Jinbo Xiong, "Ciphertext-policy Weighted Attribute-based Encryption Scheme in Cloud Computing", *Journal of Sichuan University(Engineering Science Edition)*, vol. 45, no. 6, pp. 21-26, 2013

[7] Amit Sahai and Brent Waters, "Fuzzy identity-based encryption", *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology-EUROCRYPT'05*, pp. 457-473, Springer.

[8] B. Sharma and R. Delhi, "Security architecture of cloud computing based on elliptic curve cryptography (ECC)", *International Journal of Advances in Engineering Sciences*, vol. 3, no. 3, pp. 58-61, 2013.

[9] G. Shilpi and J. Sharma, "A hybrid encryption algorithm based on RSA and Diffie Hellman", *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-4.

[10] H. Qin-long, M. Zhao-feng, Y. Yi-xian, F. Jing-yi and N. Xin-xin, "Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing", *The Journal of China Universities of Posts and Telecommunications*, vol. 20, no. 6, pp. 88-95, 2013.

[11] G. Craig, "A fully homomorphic Encryption Scheme", 2009.

[12] J-M. Bohli, "Security and privacy-enhancing multicloud architectures", *Dependable and Secure Computing, IEEE Transactions on*, vol. 10, no. 4, pp. 212-224, 2013.

[13] Frederick R. Carlson, "Security Analysis of Cloud Computing", *arXiv preprint arXiv: 1404*, vol. 6849, 2014.

[14] Naehrig Michael, Kristin Lauter and Vinod Vaikuntanathan, "Can homomorphic encryption be practical?",*Proceedings of the 3rd ACM workshop on Cloud computing security workshop. ACM.*

[15] "GCN Technology, Tools and Tactics for Public Sector IT", *New Encryption Method Promises End-to-End Cloud Security*, 2013, [online] Available: online

[16] Fau Simon, "Towards practical program execution over fully homomorphic encryption schemes", *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on. IEEE.*

[17]. C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in cloud computing".